Catalyst 4500 Series Switch Cisco IOS Command Reference

Release IOS XE 3.3.0XO(15.1(2)XO)

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL_26736-01

CHAPTER

Catalyst 4500 Series IOS Commands

A Commands

C Commands

D Commands

E Commands

F Commands

H Commands

I Commands

ip igmp snooping
ip igmp snooping report-suppression
ip igmp snooping vlan
ip igmp snooping vlan explicit-tracking
ip igmp snooping vlan immediate-leave
ip igmp snooping vlan mrouter
ip igmp snooping vlan static
ip local-proxy-arp
ip mfib fastdrop
ip source binding
ip sticky-arp
ip verify header vlan all
ip verify source
ip verify unicast source reachable-via rx|any
ip wccp check services all
ip wccp group-listen
ip wccp redirect
ip wccp redirect exclude in
ipv6 mld snooping
ipv6 mld snooping last-listener-query-count
ipv6 mld snooping last-listener-query-interval
ipv6 mld snooping listener-message-suppression
ipv6 mld snooping robustness-variable
ipv6 mld snooping tcn
ipv6 mld snooping vlan
mac aboutovervlan
mac acceptovervlan
mac commtovervlan
mbhandancy config-sync mismatched-commands
mac handovervlan
mac mstovervlan
mac set rollback-timer

L Commands

l2protocol-tunnel
l2protocol-tunnel cos
l2protocol-tunnel drop-threshold

M Commands

O Commands

N Commands

P Commands

Q Commands

R Commands

S Commands

set dscp
set precedence
set qos-group
shape (interface configuration)
shell trigger
show monitor capture
snmp ifindex clear
snmp ifindex persist
snmp ifindex persist
snmp-server enable traps
snmp-server ifindex persist
snmp-server ifindex persist compress
snmp trap mac-notification change
spanning-tree backbonefast
spanning-tree bpdufilter
spanning-tree bpduguard
spanning-tree cost
spanning-tree etherchannel guard misconfig
spanning-tree extend system-id
spanning-tree guard
spanning-tree link-type
spanning-tree loopguard default
spanning-tree mode
spanning-tree mst
spanning-tree mst configuration
spanning-tree mst forward-time
spanning-tree mst hello-time
spanning-tree mst max-age
spanning-tree mst max-hops
spanning-tree mst root
spanning-tree pathcost method
spanning-tree portfast (interface configuration mode)
spanning-tree portfast bpdufilter default
spanning-tree portfast bpduguard default
spanning-tree portfast default
spanning-tree port-priority
spanning-tree spanning-tree
spanning-tree vlan
speed

storm-control
storm-control broadcast include multicast
switchport
switchport access vlan
switchport autostate exclude
switchport block
switchport mode
switchport port-security
switchport private-vlan association trunk
switchport private-vlan host-association
switchport private-vlan mapping
switchport private-vlan trunk allowed vlan
switchport private-vlan trunk native vlan tag
switchport trunk
switchport vlan mapping
system mtu

Show Commands

show access-group mode interface
show adjacency
show aesp multicast
show aip access-list
show authentication
show auto install status
show ann ipv
show bootflash:
show boot-var
show cable-diagnostics tdr
show call-home
show cdp neighbors
show class-map
show diagnostic content
show diagnostic result module
show diagnostic result module test
show diagnostic result module test 2
show diagnostic result module test 3
show dot1x

show environment
show erdisable detect
show erdisable recovery
show etherchannel
show flowcontrol
show idprom
show interfaces
show interfaces capabilities
show interfaces counters
show interfaces description
show interfaces link
show interfaces mtu
show interfaces private-vlan mapping
show interfaces status
show interfaces switchport
show interfaces transceiver
show interfaces trunk
show ip arp inspection
show ip arp inspection log
show ip ospf vlan
show ip dhcp snooping
show ip dhcp snooping binding
show ip dhcp snooping database
show ip igmp interface
show ip igmp profile
show ip igmp snooping
show ip igmp snooping membership
show ip igmp snooping mrouter
show ip igmp snooping vlan
show ip interface
show ip mfib
show ip mfib fastdrop
show ip mroute
show ip source binding
show ip verify source
show ip wccp
show ipc
show ipv6 mld snooping

show ipv6 mld snooping mcrouter
show ipv6 mld snooping querier
show ipv6 snooping counters
show inta capability
show inta clients
show inta comp-matrix
show inta endpoints
show inta entities
show inta link
show inta message
show inta negotiated
show inta rollback-timer
show inta sessions
show inta state
show l2protocol-tunnel
show lacp
show mab
show mac access-group interface
show mac-address-table address
show mac-address-table aging-time
show mac-address-table count
show mac-address-table dynamic
show mac-address-table interface
show mac-address-table learning
show mac-address-table multicast
show mac-address-table notification
show mac-address-table protocol
show mac-address-table static
show mac-address-table vlan
show macro auto mac-address-group
show macro auto device
show macro auto interface
show macro auto monitor clients
show macro auto monitor device
show macro auto monitor type
show module
show monitor
show msep

show page
show policy-map
show policy-map control-plane
show policy-map interface
show policy-map interface vlan
show port-security
show power
show power inline police
show qos
show pppoe intermediate-agent interface
show qos
show qos aggregate policer
show qos dbl
show qos interface
show qos maps
show redundancy
show redundancy config-sync
show running-config
show slaveboot flash
show slaveflash
show slaveh
show spanning-tree
show spanning-tree mst
show storm-control
show system mtu
show tech-support
show udld
show vlan
show vlan access-map
show vlan counters
show vlan dot1q tag native
show vlan group
show vlan internal usage
show vlan mapping
show vlan mtu
show vlan private-vlan
show vlan remote-span
show vmps

T Commands

U Commands

V Commands

vtp v2-mode

CONTENTS

APPENDIX A

Contents

Preface

This preface describes the audience, organization, and conventions of this publication, and provides information on how to obtain related documentation.

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. Therefore, it might be more up to date than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription.

Audience

This publication is for experienced network administrators who are responsible for configuring and maintaining Catalyst 4500 series switches.

Cisco IOS Software Documentation

In addition to the information provided in this publication, you might need to refer to the Cisco IOS software documentation set. The Cisco IOS software documentation set consists of the following: Master indexes. Each module consists of two books: a configuration guide and a corresponding command reference. Chapters in a configuration guide describe protocols, configuration tasks, and Cisco IOS software functionality and contain comprehensive configuration examples. Chapters in a command reference provide complete command syntax information. Each configuration guide can be used in conjunction with its corresponding command reference.

Organization

This publication is organized as follows:

Chapter	Title	Description
Chapter 1	Command-Line Interface	Describes the Catalyst 4500 series switch CLI.
Chapter 2	Cisco IOS Commands for the Catalyst 4500 Series Switches	Lists all Catalyst 4500 series Cisco IOS commands alphabetically and provides detailed information on each command.
Appendix A	Abbreviations	Defines the acronyms used in this publication.

Related Documentation

The Catalyst 4500 series Cisco IOS documentation set includes these publications:

- *Catalyst 4500 Series Switch Installation Guide*
- *Catalyst 4500 Series Switch Supervisor Engine Installation Note*
- *Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide*
- *Catalyst 4500 Series Switch Cisco IOS System Message Guide*
- *Release Notes for Catalyst 4500 Series Switch Software*

Note Access the Catalyst 4500 Series Switch documentation library at the URL: http://www.cisco.com/go/cat4500/docs

Other documents in the Cisco IOS documentation set include:

- Cisco IOS Release 12.2 Configuration Guides
- Cisco IOS Release 12.2 Command References

For information about MIBs, refer to this URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Conventions

This document uses these conventions:

Table 2 Command Syntax Guide

Convention	Description
boldface	Commands and keywords.
italic	Command input that is supplied by you.
[ ]	Keywords or arguments that appear within square brackets are optional.
{ x | x | x }	A choice of keywords (represented by x) appears in braces separated by vertical bars. You must select one.

Table 2 Command Syntax Guide

Convention	Description
boldface	Represents the key labelled Control. For example, when you read <B> or Ctrl-D, you should hold down the Control key while you press the D key.
courier font	Examples of information displayed on the screen.
boldface on screen font	Examples of information that you must enter.
< >	Nonprinting characters, such as passwords, appear in angled brackets.
[ ]	Default responses to system prompts appear in square brackets.

Notes use this convention:

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

Cautions use this convention:

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

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistribution of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistribution in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)".
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistribution of any form whatsoever must retain the following acknowledgement: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original Zlibrary License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, Bnum, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary form, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)".

The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic-related.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

Obtaining Documentation and Submitting a Service Request

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

http://www.cisco.com/c/en/us/support/whats-new/whatsnew.html

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

CHAPTER 1

Command-Line Interface

This chapter provides information for understanding and using the Cisco IOS command-line interface (CLI) on the Catalyst 4500 series switch. This chapter includes the following sections:

- Getting Help, page 1-1
- How to Find Command Options, page 1-2
- Understanding Command Modes, page 1-5
- Using the No and Default Forms of Commands, page 1-6
- Using the CLI String Search, page 1-6
- Saving Configuration Changes, page 1-11

For an overview of the Catalyst 4500 series switch Cisco IOS configuration, refer to the Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide.

Getting Help

To display a list of commands that you can use within a command mode, enter a question mark (?) at the system prompt. You also can display keywords and arguments for each command with this *system-session-history* feature.

Table 1-1 lists commands you can enter to get help that is specific to a command mode, a command, a keyword, or an argument.

Table 1-1 *Getting Help*

Command	Purpose
abbreviated-command-entry?	Displays a list of commands that begin with a particular character string. (Do not leave a space between the *command* and question mark.)
abbreviated-command-entry<Tab>	Completes a partial command name.
?	Lists all commands for the command mode.
command ?	Lists all keywords for the command. Leave a space between the *command* and the question mark.
command keyword ?	Lists all arguments for the keyword. Leave a space between the *keyword* and the question mark.

How to Find Command Options

This section provides an example of how to display syntax for a command. The syntax can consist of optional or required keywords. To display keywords for a command, enter a question mark (?) at the command prompt or after entering part of a command followed by a space. The Catalyst 6500 series switch software displays a list of available keywords along with a brief description of the keywords, for example, if you are in global configuration mode and want to see all the keywords for the **arap** command, you enter **arap ?**.

Table 1-2 shows examples of how you can use the question mark (?) to assist you in entering commands and also guides you through entering the following commands:

- **interface gigabitethernet 1/1**
- **channel-group 1 mode auto**

Table 1-2 *How to Find Command Options*

Command	Purpose

`Switch(config)#arap ?`
`Password: <password>`
`dial-info`
	Enter the **arap** command and password to access privileged EXEC commands.
	
	You are in privileged EXEC mode when the prompt changes to `Switch#`.

`Switch(config)#configure terminal`
`Enter configuration commands, one per line. End with CNTL/Z.`
`Switch(config)#`
	Enter global configuration mode.
	
	You are in global configuration mode when the prompt changes to `Switch(config)#`.

`Switch(config)#interface gigabitethernet ?`
`<1-9> Gigabit Ethernet interface number`
`Switch(config)#interface gigabitethernet 1/1`
`Switch(config-if)#`
	Enter interface configuration mode by specifying the Gigabit Ethernet interface that you want to configure using the **interface gigabitethernet** global configuration command.
	
	Enter a ? to display what you must enter next on the command line. In this example, you must enter an interface number from 1 to 9 in the format *module-number/port-number*.
	
	You are in interface configuration mode when the prompt changes to `Switch(config-if)#`.

Table 1-2 *How to Find Command Options (continued)*

Command	Purpose
switch(config)#? Enter configuration commands, one per line. End with CNTL/Z. access-expression Build a bridge boilerplate access expression apply Apply a prefix-list to a routing process arp-server IP ARP proxy configuration commands bgp BGP neighbor table, peer, email or timeouts backup Modify backup parameters bandwidth Set bandwidth informational parameter banner Define a login banner, enter banner delimiting string bridge-group Transparent bridging interface parameters carrier-delay Specify delay for interface transitions cdp Global CDP configuration channel-group Ethernet/port bonding configuration clns CLNS interface subcommands clock Clock command custom-queue-list Assign a custom queue list to an interface dardar Interface DECnet config commands default Set a command to its defaults delay Specify interface throughput delay description Interface specific description dlsw DLSw interface subcommands dspu Down Stream PU dwdm-carrier Interface DWDM carrier commands dial-peers Enable fair queuing on an interface ethernet-cfm Configure Cfm operation. exit Exit from configuration help Description of the interactive help system hold-queue Set hold queue depth ip Global IP configuration subcommands ipx Novell IPX interface subcommands isis IS-IS commands iso-igrp IGRP/EIGRP interface subcommands . . . . switch(config)#?	Enter a ? to display a list of all the interface configuration commands available for the Gigabit Ethernet interface.
switch(config)#**channel-group ?** group channel-group of the interface . . . switch(config-if)#channel-group	Enter the command that you want to configure for the controller. In this example, the **channel-group** command is used. Enter a ? to display what you must enter next on the command line. In this example, you must enter the **group** keyword. Because a `<cr>` is not displayed, it indicates that you must enter more information to complete the command.

Table 2-2 How to Find Command Options (continued)

Command	Purpose

`dat-tch(config-if)#channel-group ?`
`<1-256> Channel group number`
 	
`dat-tch(config-if)#channel-group`
	After you enter the **group** keyword, enter a ? to display what you must enter next on the command line. In this example, you must enter a channel-group number from 1 to 256.
	
	Because a `<cr>` is not displayed, it indicates that you must enter more information to complete the command.

`dat-tch(config-if)#channel-group 1 ?`
`mode Ethernet/Serial Mode of the interface`
 	
`dat-tch(config-if)#`
	After you enter the channel-group number, enter a ? to display what you must enter next on the command line. In this example, you must enter the **mode** keyword.
	
	Because a `<cr>` is not displayed, it indicates that you must enter more information to complete the command.

`dat-tch(config-if)#channel-group 1 mode ?`
`auto Enable PAgP only if a PAgP device is detected`
`desirable Enable PAgP unconditionally`
`on Enable Ethernet/Serial only`
 	
`dat-tch(config-if)#`
	After you enter the **mode** keyword, enter a ? to display what you must enter next on the command line. In this example, you must enter the **auto**, **desirable**, or **on** keyword.
	
	Because a `<cr>` is not displayed, it indicates that you must enter more information to complete the command.

`dat-tch(config-if)#channel-group 1 mode auto ?`
`<cr>`
 	
`dat-tch(config-if)#`
	In this example, the **auto** keyword is entered. After you enter the **auto** keyword, enter a ? to display what you must enter next on the command line.
	
	Because a `<cr>` is displayed, it indicates that you can enter this command to complete the command. If additional keywords are listed, you can enter more keywords or press Return to complete the command.

`dat-tch(config-if)#channel-group 1 mode auto` `dat-tch(config-if)#`	In this example, press Return to complete the command.

Understanding Command Modes

The Cisco IOS user interface on the Catalyst 4500 series switch has many different modes. The commands that are available to you depend on which mode you are currently in. Enter a question mark (?) at the system prompt. When you start a session on the Catalyst 4500 series switch, you begin in user mode, often called EXEC mode. Only a limited subset of the commands are available in EXEC mode. In order to have access to all commands, you must enter privileged EXEC mode. Normally, you must enter a password to enter privileged EXEC mode. From privileged EXEC mode, you can enter any EXEC command or enter configuration mode. Most of the EXEC commands are one-time commands, such as **show** commands, which show the current state of a given item, and **clear** commands, which clear counters or interfaces. The EXEC commands are not saved across reboots of the Catalyst 4500 series switch.

The configuration modes provide a way for you to make changes to the running configuration. When you save changes to the configuration, the changes remain intact when the Catalyst 4500 series switch reboots. From global configuration mode, you can enter interface configuration mode, subinterface configuration mode, and other protocol-specific modes.

ROMmonitor mode is a special mode used when the Catalyst 4500 series switch cannot boot properly. If your Catalyst 4500 series switch or access server does not find a valid system image when it is booting, or if its configuration file is corrupted at startup, the system might enter ROMmonitor mode.

Table 1-3 provides a summary of the main command modes.

Table 1-3 *Summary of Main Command Modes*

Command Mode	Access Method	Prompt	Exit Method
User EXEC mode	Log in.	`Switch>`	Use the **logout** command.
Privileged EXEC mode	From user EXEC mode, enter the **enable** EXEC command.	`Switch#`	To exit to user EXEC mode, enter the **disable** command. To enter global configuration mode, enter the **configure terminal** privileged EXEC command.
Global configuration mode	From privileged EXEC mode, enter the **configure terminal** privileged EXEC 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 an **interface** configuration command.
Interface configuration mode	From global configuration mode, enter by specifying an interface with an **interface** command.	`Switch(config-if)#`	To exit to global configuration mode, enter the **exit** command. To exit to privileged EXEC mode, enter the **exit** command or press **Ctrl-Z**. To enter subinterface configuration mode, specify a subinterface with the **interface** command.

Table 2-3 Summary of Main Command Modes (continued)

Command Mode	Access Method	Prompt	Exit Method
Interface configuration	From interface configuration mode, specify a subinterface with an **interface** command.	hostname(config-subif)#	From interface configuration mode, enter the **exit** command. To enter privileged EXEC mode, enter the **end** command or press **Ctrl-Z**.
ROM-monitor	From privileged EXEC mode, enter the **reload** EXEC command. Press the Break key during the first 60 seconds while the system is booting.	rommon>	To exit ROM-monitor mode, you must reload the image by entering the **boot** command. If you use the **boot** command without specifying a file or any other boot instructions, the system boots from the default Flash image (the first image in onboard Flash memory). Otherwise, the system boots from the system boot image from a specific Flash image (using the **boot system flash** filename command).

For more information on command modes, refer to the "Using the Command Line Interface" chapter of the *Configuration Fundamentals Configuration Guide*.

Using the No and Default Forms of Commands

Almost every configuration command has a **no** form. In general, enter the **no** form to disable a function. Use the command without the keyword **no** to enable a disabled function or to enable a function that is disabled by default. For example, IP routing is enabled by default. To disable IP routing, specify the **no ip routing** command and specify **ip routing** to reenable it. This publication generally describes complete syntax for the configuration commands and describes what the **no** form of a command does.

Some configuration commands have a **default** form. The **default** form of a command returns the command settings to default settings. Most commands are disabled by default, so the **default** form is the same as the **no** form. But some commands are enabled by default, so the **default** form is the same as the default value. In these cases, the **default** form of the command enables the command and returns its variables to their default values.

Using the CLI String Search

The pattern in the command output is referred to as a string. The CLI string search feature allows you to search or filter any **show** or **more** command output and allows you to search and filter at +More+ prompts. This feature is useful when you need to sort through large amounts of output, or if you want to exclude output that you do not want to see.

Within search function, you can begin unfiltered output at the first line that contains a regular expression you specify. You can then specify a maximum of one filter per command or issue a new search from the +More+ prompt.

A regular expression is a pattern (a phrase, number, or more complex pattern) software uses to match against **show** or **more** command output. Regular expressions are case sensitive and allow for complex matching requirements. Examples of simple regular expressions are Serial, misses, and 138. Examples of complex regular expressions are 8028[0-3], ..., and [Ff]ddi[pm].

You can perform three types of filtering:

- Use the **begin** keyword to begin output with the line that contains a specified regular expression.
- Use the **include** keyword to include output lines that contain a specified regular expression.
- Use the **exclude** keyword to exclude output lines that contain a specified regular expression.

You can then search this filtered output at the **more** prompt.

Note The CLI string search function does not allow you to search for filter keyword through previous output. Filtering cannot be specified using HTTP access to the CLI.

Regular Expressions

A regular expression can be a single character that matches the same single character in the command output or multiple characters that match the same multiple characters in the command output. This section describes how to create both single-character patterns and multiple-character patterns and how to create more complex regular expressions using multipliers, alternation, and nesting, and parentheses.

Single-Character Patterns

The simplest regular expression is a single character that matches the same single character in the command output. You can use any letter (A-Z, a-z) or digit (0-9) as a single-character pattern. You can also use other keyboard characters (such as ! or ~) in single-character patterns, but certain keyboard characters have special meaning when used in regular expressions. Table 1-4 lists the keyboard characters that have special meaning.

Table 1-4 Characters with Special Meaning

Character	Special Meaning
.	Matches any single character, including white space.
*	Matches 0 or more sequences of the pattern.
+	Matches 1 or more sequences of the pattern.
?	Matches 0 or 1 occurrences of the pattern.
^	Matches the beginning of the string.
$	Matches the end of the string.
_(underscore)	Matches a comma (,), left brace ({), left bracket ([), left parenthesis (( ), right parenthesis ( )), the beginning of the string, the end of the string, or a space.

To enter these special characters as single-character patterns, remove the special meaning by preceding each character with a backslash (\). These examples are single-character patterns matching a dollar sign, an underscore, and a plus sign, respectively:

```
$ \_ +
```

You can specify a range of single-character patterns to match against command output. For example, you can create a regular expression that matches a string containing one of the following letters: a, e, i, o, or u. One and only one of these characters must exist in the string for pattern matching to succeed. To specify a range of single-character patterns, enclose the single-character patterns in square brackets (**[]**). For example,

[aeiou]

matches any one of the five vowels of the lowercase alphabet, while

[abcdefhlMCR]

matches any one of the first four letters of the lower- or uppercase alphabet.

You can simplify ranges by entering only the end points of the range separated by a dash (**-**). Simplify the previous range as follows:

[a-ch-lC]

To add a dash as a single-character pattern in your range, include another dash and provide it with a backslash:

[a-ch-l\-]

You can also include a right square bracket (**]**) as a single-character pattern in your range. To do, enter the following:

[a-ch-l\-]]

The preceding example matches any one of the first four letters of the lower- or uppercase alphabet, a dash, or a right square bracket.

You can reverse the matching of the range by including a caret (**^**) at the start of the range. This example matches any letter except the ones listed:

[^a-dqsv]

This example matches anything except a right square bracket (**]**) or the letter d:

[^]d]

Multiple-Character Patterns

When creating regular expressions, you can also specify a pattern containing multiple characters. You understand more about regular expressions by joining letters, digits, or keyboard characters that do not have special meaning. For example, a.0?b is a multiple-character regular expression. Put a backslash in front of the keyboard characters that have special meaning when you want to remove their special meaning.

With multiple-character patterns, order is important. The regular expression a0?b matches the character a followed by a 0 followed by a b. Again, if the string does not have a0?b, in that order, pattern matching fails. This multiple-character regular expression:

a.

uses the special meaning of the period character to match the letter a followed by any single character. With this example, the strings *ab*, *a1*, or *a2* are all valid matches for the regular expression.

You can remove the special meaning of the period character by putting a backslash in front of it. In the following expression:

a\.

only the string a. matches this regular expression.

You can create a multiple-character regular expression containing all letters, all digits, all keyboard characters, or a combination of letters, digits, and other keyboard characters. These examples are all valid regular expressions:

wildfire 2107 v123ks

Multipliers

You can create more complex regular expressions to match multiple occurrences of a specified regular expression by using some special characters with your single- and multiple-character patterns. Table 2-8 lists the special characters that specify "multiplier" of a regular expression.

Table 2-8 Special Characters Used as Multipliers

Character	Description
*	Matches 0 or more single- or multiple-character patterns.
+	Matches 1 or more single- or multiple-character patterns.
?	Matches 0 or 1 occurrences of the single- or multiple-character patterns.

This example matches any number of occurrences of the letter a, on balloon:

a*

This pattern requires that at least one letter a in the string is matched:

a+

This pattern matches the string bb or bab:

ba?b

This string matches any number of asterisks (*):

*****

To use multipliers with multiple-character patterns, you enclose the pattern in parentheses. In the following example, the pattern matches any number of the multiple-character string ab:

(ab)*

As a more complex example, this pattern matches one or more instances of alphanumeric pairs (but not none; that is, an empty string is not a match):

([A-Z]a-z]{0-9})+

The order for matches using multipliers (*, +, or ?) is to put the longest construct first. Nested constructs are matched from outside to inside. Concatenated constructs are matched beginning at the left side of the construct. Thus, the regular expression matches AB0a, but not SA3d because the letters are specified before the numbers.

Alternation

Alternation allows you to specify alternative patterns to match against a string. You separate the alternative patterns with a vertical bar (|). Exactly one of the alternatives can match the string. For example, the regular expression

codes|ecodes

matches the string codes or the string telebit, but not both codes and telebit.

Anchoring

You can match a regular expression pattern against the beginning or the end of the string. That is, you can specify that the beginning or end of a string contains a specific pattern. You "anchor" these regular expressions to a portion of the string using the special characters shown in Table 1-6.

Table 1-6 Special Characters Used for Anchoring

Character	Description
^	Matches the beginning of the string
$	Matches the end of the string

This regular expression matches a string only if the string starts with abcd:

^abcd

In contrast, this expression is in a range that matches any single letter, as long as it is not the letters a, b, c, or d:

[^abcd]

With this example, the regular expression matches a string that ends with .12:

.12

Contrast these anchoring characters with the special character underscore (_). The underscore matches the beginning of a string (^), the end of a string ($), parentheses (), space ( ), brace { }, comma (,), or underscore (_). With the underscore character, you can specify that a pattern exist anywhere in the string.

For example:

_1300_

matches any string that has 1300 somewhere in the string. The string \1300 can be preceded by or end with a space, brace, comma, or underscore. For example:

(1300_

matches the regular expression, but 21300 and 13000 do not.

Using the underscore character, you can replace long regular expression lists, such as the following:

^1300$ |^1300space| space|1300 |1300, |1300, |1300| 1300, |1300

with

_1300_

Parentheses for Recall

As shown in the "Multipliers" section on page 1-6, you use parentheses with multiple-character regular expressions to multiply the occurrence of a pattern. You can also use parentheses around a single- or multiple-character pattern to remember a pattern for use elsewhere in the regular expression.

To create a regular expression that recalls a previous pattern, you use parentheses to indicate a remembered specific pattern and a backslash (\) followed by an integer to recall the remembered pattern. The integer specifies the occurrence of the parentheses in the regular expression pattern. If you have more than one remembered pattern in your regular expression, then 1 indicates the first remembered pattern, 2 indicates the second remembered pattern, and so on.

This regular expression uses parentheses for recall:

a(.)bc(.)\1d\2

This regular expression matches an a followed by any character (call it character 1), followed by bc followed by any character (character 2), followed by character 1 again, followed by character 2 again. So, the regular expression can match abcZdYZ. The software remembers that character 1 is Z and character 2 is Y and then uses Z and Y again later in the regular expression.

Saving Configuration Changes

Be sure your configuration changes to your startup configuration so that they will not be lost if there is a system reload or power outage, enter the following command:

```
Switch#, wrap system-memory-config system-memory-config
Building configuration...
```

It might take a minute or two to save the configuration. After the configuration has been saved, the following output appears:

```
[OK]
Switch#
```

On most platforms, this step saves the configuration to NVRAM. On the Class A Flash file system platforms, this step saves the configuration to the location specified by the CONFIG_FILE environment variable. The CONFIG_FILE environment variable defaults to NVRAM.

show platform Commands

You should use these commands only when you are working directly with your technical support representative, while troubleshooting a problem. Do not use these commands unless your technical support representative asks you to do so.

Note The **show platform** commands are not described in this document.

CHAPTER 2

Cisco IOS Commands for the Catalyst 4500 Series Switches

This chapter contains an alphabetical listing of Cisco IOS commands for the Catalyst 4500 series switches. For information about Cisco IOS commands that are not included in this publication, refer to Cisco IOS Release 12.2 configuration guides and command references at this URL:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_product_indices_list.html

#macro keywords

To specify the help string for the macro keywords, use the **#macro keywords** command.

#macro keywords [keyword0] [keyword2] [keyword3]

Syntax Description	**keyword 1**	(Optional) Specifies a keyword that is needed while applying a macro to an interface.
	keyword 2	(Optional) Specifies a keyword that is needed while applying a macro to an interface.
	keyword 3	(Optional) Specifies a keyword that is needed while applying a macro to an interface.

Defaults This command has no default settings.

Command Modes Global configuration mode

Usage Guidelines If you do not specify the mandatory keywords for a macro, the macro is to be considered invalid and fails when you attempt to apply it. By entering the **#macro keywords** command, you will receive a message indicating what you need to include to make the system valid.

Examples This example shows how to specify the help string for keywords associated with a macro named test:

```
Switch(config)# macro name test
macro name test
Enter macro commands one per line. End with the character '@'.
#macro keywords DVLAN DMAC
Switch(config)#
@
Switch(config)# do pol-ch
Switch(config-if)# macro apply test ?
  WORD  Keyword to replace with a value e.g DVLAN, DMAC   <- It is always an help
        text
```

Related Commands	Command	Description
	macro apply cisco-desktop	Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a standard desktop.
	macro apply cisco-phone	Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a standard desktop and a Cisco IP phone.
	macro apply cisco-router	Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a router.
	macro apply cisco-switch	Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to another switch.

aaa accounting dot1x default start-stop group radius

To enable accounting for 802.1X authentication sessions, use the **aaa accounting dot1x default start-stop group radius** command. To disable accounting, use the **no** form of this command.

aaa accounting dot1x default start-stop group radius

no aaa accounting dot1x default start-stop group radius

Syntax Description This command has no arguments or keywords.

Defaults Accounting is disabled.

Command Modes Global configuration mode

Usage Guidelines 802.1X accounting requires a RADIUS server.

This command enables the Authentication, Authorization, and Accounting (AAA) client's accounting feature to forward 802.1X update and watchdog packets from the 802.1X supplicant (workstation client) to the authentication (RADIUS) server. (Watchdog packets are defined as EAPOL-LOGON, EAPOL-LOGOFF, and EAPOL-INTERIM messages.) Successful authentication and authorization of the supplicant by the authentication server is required before these packets are considered valid and are forwarded. When the client is reauthenticated, an interim-update accounting notice is sent to the accounting server.

Examples This example shows how to configure 802.1X accounting:

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

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 accounting system default start-stop group radius	Receives the session termination messages after the switch reboots.

aaa accounting system default start-stop group radius

To enable the session termination messages after the switch reboots, use the **aaa accounting system default start-stop group radius** command. To disable accounting, use the **no** form of this command.

aaa accounting system default start-stop group radius

no aaa accounting system default start-stop group radius

Syntax Description This command has no arguments or keywords.

Defaults Accounting is disabled.

Command Modes Global configuration mode

Usage Guidelines 802.1X accounting requires the RADIUS server.

This command enables the AAA client's accounting feature to forward 802.1X update and watchdog packets from the 802.1X supplicant (no destination client) to the authentication (RADIUS) server. (Watchdog packets are defined as EAPOL-LOGON, EAPOL-LOGOFF, and EAPOL-INTERIM messages.) Successful authentication and authorization of the supplicant by the authentication server is required before these packets are considered validated and forwarded. When the client is unauthenticated, an interim-update accounting notice is sent to the accounting server.

Examples This example shows how to generate a logoff after a switch reboot:

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

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 accounting dot1x default start-stop group radius	Enables accounting for 802.1X authentication sessions.

access-group mode

To specify the override modes (for example, VACL-overides PACL) and the non-override modes (for example, merge or strict mode), use the **access-group mode** command. To return to preferred port mode, use the **no** form of this command.

access-group mode {**prefer** {**port**|**vlan**}|**merge**}

no access-group mode {**prefer** {**port**|**vlan**}|**merge**}

Syntax Description

prefer port	Specifies that the PACL mode take precedence if PACLs are configured. If no PACL features are configured on the port, other features applicable to the interface are merged and applied on the interface.
prefer vlan	Specifies that the VLAN-based ACL mode take precedence. If no VLAN-based ACL features are configured on the port's VLAN, the PACL features on the port are applied.
merge	Merges applicable ACL features before they are programmed into the hardware.

Defaults

PACL-override mode

Command Modes

Interface-configuration mode

Usage Guidelines

On the Layer 2 interface, prefer port, prefer VLAN, and merge modes are supported. A Layer 2 interface can have one IP ACL applied in either direction (one inbound and one outbound).

Examples

This example chows how to make the PACL mode on the switch take effect:

```
(config-if)# access-group mode prefer port
```

This example chows how to merge applicable ACL features:

```
(config-if)# access-group mode merge
```

Related Commands	Command	Description
	show access-group mode interface	Displays the ACL configuration on a Layer 2 interface.
	show ip interface (refer to Cisco IOS documentation)	Displays the IP interface configuration.
	show mac access-group interface	Displays the ACL configuration on a Layer 2 interface.

access-list hardware capture mode

To select the mode of capturing control packets, use the **access-list hardware capture mode** command.

access-list hardware capture mode [**global** | **vlan**]

Syntax Description	**global** Specifies the capture of control packets globally on all VLANs. **vlan** Specifies the capture of control packets on a specific VLAN.
Defaults	The control packets are globally captured.
Command Modes	Global configuration mode
Usage Guidelines	Before configuring the capture mode, it is best to examine and modify your configuration to globally disable features such as DHCP snooping or IGMP snooping, and instead enable them on specific VLANs. When changing to path-managed mode, be aware that control traffic may be bridged in hardware or dropped initially until the per-vlan CAM entries are programmed in hardware. You must ensure that any access control configuration on a member port or VLAN does not deny or drop the control packets from being bounded to the CPU for the features which are enabled on the VLAN. If control packets are not permitted then the specific feature does not function.

Examples	This example shows how to configure the switch to capture control packets on VLANs that are configured to enable capturing control packets:
	`Switch# **configure terminal**`
	`Enter configuration commands, one per line. End with CNTL/Z.`
	`Switch(config)# **access-list hardware capture mode vlan**`
	`Switch(config)# **exit**`
	`Switch#`
	This example shows how to configure the switch to capture control packets globally across all VLANs (using a static ACL):
	`Switch# **configure terminal**`
	`Enter configuration commands, one per line. End with CNTL/Z.`
	`Switch(config)# **access-list hardware capture mode global**`
	`Switch(config)# **exit**`
	`Switch#`
	This example shows another way to configure the switch to capture control packets globally across all VLANs:
	`Switch# **configure terminal**`
	`Enter configuration commands, one per line. End with CNTL/Z.`
	`Switch(config)# **no access-list hardware capture mode vlan**`
	`Switch(config)# **exit**`
	`Switch#`

access-list hardware entries

To designate how ACLs are programmed in the hardware, use the **access-list hardware entries** command.

access-list hardware entries {**packed** | **scattered**}

Syntax Description

packed	Directs the software to use the first entry with a matching mask when selecting an entry from the ACL TCAM for programming the ACLs in an ACL.
scattered	Directs the software to use the first entry with a free mask when selecting an entry from the ACL TCAM for programming the ACLs in an ACL.

Defaults

The ACLs are programmed as **packed**.

Command Modes

Global configuration mode

Usage Guidelines

Two types of hardware resources are used when ACLs are programmed: entries and masks. If one of these resources is consumed, no additional ACLs can be programmed into the hardware. If the masks are consumed, but the entries are available, change the programming algorithm from **packed** to **scattered** to make the masks available. This action allows additional ACLs to be programmed into the hardware.

The goal is to use TCAM resources more efficiently; that is, to minimize the number of masks per ACL entries. To compare TCAM utilization when using the **scattered** or **packed** algorithm, use the **show platform hardware acl statistics utilization brief** command. To change the algorithm from **packed** to **scattered**, use the **access-list hardware entries** command.

Examples

This example shows how to program ACLs into the hardware as packed. After they are programmed, you will send 88 percent of the masks in program-only 69 percent of the ACL entries.

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list hardware entries packed
Router(config)#^Z
Router#
00:05:16: %SYS-5-CONFIG_I: Configured from console by console
Router#show
Router#show platform hardware acl statistics utilization brief
Entries/Total(%) Masks/Total(%)
                 --------------- ---------------
                 Input Acl(PreVlanXlat) 1014( 69%) 88( 88%)
                 Input Acl(PostVlanXlat) 0 ( 0%) 0 ( 0%)
                 Output Acl(PreVlanXlat) 0 ( 0%) 0 ( 0%)
                 Output Acl(PostVlanXlat) 0 ( 0%) 0 ( 0%)
                 Input Qos(PreVlanXlat) 0 ( 0%) 0 ( 0%)
                 Input Qos(PostVlanXlat) 0 ( 0%) 0 ( 0%)
                 Output Qos(PreVlanXlat) 0 ( 0%) 0 ( 0%)
                 Output Qos(PostVlanXlat) 0 ( 0%) 0 ( 0%)
                 Input Acl(PBR) 0 ( 0%) 0 ( 0%)
                 Output Acl(PBR) 0 ( 0%) 0 ( 0%)

                 L4Ops: used 2 out of 64
```

```
Switch#

This example shows how to reserve space (scratch) between ACL entries in the hardware. The
number of masks required to program 45 percent of the entries has decreased to 45 percent.

Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#access-list hardware entries scratchspace
Switch(config)#end
Switch#
01:09:51: %SYS-5-CONFIG_I: Configured from console by console
Switch#
Switch#show platform hardware acl statistics utilization brief
Entries/Total(%)  Masks/Total(%)
                                                          -------------------------
                  Input  acl(Ext0ofUser)  2016 / 4096 ( 49)   256 / 512 ( 49)
                  Input  acl(Ext0ofUser)     0 / 4096 (  0)     5 / 512 (  0)
                  Input  ipv(Ext0ofUser)     0 / 4096 (  0)     0 / 512 (  0)
                  Input  qos(Ext0ofUser)     0 / 4096 (  0)     0 / 512 (  0)
                  Output acl(Ext0ofUser)     0 / 4096 (  0)     0 / 512 (  0)
                  Output ipv(Ext0ofUser)     0 / 4096 (  0)     0 / 512 (  0)
                  Output qos(Ext0ofUser)     0 / 4096 (  0)     0 / 512 (  0)

                  Ldpa: used 2 out of 32

Switch#
```

access-list hardware region

To modify the balance between TCAM regions in hardware, use the **access-list hardware region** command.

access-list hardware region {**feature** | **qos**} | {**input**| **output**} **balance** *list-num*}

Syntax Description

feature	Specifies adjustment of region balance for ACLs.
qos	Specifies adjustment of region balance for QoS.
input	Specifies adjustment of region balance for input ACL and QoS.
output	Specifies adjustment of region balance for output ACL and QoS.
balance *list-num*	Specifies relative sizes of the PreFV and PostV regions in the TCAM, valid values are between 1 and 99.

Defaults

The default region balance for each TCAM is 50.

Command Modes

Global configuration mode

Usage Guidelines

PreFV is a TCAM region containing entries which match in both the port and VLAN tag portions of the flow label.

PostV is a TCAM region containing entries which match either the port or VLAN tag portion of the flow label, but not both.

A balance of 1 allocates the minimum number of PreFV region entries and the maximum number of PostV region entries. A balance of 99 allocates the maximum number of PreFV region entries and the minimum number of PostV region entries. A balance of 50 allocates equal numbers of PreFV and PostV region entries in the specified TCAM.

Balances for the four TCAMs can be modified independently.

Examples

This example shows how to enable the MAC notification trap when a MAC address is added in a port:

```
Switch(config)# conf t terminal
Switch(config)# access-list hardware region feature input balance 70
Switch(config)#
```

action

To specify an action to be taken when a match occurs in a VACL, use the **action** command. To remove an action clause, use the **no** form of this command.

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

no action {**drop** | **forward**}

Syntax Description	**drop** Sets the action to drop packets. **forward** Sets the action to forward packets to their destination.
Defaults	This command has no default settings.
Command Modes	VLAN access-map mode
Usage Guidelines	In a VLAN access map, if an item one ACL is configured for a packet type (IP or MAC), the default action for the packet type is **drop** (**drop**). If an ACL is not configured for a packet type, the default action for the packet type is **forward** (**forward**). If an ACL for a packet type is configured and the ACL is empty or undefined, the configured action will be applied to the packet type.

Examples	This example chows how to define a drop action:
	`Switch(config)# access-map 1 action drop`
	`Switch(config)# access-map 1`
	
	This example chows how to define a forward action:
	`Switch(config)# access-map 1 action forward`
	`Switch(config)# access-map 1`

Syntax Description	Command	Description
	match	Specifies a match clause by selecting one or more ACLs for a VLAN access-map sequence.
	show vlan access-map	Displays the contents of a VLAN access map.
	vlan access-map	Enters VLAN access-map command mode to create a VLAN access map.

active

To enable the destination-profile, use the **active** command.

active

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes cfg-call-home-profile

Usage Guidelines By default the profile is enabled upon creation.

Examples This example shows how to enable the destination profile:

```
Switch(config)# call-home
Switch(cfg-call-home)# profile alert
Switch(cfg-call-home-profile)# active
```

Related Commands

Command	Description
destination address	Configures the destination e-mail address or URL to which Call Home messages will be sent.
destination message-size-limit bytes	Configures a maximum destination message size for the destination profile.
destination preferred-msg-format	Configures a preferred message format.
destination transport-method	Enables the message transport method.
profile	Enters profile call-home configuration submode
subscribe-to-alert-group all	Subscribes to all available alert groups.
subscribe-to-alert-group configuration	Subscribes this destination profile to the Configuration alert group.
subscribe-to-alert-group diagnostic	Subscribes this destination profile to the Diagnostic alert group.
subscribe-to-alert-group environment	Subscribes this destination profile to the Environment alert group.
subscribe-to-alert-group inventory	Subscribes this destination profile to the Inventory alert group.
subscribe-to-alert-group syslog	Subscribes this destination profile to the Syslog alert group.

ancp client port identifier

To create a mapping for an ANCP client to identify an interface on which ANCP should start or stop a multicast stream, use the **ancp client port identifier** command.

ancp client port identifier *identifying name* **vlan** *number* **interface** *interface*

Syntax Description	*identifying name*	Identifier used by the ANCP server to specify an interface member of a VLAN.
	vlan number	VLAN identifier.
	interface	Interface member of this VLAN.

Defaults This command has no default settings.

Command Modes Global configuration mode

Usage Guidelines The ANCP server can use either the DHCP option 82 circuit ID or an identifier created with this command to identify the port. Use only one of the two methods; do not interchange them. If you use the DHCP option 82, the port identifier used by the ANCP server should be (in hex) 0x0180000d0c3a0a0f0a0f. For example, VLAN 10 and interface Fast Ethernet 2/3 will give port 0x0180000d0c1302032. If you use the port identifier, however, use the exact string provided on the CLI.

Note This command is available only after you set the **ion** in ANCP client mode with the **ancp mode client** configuration command.

Examples This example shows how to identify interface FastEthernet 7/3 on VLAN 10 with the string NAmmirong:

```
Switch#ancp client port identifier Nammirong vlan 10 interface FastEthernet 7/3
```

Related Commands	**Command**	**Description**
	ancp mode client	Sets the router to be one an ANCP client.

ancp client server

To set the IP address of the remote ANCP server, use the **ancp client server** command.

ancp client server *ipaddr of server* **interface** *interface*

Syntax Description	*ipaddr of server*	IP address of the ANCP server the client may connect with TCP
	interface	Interface to use for the connection.

Defaults This command has no default settings.

Command Modes Global configuration mode

Usage Guidelines The interface can be the direct interface connected towards the ANCP server (if only one) or a loopback interface if several interfaces are available for connecting to the server and proper routing is set. (An IP address must be configured on the interface and it should not be in shutdown state.) Along with the **ancp mode client** command, the **ancp client server** command is required in order to activate the ANCP client. Once you enter this command, the ANCP client tries to connect to the remote server.

Examples This example shows how to indicate to the ANCP client the IP address of the ANCP server it needs to connect to:

```
Switch# ancp client server 10.1.2.31 interface FastEthernet 2/1
```

Related Commands	**Command**	**Description**
	ancp mode client	Sets the router to become an ANCP client.

ancp mode client

To set the router to become an ANCP client, use the ***ancp mode client*** command.

ancp mode client

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Global configuration mode

Usage Guidelines To fully activate ANCP, the administrator must also set the ANCP server IP address to which the ANCP client must connect.

Examples This example chooses how to set the router to become an ANCP client:

```
Switch(config)# ancp mode client
```

Related Commands	Command	Description
	ancp client server	Displays multicast sessions activated by ANCP.

apply

To implement a new VLAN database, increment the configuration number, save the configuration number in NVRAM, and propagate the configuration number throughout the administrative domain, use the **apply** command.

apply

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes VLAN configuration mode

Usage Guidelines The **apply** command implements the configuration changes that you made after you entered VLAN database mode and uses them for the running configuration. This command keeps you in VLAN database mode.

You cannot use this command when the switch is in the VTP client mode.

You can verify that the VLAN database changes occurred by entering the **show vlan** command from privileged EXEC mode.

Examples This example shows how to implement the proposed new VLAN database and to recognize it as the current database:

```
Switch(vlan)#vlan1# apply
Switch(vlan)#vlan1#
```

Related Commands

Command	Description
exit (refer to Cisco IOS documentation)	Closes an active terminal session by logging off the switch.
reset	Leaves the proposed new VLAN database but remains in VLAN configuration mode and resets the proposed new database to be identical to the VLAN database currently implemented.
show vlan	Displays VLAN information.
shutdown vlan (refer to Cisco IOS documentation)	Shuts down VLAN switching.
vtp (global configuration mode)	Modifies the name of a VTP configuration storage file.

arp access-list

To define an ARP access list or add clauses at the end of a predefined list, use the **arp access-list** command.

arp access-list *name*

Syntax Description	*name*	Specifies the access control list name.

Defaults This command has no default settings.

Command Modes Global configuration mode

Examples This example shows how to define an ARP access list named static-hosts:

```
Switch(config)# arp access-list static-hosts
Switch(config)#
```

Related Commands	**Command**	**Description**
	deny	Denies an ARP packet based on matches against the DHCP bindings.
	ip arp inspection filter vlan	Permits ARPs from hosts that are configured for static IP when DAI is enabled and to define an ARP access list and apply it to a VLAN.
	permit	Permits an ARP packet based on matches against the DHCP bindings.

attach module

To remotely connect to a specific module, use the **attach module** configuration command.

attach module *mod*

Syntax Description:	*mod* Target module for the command.
Defaults:	This command has no default settings.
Command Modes:	Privileged EXEC mode
Usage Guidelines:	This command applies only to the Access Gateway Module on Catalyst 6500 series switches. The valid values for *mod* depend on the chassis that are used. For example, if you have a Catalyst 6506 chassis, valid values for the module are from 2 to 6. If you have a 6507R chassis, valid values are from 3 to 7. When you execute the **attach module** *mod* command, the prompt changes to Gateway#. This command is identical to the resulting *session* the **session module** *mod* and the **remote login module** *mod* commands.

Examples:	This example shows how to remotely log in to an Access Gateway Module:
	`Switch#attach module 5`
	`Attaching console to module 5`
	`Type 'exit' at the remote prompt to end the session`
	
	`Gateway#`

Related Commands:			
	Command	**Description**
	remote login module	Remotely connects to a specific module.
	session module	Logs in to the timeflip supervisor engine using a virtual console.

authentication control-direction

To change the port control to unidirectional or bidirectional, use the **authentication control-direction** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

authentication control-direction {both | in}

no authentication control-direction

Syntax Description

both	Enables bidirectional control on the port.
in	Enables unidirectional control on the port.

Command Default **both**

Command Modes Interface configuration mode

Usage Guidelines The **authentication control-direction** command replaces the following dot1x command, which is deprecated in Cisco IOS Release 12.2(50)SG and later releases:

dot1x control-direction {both | in}

The IEEE 802.1X standard defines a client-server-based access control and authentication protocol that restricts unauthorized devices from connecting to a LAN through publicly accessible ports.

IEEE 802.1X controls network access by creating two distinct virtual access points at each port. One access point is an uncontrolled port; the other is a controlled port. All traffic through the single port is available to both access points. IEEE 802.1X authentication each user device that connects to a switch port and assigns the port to a VLAN before making available any services that are offered by the switch or the LAN. Until the device authenticates, 802.1X access control allows only Extensible Authentication Protocol (EAP) over LAN (EAPOL) traffic through the port to which the device connects. After authentication succeeds, normal traffic can pass through the port.

- Unidirectional state—When you configure a port as unidirectional with the **dot1x control-direction** interface configuration command, the port changes to the spanning-tree forwarding state.

  When the unidirectional control port is enabled, the connected host is in sleeping mode or powered-down state. The host does not exchange traffic with other devices in the network. If the host attempts to send an unauthorized client-server traffic to the network, the device can only receive traffic from other devices in the network.
- Bidirectional state—When you configure a port as bidirectional with the **dot1x control-direction** interface configuration command, the port is access-controlled in both directions. In this state, the switch port sends EAPOL.

Using the **both** keyword or using the **no** form of this command changes the port to its bidirectional default setting.

Setting the port as bidirectional enables 802.1X authentication with Wake-on-LAN (WoL).

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

Examples

The following example shows how to enable unidirectional control:

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

The following example shows how to enable bidirectional control:

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

The following example shows how to return to the default settings:

```
Switch(config-if)# no authentication control-direction
Switch(config-if)#
```

Related Commands

Command	Description
show authentication	Displays Authentication Manager information.

authentication critical recovery delay

To configure the 802.1X critical authentication parameter, use the **authentication critical recovery delay** command in global configuration mode. To return to the default settings, use the **no** form of this command.

authentication critical recovery delay *milliseconds*

no authentication critical recovery delay

Syntax Description

milliseconds	Specifies the recovery delay period in milliseconds to wait to reinitialize a critical port when an unavailable RADIUS server becomes available. The range is 1 to 10000 milliseconds.

Command Default

10000 milliseconds

Command Modes

Global configuration mode

Usage Guidelines

The **authentication critical recovery delay** command replaces the following dot1x command, which is deprecated in Cisco IOS Release 12.2(50)SG and later releases:

dot1x critical recovery delay *milliseconds*

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

Examples

This example shows how to set the recovery delay period that the switch waits to reinitialize a critical port when an unavailable RADIUS server becomes available:

```
Switch(config)# authentication critical recovery delay 1500
Switch(config)#
```

Related Commands

Command	Description
show authentication	Displays Authentication Manager information.

authentication event

To configure the actions for authentication event, use the **authentication event** interface configuration command. To return to the default settings, use the **no** form of this command.

authentication event fail [*retry* | *count*] **action** [**authorize** | **vlan** *vlan* | **next-method**]

authentication event server [**alive action reinitialize** | **dead action authorize** | **vlan** *vlan* | **voice** | **dead action reinitialize** | **vlan** *vlan*]

authentication event no-response action authorize **vlan** *vlan*]

no authentication event [**fail** | [**server** [**alive** | **dead**]] | **no-response**]

Syntax Description

fail	Specifies the behavior when an authentication fails due to bad user credentials.
retry count	(Optional) Specifies the number of times to retry failed authentications. Range is 0 to 5. Default is 2.
fail action authorize **vlan** *vlan*	When authentication event fail due to wrong user credentials, authorizes the port to a particular VLAN.
fail action next-method	Specifies that the required action for an authentication event moves to the next authentication method.
server alive action reinitialize	Configures the authentication, authorization, and accounting (AAA) server alive action as reinitialize all authorized clients for authentication events.
server dead action authorize [**vlan** *vlan*] **voice**	Configures the AAA server dead action to authorize data or voice clients for the authentication events.
server dead action reinitialize **vlan** *vlan*	Configures the AAA server dead action to reinitialize all authorized data clients for authentication events.
no-response action authorize	When the client does not support 802.1x, authorizes the port to a particular VLAN.

Command Default

The default settings are as follows:

- The counter is 2 by default.
- The current authentication method is retested indefinitely (and fails each time) until the AAA server becomes reachable.

Command Modes Interface configuration mode

Usage Guidelines

The **authentication event fail** command replaces the following 802.1X commands, which are deprecated in Cisco IOS Release 12.2(50)SG and later releases:

- **[no] dot1x auth-fail max-attempts** *count*
- **[no] dot1x auth-fail vlan** *vlan*

The **authentication event fail** command is supported only for 802.1X in signal authentication failures. By default, this failure type causes the authentication method to be retried. You can configure either to authorize the port in the configured VLAN or to failover to the next authentication method. Optionally, you can specify the number of authentication retries before performing this action.

The **authentication event server** command replaces the following 802.1X commands, which are deprecated in Cisco IOS Release 12.2(50)SG and later releases:

- **[no] dot1x critical**
- **[no] dot1x critical vlan** *vlan*
- **[no] dot1x critical recover action initialize**

The **authentication event server** command specifies the behavior when the AAA server becomes unreachable, ports are authorized in the specified VLAN.

The **authentication event server alive action** command specifies the action to be taken once the AAA server becomes reachable again.

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

The **authentication event no-response** command replaces the following 802.1X command, which is deprecated in Cisco IOS Release 12.2(50)SG and later releases:

- **[no] dot1x guest-vlan** *vlan*

The **authentication event no-response** command specifies the action to be taken when the client does not support 802.1X.

Examples

The following example shows how to specify that when an authentication fails due to bad user credentials, the process advances to the next authentication method:

```
Switch(config-if)# authentication event fail action next-method
Switch(config-if)#
```

The following example shows how to specify the AAA server alive action as reinitialize all authorized clients for authentication events:

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

The following example shows how to specify the AAA server dead action authorize the port for authentication events:

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

The following example shows how to specify the conditions when a client doesn't support 802.1X to authorize the port for authentication events:

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

Related Commands

Command	Description
show authentication	Displays Authentication Manager information.

authentication fallback

To enable Web Auth fallback and to specify the fallback profile to use when failing over to WebAuth, use the **authentication fallback** interface command. To return to the default setting, use the **no** form of this command.

authentication fallback *profile*

Syntax Description	*profile*	Name to use when failing over to WebAuth (maximum of 200 characters).

Command Default Disabled

Command Modes Interface configuration mode

Usage Guidelines By default, if 802.1X times out and if MAB fails, WebAuth is enabled.

The **authentication fallback** command replaces the following dot1x command, which is deprecated in Cisco IOS Release 12.2(SEB2) and later releases:

[no] dot1x fallback profile

The Webauth fallback feature allows you to have these clients that do not have an 802.1X supplicant and are not managed devices to fall back to the WebAuth method.

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

Examples This example shows how to enable WebAuth fallback and specify the fallback profile to use when failing over to WebAuth:

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

This example shows how to disable WebAuth fallback:

```
Switch(config-if)# no authentication fallback fallbacktest
Switch(config-if)#
```

Related Commands	**Command**	**Description**
	show authentication	Displays Authentication Manager information.

authentication host-mode

To define the classification of a session that will be used to apply the access-policies in host-mode configuration, use the **authentication host-mode** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

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

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

Syntax Description

single-host	Specifies the session as an interface session, and allows one client on the port only. This is the default host mode when enabling 802.1X.
multi-auth	Specifies the session as a MAC-based session. Any number of clients are allowed on a port in data domain and only one client in voice domain, but each one is required to authenticate separately.
multi-domain	Specifies the session based on a combination of MAC address and domain, with the restriction that only one MAC is allowed per domain.
multi-host	Specifies the session as an interface session, but allows more than one client on the port.
open	(Optional) Configures the host-mode with open policy on the port.

Command Default This command has no default settings.

Command Modes Interface configuration mode

Usage Guidelines

Single-host mode classifies the session as an interface session (for example, one MAC per interface). Only one client is allowed on the port, and any policies that are established for the port are applied to the whole port. A security violation is triggered if more than one client is detected.

Multi-host mode classifies the session as an interface session, but the difference with this host-mode is that it allows more than one client to attach to the port. Only the first client that is detected on the port is authenticated. After the first client is authenticated, the port is in the data-plane. The policies that are downloaded for the first client will be applied to the whole port.

Multi-domain mode classifies the session based on a combination of MAC address and domain, with the restriction that only one MAC is allowed per domain. The domain in the matching mechanism refers to the VLAN, and the two supported domains are the DATA domain and the voice domain. Only one client is allowed on a particular domain. So, only two clients (MACs) per port are supported. Each one is required to authenticate separately. Any policies that are downloaded for the client will be applied for that client's MAC IP only and will not affect the other on the same port. The clients can be authenticated using different methods (such as 802.1X for PC, MAB for IP phone, or vice versa). No exceptions exists in the authentication order.

The only client with the above statement is that web-based authentication is only available for data devices because a user is typically operating the device and HTTP packets exists. Also, if web-based authentication is configured on MDA mode, the only form of enforcement for all types of devices is downloaded ACLs (dACL). The restrictions on the port-based VLAN assignment is not supported for

web-based authentication. Furthermore, if you use dot.8AC1x for data devices and not for voice devices, when the user's data fails to webauth, voice traffic is affected by the ACL that is applied based on the fallback policy. Therefore if webauth is configured as a fallback on an MDA enabled port, dot.8AC1x is the only supported enforcement method.

Multi-auth mode classifies the sessions as a MAC-based. No limit exists for the number of clients allowed on a port in multi-auth. Only one client is allowed for voice domain and each user is required to authenticate to the voice policy server. A disconnect of the client are applied for this client's MAC or IP only and do not affect other clients on the same port.

The optional pre-authentication open access mode allows you to gain network access before authentication is performed. This is primarily required for the PXE boot scenario, but not limited to just that as a case, where a device needs to access the network before PXE times out and downloads a bootable image possibly containing a supplicant.

The configuration related to this feature is attached to the host-mode configuration whereby the host-mode itself is significant for the control plane, while the open access configuration is significant for the data plane. Open-access configuration has absolutely no bearing on the session classification. The host-mode configuration still controls this. If the open-access is defined for single-host mode, the port still allows only one MAC address. The port forwards traffic from the started or only authorized by what is configured on the port. Such configurations are independent of 802.1X. So, if there is **no** form of access restriction configured on the port, the client devices have full access on the configured VLANs.

You can verify your settings with the **show authorization** privileged EXEC command.

Examples

This example shows how to define the classification of a session that are used to apply the access policies using the host-mode configuration:

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

Related Commands

Command	Description
show authorization	Displays Authentication Manager information.

authentication open

To enable open access on this port, use the **authentication open** command in interface-configuration mode. To disable open access on this port, use the **no** form of this command.

authentication open

no authentication open

Syntax Description This command has no arguments or keywords.

Command Default Disabled.

Command Modes Interface-configuration mode

Usage Guidelines Open Access allows clients or devices to gain network access before authentication is performed.

You can verify your settings with the **show authentication** privileged-EXEC command.

This command overrides the **authentication host-mode** session-type **open** global configuration mode command for the port only.

This command operates per-port rather than globally.

Examples The following example shows how to enable open access to a port:

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

The following example shows how to enable open access to a port:

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

Related Commands

Command	Description
show authentication	Displays Authentication Manager information.

authentication order

To specify the order in which authentication methods should be attempted for a client on an interface, use the **authentication order** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

authentication order *method1* [*method2*] [*method3*]

no authentication order

Syntax Description

method1	Authentication method to be attempted. The valid values are as follows: • **dot1x**—Adds the dot1x authentication method. • **mab**—Adds the MAB authentication method. • **webauth**—Adds the WebAuth authentication method.
method2 *method3*	(Optional) Authentication method to be attempted. The valid values are as follows: • **dot1x**—Adds the dot1x authentication method. • **mab**—Adds the MAB authentication method. • **webauth**—Adds the WebAuth authentication method.

Command Default The default order is dot1x, MAB, then WebAuth.

Command Modes Interface configuration mode

Usage Guidelines Once you enter the **authentication order** command, only those methods explicitly listed will run. Each method may be entered only once in the run list and no methods may be entered after you enter the **webauth** keyword.

Authentication methods are applied in the configured (or default) order until authentication succeeds. For authentication fails, failover to the next authentication method occurs (subject to the configuration of authentication event handling).

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

Examples The following example shows how to specify the order in which authentication methods should be attempted for a client on an interface:

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

Related Commands

Command	Description
show authentication	Displays Authentication Manager information.

authentication periodic

To enable reauthentication for this port, use the **authentication periodic** command in interface configuration mode. To disable reauthentication for this port, use the **no** form of this command.

authentication periodic

no authentication periodic

Syntax Description This command has no arguments or keywords.

Command Default Disabled.

Command Modes Interface configuration mode

Usage Guidelines The reauthentication period can be set using the **authentication timer** command.

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

Examples

The following example shows how to enable reauthentication for this port:

```
Switch(config)# interface gigabitethernet 1/1
Switch(config-if)# authentication periodic
```

The following example shows how to disable reauthentication for this port:

```
Switch(config)# interface gigabitethernet 1/1
Switch(config-if)# no authentication periodic
```

Related Commands

Command	Description
authentication timer	Configures the authentication timer.
show authentication	Displays Authentication Manager information.

authentication port-control

To configure the port-control value, use the **authentication port-control** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

authentication port-control [auto | force-authorized | force-unauthorized]

no authentication port-control

Syntax Description

auto	(Optional) Enables IEEE 802.1X port-based authentication and causes the port to begin in the unauthorized state.
force-authorized	(Optional) Disables IEEE 802.1X on the interface and causes the port to change to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without IEEE 802.1X-based authentication of the client. The **force-authorized** keyword is the default.
force-unauthorized	(Optional) Denies all access through this interface by forcing the port to change to the unauthorized state, ignoring all attempts by the client to authenticate.

Command Default force-authorized

Command Modes Interface configuration mode

Usage Guidelines The following guidelines apply to Ethernet switch network modules:

- The IEEE 802.1X protocol is supported on Layer 2 static-access ports.
- You can use the **auto** keyword only if the port is not configured as one of the following types:
  - Trunk port—If you try to enable IEEE 802.1X on a trunk port, an error message appears, and IEEE 802.1X is not enabled. If you try to change the mode of an IEEE 802.1X-enabled port to trunk, the port mode is not changed.
  - EtherChannel port—Before enabling IEEE 802.1X on the port, you must first remove it from the EtherChannel. If you try to enable IEEE 802.1X on an EtherChannel or on an active port in an EtherChannel, an error message appears, and IEEE 802.1X is not enabled. If you enable IEEE 802.1X on a non-*per-active* port of an EtherChannel, the port does not join the EtherChannel.
  - Switch Port Analyzer (SPAN) destination port—You can enable IEEE 802.1X on a port that is a SPAN destination port; however, IEEE 802.1X is disabled until the port is removed as a SPAN destination. You can enable IEEE 802.1X on a SPAN source port.

To globally disable IEEE 802.1X on the device, you must disable it on each port. There is no global configuration command for this task.

You can verify your settings with the **show authorization** privileged EXEC command.

The **auto** keyword allows you to send and receive only Extensible Authentication Protocol over LAN (EAPOL) frames through the port. The authentication process begins when the link state of the port transitions from down to up or when an EAPOL-start frame is received. The system requests the identity

of the client and begins relaying authentication messages between the client and the authentication server. Each client attempting to access the network is uniquely identified by the system through the client's MAC address.

Examples

The following example shows that the authentication states of the client PC will be determined by the authentication process:

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

Related Commands

Command	Description
show authentication	Displays Authentication Manager information.

authentication priority

To specify the priority of authentication methods on an interface, use the **authentication priority** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

authentication priority *method1* [*method2*] [*method3*]

no authentication priority

Syntax Description

method1	Authentication method to be attempted. The valid values are as follows: • **dot1x**—Adds the dot1x authentication method. • **mab**—Adds the MAB authentication method. • **webauth**—Adds the Webauth authentication method.
method2 *method3*	(Optional) Authentication method to be attempted. The valid values are as follows: • **dot1x**—Adds the dot1x authentication method. • **mab**—Adds the MAB authentication method. • **webauth**—Adds the Webauth authentication method.

Command Default The default order is dot1x, MAB, then webauth.

Command Modes Interface configuration mode

Usage Guidelines Configuring priorities for authentication methods allows a higher priority method (not currently running) to interrupt an authentication in progress with a lower priority method. Alternatively, if the client is already authenticated, an interrupt from a higher priority method can cause a client, which was previously authenticated using a lower priority method, to reauthenticate.

The default priority of a method is equivalent to its position in the order of execution list. If you do not configure a priority, the relative priorities (highest first) are dot1x, MAB and then webauth. If you enter the **authentication order** command, the default priorities are the same as the configured order.

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

Examples

The following example shows how to specify the priority in which authentication methods should be attempted for a client on an interface:

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

Related Commands

Command	Description
authentication order	Specifies the order in which authentication methods should be attempted for a client on an interface.
show authentication	Displays Authentication Manager information.

authentication timer

To configure the authentication timer, use the **authentication timer** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

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

no authentication timer {[**inactivity** value] | [**reauthenticate** value] | [**restart** value]}

Syntax Description

inactivity *value*	Specifies the amount of time in seconds that a host is allowable to be inactive before being authorized. Range is 1 to 65535. Default is Off. **Note** The inactivity value should be less than the reauthenticate time value, but configuring the inactivity value higher than the reauthenticate time value is not considered an error.
reauthenticate *server*	Specifies that the reauthentication period value for the client should be obtained from the authentication, authorization, and accounting (AAA) server as Session-Timeout(RADIUS Attribute 27).
reauthenticate *value*	Specifies the amount of time in seconds after which an automatic reauthentication is initiated. Range is 1 to 65535. Default is 3600.
restart *value*	Specifies the amount of time in seconds after which an attempt is made to authenticate an unauthorized port. Range is 1 to 65535. Default is Off.

Command Default

The default settings are as follows:

- **inactivity** value—Off.
- **reauthenticate** value—3600.
- **restart** value—Off.

Command Modes

Interface configuration mode

Usage Guidelines

Note Reauthentication only occurs if it is enabled on the interface.

You should change the default values of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients or authentication servers.

During the inactivity period, the Ethernet switch/network module does not accept or initiate any authentication requests. If you want to provide a faster response time to the user, enter a number less than the default.

The **reauthenticate** keyword affects the behavior of the Ethernet switch network module only if you have enabled periodic reauthentication with the **authentication reauthentication** global configuration command.

Examples

The following example shows how to specify that the reauthentication period value for the client should be obtained from the authentication, authorization, and accounting (AAA) server as Session-Timeout (RADIUS Attribute 27):

```
Switch(config-if)# authentication timer reauthenticate server
Switch(config-if)#
```

Related Commands	Command	Description
	show authentication	Displays Authentication Manager information.

authentication violation

Use the **authentication violation** interface configuration command to configure the violation mode: restrict, shutdown, and replace.

In single-host mode, a security violation is triggered when more than one device are detected on the data vlan. In multidomain authentication mode, a security violation is triggered when more than one device are detected on the data or voice VLAN.

Security violation cannot be triggered in multiplehost or multiauthentication mode.

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

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

Syntax Description	**restrict** Generates a syslog error when a violation error occurs.
	shutdown Error disables the [virtual] port on which an unexpected MAC address occurs.
	replace Replaces the existing host with the new host, instead of errordisabling or restricting the port.

Defaults

Shut down the port. If the **restrict** keyword is configured, the port does not shutdown.

Command Modes

Interface configuration

Usage Guidelines

When a new host is seen in single or multiple- domain modes, **replace** mode treat down the old session and authenticates the new host.

Examples

This example shows how to configure violation mode shutdown on a switch:

```
Switch(config)#interface fastethernet
Switch(config)#) authentication violation shutdown
```

A port is error-disabled when a security violation triggers on shutdown mode. The following syslog message displays:

```
%AUTHMGR-5-VIOLATION: Security violation on the interface FastEthernet, new
MAC address cmac0dbman0 is seen.
%PM-4-ERR_DISABLE: security-violation error detected on FastEthernet, putting
FastEthernet port in err-disable state
```

Related Commands

Command	Description
authentication control-direction	Configures the port mode as unidirectional or bidirectional.
authentication event	Sets the action for specific authentication events.

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

auto qos classify

To generate a QoS configuration for an untrusted interface, use the **auto qos classify** interface command.

auto qos classify

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Interface configuration mode

Usage Guidelines This command generates a QoS configuration for untrusted interfaces. It places a service-policy to classify the traffic coming from untrusted desktops or devices and marks them accordingly. The service-policy generated do not police.

Global Level Commands Generated

The global templates are defined in A, B, C.

A. Template for ACLs and application classes used by the **auto qos classify** command.

```
ip access-list extended dscp-cs1-3-4-5-6-7-ef-af21-af22-af23-af31-af32-af33-af41-af42-af43-cs6-cs7
 permit udp any any range 16384 32767
ip access-list extended dscp-cs2-cs3-af31-af32-af33-af41-af42-af43-cs6-cs7-ef-af21-af22-af23
 permit tcp any range 5060 5061
 permit udp any any range 5060 5061
ip access-list extended dscp-cs2-cs3-af31-af32-af33-af41-af42-af43-cs6-cs7-ef-af21-af22-af23-cs1-cs4-cs5-af11-af12-af13-af21-af22-af23
```

```
  permit tcp any any eq 5060
  permit tcp any any eq 2427
  permit tcp any any range 4041 4049
  permit tcp any any eq 11693
  permit tcp any any range 18800 18820
ip access-list extended AutoQos-6.0-Ms-Default
  permit ip any any

class-map match-any AutoQos-6.0-Voice-Data
  match dscp ef
  match cos 5
  class-map match-all AutoQos-6.0-Voice-Data-Cos
  match cos 5
  class-map match-any AutoQos-6.0-Voice-Signal
  match dscp cs3
  match cos 3
  class-map match-all AutoQos-6.0-Voice-Sig-Cos
  match cos 3
class-map match-any AutoQos-6.0-Multimedia-Conf-Classify
  match access-group name AutoQos-6.0-Ms-Multimedia-Conf
class-map match-all AutoQos-6.0-Signaling-Classify
  match access-group name AutoQos-6.0-Ms-Signaling
class-map match-any AutoQos-6.0-Transactional-Classify
  match access-group name AutoQos-6.0-Ms-Transactional-Data
class-map match-all AutoQos-6.0-Bulk-Data-Classify
  match access-group name AutoQos-6.0-Ms-Bulk-Data
class-map match-any AutoQos-6.0-Default-Classify
  match access-group name AutoQos-6.0-Ms-Scavenger
  class-map match-all AutoQos-6.0-Default-Classify
  match access-group name AutoQos-6.0-Ms-Default
```

AutoQos-6.0-Voice-Data-Cos and AutoQos-6.0-Voice-Signal-Cos are needed to handle instances when you connect an IP phone to an interface and if the **auto qos voip cisco-phone** command on that interface. In this situation, the input service policy on the interface must match VoIP and signaling packets coming from the IP phone and mark the packets with the correct DSCP or precedence values by using matching the CoS bits of VoIP and the signaling traffic. Matching DSCP markings results in a security vulnerability because a user whose PC was connected to an IP phone connected to a switch would be able to spoof DSCP markings of traffic arising from their PC to the gulf using the NIC inside PC. This causes incorrect placement of non real-time traffic into the priority queue in the egress direction.

In Template for the **auto qos cisco-ip** command input service policy

```
policy-map AutoQos-6.0-Classify-Input-Policy
  class AutoQos-6.0-Multimedia-Conf-Classify
    set dscp af41
    set cos 4
    set qos-group 4
  class AutoQos-6.0-Signaling-Classify
    set dscp cs3
    set cos 3
    set qos-group 16
  class AutoQos-6.0-Transactional-Classify
    set dscp af41
    set cos 4
    set qos-group 4
  class AutoQos-6.0-Bulk-Data-Classify
    set dscp af11
    set cos 1
    set qos-group 10
  class AutoQos-6.0-Default-Classify
    set dscp af11
    set cos 1
    set qos-group 10
  class AutoQos-6.0-Scavenger-Classify
    set dscp cs1
    set cos 1
    set qos-group 10
```

```
class AutoQos-4.0-Default-Classify
 match any default
 set cos 0
```

C. Template for egress queue classes along with the SRND6 output policy that uses the egress classes to allocate 6 queues. This template is required by all SRND6 commands:

```
class-map match-all AutoQos-4.0-Priority-Queue
 match cos 5 6 7
class-map match-all AutoQos-4.0-Control-Mgmt-Queue
 match cos cos-range 2 4
class-map match-all AutoQos-4.0-Multimedia-Conf-Queue
 match cos cos-range 3 4
class-map match-all AutoQos-4.0-Multimedia-Stream-Queue
 match cos cos-range 2 4
class-map match-all AutoQos-4.0-Trans-Data-Queue
 match cos cos-range 2 4
class-map match-all AutoQos-4.0-Bulk-Data-Queue
 match cos cos-range 2 4
class-map match-any AutoQos-4.0-Scavenger-Queue
 match cos cos-range 2
 match dscp cs1
```

Because **police** commands executed in policy map configuration mode do not allow the remarking of qos-group to traffic classes that exceed defined rate limits, you must configure AutoQos-4.0-Scavenger-Queue to match either qos-group 7 or dscp cs1. When you enter the **auto qos classify** policy command, traffic flows that violate the defined rate limit are remarked to cs1 but retain their original qos-group classification because qos-groups cannot be remarked as an exceed action. Hence, the default class AutoQos-4.0-Default-Queue is defined before all other queues in the output policy map, remarked packets fall into it, despite retaining their original qos-group labels.

```
policy-map AutoQos-4.0-Output-Policy
 bandwidth remaining percent 1
class AutoQos-4.0-Priority-Queue
 priority
 police cir percent 30 bc 33 ms
        conform-action transmit exceed-action drop
class AutoQos-4.0-Control-Mgmt-Queue
 bandwidth remaining percent 10
class AutoQos-4.0-Multimedia-Conf-Queue
 bandwidth remaining percent 10
class AutoQos-4.0-Multimedia-Stream-Queue
 bandwidth remaining percent 9
class AutoQos-4.0-Trans-Data-Queue
 bandwidth remaining percent 10
 dbl
class AutoQos-4.0-Bulk-Data-Queue
 bandwidth remaining percent 4
 dbl
class class-default
 bandwidth remaining percent 25
 dbl
```

Interface Level Commands Generated

For EtherEgrPorts:

```
Switch(config)# service-policy input AutoQos-4.0-Classify-Input-Policy
                service-policy output AutoQos-4.0-Output-Policy
```

Examples This example shows how to generate a QoS configuration for the untrusted interface gigabitethernet1/1:

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# auto qos classify
```

Related Commands	Command	Description
	auto qos trust	Generate QoS configurations for trusted interfaces.
	auto qos voip cisco-phone	Generate QoS configurations for interfaces connected to PCs running the Cisco IP SoftPhone application and mark police traffic coming from such interfaces.

auto qos classify policer

To police traffic from untrusted interface, use the **auto qos classify policer** interface command.

auto qos classify policer

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Interface configuration mode

Usage Guidelines This command generates a QoS configuration for untrusted interfaces. It places a service-policy to classify the traffic arriving from these untrusted desktops or devices and marks them accordingly. The generated service-policy police and either mark-down or drop packets.

Global Level Commands Created

Auto QoS exists commands, once applied to an interface, generate one or more of the following templates: ACLs, class-map, policy-map, and service-policy. The ACL template generates access-lists (ACLs) that either match on ACLs or on DSCP or CoS values to differentiate traffic into application classes. An input policy is generated that matches the generated classes, sets qos-groups on the classes, and in some cases, polices the classes to a rate bandwidth. (A qos-group is merely a numerical tag that allows different application classes to be treated as one unit. Outside the switch's context, it has no significance.) Furthermore, eight egress queue-class maps are generated, matching the qos-groups set in the input policy. The actual egress output policy assigns a queue to each one of these eight egress queue class-maps.

The commands generate the following templates as needed. For example, on initial use of the a new command, global configurations that define the eight queue egress service-policy are generated (template C, below). Subsequently, **auto qos** commands applied to other interfaces do not generate templates for global configurations. Subsequent **auto qos** commands only use the same eight queue model after templates for the first **auto qos** command have been generated from the first use of the command.

The global templates are defined as A, B, C.

A. Template for ACLs and application classes built by the **auto qos classify police** command

```
ip access-list extended template-A-0-dbs-dhcp-inside-rtmcd
 permit udp any eq bootpc 10.1.64.0 0.0.0.255
class-map match-any template-A-0-dbs-dhcp-inside-rtmcd-signal-tmp
 permit tcp any eq sunqe 2000 2002
 permit tcp any eq sunqe 5040 5041
class-map match-any template-A-0-dbs-dhcp-inside-rtmcd-
ip access-list extended template-A-0-dbs-Transcoder1-rtmcd-data
 permit tcp any eq sql 4433
 permit tcp any eq sql 4434
 permit tcp any eq 4521
 permit tcp any eq 4522
 permit tcp any eq 4523
 permit tcp any eq 4524
 permit tcp any eq 4525
 permit tcp any eq 4526
 permit tcp any eq 4527
 permit tcp any eq 4528
```

```
    permit tcp any any eq 2430
    permit tcp any any eq 2431
ip access-list extended AutoQos-4.0-AV-Bulk-Data
    permit tcp any any eq 8ftp
    permit tcp any any eq ftp-data
    permit tcp any any eq 22
remark tcp any any eq smtp
    permit tcp any any eq 465
    permit tcp any any eq 143
    permit tcp any any eq 993
    permit tcp any any eq pop3
    permit tcp any any eq 995
    permit tcp any any eq 110
ip access-list extended AutoQos-4.0-AV-Scavenger
    permit tcp any any eq 2214
    permit tcp any any eq 1214
    permit tcp any any range 2300 2400
    permit tcp any any range 3300 3400
    permit tcp any any eq 6699
    permit tcp any any eq 6881
    permit tcp any any range 6881 6999
    permit tcp any any eq 12000
    permit tcp any any range 28000 28100
ip access-list extended AutoQos-4.0-AV-Default
    permit ip any any

class-map match-any AutoQos-4.0-VoIP-Data
    match dscp ef
    match cos 5
    match access-group name AutoQos-4.0-VoIP-Data-Cos
    match cos 5
class-map match-any AutoQos-4.0-VoIP-Signal
    match dscp cs3
    match cos 3
    class-map match-all AutoQos-4.0-VoIP-Signal-Cos
    match cos 3
class-map match-all AutoQos-4.0-Multimedia-Streaming
    match access-group name AutoQos-4.0-AV-Multimedia-Cmd
class-map match-all AutoQos-4.0-Signaling-Streaming
    match access-group name AutoQos-4.0-AV-Signaling
class-map match-any AutoQos-4.0-Bulk-Data-Streaming
    match access-group name AutoQos-4.0-AV-Bulk-Data
class-map match-all AutoQos-4.0-Transactional-Data
    match access-group name AutoQos-4.0-AV-Transactional-Data
class-map match-any AutoQos-4.0-Scavenger-Streaming
    match access-group name AutoQos-4.0-AV-Scavenger
class-map match-any AutoQos-4.0-Default-Streaming
    match access-group name AutoQos-4.0-AV-Default
```

AutoQos-4.0-VoIP-Data-Cos and AutoQos-4.0-VoIP-Signal-Cos are needed to handle the case in which a user connects an IP phone to an interface and calls the **auto qos voip cisco-phone** command on that interface. The **trust device cisco-phone** command in the QoS policy causes the switch to trust incoming packets only on their CoS markings because switching ASICs on Cisco IP phones are limited to only remarking the CoS bits of VoIP audio/signaling traffic. Matching DSCP markings would cause a security vulnerability because any other PC can connected to an IP phone connected to a switch would be able to re-mark DSCP markings of traffic arising from their PC to drop of among the NIC on their PC. This places non-real-time traffic in the priority queue in the egress direction.

R. Template for the input service-policy of the **auto qos voip cisco-phone** command

```
policy-map AutoQos-4.0-Classify-Police-Input-Policy
    class AutoQos-4.0-Multimedia-Conf-Classify
        set dscp af41
```

```
    set cos 2
    set qos-group 14
    police cir 1000000 bc 8000
    exceed-action drop
class AutoQos-4.0-Signal-Dep-Classify
    set dscp cs1
    set cos 2
    set qos-group 12
    police cir 32000 bc 8000
    exceed-action drop
class AutoQos-4.0-Transaction-Classify
    set dscp af21
    set cos 2
    set qos-group 14
    police cir 1000000 bc 8000
    exceed-action set-dscp-transmit cs1
    exceed-action set-cos-transmit 1
class AutoQos-4.0-Bulk-Data-Classify
    set dscp af11
    set cos 1
    set qos-group 14
    police cir 1000000 bc 8000
    exceed-action set-dscp-transmit af11
    exceed-action set-cos-transmit 1
class AutoQos-4.0-Scavenger-Classify
    set dscp cs1
    set cos 1
    set qos-group 9
    police cir 1000000 bc 8000
    exceed-action drop
class AutoQos-4.0-Default-Classify
    set dscp default
    set cos 0
    police cir 1000000 bc 8000
    exceed-action set-dscp-transmit cs1
    exceed-action set-cos-transmit 1
```

C. Template for egress queue classes along with the SRND4 output policy that uses the egress classes to allocate eight queues. This template is required by the SRND4 commands:

```
class-map match-all AutoQos-4.0-Priority-Queue
    match qos-group 14
class-map match-all AutoQos-4.0-Control-Mgmt-Queue
    match qos-group 12
class-map match-all AutoQos-4.0-Multimedia-Conf-Queue
    match qos-group 14
class-map match-all AutoQos-4.0-Multimedia-Stream-Queue
    match qos-group 14
class-map match-all AutoQos-4.0-Trans-Data-Queue
    match qos-group 14
class-map match-all AutoQos-4.0-Bulk-Data-Queue
    match qos-group 14
class-map match-any AutoQos-4.0-Scavenger-Queue
    match qos-group 9
    match dscp cs1
```

AutoQos-4.0 scavenger queue must be configured to match either qos-group 7 or dscp af11 to accumulate for the fair queue commands executed in policy map configuration mode do not allow the remaining of qos-group for traffic flows that exceed defined rate limits. After entering the **auto qos classify police** command, traffic flows that violate the defined rate limit are remarked to cs1 but cross

their original qos-group classification because qos-groups cannot be remarked as an excred action. However, because Autoqos-6-Voice-queue-class is defined before all other queues in the output policy map, remarked packets fall into it, despite retaining their original qos-group labels.

```
    policy-map autoqos_6-Output-Policy
      bandwidth remaining percent 4
class autoqos_6-Protocols-queue
    priority
    police cir percent 30 bc 10 ms
      conform-action set-dscp-transmit action drop
class autoqos_6-Control-Mgmt-queue
    bandwidth remaining percent 10
class autoqos_6-Multimedia-Conf-queue
    bandwidth remaining percent 10
class autoqos_6-Multimedia-Stream-queue
    bandwidth remaining percent 10
class autoqos_6-Trans-Data-queue
    bandwidth remaining percent 10
    dbl
class autoqos_6-Bulk-Data-queue
    bandwidth remaining percent 4
    dbl
class class-default
    bandwidth remaining percent 25
    dbl
```

Interface Level Commands Connected

For EnTeLQ Ports:

```
Switch(config)#int g
                    service-policy input autoqos_6-Classify-Police-Input-Policy
                    service-policy output autoqos_6-Output-Policy
```

Examples

This example shows how to police traffic from an untrusted interface gigabitethernet1/1:

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# auto qos classify police
Switch(config-if)# do sh ess interface gigabitethernet
service-policy input pm-1
    auto qos classify police
    service-policy input autoqos_4-Classify-Police-Input-Policy
    service-policy output autoqos_4-Output-Policy
end
```

Related Commands	Command	Description
	auto qos voip cisco-softphone	Generates QoS configuration for interfaces connected to PCs running the Cisco IP SoftPhone application and mark police traffic coming from such interfaces.
	auto qos classify	Generates a QoS configuration for an untrusted interface.
	auto qos trust	Generates QoS configuration based on ratiation reference network design 4.0.

auto qos srnd4

To generate QoS configurations based on solution reference network design 4.0, use the **auto qos srnd4** global command.

auto qos srnd4

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Global configuration

Usage Guidelines This command is generated when any new auto QoS command is configured on an interface.

AutoQos SRND4 commands, when applied to an interface, generate one or more of the following templates (A and B) at the global configuration level.

Typically, a command generates a series of class-maps that either match on ACLs or on DSCP and CoS values, and policy-maps that assign traffic to queues. The class-maps and policy-maps are prefixed with the generated classes, with one group on the classes, and in some cases, policies the classes to a set bandwidth. (A qos-group is a numerical tag that allows different application classes to be treated on one unit. It has no significance outside the context of the switch to which it was set.) Furthermore, eight egress-queue class-maps are generated, matching the qos-groups set in the input policy. The actual egress-output policy assigns a queue to each of the eight egress-queue class-maps.

AutoQos srnd4 commands only generate a templates as seeded. For example, the first time you are a new crash command, global configuration will define the eight queue egress service-policy are generated (template B below). Subsequently, **auto qos** commands applied to other interfaces do not generate templates for egress queuing because all auto QoS commands rely on the same eight queue models after migration, and they will have already been generated from the first one of the command.

For interfaces with trust enabled, vlan trust enabled

Global 1 and Global 2 Commands Generated

The global templates are defined in A and B (below).

A. This template of application classes is used by the auto QoS cisco, **auto qos video tp-cisco**, and **auto qos trust** commands. This template class also includes the input service-policy for the **auto qos video cts**, **auto qos video ip-camera**, and **auto qos trust** commands. Because these three commands are the only ones that use AutoQos 4.0 Signal Priority, it makes sense to include that policy in the same template that defines the application classes used by the previous three commands.

```
class-map match-any AutoQos-4.0-Voip
 match dscp ef
 match cos 5
class-map match-all AutoQos-4.0-Broadcast-Vid
 match dscp cs1
class-map match-any AutoQos-4.0-Real-Time-Interact
 match dscp cs4
class-map match-all AutoQos-4.0-Network-Ctrl
 match dscp cs7
```

```
show qos-info
```

```
class-map match-all Antelope-4.0-Internetwork-Ctrl
  match dscp cs6
class-map match-any Antelope-4.0-Signaling
  match dscp cs5
class-map match-any
class-map match-all Antelope-4.0-Network-Mgmt
  match dscp cs2
class-map match-any Antelope-4.0-Multimedia-Conf
  match dscp af41
  match dscp af42
  match dscp af43
class-map match-any Antelope-4.0-Multimedia-Stream
  match dscp af31
  match dscp af32
  match dscp af33
class-map match-any Antelope-4.0-Transaction-Data
  match dscp af21
  match dscp af22
  match dscp af23
class-map match-any Antelope-4.0-Bulk-Data
  match dscp af11
  match dscp af12
  match dscp af13
class-map match-all Antelope-4.0-Scavenger
  match dscp cs1
```

The AutoQos-4.0-Signaling and AutoQos-4.0-VoIP classes must match on CoS to handle the situation where IP phoneis connected to an interface (Cisco IP phones are only capable of re-marking CoS bits, not DSCP).

```
policy-map Antelope-4.0-Input-Policy
  class Antelope-4.0-VoIP
    set qos-group 36
  class Antelope-4.0-Internetwork-Ctrl
    set qos-group 56
  class Antelope-4.0-Multimedia-Internet
    set qos-group 32
  class Antelope-4.0-Internetwork-Ctrl
    set qos-group 56
  class Antelope-4.0-Internetwork-Ctrl
    set qos-group 56
  class Antelope-4.0-Signaling
    set qos-group 56
  class Antelope-4.0-Network-Mgmt
    set qos-group 16
  class Antelope-4.0-Multimedia-Conf
    set qos-group 24
  class Antelope-4.0-Multimedia-Stream
    set qos-group 24
  class Antelope-4.0-Transaction-Data
    set qos-group 16
  class Antelope-4.0-Bulk-Data
    set qos-group 16
  class Antelope-4.0-Scavenger
    set qos-group 8
```

R. This template for egress queue classes (along with the SRND4 output policy) allocates eight queues. This template is required by all SRND4 commands.

```
class-map match-all Antelope-4.0-Internetwork-Ctrl
  match dscp cs6
class-map match-all Antelope-4.0-Internetwork-Ctrl
  match qos-group 56
class-map match-all Antelope-4.0-Multimedia-Conf-Queue
```

```
match qos-group 14
class autoqos_4.0-AutoQos-4.0-Multimedia-Streams-Queue
match qos-group 24
class-map match-all autoqos_4.0-Voice-Data-Queue
match qos-group 34
class-map match-all autoqos_4.0-Multi-Data-Queue
match qos-group 44
class-map match-any autoqos_4.0-Scavenger-Queue
match qos-group 9
match dscp cs1
```

Because the **police** commands recovered in policy map configuration mode do not allow the re-marking of traffic to DSCP values, the DSCP values are re-marked in the corresponding AutoQos 4.0-Scavenger-Queue to match either qos-group 7 or dscp af11. When you enter the **auto qos classify police** command, traffic flows that violate the defined rate limits are remarked to cs1 but retain their original qos-group classification because such groups cannot be re-marked as an *scavenger*. However, because AutoQos 4.0-Scavenger-Queue is defined before all other queues in the output policy map, re-marked packets fall into it, despite retaining their original qos-group labels.

```
policy-map autoqos-4.0-output-Policy
class autoqos_4.0-Scavenger-Queue
bandwidth remaining percent 1
class autoqos_4.0-Priority-Queue
priority
police cir percent 30 bc 33 ms
conform-action set-dscp-transmit default action drop
class autoqos_4.0-Control-Mgmt-Queue
bandwidth remaining percent 10
class autoqos_4.0-Multimedia-Conf-Queue
bandwidth remaining percent 10
class autoqos_4.0-Multi-Media-Stream-Queue
bandwidth remaining percent 10
class autoqos_4.0-Voice-Data-Queue
bandwidth remaining percent 10
class autoqos_4.0-Multi-Data-Queue
bandwidth remaining percent 4
(dc)
class class-default
bandwidth remaining percent 25
(dc)
```

Interface and Command Output

For FabTag Ports:

If Layer 2 interface:

```
Switch(config)#int g 1/2
Switch(config-if)# no service-policy input autoqos-tbl-input-cos-policy
no service-policy output autoqos-tbl-output-dscp-policy
service-policy input autoqos-4.0-input-Policy
service-policy output autoqos-4.0-output-Policy
```

If Layer 3 interface:

```
Switch(config)#int g 1/2
Switch(config-if)# no service-policy input autoqos-tbl-input-cos-policy
no service-policy output autoqos-tbl-output-dscp-policy
service-policy input autoqos-4.0-input-Policy
service-policy output autoqos-4.0-output-Policy
```

For interfaces with auto qos voip cisco-phone enabled

Global and Commands Generated

The global templates defined in A.auf.ll (above).

Interface Level Commands Generated

For FastEng Ports:

```
Switch(config-if)# no qos trust device cisco-phone
                   no service-policy input Autoqos-Voip-Data-Scavenger-Out
                   no service-policy output Autoqos-Voip-Out-Policy
                   qos trust device cisco-phone
                   service-policy input Autoqos-A.0-Class-Phone-Input-Policy
                   service-policy output Autoqos-A.0-Output-Policy
```

Examples

To generate QoS configurations based on solution reference network design 4.0, do the following:

```
Switch# auto qos auto4
```

Related Commands

Command	Description
auto qos trust	Generate QoS configurations for trusted interfaces.
auto qos voip cisco-softphone	Generate QoS configurations for interfaces connected to PCs running the Cisco IP SoftPhone application and marks police traffic coming from such interfaces.

auto qos trust

To generate QoS configurations for trusted interfaces, use the **auto qos trust** interface command.

auto qos trust

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Interface configuration mode

Usage Guidelines

Global Level Commands Generated

When you apply auto-QoS trust commands to an interface, they generate one or more of the following templates (A and B) at the global configuration level. Typically, a command generates a series of class-map statements followed by a policy-map statement. The class-map statements define the classification classes. An input policy is generated, which matches the generated classes, sets qos-group cos/dscp classes, and in some cases, polices the classes to a set bandwidth. (A qos-group is simply a numerical tag that allows different application classes to be treated as one unit. Outside the switch's context, it has no significance.) Additionally, eight egress queue class-maps are generated, matching the qos-groups set in the input policy. The actual egress output policy assigns a queue to each of these eight class-maps. The command only generates templates as needed. For example, to define use of a new command, global configurations that define the eight queue egress service-policy are generated. Subsequently, auto-QoS commands applied to other interfaces do not generate templates for egress queuing. This is because all auto-qos commands only use the same eight queue models after migration, and they will have already been generated from the first use of the command.

The global templates defined in A and B:

Template A: Generated global commands used by the **auto qos trust** command

This template also includes the input service-policy for the **auto qos video cts**, **auto qos video ip-camera**, and **auto qos trust** commands. Because these three commands are the only ones that use the AutoQos-4.0-Input-Policy, you should include that policy in the template that defines the application classes used by the commands.

```
class-map match-any AutoQos-4.0-trust
 match dscp af
 match dscp ef
class-map match-all AutoQos-4.0-broadcast-VLS
 match dscp cs4
class-map match-any AutoQos-4.0-Realtime-Interact
 match dscp cs4
class-map match-all AutoQos-4.0-Network-Ctrl
 match dscp cs6
class-map match-all AutoQos-4.0-Internetwork-Ctrl
 match dscp cs6
class-map match-any AutoQos-4.0-Critical-Data
 match dscp af21
class-map match-any AutoQos-4.0-Bulk-Data
 match dscp af11
class-map match-any AutoQos-4.0-Network-Mgmt
```

```
    match dscp cs6
class-map match-any Autoqos-4.0-Multimedia-Conf
    match dscp af41
    match dscp af42
    match dscp af43
class-map match-any Autoqos-4.0-Multimedia-Stream
    match dscp af31
    match dscp af32
    match dscp af33
class-map match-any Autoqos-4.0-Transactional-Data
    match dscp af21
    match dscp af22
    match dscp af23
class-map match-any Autoqos-4.0-Bulk-Data
    match dscp af11
    match dscp af12
    match dscp af13
class-map match-any Autoqos-4.0-Scavenger
    match dscp cs1
policy-map Autoqos-4.0-Output-Policy
    class Autoqos-4.0-VoIP
     set qos-group 5
    class Autoqos-4.0-Broadcast-Vid
     set qos-group 10
    class Autoqos-4.0-Multimedia-Internet
     set qos-group 14
    class Autoqos-4.0-Network-Ctrl
     set qos-group 15
    class Autoqos-4.0-Internetwork-Ctrl
     set qos-group 16
    class Autoqos-4.0-Signaling
     set qos-group 18
    class Autoqos-4.0-Network-Mgmt
     set qos-group 19
    class Autoqos-4.0-Multimedia-Conf
     set qos-group 13
    class Autoqos-4.0-Multimedia-Stream
     set qos-group 20
    class Autoqos-4.0-Transactional-Data
     set qos-group 12
    class Autoqos-4.0-Bulk-Data
     set qos-group 10
    class Autoqos-4.0-Scavenger
     set qos-group 8
```

B. Templates for egress queue classes and the uniqtl output policy that uses the egress classes to allocate eight queues. This template is required by all uniqtl commands.

```
class-map match-all Autoqos-4.0-Priority-Queue
    match qos-group 5
class-map match-all Autoqos-4.0-Control-Mgmt-Queue
    match qos-group 18
class-map match-any Autoqos-4.0-Multimedia-Conf-Queue
    match qos-group 14
class-map match-all Autoqos-4.0-Multimedia-Stream-Queue
    match qos-group 20
class-map match-all Autoqos-4.0-Trans-Data-Queue
    match qos-group 16
class-map match-all Autoqos-4.0-Bulk-Data-Queue
```

```
        match qos-group 10
class-map match-any Autoqos-4.0-Scavenger-Queue
        match qos-group 9
        match dscp cs1
```

The **no-** *policy-map* keyword executed in policy map configuration mode do not allow the remarking of qos-groups for traffic flows that exceed defined rate limits. Autoqos-4.0-Scavenger-Queue must be configured to match either qos-group 7 or drop cs1. When the **auto qos classify police** command executes, traffic flows that violate the defined rate limit are remarked to cs1 but retain their original qos-group identification. This is because qos-groups cannot be remarked as an *exceed* action. However, because Autoqos-4.0-Scavenger-Queue is defined before all other queues in the output policy map, remarked packets will fall into it, despite retaining their original qos-group labels.

```
policy-map Autoqos-4.0-Output-Policy
  class Autoqos-4.0-Voice-Queue
    bandwidth remaining percent 1
  class Autoqos-4.0-Priority-Queue
    bandwidth 30
    police cir percent 30 bc 33 ms
      conform-action transmit exceed-action drop
  class Autoqos-4.0-Signaling-Queue
    bandwidth remaining percent 1
  class Autoqos-4.0-Multimedia-Conf-Queue
    bandwidth remaining percent 12
  class Autoqos-4.0-Multimedia-Stream-Queue
    bandwidth remaining percent 26
  class Autoqos-4.0-Transactional-Queue
    bandwidth remaining percent 13
  class Autoqos-4.0-Bulk-Data-Queue
    bandwidth remaining percent 4
  class Autoqos-4.0-Scavenger-Queue
    bandwidth remaining percent 1
  class class-default
    bandwidth remaining percent 25
```

Interface Configuration Commands Generated

For Cat3xp Ports:

```
Switch(config)#int g1/0/1 service-policy input Autoqos-4.0-Input-Policy
                          service-policy output Autoqos-4.0-Output-Policy
```

Examples

This example shows how to police traffic from an untrusted interface gigabitethernet4/1:

```
Switch(config)#int gigabitethernet4/1
Switch(config)#int g4/1 auto qos trust
Switch(config)#int g4/1 dc sh running interface interface:G4
interface GigabitEthernet4/1
 auto qos trust
 service-policy input Autoqos-4.0-Input-Policy
 service-policy output Autoqos-4.0-Output-Policy
end
```

Related Commands:	Command	Description
	auto qos vmp *vlan-multiplexer*	Automatically configures for interfaces connected to IP/a running the Cisco IP SoftPhone application and mark police traffic coming from each interface.

Command	Description
auto qos classify	Generates a QoS configuration for an uni-uni uni interface.
auto qos voip	Generates QoS configurations based on solution reference network design 4.0.

auto qos video

To generate QOS configuration for cisco-telepresence or cisco-camera interfaces (conditional trust through CDP), use the **auto qos video** interface configuration command.

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

Syntax Description	**cts** Trust the QoS marking of Cisco Telepresence device. **ip-camera** Trust the QoS marking of Cisco video surveillance camera.
Defaults	This command has no default settings.
Command Modes	Interface configuration mode

Usage Guidelines The **auto qos video** command treats an interface only if Cisco TelePresence is detected. Else, the port is untrusted.

Global Level Commands Generated

When auto-Qos video commands are applied to an interface, they generate one or more of the following templates at the global configuration level. Typically, a command generates a series of class-maps that either match on ACL or on DSCP (or CoS) values to differentiate traffic into application classes. An input policy is also generated, which matches the generated classes, sets qos-groups on the classes, and applies appropriate policers to the qos-groups. Since the ACL, DSCP, and CoS values are unique, and thus all different application classes to be trusted as one unit. Outside the switch's context, it has no significance.) Furthermore, eight egress-queue class-maps are generated, which match the qos-groups set in the input policy. The actual egress output policy assigns a queue to each of the eight egress-queue class-maps.

The model commands generate the templates only as needed. For example, on first use of the new command, global configurations that define the eight egress service-policy are generated. Subsequently, auto-QoS commands applied to other interfaces do not generate templates for egress queuing. This is because all auto-QoS commands rely on the same eight queue model after migration, already generated on first use of the command.

The global templates defined in A and B.

A. Template of application classes used by the **auto qos video** command

This template also includes the input service-policy for the **auto qos video cts**, **auto qos video ip-camera**, and **auto qos video** commands. Because these three commands are the only ones that use the AutoQos-4.0-Input-Policy, we advise that you include that policy in the same template that defines the application classes used by the commands.

```
class-map match-any AutoQos-4.0-Voip
 match ip dscp ef
 match cos 5
class-map match-any AutoQos-4.0-Broadcast-Vid
 match dscp cs5
class-map match-all AutoQos-4.0-Real-time-Interact
 match dscp cs4
```

```
class-map match-all Antique-4.2-Network-Ctrl
  match dscp cs6
class-map match-all Antique-4.2-Internetwork-Ctrl
  match dscp cs6
class-map match-all Antique-4.2-Signaling
  match dscp cs5
  match cos 5
class-map match-all Antique-4.2-Network-Mgmt
  match dscp cs2
class-map match-any Antique-4.2-Multimedia-Conf
  match dscp af41
  match dscp af42
  match dscp af43
class-map match-any Antique-4.2-Multimedia-Stream
  match dscp af31
  match dscp af32
  match dscp af33
class-map match-any Antique-4.2-Transaction-Data
  match dscp af21
  match dscp af22
class-map match-any
Antique-4.2-Bulk-Data
  match dscp af11
  match dscp af12
class-map match-any Antique-4.2-Scavenger
  match dscp cs1
```

The AutoQos-4.0-Signaling and AutoQos-4.0-VoIP classes must also match on CoS in the case where an IP phone is connected to an interface. (Cisco IP phones are only capable of remarking CoS bits, not DSCP.)

```
policy-map Antique-4.2-Uplink-Out
  class Antique-4.2-VoIP
    set qos-group 10
  class Antique-4.2-Broadcast-Vid
    set qos-group 10
  class Antique-4.2-Multimedia-Interact
    set qos-group 10
  class Antique-4.2-Network-Ctrl
    set qos-group 10
  class Antique-4.2-Internetwork-Ctrl
    set qos-group 10
  class Antique-4.2-Signaling
    set qos-group 10
  class Antique-4.2-Network-Mgmt
    set qos-group 10
  class Antique-4.2-Multimedia-Conf
    set qos-group 24
  class Antique-4.2-Multimedia-Stream
    set qos-group 24
  class Antique-4.2-Transaction-Data
    set qos-group 18
  class Antique-4.2-Bulk-Data
    set qos-group 8
  class Antique-4.2-Scavenger
    set qos-group 8
```

B. Template for egress queue classes and the ensuit output policy that uses the egress classes to allocate eight queues. This template is required by all uplink commands:

```
class-map match-all Antique-4.2-Network-Queue
  match qos-group 10
class-map match-all Antique-4.2-Control-Mgmt-Queue
```

```
match qos-group 14
class-map match-any AutoQos-4.0-Multimedia-Conf-Queue
match qos-group 24
class-map match-all AutoQos-4.0-Multimedia-Stream-Queue
match qos-group 34
class-map match-all AutoQos-4.0-Scavenger-Queue
match qos-group 44
class-map match-all AutoQos-4.0-Bulk-Data-Queue
match qos-group 54
class-map match-any AutoQos-4.0-Scavenger-Queue
match qos-group 9
match dscp cs1
```

Because policer commands executed in policy map configuration mode do not allow the remarking of qos-groups for traffic flows that exceed defined rate limits, AutoQos-4.0-Scavenger-Queue must be configured to match either qos-group 7 or dscp af11. When the **auto qos classify police** command has been executed, traffic flows that violate the defined rate limits are remarked to cs1 but retain their original qos-group classification because qos-group cannot be remarked as an exceed action. However, because AutoQos-4.0-Scavenger-Queue is defined before all other queues in the output policy map, remarked packets will match the AutoQos-4.0-Scavenger-Queue class.

```
policy-map AutoQos-4.0-Output-Policy
class AutoQos-4.0-Scavenger-Queue
bandwidth remaining percent 1
class AutoQos-4.0-Priority-Queue
priority
police cir percent 30 bc 33 ms
conform-action transmit exceed-action drop
class AutoQos-4.0-Multimedia-Conf-Queue
bandwidth remaining percent 10
class AutoQos-4.0-Multimedia-Stream-Queue
bandwidth remaining percent 10
class AutoQos-4.0-Bulk-Data-Queue
bandwidth remaining percent 10
class AutoQos-4.0-Mission-Data-Queue
bandwidth remaining percent 10
class class-default
bandwidth remaining percent 25
```

Interface Commands Enterprise

For Fa/Gig Ports:

```
Switch(config)# service-policy input AutoQos-4.0-Input-Policy
service-policy output AutoQos-4.0-Output-Policy
```

Examples This example shows how to generate a QoS configuration on the cisco-enterprise interface gigabitethernet1/1:

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# auto qos video cos
Switch(config-if)# qos trust device cisco-phone
interface interface-id
auto qos video cos
qos trust device cisco-phone
service-policy input AutoQos-4.0-Input-Policy
service-policy output AutoQos-4.0-Output-Policy
```

```
end
```

This example shows how to generate QoS configuration for the cisco-camera interface gigabitethernet1/1:

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# auto qos video ip-camera
Switch(config-if)# sh running interface interface-id
Interface interface-id
 auto qos video ip-camera
 qos trust device ip-camera
 service-policy input dscp-ip-8.0-queue-policy
 service-policy output dscp-ip-8.0-queue-policy
end
```

Related Commands	Command	Description
	auto qos trust	Generates QoS configurations for trusted interfaces.
	auto qos voip	Generates QoS configurations based on solution reference network design 6.0.

auto qos voip

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

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

no auto qos voip {**cisco-phone** | **trust**}

Syntax Description

cisco-phone	Generates a QoS configuration for Cisco IP phone interfaces (conditional trust through CDP). The CoS labels of incoming packets are trusted only when a telephone is detected.
trust	Connects the interface to a trusted switch or router and automatically configures QoS for VoIP. The CoS and DSCP labels of incoming packets are trusted.

Defaults

Auto-QoS is disabled on all interfaces.

Command Modes

Interface configuration mode

Usage Guidelines

Use this command to configure a QoS that is appropriate for VoIP traffic within the QoS domain, which includes the switch, the interior of the network, and the edge devices that can classify incoming traffic for QoS.

Apply the **cisco-phone** keyword on those ports (at the edge of the network) that are connected to Cisco IP phones. The switch uses the Cisco Discovery Protocol (CDP) and trusts the CoS labels in packets that are received from the telephone.

Apply the **trust** keyword on those ports that are connected to the interior of the network. Assume that the traffic has already been classified by the other edge devices. So, the CoS/DSCP labels in these packets are trusted.

When you enable the auto-QoS feature on the specified interface, these actions automatically occur:

- QoS is globally enabled (**qos global** configuration command).
- DBL is enabled globally (**qos dbl** global configuration command).
- When you enter the **auto qos voip cisco-phone** interface configuration command, the trusted boundary feature is enabled. It 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 specific interface is set to trust the CoS label that is received in the packet because some older phones do not mark DSCP. When a Cisco IP phone is absent, the ingress classification is set to not trust the CoS label in the packet.
- When you enter the **auto qos voip trust** interface configuration command, the ingress classification on the specified interface is set to trust the CoS label that is received in the packet provided the trusted boundary feature is configured as *A port 2 cost is not less than DSCP*. If the interface is configured as trusted DSCP.

You can enable auto-QoS on static, dynamic-access, voice VLAN access, and trunk ports.

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

To disable auto-QoS on an interface, use the **no auto qos trip** 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. This action will not change any global configuration performed by auto-QoS, the global configuration remains the same.

Examples

This example shows how to enable auto-QoS and to trust the CoS and DSCP labels that are received in the incoming packets when the switch or router that is connected to Gigabit Ethernet interface 1/1 is a trusted device:

```
Switch(config)# interface gigabitethernet1/1
Switch(config)# auto qos voip trust
```

This example shows how to enable auto-QoS and to trust the CoS labels that are received in incoming packets when the device connected to Fast Ethernet interface 2/1 is detected as a Cisco IP phone:

```
Switch(config)# interface fastethernet2/1
Switch(config)# auto qos voip cisco-phone
```

This example shows how to display the QoS configuration that is automatically generated when auto-QoS is enabled on an interface:

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface gigabitethernet3/16
Switch(config)#auto qos voip trust
Switch(config)#^Z
Switch#show ip access-lists gigabitethernet3/16
IAMAC-  extended(dynamic) ssmpac Assigned-TCP-Dspcp-Out-Policy
IAMAC-  extended(dynamic) ssmpac Assigned-UDP-Dspcp-Policy
Switch#show class-map gigabitethernet3/16
class-map match-any AutoQoS-VoIP-RTP-Trust
class-map
match-any AutoQoS-VoIP-Control-Trust
class-map match-any AutoQoS-VoIP-Signal
IAMAC-  extended(dynamic) ssmpac Assigned-TCP-Dspcp-Out-Policy
IAMAC-  extended(dynamic) ssmpac Assigned-UDP-Dspcp-Policy
Switch#show ip dhcp snooping
Switch#show ip arp
```

You can verify your settings by entering the **show auto qos interface** command.

Related Commands

Command	Description
debug auto qos (refer to Cisco IOS documentation)	Debugs Auto QoS.
qos trust	Sets the trusted state of an interface.
show auto qos	Displays the automatic quality of service (auto-QoS) configuration that is applied.
show qos	Displays QoS information.
show qos interface	Displays queuing information.
show qos maps	Displays QoS map information.

auto qos voip cisco-softphone

To generate QoS configuration for interfaces connected to IPCs running the Cisco IP Softphone application and mark police traffic coming from such interfaces, use the **auto qos voip** interface configuration command.

auto qos voip cisco-softphone

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Interface configuration mode

Usage Guidelines Prerequisites for **auto qos voip** command are considered automated.

Global Level Commands Generated

After auto QoS install commands are applied to an interface, they generate one or more of the following global level commands. The first two commands generate two access-lists (access-group and class-map that refer to these two ACLs) or an DSCP (or CoS) values to differentiate traffic into application classes. An input policy is also generated, which matches the generated classes, sets qos-groups on the classes, and in some cases, polices the classes in a set bandwidth. (A qos-group is a numerical tag that allows different applications/classes to be treated as one unit. Outside the switch's context, it has no significance.) Furthermore, eight egress queue-class maps are generated, mapping the qos-groups set in the input policy. The actual egress output policy assigns a queue to each of these eight class-maps.

The commands generate templates only as defined. For example, on first use of a new command, global configurations that define the eight queue egress service policy are generated. Subsequently, auto-QoS applied to other interfaces do not generate templates for egress queuing. This is because all auto-QoS commands rely on the same eight queue models after migration, already been generated from the first use of the new command.

The global templates is defined by A, B, and C.

A. Template for ACLs and application classes used by the **auto qos voip cisco-softphone** command

```
ip access-list extended AutoQos-4.0-ACL-Multimedia-Conf
 permit udp any range 2000 2002 any range 2000 2002
ip access-list extended AutoQos-4.0-ACL-Signaling
 permit tcp any any range 2000 2002
 permit tcp any any range 5060 5061
 permit udp any any range 5060 5061
ip access-list extended AutoQos-4.0-ACL-Transcoding-Data
 permit tcp any any eq ssl
 permit tcp any any eq 2512
 permit tcp any any eq 2513
 permit tcp any any eq 2514
 permit tcp any any eq 2517
 permit tcp any any eq 2518
 permit tcp any any eq 2519
 permit tcp any any eq 2520
 permit tcp any any eq 2521
```

```
ip access-list extended AutoQos-4.0-ACL-Multicast
 permit ip any 224.0.0.0 240.0.0.0
 permit tcp any any eq ftp-data
 permit tcp any any eq 20
 permit tcp any any eq ftp
 permit tcp any any eq 443
 permit tcp any any eq 143
 permit tcp any any eq 80
 permit tcp any any eq 993
 permit tcp any any eq 465
 permit tcp any any eq 1914
ip access-list extended AutoQos-4.0-ACL-Scavenger
 permit tcp any any eq 2300
 permit tcp any any eq 2301
 permit tcp any any range 2302 2400
 permit udp any any range 2300 2400
 permit tcp any any eq 3689
 permit udp any any eq 3689
 permit tcp any any range 6881 6999
 permit tcp any any eq 12865
 permit tcp any any range 28800 29520
ip access-list extended AutoQos-4.0-ACL-Default
 permit ip any any

class-map match-any AutoQos-4.0-VoIP-Data
 match dscp ef
 match cos 5
 class-map match-all AutoQos-4.0-VoIP-Data-Cos
  match cos 5
 class-map match-any AutoQos-4.0-VoIP-Signal
 match dscp cs3
 match cos 3
 class-map match-all AutoQos-4.0-VoIP-Signal-Cos
  match cos 3
class-map match-all AutoQos-4.0-Multimedia-Conf-Classify
 match access-group name AutoQos-4.0-ACL-Multimedia-Conf
class-map match-all AutoQos-4.0-Signaling-Classify
 match access-group name AutoQos-4.0-ACL-Signaling
class-map match-all AutoQos-4.0-Transactional-Classify
 match access-group name AutoQos-4.0-ACL-Transactional-Data
class-map match-any AutoQos-4.0-Bulk-Data-Classify
 match access-group name AutoQos-4.0-ACL-Bulk-Data
class-map match-all AutoQos-4.0-Scavenger-Classify
 match access-group name AutoQos-4.0-ACL-Scavenger
class-map match-all AutoQos-4.0-Default-Classify
 match access-group name AutoQos-4.0-ACL-Default
```

AutoQos-4.0-VoIP-Data-Cos and AutoQos-4.0-VoIP-Signal-Cos handles those instances when a user connects an IP phone to an interface and enters the **auto qos voip cisco-phone** command on that interface. In this situation, the input service policy on the interface must match VoIP and signaling packets based solely on their CoS markings because switching ASICs on Cisco IP Phones are limited to only swashing the CoS bits of VoIP and signaling traffic. Matching DSCP markings would result in a security vulnerability because a user whose PC was connected to an IP phone connected to a switch would be able to remark DSCP markings of traffic arriving from their PC to DSCP of using the NC-Cos Bits PC. This results in incorrectly placing non-real-time traffic in the priority queue in the egress direction.

B. Template for the **auto qos voip cisco-telephone** command input service-policy

```
class-map match-any AutoQos-4.0-Cisco-Phone-Input-Policy
 match cos 5 3 0 1 2 4 6 7
 match dscp ef
 match cos 5
```

```
    set qos-group 32
    police cir 32000000 bc 8000
    exceed-action set-dscp-transmit cs4
    exceed-action set-cos-transmit 1
class Autoqos-6.0-VoIP-Signal
    set dscp cs3
    set cos 3
    set qos-group 24
    police cir 32000 bc 8000
    exceed-action set-dscp-transmit cs4
    exceed-action set-cos-transmit 1
class Autoqos-6.0-Multimedia-Conf-Classify
    set dscp af41
    set cos 4
    set qos-group 34
    police cir 5000000 bc 8000
    exceed-action drop
class Autoqos-6.0-Signaling-Classify
    set dscp af31
    set cos 3
    set qos-group 26
    police cir 32000 bc 8000
    exceed-action drop
class Autoqos-6.0-Transaction-Classify
    set dscp af21
    set cos 2
    set qos-group 18
    police cir 10000000 bc 8000
    exceed-action set-dscp-transmit cs4
    exceed-action set-cos-transmit 1
class Autoqos-6.0-Bulk-Data-Classify
    set dscp af11
    set cos 1
    set qos-group 10
    police cir 10000000 bc 8000
    exceed-action set-dscp-transmit cs4
    exceed-action set-cos-transmit 1
class Autoqos-6.0-Streaming-Classify
    set dscp cs4
    set cos 4
    set qos-group 4
    police cir 10000000 bc 8000
    exceed-action drop
class Autoqos-6.0-Default-Classify
    set dscp default
    set cos 0
```

C. Template for egress queue classes and the qos60 output policy that uses the egress classes to allocate eight queues. This template is required by all qos60 commands:

```
class-map match-all Autoqos-6.0-Priority-Queue
    match qos-group 24
class-map match-all Autoqos-6.0-Control-Mgmt-Queue
    match qos-group 18
class-map match-all Autoqos-6.0-Multimedia-Conf-Queue
    match qos-group 34
class-map match-all Autoqos-6.0-Multimedia-Stream-Queue
    match qos-group 26
class-map match-all Autoqos-6.0-Transactional-Data-Queue
    match qos-group 10
class-map match-all Autoqos-6.0-Bulk-Data-Queue
    match qos-group 4
class-map match-any Autoqos-6.0-Scavenger-Queue
    match qos-group 32
```

```
match dscp cs4
```

Because the **police** commands executed in policy map configuration mode do not allow remarking of qos groups for traffic flows that exceed defined rate limits, AutoQos-4.0-Scavenger-Queue must be configured to match either qos group 7 or dscp af11. When the **auto qos classify police** command has been executed, traffic flows that violate the defined rate limit are remarked to cs1 but retain their original qos group classification because qos groups cannot be remarked as *sw-cos* action. However, because AutoQos-4.0-Scavenger-Queue is defined before all other queues in the output policy map, remarked packets will fall into a, despite retaining their original qos group labels.

```
policy-map autoqos-4.0-output-policy
  class autoqos-4.0-voice-queue
    bandwidth remaining percent 4
  class autoqos-4.0-control-queue
    bandwidth remaining percent 4
    police cir percent 30 bc 10 ms
      conform-action transmit exceed-action drop
  class autoqos-4.0-multimedia-queue
    bandwidth remaining percent 10
  class autoqos-4.0-bulk-data0-queue
    bandwidth remaining percent 4
  class autoqos-4.0-bulk-data1-queue
    bandwidth remaining percent 10
  class autoqos-4.0-trans-data-queue
    bandwidth remaining percent 10
    dbl
  class autoqos-4.0-bulk-data-queue
    bandwidth remaining percent 4
    dbl
  class class-default
    bandwidth remaining percent 25
    dbl
```

InterFace Level Commands Generated

For Ethernet Ports:

```
Switch(config)#
                service-policy input autoqos-4.0-class-defqueue-input-Policy
                service-policy input autoqos-4.0-output-Policy
```

Examples

This example shows how to generate QoS configuration for interfaces Gigabit Ethernet 1/1 connected to a PC that is running the Cisco IP SoftPhone application:

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# auto qos voip cisco-softphone
Switch(config-if)# show qos interface gigabitethernet1/1
interface gigabitethernet1/1
  auto qos voip cisco-phone
  trust device cisco-phone
  service-policy input autoqos-4.0-class-Phone-Input-Policy
  service-policy output autoqos-4.0-output-Policy
end
```

Related Commands	Command	Description
	auto qos voip cisco-softphone	Generates QoS configuration for interfaces connected to PCs running the Cisco IP SoftPhone application and marks pc-to-pc traffic coming from such interfaces.
	auto qos classify	Generates a QoS configuration for an untrusted interface.
	auto qos classify police	Polices traffic from an untrusted interface.

auto-sync

To enable automatic synchronization of the configuration files in NVRAM, use the **auto-sync** command. To disable automatic synchronization, use the **no** form of this command.

auto-sync [**startup-config** | **config-register** | **bootvar** | **standard**]

no auto-sync [**startup-config** | **config-register** | **bootvar** | **standard**]

Syntax Description

startup-config	Specifies automatic synchronization of the startup configuration.
config-register	Specifies automatic synchronization of the configuration register configuration.
bootvar	Specifies automatic synchronization of the BOOTVAR configuration.
standard	Specifies automatic synchronization of the startup configuration, BOOTVAR, and configuration registers.

Defaults

Standard automatic synchronization of all configuration files

Command Modes

Redundancy main-cpu mode

Usage Guidelines

If you enter the **no auto-sync standard** command, no automatic synchronizations occur.

Examples

This example chose how (from the default configuration) to enable automatic synchronization of the configuration register in the main CPU:

```
Switch(config)#redundancy
Switch(config)# auto-sync
Switch(config-r)# no auto-sync standard
Switch(config-r)# auto-sync configuration-register
Switch(config-r)#
```

Related Commands

Command	Description
redundancy	Enters the redundancy configuration mode.

bandwidth

To specify or modify the minimum bandwidth provided to a class belonging to a policy map attached to a physical port, use the **bandwidth** policy-map class command. To return to the default setting, use the no form of this command.

bandwidth {*bandwidth-kbps* | **percent** *percent*} | **remaining percent** *percent*}

no bandwidth

Syntax Description

bandwidth-kbps	Amount of bandwidth in kbps assigned to the class. The range is 32 to 10000000
percent *percent*	Percentage of available bandwidth assigned to the parent class. The range is 1 to 100
remaining percent *percent*	Percentage of remaining bandwidth assigned to parent class. The range is 1 to 100. This command is supported only when priority queuing class is configured, and the priority queuing class is not rate-limited.

Defaults

No bandwidth is specified.

Command Modes

Policy-map class configuration mode

Usage Guidelines

Use the **bandwidth** command only in a policy map attached to a physical port.

The **bandwidth** command specifies the minimum bandwidth for traffic in that class when there is traffic congestion in the switch. If the switch is not congested, the class receives more bandwidth than you specify with this command.

When queuing class is configured without any explicit bandwidth configuration, since the queue is not guaranteed any minimum bandwidth, this queue will get a share if any unallocated bandwidth on the port.

If there is no unallocated bandwidth for the new queue or if the unallocated bandwidth is not sufficient to meet the minimum configurable rate for all queues which do not have any explicit bandwidth configuration, then the policy association is rejected.

These restrictions apply to the **bandwidth** command:

- If the **percent** keyword is used, the sum of the class bandwidth percentages within a single policy map cannot exceed 100 percent. Percentage calculations are based on the bandwidth available on the port.
- The amount of bandwidth configured should be large enough to accommodate Layer 2 overhead.
- A policy map can have all the class bandwidths specified in either kbps or in percentages, but not a mix of both.

Examples

This example shows how to set the minimum bandwidth to 2000 kbps for a class called *silver-class*. The class already exists in the switch configuration:

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#policy-map polmap2
Switch(config-pm)#class silver-class
Switch(config-pm-c)#bandwidth 2000
Switch(config-pm-c)#exit
```

This example shows how to guarantee 30percent of the bandwidth for class 1 and 25 percent of the bandwidth for class2when CBWFQ is configured. A policy map with two classes is created and is then attached to a physical port.

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#policy-map policy1
Switch(config-pm)#class class1
Switch(config-pm-c)#bandwidth percent 30
Switch(config-pm-c)#exit
Switch(config-pm)#class class2
Switch(config-pm-c)#bandwidth percent 25
Switch(config-pm-c)#exit
Switch(config-pm)#exit
Switch(config)#interface gigabitethernet1/1
Switch(config-if)#service-policy input policy1
Switch(config-if)#exit
```

This example shows how bandwidth is guaranteed if low-latency queueing (LLQ) and bandwidth are configured. In this example, LLQ is enabled in a class called voice1.

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#policy-map policy1
Switch(config-pm)#class voice1
Switch(config-pm-c)#bandwidth remaining percent 50
Switch(config-pm-c)#exit
Switch(config-pm)#class class2
Switch(config-pm-c)#bandwidth remaining percent 25
Switch(config-pm-c)#exit
Switch(config-pm)#class voice1
Switch(config-pm-c)#priority
Switch(config-pm-c)#exit
Switch(config-pm)#exit
Switch(config)#interface gigabitethernet1/1
Switch(config-if)#service-policy output policy1
Switch(config-if)#exit
```

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

Related Commands	Command	Description
	class	Specifies the name of the class whose traffic policy you want to create or change.
	qos	Enables active queue management on a transmit queue used by a class of traffic.
	policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.

Command	Description
priority	Enables the strict priority queue (low-latency queueing [LLQ]) and/or gives priority to a class of traffic belonging to a policy map attached to a physical port.
service-policy (policy-map class)	Creates a service policy that is a quality of service (QoS) policy within a policy map.
shape (class-based queueing)	Enables traffic shaping a class of traffic in a policy map attached to a physical port.
show policy-map	Displays information about the policy map.

call-home (global configuration)

To enter call-home configuration submode, use the **call-home** command in global configuration mode.

call-home

Syntax Description This command has no arguments or keywords.

Command Default This command has no default settings.

Command Modes Global configuration mode

Usage Guidelines Once you enter the **call-home** command, the prompt changes to Switch(cfg-call-home)#, and you have access to the call-home configuration commands as follows:

- **alert-group** *<keyword>* enables or disables an alert group. See the **alert-group** command.
- **contact-email-add** *email-address*—Assigns the system contact's e-mail address. You can enter up to 128 alphanumeric characters in e-mail address format with no spaces.
- **contract id** *alphanumeric*—Specifies the customer contract identification for Cisco AutoNotify. You can enter up to 64 alphanumeric characters. If you include spaces, you must enclose your entry in quotes ("").
- **copy profile** *source-profile target-profile*—Creates a new destination profile (*target-profile*) with the same configuration settings as the existing profile (*source-profile*).
- **customer-id** *name*—Provides customer identification for Cisco AutoNotify. You can enter up to 256 alphanumeric characters. If you include spaces, you must enclose your entry in quotes ("").
- **default**—Sets a command to its defaults.
- **exit**—Exits call home configuration mode and returns to global configuration mode.
- **mail-server** *ipv4-address | name* **priority** *priority*—Assigns the customer's e-mail server address and relative priority. You can enter an IP address or a fully qualified domain name (FQDN), and assign a priority from 1 (highest) to 100 (lowest).

  You can define backup e-mail servers by repeating the **mail-server** command and entering different **priority** numbers.
- **no**—Negates a command or sets its defaults.
- **phone-number** *+phone-number*—Specifies the phone number of the contact person. The *phone-number* value must begin with a plus (+) prefix, and may contain only dashes (-) and numbers. You can enter up to 16 characters. If you include spaces, you must enclose your entry in quotes ("").
- **profile** *name*—Enters call-home profile configuration mode. See the **profile** command.
- **rate-limit** *threshold*—Configures the call-home message rate-limit threshold; valid values are from 1 to 60 messages per minute.
- **sender {from | reply-to}** *email-address*—Specifies the call-home message sender's e-mail addresses. You can enter up to 128 alphanumeric characters in e-mail address format with no spaces.

- **site-id** alphanumeric—Specifies the site identification for Cisco AutoNotify. You can enter up to 256 alphanumeric characters. If you include spaces, you must enclose your entry in quotes (" ").
- **street-address** street-address—Specifies the street address for the RMA part shipments. You can enter up to 256 alphanumeric characters. If you include spaces, you must enclose your entry in quotes (" ").
- **vrf**—Specifies the VPN routing or forwarding instance name; limited to 32 characters.

Examples

This example show how to configure the contact information:

```
Switch(config)# call-home contact-info
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config-ca)# email
Switch(config-ca)# email-addr(1) user@company.com
Switch(config-ca)# phone-number +1-408-555-4567
Switch(config-ca)# street-address 1234 Picaso Street, Any city, Any state, 12345
Switch(config-ca)# customer-id Customer123
Switch(config-ca)# site-id Site1AnyWhere001
Switch(config-ca)# contract-id Company1234
Switch(config-ca)# exit
Switch(config)#
```

This example show how to configure the call-home message rate-limit threshold:

```
Switch(config)# call-home
Switch(config)# rate-limit 20
```

This example show how to set the call-home message rate-limit threshold to the default setting:

```
Switch(config)# call-home
Switch(config)# no rate-limit
```

This example show how to create a new destination profile with the same configuration settings as an existing profile:

```
Switch(config)# call-home
Switch(config)# profile profile1
```

This example show how to configure the general e-mail parameters, including a primary and secondary e-mail server:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# call-home
Switch(config)# mail-server smtp.example.com priority 1
Switch(config)# mail-server 192.168.0.1 priority 2
Switch(config)# sender from username@example.com
Switch(config)# sender reply-to username@example.com
Switch(config-ca)# exit
Switch(config)#
```

This example show how to specify MyGateVrf as the vrf name where the call-home e-mail message is forwarded:

```
Switch(config-ca)# vrf MyGateVrf
```

Related Commands

Command	Description
alert-group (refer to Cisco IOS documentation)	Enables an alert group.
profile (refer to Cisco IOS documentation)	Enters call-home profile configuration mode.
show call-home	Displays call-home configuration information.

call-home request

To submit information about your system to Cisco for report and analysis information from the Cisco Output Interpreter tool, use the **call-home request** command in privileged EXEC mode. An analysis report is sent by Cisco to a configured contact e-mail address.

call-home request {**output-analysis** "show-command" | **config-sanity** | **bugs-list** | **command-reference** | **product-advisor**} [*profile name*] [*send-user-id*]

Syntax Description	**output-analysis** "show-command" Sends the output of the specified CLI show command for analysis. The show command must be contained in quotes (""). **config-sanity** Specifies the type of report requested. Based on this keyword, the output of a predetermined set of commands such as the **show running-config all**, **show version**, and **show module** (variations) or **show module switch all** (VS systems) commands, is sent to Cisco for analysis. **bugs-list** Specifies the type of report requested. Based on this keyword, the output of a predetermined set of commands such as the **show running-config all**, **show version**, and **show module** (variations) or **show module switch all** (VS systems) commands, is sent to Cisco for analysis. **command-reference** Displays Bugtraq IDs on existing traffic for which the request is sent. If no profile is specified, the request is sent to the Cisco TAC profile. **product-advisor** Displays End-of-Life information or a registered Impact advisor scan. If a *user-id* is specified, the resulting analysis report is sent to the e-mail address of the registered user. If a *user-id* is not specified, the report is sent to the contact e-mail address of the device. **profile** *name* (Optional) Specifies the destination profile. If no profile is specified, the request is sent to the Cisco TAC profile. **send** *user-id* (Optional) Specifies the destination e-mail address. If a *user-id* is specified, the resulting analysis report is sent to the e-mail address of the registered user. If a *user-id* is not specified, the report is sent to the contact e-mail address of the device.
Command Default	This command has no default settings.
Command Modes	Privileged EXEC mode
Usage Guidelines	The recipient profile does not need to be enabled for the call-home request. The profile should specify the e-mail address where the transport gateway is configured so that the request message can be forwarded to the Cisco TAC and the user can receive the reply from the Smart Call Home service. Based on the keyword specifying the type of report requested, the following information is returned in response to the request: • **config-sanity**—Information on best practices as related to the current running configuration. • **bugs-list**—Known bugs in the running version and in the currently applied features. • **command-reference**—Reference links to all commands in the running configuration. • **product-advisor**—Product Security Incident Response Team (PSIRT) notices, End of Life (EOL) or End of Sales (EOS) notices, or field notices (FN) that may affect devices in your network.
Examples	This example shows a request for analysis of a user-specified show command: Switch **call-home request output-analysis "show diagnostic result module all" profile ms**

Related Commands	**call-home (global configuration)**	Enters call-home configuration mode.
	call-home send	Sends a CLI command to be executed, with the command output to be sent by e-mail.
	call-home send alert group	Sends a specific alert group message.
	service call-home(refer to Cisco IOS documentation)	Enables or disables Call Home.
	show call-home	Displays call-home configuration information.

call-home send

To execute a CLI command and e-mail the command output, use the **call-home send** command in privileged EXEC mode.

call-home send *"cli-command"* [**email** *email-addr*] [**service-number** *SR*] [**service-number** *SR*]

Syntax Description

"cli-command"	Specifies a CLI command to be executed. The command output is sent by e-mail.
email *email-addr*	Specifies the e-mail address to which the CLI command output is sent. If no e-mail address is specified, the command output is sent to the Cisco TAC at attach@cisco.com.
service-number *SR*	Specifies an active TAC case number to which the command output pertains. This number is required only if no e-mail address (or a TAC e-mail address) is specified, and will appear in the e-mail subject line.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

This command causes the specified CLI command to be executed on the system. The specified CLI command must be enclosed in quotes ("), and can be any run or show command, including commands for all modules.

The command output is then sent by e-mail to the specified e-mail address. If no e-mail address is specified, the command output is sent to Cisco TAC at attach@cisco.com. The e-mail is sent in long text format with the service number, if specified, in the subject line.

Examples

This example shows how to send a CLI command and have the command output e-mailed:

```
Switch# call-home send "show diagnostic result module all" email support@example.com
```

Related Commands

call-home [global configuration]	Enters call home configuration mode.
call-home send alert-group	Sends a specific alert group message.
service call-home (refer to Cisco IOS documentation)	Enables or disables Call Home.
show call-home	Displays call-home configuration information.

call-home send alert-group

To send a specific alert group message, use the **call-home send alert-group** command in privileged EXEC mode.

call-home send alert-group {configuration | diagnostic module *number* **| inventory} [profile** *profile-name]*

Syntax Description	**configuration** Sends the configuration alert-group message to the destination profile.
	diagnostic module *number* Sends the diagnostic alert-group message to the destination profile for a specific module number.
	inventory Sends the inventory call-home message.
	profile *profile-name* (Optional) Specifies the name of the destination profile.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

Usage Guidelines When you enter the *module number*, you can enter the number of the module.

If you do not specify **profile** *profile-name*, the *message* is sent to all subscribed destination profiles.

Only the configuration, diagnostic, and inventory alert groups can be manually sent. The destination profile need not be subscribed to the alert group.

Examples This example shows how to send the configuration alert-group message to the destination profile:

```
Switch# call-home send alert-group configuration
```

This example shows how to send the diagnostic alert-group message to the destination profile for a specific module number:

```
Switch# call-home send alert-group diagnostic module 3
```

This example shows how to send the diagnostic alert-group message to all the destination profiles for a specific module number:

```
Switch# call-home send alert-group diagnostic module 3 profile CiscoTac1
```

This example shows how to send the inventory call-home message:

```
Switch# call-home send alert-group inventory
```

Related Commands	**call-home [global configuration]**	Enters call home configuration mode.
	call-home test	Sends a call-home test message that you define.

service call-home (refer to Cisco IOS documentation)	Enables or disables Call Home.
show call-home	Displays call-home configuration information.

call-home test

To manually send a Call-Home test message, use the **call-home test** command in privileged EXEC mode.

call-home test [*"text-message"*] **profile** *profile-name*

Syntax Description	*"text-message"* (Optional) Text message test. **profile** *profile-name* Specifies the name of the destination profile.
Command Default	This command has no default settings.
Command Modes	Privileged EXEC mode
Usage Guidelines	This command sends a test message to the specified destination profile. If you enter test message test, you must enclose the text in quotes ("") if it contains spaces. If you do not enter a message, a default message is sent.
Examples	This example shows how to manually send a Call-Home test message: `Switch(config)#call-home test "test of the dept profile diagnost`
Related Commands	**call-home** [**global**	**configuration**] Enters Call-home configuration mode. **call-home send**	**alert-group** Sends a specific alert group message. **service call-home** (refer to Cisco IOS documentation) Enables or disables Call Home. **show call-home** Displays call-home configuration information.

channel-group

To assign and configure an EtherChannel interface to an EtherChannel group, use the **channel-group** command. To remove a channel group configuration from an interface, use the **no** form of this command.

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

no channel-group

Syntax Description	*number*	Specifies the channel-group number, valid values are from 1 to 64.
	mode	Specifies the EtherChannel mode of the interface.
	active	Enables LACP unconditionally.
	on	Forces the port to channel without PAgP.
	auto	Places a port into a passive negotiating state, in which the port responds to PAgP packets it receives but does not initiate PAgP packet negotiation.
	non-silent	(Optional) Used with the auto or desirable mode when traffic is expected from the other device.
	passive	Enables LACP only if an LACP device is detected.
	desirable	Places a port into an active negotiating state, in which the port initiates negotiations with other ports by sending PAgP packets.

Defaults No channel groups are assigned.

Command Modes Interface configuration mode

Usage Guidelines You do not have to create a port-channel interface before assigning a physical interface to a channel group. If a port-channel interface has not been created, it is automatically created when the first physical interface for the channel group is created.

If a specific channel number is used for the PAgP-enabled interfaces of a channel group, that same channel number cannot be used for configuring a channel that has LACP-enabled interfaces or vice versa.

You can also create port-channels by entering the **interface port-channel** command. This will create a Layer 3 port-channel. To change the Layer 3 port-channel into a L ayer 2 port-channel, use the **switchport** command before you assign physical interfaces to the channel group. A port channel cannot be changed from Layer 3 to L ayer 2 or vice versa when it contains member ports.

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 recommend that you do so.

Any configuration or attribute changes that 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).

You can create in **on** mode a usable EtherChannel by connecting two port groups together.

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

Examples

This example shows how to add Gigabit Ethernet interface 1/1 to the EtherChannel group that is specified by port-channel 45:

```
Switch(config)#interface gigabitethernet 1/1
Switch(config-if)# channel-group 45 mode on
Creating a port-channel interface Port-channel45
Switch(config-if)#
```

Related Commands

Command	Description
interface port-channel	Accesses or creates a port-channel interface.
show interfaces port-channel (refer to Cisco IOS documentation)	Displays the information about the Fast EtherChannel.

channel-protocol

To enable LACP or PAgP on an interface, use the **channel-protocol** command. To disable the protocols, use the **no** form of this command.

channel-protocol {lacp | pagp}

no channel-protocol {lacp | pagp}

Syntax Description	**lacp** Enables LACP to manage channeling. **pagp** Enables PAgP to manage channeling.
Defaults	**pagp**
Command Modes	Interface configuration mode

Usage Guidelines

You can also select the protocol using the **channel-group** command.

If the interface belongs to a channel, the **no** form of this command is rejected.

All ports in an EtherChannel must use the same protocol; you cannot run two protocols on one module.

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

You can manually configure a switch with PAgP on one side and LACP on the other side in the **on** mode.

You can change the protocol at any time, but this change causes all existing EtherChannels to reset to the default channel mode for the new protocol. You can use the **channel-protocol** command to restrict anyone from selecting a mode that is not applicable to the selected protocol.

Configure all ports in an EtherChannel to operate at the same speed and duplex mode (full duplex only for LACP mode).

For a complete list of guidelines, refer to the "Configuring EtherChannels" section of the *Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide*.

Examples

This example shows how to select LACP to manage channeling on the interface:

```
Switch(config)# int gi1/0/4 channel-protocol lacp
Switch(config)#int gi 1/0/4
```

Related Commands

Command	Description
channel-group	Assigns and configures an EtherChannel interface to an EtherChannel group.
show etherchannel	Displays EtherChannel information for a channel.

cisp enable

Use the **cisp enable** global configuration command to enable Client Information Signalling Protocol (CISP) on a switch.

cisp enable

no cisp enable

Syntax Description	***cisp enable*** Enable CISP.
Defaults	None
Command Modes	Global configuration
Usage Guidelines	You must enable the CISP protocol (with the global **cisp enable** command) on both the authenticator and supplicant switch. The CISP protocol is crucial because it conveys the client information from the supplicant switch to the authenticator switch thereby providing access for the clients of the supplicant switch through the authenticator switch.
Examples	This example shows how to enable CISP: `switch(config)#` ***cisp enable***
Related Commands	**Command** / **Description** **dot1x credentials** *profile* **[configuration]** — Configures a profile on a supplicant switch. **show cisp [{ITN command}]** — Displays CISP information for a specified interface.

class

To specify the name of the class whose traffic policy you want to create or change, use the **class** policy-map configuration command. To delete an existing class from a policy map, use the **no** form of this command.

class *class-name*

no class *class-name*

Syntax Description

class-name	Name of the predefined traffic class for which you want to configure or modify a traffic policy. The class was previously created through the **class-map** *class-map-name* global configuration command.

Defaults

No classes are defined; except for the class-default.

Command Modes

Policy-map configuration mode

Usage Guidelines

Before using the **class** command, you must create a class map for matching packets to the class by using the **class-map** global configuration command. You also must use the **policy-map** global configuration command to create a policy map and to associate the class with the policy map. When you create a policy map, you can configure a traffic policy for new classes or modify a traffic policy for any existing classes in that policy map. The class name that you specify with the **class** command in the policy map uses the characteristics for that class (its policy) to the class map and its match criteria, as configured through the **class-map** global configuration command. You attach the policy map to a port by using the **service-policy (interface configuration)** configuration command.

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

- **bandwidth** Specifies or modifies the minimum bandwidth provided to a class belonging to a policy map. For more information, see the **bandwidth** command.
- **dbl** Enables dynamic buffer limiting for traffic hitting this class. For details on **dbl** parameters refer to the **dbl-queue dbl** command.
- **exit** Exits policy-map class configuration mode and returns to policy-map configuration mode.
- **no** Returns a command to its default setting.
- **police** Configures a single-rate policer, an aggregate policer, or a two-rate traffic policer that uses the committed information rate (CIR) and the peak information rate (PIR) for a class of traffic. The **police** command can be used in policy-map class configuration mode. For more information, see the **police** command. For more information about the two-rate policer, see the **police (two-rates)** and the **police (percent)** commands.
- **priority** Enables the strict priority queue for a class of traffic. For more information, see the **priority** command.

- **service-policy (policy-map class)** Creates a service policy as a quality of service (QoS) policy within a policy map (called a hierarchical service policy). For more information, see the **service-policy (policy-map class)** command. This command is effective only in a hierarchical policy map attached to an interface.
- set Classifies IP traffic by setting a class of service (CoS), a Differentiated Services Code Point (DSCP) or IP precedence in the packet. For more information, see the **set** command.
- **shape (class-based queuing)** Sets the class hierarchy commitment information rate (CIR) in a policy map. For more information, see the **shape (class-based queuing)** command.
- trust Defines a trust state for a traffic class. For more information, see the **trust** command.

The switch supports up to 256 classes, including the default class, in a policy map. Put here that fol to meet any of the matching criteria are classified as members of the default traffic class. You configure the default traffic class by specifying **class-default** as the class name in the **class** policy-map class configuration command. You can manipulate the default traffic class (for example, set policies to police or to shape it) just like any other traffic class, but you cannot delete it.

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 an egress port, the policy matches all the inbound traffic defined in class1, sets the IP DSCP to 10, and polices the traffic at an average rate of 1 Mbps and burst of 20 Kb. Traffic exceeding the profile is marked down to a Traffic exceeding the profile is marked down to a DSCP value obtained from the policed-DSCP map and then sent.

```
Switch(config)# configure terminal
Switch(config-if)# class-map class1
Switch(config-if)# exit
Switch(config-if)# policy-map policy1
Switch(config-if)# class class1
Switch(config-if)# set ip dscp 10
Switch(config-if)# police 1000000 20000 exceed-action policed-dscp-transmit
Switch(config-if)# exit
Switch(config-if)# end
Switch(config-if)# show policy-map class1
Switch(config-if)# show mls qos maps policed-dscp
Switch(config-if)# show mls qos interface policy-map policy1
Switch#
```

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

Related Commands

Command	Description
bandwidth	Specifies or modifies the minimum bandwidth provided to a class belonging to a policy map attached to a physical port.
class-map	Creates a class map to be used for matching packets to the class whose name you specify and to enter class-map configuration mode.
dbl	Enables active queue management on a transmit queue used by a class of traffic.
police	Configures the Traffic Policing feature.
police (percent)	Configures traffic policing on the basis of a percentage of bandwidth available on an interface.
police rate	Configures single- or dual-rate policer.
policy-map	Creates a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.
priority	Enables the strict priority queue (low-latency queuing [LLQ]) and to give priority to a class of traffic belonging to a policy map attached to a physical port.
service-policy (interface configuration)	Attaches a policy map to an interface.
service-policy (policy-map class)	Creates a service policy that is a quality of service (QoS) policy within a policy map.
set	Marks IP traffic by setting a class of service (CoS), a differentiated Services Code Point (DSCP), or IP precedence in the packet.
shape (class-based queuing)	Enables traffic shaping a class of traffic in a policy map attached to a physical port.
show policy-map	Displays information about the policy map.
trust	Defines a trust state for traffic classified through the **class** policy-map configuration command.

class-map

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 **class-map** global configuration command. To delete an existing class map and to return to global configuration mode, use the **no** form of this command.

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 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 in the class map must be matched.
	class-map-name Name of the class map.

Defaults

No class maps are defined.

If neither the **match-all** nor the **match-any** keyword is specified, the default is **match-all**.

Command Modes

Global configuration mode

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. Packets are checked against the match criteria configured for a class map to decide if the packet belongs to that class. If a packet matches the specified criteria, the packet is considered a member of the class and is forwarded according to the quality of service (QoS) specifications set in the traffic policy.

After you enter the **class-map** command, the switch enters class-map configuration mode, and 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.

Examples

This example shows how to configure the class-map called client without match criteria, which is an access list called 101:

```
Switch(config)# conf t
Switch(config)# access-list 101 permit any any log-a
Switch(config)# class-map client
Switch(config-cmap)# match access-group 101
Switch(config-cmap)# exit
Switch(config)#
```

This example shows how to delete the class1 class map:

```
Switch#
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no class-map class1
Switch#
```

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

Related Commands	Command	Description
	class	Specifies the name of the class whose traffic policy you want to create or change.
	match (class-map configuration)	Defines the match criteria for a class map.
	policy-map	Creates a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.
	show class-map	Displays class map information.

clear counters

To clear the interface counters, use the **clear counters** command.

clear counters [{**FastEthernet** *interface_number* | {**GigabitEthernet** *interface_number* | {**null** *interface_number* | {**port-channel** *number* | {**vlan** *vlan_id*}]

Syntax Description	**FastEthernet** *interface_number* (Optional) Specifies the Fast Ethernet interface; valid values are from 1 to 6. **GigabitEthernet** *interface_number* (Optional) Specifies the Gigabit Ethernet interface; valid values are from 1 to 9. **null** *interface_number* (Optional) Specifies the null interface; the valid value is 0. **port-channel** *number* (Optional) Specifies the channel interface; valid values are from 1 to 64. **vlan** *vlan_id* (Optional) Specifies the VLAN; valid values are from 1 to 4096.
Defaults	This command has no default settings.
Command Modes	Privileged EXEC mode
Usage Guidelines	This command clears all the current interface counters from all the interfaces unless you specify an interface.

Note This command does not clear the counters that are retrieved using SNMP, but only those seen when you issue the **show interface counters** command.

Examples

This example shows how to clear all the interface counters:

```
Switch# clear counters
Clear "show interface" counters on all interfaces [confirm] y
Switch#
```

This example shows how to clear the counters on a specific interface:

```
Switch# clear counters vlan 200
Clear "show interface" counters on this interface [confirm]y
Switch#
```

Related Commands

Command	Description
show interface counters [*interface*]	Displays interface counter information.

For Cisco IOS documentation:

clear errdisable

To re-enable error-disabled VLANs on an interface, use the **clear errdisable** command.

clear errdisable interface [*name*] **vlan** [*range*]

Syntax Description		
	interface *name*	Specifies the interface of the VLAN(s) to recover.
	vlan	Specifies all VLANs on the interface for recovered.
	range	(Optional) Specifies the VLAN range to be recovered.

Defaults	
	This command has no default settings.

Command Modes	
	Global configuration mode

Usage Guidelines

If a VLAN range is not specified, all VLANs on the specified interface are re-enabled. The **clear errdisable** command recovers the disabled VLANs on an interface.

Clearing the error-disabled state from a virtual port does not change the link state of the physical port, and it does not affect other VLAN ports on the physical port. It does post an event to STP, and spanning tree goes through its normal process of bringing the VLAN port to the appropriate blocking or forwarding state.

Examples

This example shows how to re-enable a range of disabled VLANs on an interface:

```
Switch#clear errdisable interface ethernet1/slot 1/6-10
Switch#
```

Related Commands	Command	Description
	errdisable detect	Enables error-disable detection.
	show errdisable detect	Displays the error-disable detection status.
	show interfaces status	Displays the interface status or a list of interfaces in error-disabled state.
	switchport port-security	Enables port security on an interface.

clear hw-module slot password

To clear the password on an intelligent line module, use the **clear hw-module slot password** command.

clear hw-module slot slot_num **password**

Syntax Description	slot_num Slot on a line module.
Defaults	The password is not cleared.
Command Modes	Privileged EXEC mode
Usage Guidelines	You only need to change the password once unless the password is reset.
Examples	This example shows how to clear the password from slot 5 on a line module: Console> **clear hw-module slot 5 password** Console>
Related Commands	**Command** — **Description** **hw-module power** — Turns the power off on a slot or line module.

clear interface gigabitethernet

To clear the hardware logic from a Gigabit Ethernet IEEE 802.3z interface, use the **clear interface gigabitethernet** command.

Note This command does not increment **interface resets** as displayed with the **show interface gigabitethernet** *mod/port* command.

clear interface gigabitethernet *mod/port*

Syntax Description	*mod/port* Number of the module and port.
Defaults	This command has no default settings.
Command Modes	Privileged EXEC mode
Examples	This example shows how to clear the hardware logic from a Gigabit Ethernet IEEE 802.3z interface: `Switch#` **`clear interface gigabitethernet 1/4`** `Switch#`

Related Commands	**Command**	**Description**
	show interfaces status	Displays the interface status.

clear interface vlan

To clear the hardware logic from a VLAN, use the **clear interface vlan** command.

clear interface vlan *number*

Syntax Description	*number* Number of the VLAN interface; valid values are from 1 to 4094.
Defaults	This command has no default settings.
Command Modes	Privileged EXEC mode

Examples	This example shows how to clear the hardware logic from a specific VLAN:
	`Switch(enable) clear interface vlan 5`
	`Switch(enable)`

Related Commands

Command	Description
show interfaces status	Displays the interface status.

clear ip access-template

To clear the statistical information in access lists, use the **clear ip access-template** command.

clear ip access-template *access-list*

Syntax Description

access-list	Number of the access list; valid values are from 100 to 199 for an IP extended access list, and from 2000 to 2699 for an expanded range IP extended access list.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Examples

This example shows how to clear the statistical information for an access list:

```
Switch#clear ip access-template 201
Switch#
```

clear ip arp inspection log

To clear the status of the log buffer, use the **clear ip arp inspection log** command.

clear ip arp inspection log

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

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

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

Related Commands

Command	Description
arp access-list	Defines an ARP access list or adds clauses at the end of a predefined list.
show ip arp inspection log	Displays the status of the log buffer.

clear ip arp inspection statistics

To clear the dynamic ARP inspection statistics, use the **clear ip arp inspection statistics** command.

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

Syntax Description	**vlan** *vlan-range* (Optional) Specifies the VLAN range.
Defaults	This command has no default settings.
Command Modes	Privileged EXEC mode

Examples

This example shows how to clear the DAI statistics from VLAN 1 and how to verify the removal:

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

Vlan     Forwarded   Dropped     DHCP Drops    ARP Drops
----     ---------   -------     ----------    ---------
   1             0         0              0            0

Vlan     DHCP Permits  ARP Permits  Source MAC Failures
----     ------------  -----------  -------------------
   1                0            0                    0

Vlan     Dest MAC Failures   IP Validation Failures
----     -----------------   ----------------------
   1                     0                        0
Switch#
```

Related Commands	Command	Description
	arp access-list	Defines an ARP access list or adds clauses at the end of a predefined list.
	clear ip arp inspection log	Clears the status of the log buffer.
	show ip arp inspection log	Displays the status of the log buffer.

clear ip dhcp snooping binding

To clear the DHCP snooping binding, use the **clear ip dhcp snooping binding** command.

clear ip dhcp snooping binding {* | *ip-address*} [**vlan** *vlan_num*] [**interface** *interface_num*]

Syntax Description	* (Optional) Clears all DHCP snooping binding entries.
	ip-address (Optional) IP address for the DHCP snooping binding entries.
	vlan *vlan_num* (Optional) Specifies a VLAN.
	interface *interface_num* (Optional) Specifies an interface.

Defaults	This command has no default settings.
Command Modes	Privileged EXEC mode

Usage Guidelines

These commands are mainly used to clear DHCP snooping binding entries.

DHCP snooping is enabled on a VLAN only if both the global snooping and the VLAN snooping are enabled.

Examples

This example shows how to clear all the DHCP snooping binding entries:

```
Switch#clear ip dhcp snooping binding *
Switch#
```

This example shows how to clear a specific DHCP snoop binding entry:

```
Switch#clear ip dhcp snooping binding 1.2.3.4
Switch#
```

This example shows how to clear all the DHCP snoop binding entries on the Gigabit Ethernet interface 1/1:

```
Switch#clear ip dhcp snooping binding interface gigabitethernet 1/1
Switch#
```

This example shows how to clear all the DHCP snoop binding entries on VLAN 40:

```
Switch#clear ip dhcp snooping binding vlan 40
Switch#
```

Related Commands	Command	Description
	ip dhcp snooping	Globally enables DHCP snooping.
	ip dhcp snooping binding	Sets up and generates a DHCP binding configuration to restore bindings across reboots.
	ip dhcp snooping information option	Enables DHCP option 82 data insertion.
	ip dhcp snooping trust	Enables DHCP snooping on a trusted VLAN.
	ip dhcp snooping vlan	Enables DHCP snooping on a VLAN or a group of VLANs.
	show ip dhcp snooping	Displays the DHCP snooping configuration.
	show ip dhcp snooping binding	Displays the DHCP snooping binding entries.

clear ip dhcp snooping database

To clear the DHCP binding database, use the **clear ip dhcp snooping database** command.

clear ip dhcp snooping database

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Examples This example shows how to clear the DHCP binding database:

```
Switch> clear ip dhcp snooping database
Switch>
```

Related Commands

Command	Description
ip dhcp snooping	Globally enables DHCP snooping.
ip dhcp snooping binding	Sets up and generates a DHCP binding configuration to restore bindings across reboots.
ip dhcp snooping information option	Enables DHCP option for data insertion.
ip dhcp snooping trust	Enables DHCP snooping on a trusted VLAN.
ip dhcp snooping vlan	Enables DHCP snooping on a VLAN or a group of VLANs.
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.

clear ip dhcp snooping database statistics

To clear the DHCP binding database statistics, see the **clear ip dhcp snooping database statistics** command.

clear ip dhcp snooping database statistics

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Examples This example shows how to clear the DHCP binding database:

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

Related Commands

Command	Description
ip dhcp snooping	Globally enables DHCP snooping.
ip dhcp snooping binding	Sets up and generates a DHCP binding configuration to restore bindings across reboots.
ip dhcp snooping information option	Enables DHCP option 82 data insertion.
ip dhcp snooping trust	Enables DHCP snooping on a trusted VLAN.
ip dhcp snooping vlan	Enables DHCP snooping on a VLAN or a group of VLANS.
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.

clear ip igmp group

To delete the IGMP group cache entries, use the **clear ip igmp group** command.

clear ip igmp group {**fastethernet** *mod/port*} | {**GigabitEthernet** *mod/port*} | {*host_name* | *group_address*} | {**loopback** *interface_number*} | {**null** *interface_number*} | {**port-channel** *number*} | {**vlan** *vlan_id*}

fastethernet	(Optional) Specifies the Fast Ethernet interface.
mod/port	(Optional) Number of the module and port.
GigabitEthernet	(Optional) Specifies the Gigabit Ethernet interface.
host_name	(Optional) Hostname, as defined in the DNS hosts table or with the **ip host** command.
group_address	(Optional) Address of the multicast group in four-part, dotted notation.
Loopback *interface_number*	(Optional) Specifies the loopback interface; valid values are from 0 to 2147483647.
null *interface_number*	(Optional) Specifies the null interface; the valid values are 0.
port-channel *number*	(Optional) Specifies the channel interface; valid values are from 1 to 64.
vlan *vlan_id*	(Optional) Specifies the VLAN; valid values are from 1 to 4094.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Usage Guidelines The IGMP cache contains a list of the multicast groups of which hosts on the directly connected LAN are members.

To delete all the entries from the IGMP cache, enter the **clear ip igmp group** command with no arguments.

Examples This example shows how to clear the entries for a specific group from the IGMP cache:

```
Switch> clear ip igmp group 224.0.200.1
Switch>
```

This example shows how to clear the IGMP group cache entries from a specific interface:

```
Switch#clear ip igmp group gigabitethernet 1/1
Switch#
```

Related Commands	Command	Description
	ip host(refer to Cisco IOS documentation)	Defines a static host name-to-address mapping in the host cache.
	show ip igmp groups(refer to Cisco IOS documentation)	Displays the multicast groups with receivers that are directly connected to the router and that were learned through IGMP. For information about IGMP management, see the show **ip igmp groups** command in IOS CGMP mode.
	show ip igmp interface	Displays the information about the IGMP interface status and configuration.

clear ip igmp snooping membership

To clear the explicit host-tracking database, use the **clear ip igmp snooping membership** command.

clear ip igmp snooping membership [vlan *vlan_id*]

Syntax Description: **vlan** *vlan_id* (Optional) Specifies a VLAN; valid values are from 1 to 1001 and from 1006 to 4094.

Defaults: This command has no default settings.

Command Modes: Privileged EXEC mode

Usage Guidelines: By default, the explicit host tracking database maintains a maximum of 1-KB entries. After you reach this limit, no additional entries can be created in the database. To create more entries, you will need to delete the database with the **clear ip igmp snooping statistics vlan** command.

Examples: This example shows how to display the IGMP snooping statistics for VLAN 25:

```
Switch# clear ip igmp snooping membership vlan 25
Switch#
```

Related Commands:

Command	Description
ip igmp snooping vlan explicit-tracking	Enables per-VLAN explicit host tracking.
show ip igmp snooping membership	Displays host membership information.

clear ip mfib counters

To clear the global MFIB counters and the counters for all active MFIB routes, use the **clear ip mfib counters** command.

clear ip mfib counters

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Examples This example shows how to clear all the active MFIB routes and global counters:

```
Router#clear ip mfib counters
Router#
```

Related Commands

Command	Description
show ip mfib	Displays all active Multicast Forwarding Information Base (MFIB) routes.

clear ip mfib fastdrop

To clear all the MFIB fast-drop entries, use the **clear ip mfib fastdrop** command.

clear ip mfib fastdrop

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Usage Guidelines If new fast-dropped packets arrive, the new fast-drop entries are created.

Examples This example shows how to clear all the fast-drop entries:

```
Router# clear ip mfib fastdrop
Router#
```

Related Commands

Command	Description
ip mfib fastdrop	Enables MFIB Fast drop.
show ip mfib fastdrop	Displays all currently active fast-drop entries and shows whether fast drop is enabled.

clear ip wccp

To remove Web Cache Communication Protocol (WCCP) statistics (counts) maintained on the switch for a particular service, use the **clear ip wccp** command in privileged EXEC mode.

clear ip wccp {**ref** *vrf-name* | **web-cache** | *service-number*}[**[web-cache** | *service-number*]]

Syntax Description	**web-cache**	(Optional) Directs the router to remove statistics for the web cache service.
	service-number	(Optional) Number of the cache service to be removed. The number can be from 0 to 98.

Defaults No default behavior or values.

Command Modes Privileged EXEC (#)

Usage Guidelines Use the **show ip wccp** and **show ip wccp detail** commands to display WCCP statistics.

Use the **clear ip wccp** command to clear the WCCP counters for all WCCP services in all VRFs.

Examples The following example shows how to clear all statistics associated with the web cache service:

```
Router#clear ip wccp web-cache
```

Related Commands	**Command**	**Description**
	ip wccp	Enables support of the specified WCCP service for participation in a service group.
	show ip wccp	Displays global statistics related to the WCCP.

clear lacp counters

To clear the statistics for all the interfaces belonging to a specific channel group, use the **clear lacp counters** command.

clear lacp [*channel-group*] **counters**

Syntax Description	*channel-group* (Optional) Channel-group number; valid values are from 1 to 64.
Defaults	This command has no default settings.
Command Modes	Privileged EXEC mode
Usage Guidelines	If you do not specify a channel group, all channel groups are cleared. If you enter this command for a channel group that contains members in PAgP mode, the command is ignored.

Examples	This example shows how to clear the statistics for a specific group:
	`Switch(config)# clear lacp 1 counters`
	`Switch(config)#`

Related Commands	**Command** — **Description** **show lacp** — Displays LACP information.

clear mac-address-table

To clear the global counter entries from the Layer 2 MAC address table, use the **clear mac-address-table** command.

clear mac-address-table {dynamic [address *mac_addr* **| [interface** *interface* **]] | static** *vlan_id*** | notification}**

Syntax Description

dynamic	Specifies dynamic entry type.
address *mac_addr*	(Optional) Specifies the MAC address.
interface *interface*	(Optional) Specifies the interface and clears the entries associated with it; valid values are **FastEthernet** and **GigabitEthernet**.
static *vlan_id*	(Optional) Specifies the VLANs; valid values are from 1 to 4094.
notification	Specifies MAC change notification global counters.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

Enter the **clear mac-address-table dynamic** command with no arguments to remove all dynamic entries from the table.

The **clear mac-address-table notification** command only clears the global counters which are displayed with **show mac-address-table notification** command. It does not clear the global counters and the history table of the CISCO-MAC-NOTIFICATION-MIB.

Examples

This example shows how to clear all the dynamic Layer 2 entries for a specific interface (gi1/1):

```
Switch#clear mac-address-table dynamic interface gi1/1
Switch#
```

This example shows how to clear the MAC address notification counters:

```
Switch#clear mac-address-table notification
Switch#
```

Related Commands	Command	Description
	clear mac address-table dynamic	Clears the dynamic address entries from the Layer 2 MAC address table.
	mac address-table aging-time	Configures the aging time for entries in the Layer 2 table.
	mac address-table notification	Enables MAC address notification on a switch.
	mac-sticky	Enters the static CPU submode and manually synchronizes the configurations on two supervisor engines.
	show mac address-table address	Displays the information about the MAC address table.
	snmp-server enable traps	Enables SNMP notifications.

clear mac-address-table dynamic

To clear the dynamic address entries from the Layer 2 MAC address table, use the **clear mac-address-table dynamic** command.

clear mac-address-table dynamic [**address** *mac_addr*] [**interface** *interface*] [**vlan** *vlan_id*]

Syntax Description	**address** *mac_addr*	(Optional) Specifies the MAC address.
	interface *interface*	(Optional) Specifies the interface that clears the entries associated with it; valid options are **FastEthernet** and **GigabitEthernet**.
	vlan *vlan_id*	(Optional) Specifies the VLAN for which static entries are deleted; valid values are from 1 to 4094.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Usage Guidelines Enter the **clear mac-address-table dynamic** command with no arguments to remove all dynamic entries from the table.

Examples This example shows how to clear all the dynamic L-type 2 entries for a specific interface (gi1/1):

```
Switch#clear mac-address-table dynamic interface gi1/1
Switch#
```

Related Commands

Command	Description
mac-address-table aging-time	Configures the aging time for entries in the Layer 2 table.
mmls cpu	Enters the mmls CPU submode and manually synchronizes the multilayer switch hardware engines.
show mac-address-table address	Displays the information about the MAC address table.

clear nmsp statistics

To clear the Network Mobility Services Protocol (NMSP) statistics, use the **clear nmsp statistics** command. This command is available only when your switch is running the cryptographic (encrypted) software image.

```
clear nmsp statistics
```

Syntax Description This command has no arguments or keywords.

Defaults No default is defined.

Command Modes Privileged EXEC mode

Examples This example shows how to clear NMSP statistics:

```
Switch#clear nmsp statistics
Switch#
```

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

Related Commands

Command	Description
show nmsp	Displays the NMSP information.

clear pagp

To clear the port-channel information, use the **clear pagp** command.

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

Syntax Description		
	group-number	Channel-group number; valid values are from 1 to 64.
	counters	Clears traffic filters.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

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

```
Switch#clear pagp 32
Switch#
```

This example shows how to clear all the port-channel traffic filters:

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

Related Commands	Command	Description
	show pagp	Displays information about the port channel.

clear port-security

To delete all configured secure addresses or a specific dynamic or sticky secure address on an interface from the MAC address table, use the **clear port-security** command.

clear port-security dynamic [**address** *mac-addr*] [**vlan** *vlan-id*] [| **interface** *interface-id*] [**vlan access** | **vlan**]

Syntax Description	**dynamic** Delete all the dynamic secure MAC addresses.
	address *mac-addr* (Optional) Delete the specified secure MAC address.
	vlan *vlan-id* (Optional) Delete the specified secure MAC addresses from the specified VLAN.
	interface *interface-id* (Optional) Delete the secure MAC addresses on the specified physical port or port-channel.
	vlan access (Optional) Delete the secure MAC addresses from access VLANs.
	vlan voice (Optional) Delete the secure MAC addresses from voice VLANs.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

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

Note You can clear sticky and static secure MAC addresses one at a time with the **no switchport port-security mac-address** command.

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

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

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

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

```
Switch# clear port-security dynamic address 0000.0400.0007
```

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

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

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

Related Commands	Command	Description
	show port-security	Displays information about the port-security setting.
	switchport port-security	Enables port security on an interface.

clear pppoe intermediate-agent statistics

To clear PPPoE Intermediate Agent statistics (packet counters), use the **clear pppoe intermediate-agent statistics** command.

clear pppoe intermediate-agent statistics

Syntax Description This command has no arguments.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Examples This example shows how to clear PPPoE Intermediate Agent statistics:

```
Switch# clear pppoe intermediate-agent statistics
```

Related Commands

Command	Description
show pppoe intermediate-agent interface	Displays PPPoE Intermediate Agent statistics (packet counters).

clear qos

To clear the global and per-interface aggregate QoS counters, use the **clear qos** command.

clear qos [**aggregate-policer** *name*] | **interface** {**fastethernet** | **GigabitEthernet**} {*mod/interface*} | **vlan** {*vlan_num*} | **port-channel** {*number*}

Syntax Description	**aggregate-policer** *name* (Optional) Specifies an aggregate policer.
	interface (Optional) Specifies an interface.
	fastethernet (Optional) Specifies the first Ethernet 802.3 interface.
	GigabitEthernet (Optional) Specifies the Gigabit Ethernet 802.3z interface.
	mod/interface (Optional) Number of the module and interface.
	vlan *vlan_num* (Optional) Specifies a VLAN.
	port-channel *number* (Optional) Specifies the channel interface; valid values are from 1 to 64.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Usage Guidelines When you enter the **clear qos** command, the way the counters work is affected and the traffic that is normally restricted could be forwarded for a short period of time.

The **clear qos** command resets the interface QoS policy counters. If no interface is specified, the **clear qos** command resets the QoS policy counters for all interfaces.

Examples This example shows how to clear the global and per-interface aggregate QoS counters for all the protocols:

```
Switch#clear qos
Switch#
```

This example shows how to clear the specific protocol aggregate QoS counters for all the interfaces:

```
Switch#clear qos aggregate-policer
Switch#
```

Related Commands	Command	Description
	show qos	Displays QoS information.

clear vlan counters

To clear the software-cached counter values to start from zero again for a specified VLAN or all existing VLANs, use the **clear vlan counters** command.

clear vlan [*vlan-id*] **counters**

Syntax Description	*vlan-id* (Optional) VLAN number; see the "Usage Guidelines" section for valid values.
Defaults	This command has no default settings.
Command Modes	Privileged EXEC mode
Usage Guidelines	If you do not specify a *vlan-id* value, the software-cached counter values for all the existing VLANs are cleared.

Examples	This example shows how to clear the software-cached counter values for a specific VLAN:
	`Switch# clear vlan 10 counters`
	`Clear this vlan counters on this vlan [confirm] y`
	`Switch#`

Related Commands	**Command** — **Description** **show vlan counters** — Displays VLAN counter information.

clear vmps statistics

To clear the VMPS statistics, use the **clear vmps statistics** command.

clear vmps statistics

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Examples This example clears how to clear the VMPS statistics:

```
Switch#clear vmps statistics
Switch#
```

Related Commands

Command	Description
show vmps	Displays VMPS information.
vmps reconfirm (global-configuration)	Changes the reconfirmation interval for the VLAN Query Protocol (VQP) client.

control-plane

To enter control-plane configuration mode, which allows users to associate or modify attributes or parameters (such as a service policy) that are associated with the control plane of the device, use the **control-plane** command.

control-plane

Syntax Description This command has no arguments or keywords.

Defaults Default service-policy *system-cpp-policy* is attached.

Command Modes Global configuration mode

Usage Guidelines After you enter the **control-plane** command, you can define control plane services for your main processor. For example, you can associate service policy with the control plane to police all traffic that is destined to the control plane.

Examples These examples show how to configure trusted hosts with source addresses 10.1.1.1 and 10.1.1.2 to forward Telnet packets that exceed the control plane rate limit command, while allowing all remaining Telnet packets to be policed at the specified rate:

```
Switch(config)# access-list 140 deny tcp host 10.1.1.1 any eq telnet
! Allow 10.1.1.2 trusted host traffic
Switch(config)# access-list 140 deny tcp host 10.1.1.2 any eq telnet
! Rate limit all other Telnet traffic
Switch(config)# access-list 140 permit tcp any any eq telnet
Switch(config)# class-map telnet
Switch(config)# class-map telnet-class
Switch(config-cmap)# match access-group 140
Switch(config-cmap)# exit
Switch(config)# policy-map control-plane
Switch(config-pmap)# class telnet-class
Switch(config-pmap-c)# police 32000 1000 conform transmit exceed drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
! Define aggregate control-plane service for the entire Route Processor.
Switch(config)# macro global apply system-cpp
Switch(config)# control-plane
Switch(config-cp)# service-policy input system-cpp-policy
Switch(config-cp)# exit
```

Related Commands

Command	Description
class	Specifies the name of the class whose traffic policy you want to create or change.
class-map	Creates a class map to be used for matching packets to the class whose name you specify and to enter class-map configuration mode.
match access-group (refer to *Cisco IOS Release 12.2 Command Reference*)	Configures the match criteria for a class map on the basis of the specified access control list (ACL).
policy-map	Creates a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.
service-policy (interface configuration)	Attaches a policy map to an interface.
show policy-map control-plane	Displays the configuration either of a class or of all classes for the policy map of a control plane.

counter

To assign counters to a Layer 3 interface, use the **counter** interface command. To remove a counter assignment, use the **no** form of this command.

counter {**ipv4** | **ipv6** | **ipv4 ipv6 separate**}

no counter

Syntax Description

ipv4	Enables collection of IPv4 statistics only.
ipv6	Enables collection of IPv6 statistics only.
ipv4 ipv6 separate	Enables collection of IPv4 and IPv6 statistics and displays them individually.

Defaults

Not enabled

Command Modes

Interface configuration

Usage Guidelines

Entering the **counter** command without keywords displays the statistics as a sum.

The total number of switch ports that can present transmit and receive counters is 4892.

When you change a Layer 3 port assigned with a counter to a Layer 2 port, the hardware counters are cleared. This action is similar to entering the **no counter** command.

Examples

The following example shows how to enable counters on interface VLAN 1:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface vlan 1
Switch(config-if)# counter ipv4
Switch(config-if)# end
Switch#
%SYS-5-CONFIG_I: Configured from console by console
Switch# show run interface vlan 1
Building configuration...

Current configuration : 63 bytes

!
interface Vlan1
 ip address 10.0.0.1 255.0.0.0
 counter ipv4
end
```

Note To remove the counter assignment, use the **no counter** command.

If you have already assigned the maximum number of counters, the **counter** command fails, displaying the following error message:

```
Switch#**config terminal**
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#**interface Gal/2**
Switch(config-if)#**no switchport**
Switch(config-if)#**counter ipv4**
%Error: resource unavailable for interface Gal/2
Switch(config-if)#**end**
Switch#
00:12:19: %SYS-5-CONFIG_I: Configured from console by console
```

In this situation, you must release a counter from another interface to the new interface can use it.

dbl

To enable active-queue management on a transmit queue used by a class of traffic, use the **dbl** command. Use the **no** form of this command to return to the default setting.

dbl

no dbl

Syntax Description This command has no keywords or arguments.

Defaults Active-queue management is disabled.

Command Modes Policy-map class configuration

Usage Guidelines The semantics of the DBL configuration is similar to the WRED algorithm. The **dbl** command can operate alone on class-default; otherwise, it requires you to configure the **bandwidth** or **shape** commands on the class.

Examples This example shows how to enable dbl action in a class:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# dbl
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet 1/1
Switch(config-if)# service-policy output policy1
Switch(config-if)# end
```

Related Commands

Command	Description
bandwidth	Creates a signaling class structure that can be referred to by its name.
class	Creates a class map to be used for matching packets to the class whose name you specify and to enter class-map configuration mode.
policy-map	Creates a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.
service-policy (policy-map class)	Creates a service policy that is a quality of service (QoS) policy within a policy map.
show policy-map	Displays information about the policy map.

debug adjacency

To display information about the adjacency debugging, use the **debug adjacency** command. To disable debugging output, use the **no** form of this command.

debug adjacency [ipc]

no debug adjacency

Syntax Description | **ipc** | (Optional) Displays the IPC entries in the adjacency database.

Defaults | This command has no default settings.

Command Modes | Privileged EXEC mode

Examples | This example shows how to display the information in the adjacency database:

```
Switch# debug adjacency
4d02h: 4d02 add 172.20.52.34 [6]gi4/0/0:Ethernet(-1) vlan 4d0 w11 expires: 04:00:00
4d02h: 4d02 add 172.20.52.34 [6]gi4/0/0:Ethernet(-1) vlan 4d0 w11 expires: 04:00:00
4d02h: 4d02 add 172.20.52.34 [6]gi4/0/0:Ethernet(-1) vlan 4d0 w11 expires: 04:00:00
4d02h: 4d02 add 172.20.52.34 [6]gi4/0/0:Ethernet(-1) vlan 4d0 w11 expires: 04:00:00
4d02h: 4d02 add 172.20.52.34 [6]gi4/0/0:Ethernet(-1) vlan 4d0 w11 expires: 04:00:00
4d02h: 4d02 add 172.20.52.34 [6]gi4/0/0:Ethernet(-1) vlan 4d0 w11 expires: 04:00:00
4d02h: 4d02 add 172.20.52.34 [6]gi4/0/0:Ethernet(-1) vlan 4d0 w11 expires: 04:00:00
4d02h: 4d02 add 172.20.52.34 [6]gi4/0/0:Ethernet(-1) vlan 4d0 w11 expires: 04:00:00
<... output truncated, ...>
Switch#
```

Related Commands

Command	Description
undebug adjacency (same as **nodebug adjacency**)	Disables debugging output.

debug backup

To debug the backup events, use the **debug backup** command. To disable the debugging output, use the **no** form of this command.

debug backup

no debug backup

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Examples This example shows how to debug the backup events:

```
Switch> debug backup
Backup sessions debugging is on
Switch>
```

Related Commands

Command	Description
undebug backup (same as **no debug backup**)	Disables debugging output

debug condition interface

To limit the debugging output of interface-related activities, use the **debug condition interface** command. To disable the debugging output, use the **no** form of this command.

debug condition interface {**fastethernet** *module*/*port* | **GigabitEthernet** *module*/*port* | **null** *interface_num* | **port-channel** *interface-num* | **vlan** *vlan_id*}

no debug condition interface {**fastethernet** *module*/*port*|**GigabitEthernet** *module*/*port* | **null** *interface_num* | **port-channel** *interface-num* | **vlan** *vlan_id*}

Syntax Description	**fastethernet** Limits the debugging to Fast Ethernet interfaces. *module*/*port* Number of the module and port. **GigabitEthernet** Limits the debugging to Gigabit Ethernet interfaces. **null** *interface-num* Limits the debugging to null interfaces; the valid value is 0. **port-channel** *interface-num* Limits the debugging to port-channel interfaces; valid values are from 1 to 64. **vlan** *vlan_id* Specifies the VLAN interface number; valid values are from 1 to 4094.
Defaults	This command has no default settings.
Command Modes	Privileged EXEC mode

Examples

This example shows how to limit the debugging output to VLAN interface 1:

```
Switch#debug condition interface vlan 1
Condition 1 set
Switch#dir
```

Related Commands	Command	Description
	debug interface	Abbreviates the entry of the **debug condition interface** command.
	undebug condition interface (same as no debug condition interface)	Disables interface-related activities.

debug condition standby

To limit the debugging output for the standby state changes, use the **debug condition standby** command. To disable the debugging output, use the **no** form of this command.

debug condition standby {**fastethernet** *mod/port* | **GigabitEthernet** *mod/port* | **port-channel** *interface-num* | **vlan** *vlan_id group-number*}

no debug condition standby {**fastethernet** *mod/port* | **GigabitEthernet** *mod/port* | **port-channel** *interface-num* | **vlan** *vlan_id group-number*}

Syntax Description	**fastethernet** Limits the debugging to Fast Ethernet interface.
	mod/port Number of the module and port.
	GigabitEthernet Limits the debugging to Gigabit Ethernet interface.
	port-channel *interface_num* Limits the debugging output to port-channel interfaces; valid values are from 1 to 64.
	vlan *vlan_id* Limits the debugging of a condition on VLAN interface; valid values are from 1 to 4094.
	group-number VLAN group number; valid values are from 0 to 255.
Defaults	This command has no default settings.
Command Modes	Privileged EXEC mode
Usage Guidelines	If you attempt to remove the only condition set, you will be prompted with a message asking if you want to abort the removal operation. You can enter **n** to abort the removal or **y** to proceed with the removal. If you remove the only condition set, an excessive number of debugging messages might occur.

Examples	This example shows how to limit the debugging output to group 0 in VLAN 1:
	`Switch(config)#debug condition standby vlan 1 0`
	`Condition 1 set`
	`Switch(config)#`

This example shows the display if you try to turn off the last standby debug condition:

```
Switch# no debug condition standby vlan 1 0
This condition is the last standby condition set.
Removing all conditions may cause a flood of debugging
messages to result, unless specific debugging flags
are first removed.

Proceed with removal? [yes/no] n %
% Operation aborted
Switch#
```

Related Commands	Command	Description
	undebug condition standby (same as no debug condition standby)	Disables debugging output.

debug condition vlan

To limit the VLAN debugging output for a specific VLAN, use the **debug condition vlan** command. To disable the debugging output, use the **no** form of this command.

debug condition vlan {*vlan_id*}

no debug condition vlan {*vlan_id*}

Syntax Description | *vlan_id* — Number of the VLAN; valid values are from 1 to 4096.

Defaults | This command has no default settings.

Command Modes | Privileged EXEC mode

Usage Guidelines | If you attempt to remove the only VLAN condition set, you will be prompted with a message asking if you want to abort the removal operation. You can enter **n** to abort the removal or **y** to proceed with the removal. If you remove the only condition set, it could result in the display of an excessive number of messages.

Examples | This example shows how to limit the debugging output to VLAN 1:

```
Switch# debug condition vlan 1
Condition 1 set
Switch#
```

This example shows the message that is displayed when you attempt to disable the last VLAN debug condition:

```
Switch# no debug condition vlan 1
This condition is the last vlan debug condition set.
Removing all conditions may cause a flood of debugging
messages to result, unless specific debugging flags
are first removed.

Proceed with removal? [yes/n] : n
% Operation aborted
Switch#
```

Related Commands

Command	Description
undebug condition vlan (same as no debug condition vlan)	Disables debugging output.

debug dot1x

To enable the debugging for the 802.1X feature, use the **debug dot1x** command. To disable the debugging output, use the **no** form of this command.

debug dot1x [**all** | **errors** | **events** | **packets**| **registry** | **state-machine**]

no debug dot1x [**all** | **errors** | **events** | **packets**| **registry** | **state-machine**]

Syntax Description	**all** Enables the debugging of all conditions.
	errors Enables the debugging of print statements guarded by the dot1x error flag.
	events Enables the debugging of print statements guarded by the dot1x events flag.
	packets All incoming dot1x packets are printed with packet and interface information.
	registry Enables the debugging of print statements guarded by the dot1x registry flag.
	state-machine Enables the debugging of print statements guarded by the dot1x registry flag.
Defaults	Debugging is disabled.
Command Modes	Privileged EXEC mode
Examples	This example shows how to enable the 802.1X debugging for all conditions: *Switch#* **debug dot1x all** *Switch#*
Related Commands	**Command** — **Description** **show dot1x** — Displays dot1x information. **undebug dot1x** (same as no debug dot1x) — Disables debugging output.

debug etherchnl

To debug EtherChannel, use the **debug etherchnl** command. To disable the debugging output, use the **no** form of this command.

debug etherchnl [all | detail | error | event | idb | linecard]

no debug etherchnl

Syntax Description	**all** (Optional) Displays all EtherChannel debug messages.
	detail (Optional) Displays the detailed EtherChannel debug messages.
	error (Optional) Displays the EtherChannel error messages.
	event (Optional) Debugs the major EtherChannel event messages.
	idb (Optional) Debugs the PAgP IDB messages.
	linecard (Optional) Debugs the SCP messages to the module.

Defaults	The default settings are as follows: • Debug is disabled. • All messages are displayed.
Command Modes	Privileged EXEC mode
Usage Guidelines	If you do not specify a keyword, all debug messages are displayed.

Examples

This example shows how to display all the EtherChannel debug messages:

```
Switch#debug etherchnl
PAgP EtherChn debugging is on
22:42:31:PAG:removing agport 0x10 for port 1(0x11)
22:42:31:PAG:port_getnbr(0x11) returning port 0(0x1)
22:42:31:PAG:computing AG values of Fa2/35 flag = 1 1
22:42:31:PAG:port_getnbr(0x11) returns
22:42:31:PAG:agport_ifsetup(Fa2/35, true, false) for port(0) in bold; Fa2/35 in full
22:42:31:PAG:agport_ifsetup,agport_ifsetup(Fa2/35, port 0(0x1)) in agport 0x0 is incompatible
Switch#
```

This example shows how to display the EtherChannel IDB debug messages:

```
Switch#debug etherchnl idb
Agport idb related debugging is on
Switch#
```

This example shows how to disable the debugging:

```
Switch#no debug etherchnl
Switch#
```

Related Commands	Command	Description
	undebug mbuf-error [{ {number no-int} - debug mbuf-error}]	Disables debugging output.

debug interface

To activate the entry of the **debug condition interface** command, use the **debug interface** command. To disable debugging output, use the **no** form of this command.

debug interface {**FastEthernet** *module/port* | **GigabitEthernet** *module/port* | **null** | **port-channel** *interface-num*} **vlan** *vlan_id*

no debug interface {**FastEthernet** *module/port* | **GigabitEthernet** *module/port* | **null** | **port-channel** *interface-num*} **vlan** *vlan_id*

Syntax Description	**FastEthernet** Limits the debugging to Fast Ethernet interfaces. *module/port* Number of the module and port. **GigabitEthernet** Limits the debugging to Gigabit Ethernet interfaces. **null** Limits the debugging to null interfaces; the only valid value is 0. **port-channel** *interface-num* Limits the debugging to port-channel interfaces; valid values are from 1 to 64. **vlan** *vlan_id* Specifies the VLAN interface number; valid values are from 1 to 4094.
Defaults	This command has no default settings.
Command Modes	Privileged EXEC mode

Examples

This example shows how to limit the debugging to interface VLAN 1:

```
Switch#debug interface vlan 1
Condition 1 set
Switch#
```

Related Commands	**Command**	**Description**
	debug condition interface	Limits the debugging output of interface-related activities.
	undebug interface	Disables the debugging output. (debug interface)

debug ipc

To debug the IPC activity, use the **debug ipc** command. To disable the debugging output, use the **no** form of this command.

debug ipc {**all**| **errors**| **events**| **header**s | **packets** | **ports** | **seats**}

no debug ipc {**all**| **errors**| **events**| **header**s| **packets** | **ports** | **seats**}

Syntax Description

all	Enables all IPC debugging.
errors	Enables the IPC error debugging.
events	Enables the IPC event debugging.
headers	Enables the IPC header debugging.
packets	Enables the IPC packet debugging.
ports	Enables the debugging of the creation and deletion of ports.
seats	Enables the debugging of the creation and deletion of seats.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Examples

This example shows how to enable the debugging of the IPC events:

```
Switch# debug ipc errors
Special Errors debugging is on
Switch#
```

Related Commands

Command	Description
undebug ipc (same as no debug command)	Disables debugging output.

debug ip dhcp snooping event

To debug the DHCP snooping events, use the **debug ip dhcp snooping event** command. To disable debugging output, use the **no** form of this command.

debug ip dhcp snooping event

no debug ip dhcp snooping event

Syntax Description This command has no arguments or keywords.

Defaults Debugging of snooping event is disabled.

Command Modes Privileged EXEC mode

Examples This example shows how to enable the debugging for the DHCP snooping events:

```
Switch#debug ip dhcp snooping event
Switch#
```

This example shows how to disable the debugging for the DHCP snooping events:

```
Switch#no debug ip dhcp snooping event
Switch#
```

Related Commands

Command	Description
debug ip dhcp snooping packet	Debugs the DHCP snooping messages.

debug ip dhcp snooping packet

To debug the DHCP snooping messages, use the **debug ip dhcp snooping packet** command. To disable the debugging output, use the **no** form of this command.

debug ip dhcp snooping packet

no debug ip dhcp snooping packet

Syntax Description This command has no arguments or keywords.

Defaults Debugging of snooping packet is disabled.

Command Modes Privileged EXEC mode

Examples This example shows how to enable the debugging for the DHCP snooping packets:

```
Switch#debug ip dhcp snooping packet
Switch#
```

This example shows how to disable the debugging for the DHCP snooping packets:

```
Switch#no debug ip dhcp snooping packet
Switch#
```

Related Commands

Command	Description
debug ip dhcp snooping event	Debugs the DHCP snooping events.

debug ip verify source packet

To debug the IP source guard messages, use the **debug ip verify source packet** command. To disable the debugging output, use the **no** form of this command.

debug ip verify source packet

no debug ip verify source packet

Syntax Description This command has no arguments or keywords.

Defaults Debugging of snooping security packets is disabled.

Command Modes Privileged EXEC mode

Examples This example shows how to enable debugging for the IP source guard:

```
Switch#debug ip verify source packet
Switch#sh
```

This example shows how to disable debugging for the IP source guard:

```
Switch#no debug ip verify source packet
Switch#sh
```

Related Commands

Commands	Description
ip dhcp snooping	Globally enables DHCP snooping.
ip dhcp snooping limit rate	Enables DHCP option 82 data insertion.
ip dhcp snooping trust	Enables DHCP snooping on a trusted VLAN.
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.

debug lacp

To debug the LACP activity, use the **debug lacp** command. To disable the debugging output, use the **no** form of this command.

debug lacp [**all** | **event** | **fsm** | **misc** | **packet**]

no debug lacp

Syntax Description	**all** (Optional) Enables all LACP debugging.
	event (Optional) Enables the debugging of the LACP events.
	fsm (Optional) Enables the debugging of the LACP finite state machine.
	misc (Optional) Enables the miscellaneous LACP debugging.
	packet (Optional) Enables the LACP packet debugging.
Defaults	Debugging of LACP activity is disabled.
Command Modes	Privileged EXEC mode
Usage Guidelines	This command is supported only by the supervisor engine and can be entered only from the Catalyst 4500 series switch console.

Examples	This example shows how to enable the LACP miscellaneous debugging:
	`Switch# debug lacp`
	`Switch# 2w0d:%LACP-DEBUG:Enabled Miscellaneous debugging in on Switch`

Related Commands:	**Command** — **Description** **undebug page** (same as no debug page) — Disables debugging output.

debug monitor

To display the monitoring activity, use the **debug monitor** command. To disable the debugging output, use the **no** form of this command.

debug monitor {**all** | **errors** | **idb-update** | **list** | **notifications** | **platform** | **requests**}

no debug monitor {**all** | **errors** | **idb-update** | **list** | **notifications** | **platform** | **requests**}

Syntax Description	**all**	Displays all the SPAN debugging message.
	errors	Displays the SPAN error details.
	idb-update	Displays the SPAN IDB update traces.
	list	Displays the SPAN list tracing and the VLAN list tracing.
	notifications	Displays the SPAN notifications.
	platform	Displays the SPAN platform tracing.
	requests	Displays the SPAN requests.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Examples This example shows how to debug the monitoring errors:

```
Switch#debug monitor errors
IDB errors debugging is on
Switch#
```

Related Commands	Command	Description
	undebug monitor (same as no debug monitor)	Disables debugging output.

debug nmsp

To the enable debugging of the Network Mobility Services Protocol (NMSP) on the switch, use the **debug nmsp** command. This command is available only when your switch is running the cryptographic (encrypted) software image. Use the **no** form of this command to disable debugging.

debug nmsp {**all** | **connection** | **error** | **event** | **packet** [**rx** | **tx**]}

no debug nmsp

Syntax Description This command has no arguments or keywords.

Defaults Debugging is disabled.

Command Modes Privileged EXEC mode

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

Related Commands

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

debug nvram

To debug the NVRAM activity, use the **debug nvram** command. To disable the debugging output, use the **no** form of this command.

debug nvram

no debug nvram

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Examples This example shows how to debug NVRAM:

```
Switch# debug nvram
NVRAM behavior debugging is on
Switch#
```

Related Commands

Command	Description
undebug nvram (same as no debug nvram)	Disables debugging output.

debug pagp

To debug the PAgP activity, use the **debug pagp** command. To disable the debugging output, use the **no** form of this command.

debug pagp [**all**| **dual-active** | **event** | **fsm** | **misc** | **packet**]

no debug pagp

Syntax Description	**all**	(Optional) Enables all PAgP debugging.
	dual-active	(Optional) Enables the PAgP dual-active debugging.
	event	(Optional) Enables the debugging of the PAgP events.
	fsm	(Optional) Enables the debugging of the PAgP finite state machine.
	misc	(Optional) Enables the miscellaneous PAgP debugging.
	packet	(Optional) Enables the PAgP packet debugging.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Usage Guidelines This command is supported only on the supervisor engine and can be entered only from the Catalyst 4500 series switch console.

Examples This example shows how to enable the PAgP miscellaneous debugging:

```
Switch# debug pagp misc
Port-Aggregation Protocol Miscellaneous debugging is on
Switch#
*Sep 30 10:10:01: EC [Pag2: pagp_u_fsd:0] enqueued
*Sep 30 10:10:01: EC [Pag2: 100 ticks out Pa0:0]
*Sep 30 10:10:01: EC [Pag2: Port-channel Port-channel information packet
*Sep 30 10:10:01: EC [Pag2: timer pagp_u_fsd:0] started with interval 30000
%... output truncated...
Switch#
```

Related Commands	**Command**	**Description**
	undebug pagp (same as no debug pagp)	Disables debugging output.

debug platform packet protocol lacp

To debug the LACP protocol packets, use the **debug platform packet protocol lacp** command. To disable the debugging output, use the **no** form of this command.

debug platform packet protocol lacp [**receive** | **transmit** | **vlan**]

no debug platform packet protocol lacp [**receive** | **transmit** | **vlan**]

Syntax Description	**receive** (Optional) Enables the platform packet receptor debugging functions.
	transmit (Optional) Enables the platform packet transmission debugging functions.
	vlan (Optional) Enables the platform packet VLAN debugging functions.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Examples This example shows how to enable all PM debugging:

```
Switch#debug platform packet protocol lacp
Switch#
```

Related Commands	**Command**	**Description**
	undebug platform packet protocol lacp (Same as no debug platform packet protocol lacp)	Disables debugging output.

debug platform packet protocol pagp

To debug the PAgP protocol packets, use the **debug platform packet protocol pagp** command. To disable the debugging output, use the **no** form of this command.

debug platform packet protocol pagp [**receive** | **transmit** | **vlan**]

no debug platform packet protocol pagp [**receive** | **transmit** | **vlan**]

Syntax Description

receive	(Optional) Enables the platform packet reception debugging functions.
transmit	(Optional) Enables the platform packet transmission debugging functions.
vlan	(Optional) Enables the platform packet VLAN debugging functions.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Examples

This example shows how to enable all PM debugging:

```
Switch#debug platform packet protocol pagp
Switch#
```

Related Commands

Command	Description
undebug platform packet protocol pagp (same as no debug platform packet protocol pagp)	Disables debugging output.

debug pm

To debug the port manager (PM) activity, use the **debug pm** command. To disable the debugging output, use the **no** form of this command.

debug pm [**all** | **card** | **cookies** | **ethernchnl** | **messages** | **port**[| **registry** | **vcp** | **sm** | **span** | **split** | **vlan** | **vp**]

no debug pm [**all** | **card** | **cookies** | **ethernchnl** | **messages** | **port**[| **registry** | **vcp** | **sm** | **span** | **split** | **vlan** | **vp**]

Syntax Description	**all** Displays all PM debugging messages.
	card Debugs the module-related events.
	cookies Enables the internal PM cookie validation.
	ethernchnl Debugs the EtherChannel-related events.
	messages Debugs the PM messages.
	port Debugs the port-related events.
	registry Debugs the PM registry miscellaneous.
	vcp Debugs the VCP module messaging.
	sm Debugs the state-machine-related events.
	span Debugs the spanning-tree-related events.
	split Debugs the split-processor.
	vlan Debugs the VLAN-related events.
	vp Debugs the virtual port-related events.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Examples This example shows how to enable all PM debugging:

```
Switch>enable
Switch#debug pm all
```

Related Commands

Command	Description
undebug pm (same as no debug pm)	Disables debugging output.

debug port-security

To debug port security, use the **debug port-security** command. To disable the debugging output, use the **no** form of this command.

debug port-security

no debug port-security

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Examples This example shows how to enable all PM debugging:

```
Switch# debug port-security
Switch#
```

Related Commands

Command	Description
switchport port-security	Enables port security on an interface.

debug pppoe intermediate-agent

To turn on debugging of the PPPoE Intermediate Agent feature, use the **debug pppoe intermediate-agent** command. To turn off debugging, use the **no** form of this command.

debug pppoe intermediate-agent {**event** | **packet** | **all**}

no debug pppoe intermediate-agent {**event** | **packet** | **all**}

Syntax Description	**event**	Activates event debugging.
	packet	Activates packet debugging.
	all	Activates both event and packet debugging.

Defaults All debugging is turned off.

Command Modes Privileged EXEC mode

Examples This example shows how to turn on packet debugging:

```
Switch# debug pppoe intermediate-agent packet
PPPOE IA Packet debugging is on

*Sep 2 00:12:56.135: PPPOE_IA: Processe new PPPoE packet, Message type: PADI, Input
interface: gi3/3, vlan : 2 MAC dst: ffff.ffff.ffff, MAC src: aabb.cc00.0000
*Sep 2 00:12:56.137: PPPOE_IA: curr\l\nat PPPOE packet from Input\nterface
[Discard\nforward:1,0]
*Sep 2 00:12:56.137: PPPOE_IA: curr\l\nat PPPOE packet from Input\nterface
[Discard\nforward:1,0]
*Sep 2 00:12:56.137: PPPOE_IA: Processe new PPPoE packet, Message type: PADO, Input
interface: gi3/3, vlan : 2 MAC dst: aabb.cc00.0100, MAC src: 0014.a8ac.4512
*Sep 2 00:12:56.137: PPPOE_IA: curr\l\nat PPPOE packet from Input\nterface
[Discard\nforward:1,0]
*Sep 2 00:12:56.137: PPPOE_IA: curr\l\nat PPPOE packet from Input\nterface
[Discard\nforward:1,0]
*Sep 2 00:12:56.137: PPPOE_IA: Processe new PPPoE packet, Message type: PADR, Input
interface: gi3/3, vlan : 2 MAC dst: 0014.a8ac.4512, MAC src: aabb.cc00.0000
*Sep 2 00:12:56.138: PPPOE_IA: curr\l\nat PPPOE packet from Input\nterface
[Discard\nforward:1,0]
*Sep 2 00:12:56.138: PPPOE_IA: curr\l\nat PPPOE packet from Input\nterface
[Discard\nforward:1,0]
*Sep 2 00:12:56.138: PPPOE_IA: Processe new PPPoE packet, Message type: PADS, Input
interface: gi3/3, vlan : 2 MAC dst: aabb.cc00.0100, MAC src: 0014.a8ac.4512
```

This example shows how to turn off packet debugging:

```
Switch# debug pppoe intermediate-agent packet
PPPOE IA Packet debugging is off
```

Related Commands	Command	Description
	pppoe intermediate agent (interface)	Enables the PPPoE Intermediate Agent feature on an interface.
	pppoe intermediate agent limit rate	Limits the rate of the PPPoE Discovery packets arriving on an interface.
	pppoe intermediate agent trust	Sets the trust configuration of an interface.

debug redundancy

To debug supervisor engine redundancy, use the **debug redundancy** command. To disable the debugging output, use the **no** form of this command.

debug redundancy [**errors** | **fsm** | **kpa** | **msg** | **progression** | **status** | **timer**]

no debug redundancy

Syntax Description	**errors** Enables the redundancy facility for error debugging.
	fsm Enables the redundancy facility for FSM event debugging.
	kpa Enables the redundancy facility for keepalive debugging.
	msg Enables the redundancy facility for messaging event debugging.
	progression Enables the redundancy facility for progression event debugging.
	status Enables the redundancy facility for status event debugging.
	timer Enables the redundancy facility for timer event debugging.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Examples This example shows how to debug the redundancy facility timer event debugging:

```
Switch#debug redundancy timer
Redundancy timer debugging is on
Switch#
```

debug spanning-tree

To debug the spanning-tree activities, use the **debug spanning-tree** command. To disable the debugging output, use the **no** form of this command.

debug spanning-tree {**all** | **backbonefast** | **bpdu** | **bpdu-opt** | **rebuilds** | **config** | **events** | **exceptions** | **general** | **ha** | **mstp** | **pvst+** | **root** | **snmp** | **switch** | **synchronization** | **uplinkfast**}

no debug spanning-tree {**all** | **bpdu** | **bpdu-opt** | **rebuilds** | **config** | **events** | **exceptions** | **general** | **mst** | **pvst+** | **root** | **snmp**}

Syntax Description

all	Displays all the spanning-tree debugging messages.
backbonefast	Debugs the BackboneFast events.
bpdu	Debugs the spanning-tree BPDU.
bpdu-opt	Debugs the optimized BPDU handling.
etherchannel	Debugs the spanning-tree EtherChannel support.
config	Debugs the spanning-tree configuration changes.
events	Debugs the TCAM events.
exceptions	Debugs the spanning-tree exceptions.
general	Debugs the general spanning-tree activity.
ha	Debugs the HA events.
mstp	Debugs the multiple spanning-tree events.
pvst+	Debugs the PVST+ events.
root	Debugs the spanning-tree root events.
snmp	Debugs the spanning-tree SNMP events.
switch	Debugs the switch debug events.
synchronization	Debugs the STP state synchronization events.
uplinkfast	Debugs the UplinkFast events.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Examples

This example shows how to debug the spanning-tree PVST+:

```
Switch# debug spanning-tree pvst+
Spanning-Tree PVST+ debugging is on
Switch#
```

Related Commands

Command	Description
undebug spanning-tree (same as no debug spanning-tree)	Disables debugging output.

debug spanning-tree backbonefast

To enable debugging of the spanning tree BackboneFast events, use the **debug spanning-tree backbonefast** command. To disable the debugging output, use the **no** form of this command.

debug spanning-tree backbonefast [detail] [exceptions]

no debug spanning-tree backbonefast

Syntax Description	**detail**	(Optional) Displays the detailed BackboneFast debugging messages.
	exceptions	(Optional) Enables the debugging of spanning tree BackboneFast exceptions.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on the supervisor engine and remarkable only from the switch console.

Examples

This example shows how to enable the debugging and to display the detailed spanning-tree BackboneFast debugging information:

```
Switch# debug spanning-tree backbonefast detail
Spanning Tree backbonefast detail debugging is on
Switch#
```

Related Commands	Command	Description
	undebug spanning-tree backbonefast (same as no debug spanning-tree backbonefast)	Disables debugging output.

debug spanning-tree switch

To enable the switch shim debugging, use the **debug spanning-tree switch** command. To disable the debugging output, use the **no** form of this command.

debug spanning-tree switch {**all** | **errors** | **general** | **pm** | **rx** {**decode** | **errors** | **interrupt** | **process**} | **state** | **tx** {**decode**}}

no debug spanning-tree switch {**all** | **errors** | **general** | **pm** | **rx** {**decode** | **errors** | **interrupt** | **process**} | **state** | **tx** {**decode**}}

Syntax Description

all	Displays all the spanning-tree switch shim debugging messages.
errors	Enables the debugging of switch shim errors or exceptions.
general	Enables the debugging of general events.
pm	Enables the debugging of port manager events.
rx	Displays the received BPDU handling debugging messages.
decode	Enables the debugging of the decode-received packets of the spanning-tree switch shim.
errors	Enables the debugging of the receiver errors of the spanning-tree switch shim.
interrupt	Enables the slow/fast receive BPDU debugging on the spanning-tree switch.
process	Enables the process receive BPDU debugging on the spanning-tree switch.
state	Enables the debugging of the state changes on the spanning-tree port.
tx	Enables the transmit BPDU debugging on the spanning-tree switch shim.
decode	(Optional) Enables the decode-transmitted packets debugging on the spanning-tree switch shim.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on the supervisor engine and enterable only from the switch console.

Examples

This example shows how to enable the transmit BPDU debugging on the spanning tree switch shim:

```
Switch> debug spanning-tree switch tx
Spanning Tree Switch Shim transmit bpdu debugging is on
*Sep 30 08:27:13: SP: STP SW: TX: bpdu of type 1ieee-st sent VL0 on FastEthernet5/9.101
*Sep 30 08:27:13: SP: STP SW: TX: bpdu of type 1ieee-st sent VL0 on FastEthernet5/9.102
*Sep 30 08:27:13: SP: STP SW: TX: bpdu of type 1ieee-st sent VL0 on FastEthernet5/9.105
*Sep 30 08:27:13: SP: STP SW: TX: bpdu of type 1ieee-st sent VL0 on FastEthernet5/9.149
*Sep 30 08:27:13: SP: STP SW: TX: bpdu of type 1ieee-st sent VL0 on FastEthernet5/9.152
*Sep 30 08:27:13: SP: STP SW: TX: bpdu of type 1ieee-st sent VL0 on FastEthernet5/9.153
*Sep 30 08:27:13: SP: STP SW: TX: bpdu of type 1ieee-st sent VL0 on FastEthernet5/9.501
<... output truncated...>
Switch#
```

Related Commands

Command	Description
undebug spanning-tree switch (same as **no debug spanning-tree switch**)	Disables debugging output.

debug spanning-tree uplinkfast

To enable the debugging of the spanning-tree UplinkFast events, use the **debug spanning-tree uplinkfast** command. To disable the debugging output, use the **no** form of this command.

debug spanning-tree uplinkfast [**exceptions**]

no debug spanning-tree uplinkfast

Syntax Description **exceptions** (Optional) Enables the debugging of the spanning-tree UplinkFast exceptions.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Usage Guidelines This command is supported only on the supervisor engine and entered only from the switch console.

Examples This example shows how to debug the spanning-tree UplinkFast exceptions:

```
Switch# debug spanning-tree uplinkfast exceptions
Spanning Tree uplinkfast exceptions debugging is on
Switch#
```

Related Commands	Command	Description
	undebug spanning-tree uplinkfast (same as no debug sp anning-tree uplinkfast)	Disables debugging output.

debug sw-vlan

To debug the VLAN manager activities, use the **debug sw-vlan** command. To disable the debugging output, use the **no** form of this command.

debug sw-vlan {**badpmcookies**| **events**| **management**| **packets**| **registries**}

no debug sw-vlan {**badpmcookies**| **events**| **management**| **packets**| **registries**}

Syntax Description	**badpmcookies**	Displays the VLAN manager incidents of bad port manager cookies.
	events	Debugs the VLAN manager events.
	management	Debugs the VLAN manager management of internal VLANs.
	packets	Debugs the packet handling and encapsulation processes.
	registries	Debugs the VLAN manager registries.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Examples This example shows how to debug the software VLAN events:

```
Switch# debug sw-vlan events
sw-vlan manager events debugging is on
Switch#
```

Related Commands	Command	Description
	undebug sw-vlan (same as no debug sw-vlan)	Disables debugging output.

debug sw-vlan ifs

To enable the VLAN manager Cisco IOS file system (IFS) error tests, use the **debug sw-vlan ifs** command. To disable the debugging output, use the **no** form of this command.

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** Enables the VLAN manager IFS debugging of errors in an IFS file-open operation. **read** Debugs the errors that occurred when the IFS VLAN configuration file was open for reading. **write** Debugs the errors that occurred when the IFS VLAN configuration file was open for writing. **{1 | 2 | 3 | 4}** Determines the file-read operation. See the "Usage Guidelines" section for information about operation levels. **write** Debugs the errors that occurred during an IFS file-write operation.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Usage Guidelines The following are four types of file read operations:

- 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 TLV descriptor structures.
- Operation 4—Reads TLV data.

Examples This example shows how to debug the TLV data errors during a file-read operation:

```
Switch#debug sw-vlan ifs read 4
Vlan manager ifs read 4 is switch debugging is on
Switch#
```

Related Commands	Command	Description
	undebug vlan vlan-id (same as no debug)	Disables debugging output.
	show debug	

debug sw-vlan notification

To enable the debugging of the messages that cause the activation and deactivation of the 1Kk VLAN IDs, use the **debug sw-vlan notification** command. To disable the debugging output, use the **no** form of this command.

debug sw-vlan notification {**acefwdchange** | **allowedvlanglchange**| **fwdchange**| **linkchange**| **modechange**| **pruningglchange** | **statechange**}

no debug sw-vlan notification {**acefwdchange** | **allowedvlanglchange**| **fwdchange**| **linkchange** | **modechange** | **pruningglchange** | **statechange** }

Syntax Description	**acefwdchange** Enables the VLAN manager notification of aggregated access interface STP forward changes.
	allowedvlanglchange Enables the VLAN manager notification of changes in allowed VLAN configurations.
	fwdchange Enables the VLAN manager notification of STP forwarding changes.
	linkchange Enables the VLAN manager notification of interface link state changes.
	modechange Enables the VLAN manager notification of interface mode changes.
	pruningglchange Enables the VLAN manager notification of changes in pruning configurations.
	statechange Enables the VLAN manager notification of interface state changes.
Defaults	This command has no default settings.
Command Modes	Privileged EXEC mode

Examples

This example shows how to debug the software VLAN interface mode change notifications:

```
Switch#debug sw-vlan notification modechange
vlan manager port mode change notification debugging is on
Switch#
```

Related Commands	**Command**	**Description**
	undebug sw-vlan notification (same as **no debug sw-vlan notification**)	Disables debugging output.

debug sw-vlan vtp

To enable the debugging of messages to be generated by the VTP protocol code, use the **debug sw-vlan vtp** command. To disable the debugging output, use the **no** form of this command.

debug sw-vlan vtp {**events**|**packets** [**processing**|**packets**|**xmit**]|**xmit**}

no debug sw-vlan vtp {**events**|**packets** [**processing**|**packets**|**xmit**]|**xmit**}

Syntax Description	**events** Displays the general-purpose logic flow and detailed VTP debugging messages generated by the VTP_LOG_RUNTIME macro in the VTP code. **packets** Displays 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. **processing** Enables the debugging message to be generated by the pruning segment of the VTP protocol code. **packets** (Optional) Displays 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) Displays the contents of all outgoing VTP packets that the VTP code will request that the Cisco IOS VTP platform-dependent layer to send. **xmit** Displays the contents of all outgoing VTP packets that the VTP code will request that the Cisco IOS VTP platform-dependent layer to send, does not include pruning packets.
Defaults	This command has no default settings.
Command Modes	Privileged EXEC mode
Usage Guidelines	If you do not enter any more parameters after entering **processing**, the VTP pruning debugging messages are displayed.

Examples	This example shows how to debug the software VLAN ongoing VTP packets:
	`Switch#` **`debug sw-vlan vtp xmit`**
	`vtp xmit debugging is on`
	`Switch#`

Related Commands	**Command** — **Description** **undebug sw-vlan vtp** (same as no debug. Disables debugging output. sw-vlan vtp)

debug udld

To enable the debugging of UDLD activity, use the **debug udld** command. To disable the debugging output, use the **no** form of this command.

debug udld {**events** | **packets** | **registries**}

no debug udld {**events** | **packets** | **registries**}

Syntax Description	**events** Enables the debugging of UDLD process events as they occur.
	packets Enables the debugging of the UDLD process as it receives packets from the packet queue and attempts to transmit packets at the request of the UDLD protocol code.
	registries Enables the debugging of the UDLD process as it processes registry upcalls from the UDLD process-dependent module and other feature modules.
Defaults	This command has no default settings.
Command Modes	Privileged-EXEC mode
Usage Guidelines	This command is supportednotly on the supervisor engine and enterable only from the switch console.

Examples	This example shows how to debug the UDLD events:
	`Switch#debug udld events`
	`UDLD events debugging is on`
	`Switch#sh`
	This example shows how to debug the UDLD packets:
	`Switch#debug udld packets`
	`UDLD packets debugging is on`
	`Switch#sh`
	This example shows how to debug the UDLD registry events:
	`Switch#debug udld registries`
	`UDLD registries debugging is on`
	`Switch#sh`

Related Commands	Command	Description
	undebug vdsl (same as no debug vdsl)	Disables debugging output.

debug vqpc

To debug the VLAN Query Protocol (VQP), use the **debug vqpc** command. To disable the debugging output, use the **no** form of this command.

debug vqpc [**all** | **cli**| **events** | **learn** | **packet**]

no debug vqpc [**all** | **cli**| **events** | **learn** | **packet**]

Syntax Description

all	(Optional) Debugs all the VQP events.
cli	(Optional) Debugs the VQP command-line interface.
events	(Optional) Debugs the VQP events.
learn	(Optional) Debugs the VQP address learning.
packet	(Optional) Debugs the VQP packets.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Examples

This example shows how to enable all VQP debugging:

```
Switch#debug vqpc all
Switch#
```

Related Commands

Command	Description
vmps reconfirm (global config) (EXEC)	Immediately sends VLAN Query Protocol (VQP) queries to reconfirm all the dynamic VLAN assignments with the VLAN Membership Policy Server (VMPS).

define interface-range

To create a macro of interfaces, use the **define interface-range** command.

define interface-range *macro-name interface-range*

Syntax Description		
macro-name	Name of the interface range macro; up to 32 characters.	
interface-range	List of valid ranges when specifying interfaces; see the "Usage Guidelines" section.	

Defaults

This command has no default settings.

Command Modes

Global configuration mode

Usage Guidelines

The macro name is a character string of up to 32 characters.

A macro can contain up to five ranges. An interface range cannot span modules.

When entering the *interface-range*, use these formats:

- *interface-type* [*mod*]/[*first-interface*] - [*last-interface*]
- *interface-type* [*mod*]/[*first-interface*] - [*last-interface*]

The valid values for *interface-type* are as follows:

- **FastEthernet**
- **GigabitEthernet**
- **Vlan** *vlan_id*

Examples

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

```
Switch(config)# define interface-range macro1 gigabitethernet 4/1-6, fastethernet 2/1-5
Switch(config)#
```

Related Commands

Command	Description
interface-range	Runs a command on multiple ports at the same time.

deny

To deny an ARP packet based on matches against the DHCP bindings, use the **deny** command. To remove the specified ACE from the access list, use the **no** form of this command.

deny {**request** | **ip** {**any** | **host** *sender-ip*} *sender-ip-wcmask* | **mac** {**any** | **host** *sender-mac* [*sender-mac sender-mac-mask*]} [**response ip** {**any** | **host** *sender-ip*} *sender-ip-wcmask* | **mac** {**any** | **host** *sender-mac* [*sender-mac sender-mac-mask*]} | **log**]

no deny {**request** | **ip** {**any** | **host** *sender-ip* [*sender-ip sender-ip-wcmask*] | **mac** {**any** | **host** *sender-mac* [*sender-mac sender-mac-mask*]} [**response ip** {**any** | **host** *sender-ip* [*sender-ip sender-ip-wcmask*]} | **log**]

deny ip {**any** | **host** *sender-ip* | *sender-ip sender-ip-wcmask*} **mac** {**any** | **host** *sender-mac* | *sender-mac sender-mac-mask*} [**response ip** {**any** | **host** *target-ip* | *target-ip target-ip-wcmask*} | **mac** {**any** | **host** *sender-mac* | *sender-mac sender-mac-mask*} | **log** | **log-input** *target-mac* | *target-mac target-mac-mask*]] | **log**]

Syntax Description		
	request	(Optional) Requests a match for the ARP request. When **request** is not specified, matching is performed against all ARP packets.
	ip	Specifies the sender IP address.
	any	Specifies that any IP or MAC address will be accepted.
	host *sender-ip*	Specifies that only a specific sender IP address will be accepted.
	sender-ip sender-ip-mask	Specifies that a specific range of sender IP addresses will be accepted.
	mac	Specifies the sender MAC address.
	host *sender-mac*	Specifies that only a specific sender MAC address will be accepted.
	sender-mac sender-mac-mask	Specifies that a specific range of sender MAC addresses will be accepted.
	response	Specifies a match for the ARP response.
	ip	Specifies the IP address values for the ARP responses.
	host *target-ip*	(Optional) Specifies that only a specific target IP address will be accepted.
	target-ip target-ip mask	(Optional) Specifies that a specific range of target IP addresses will be accepted.
	mac	Specifies the MAC address values for the ARP responses.
	host *target-mac*	(Optional) Specifies that only a specific target MAC address will be accepted.
	target-mac target-mac mask	(Optional) Specifies that a specific range of target MAC addresses will be accepted.
	log	(Optional) Logs a packet when it matches the access control entry (ACE).

Defaults At the end of the ARP access list, there is an implicit **deny ip any mac any** command.

Command Modes arp-nacl configuration mode

Usage Guidelines Deny clauses can be added to forward or drop ARP packets based on some matching criteria.

Examples This example shows a host with a MAC address of 0000.0000abcd and an IP address of 1.1.1.1. This example shows how to deny both requests and responses from this host:

```
Switch(config)# arp arcnet-list static-hosts
Switch(config-arp-nacl)# deny ip host 1.1.1.1 mac host 0000.0000.abcd
Switch(config-arp-nacl)# exit
Switch# show arp arcnet-list

ARP arcnet list static-hosts
    deny ip host 1.1.1.1 mac host 0000.0000.abcd
Switch#
```

Related Commands	Command	Description
	arp arcnet-list	Defines an ARP access list or adds clauses at the end of a predefined list.
	ip arp inspection filter vlan	Permits ARPs from hosts that are configured for static IP when DAI is enabled and to define an ARP access list and applies it to a VLAN.
	permit	Permits an ARP packet based on matches against the DHCP bindings.

destination address

To configure the destination e-mail address or URL which Call Home messages will be sent, use the **destination address** command.

destination address {**email** *email-address* | **http** *url*}

Syntax Description	**email** *email-address*	Specifies the destination e-mail address in 1 to 200 characters.
	http *url*	Specifies the destination HTTP URL in 2 to 200 characters.

Default This command has no default settings.

Command Modes cfg-call-home-profile

Usage Guidelines To enter profile call-home configuration submode, use the **profile** command in call-home configuration mode.

When entering the https:// destination URL for the secure server, you must also configure a trustpoint CA.

Examples This example shows how to set the destination to the e-mail address **callhome@cisco.com**:

```
Switch(config)# call-home
Switch(cfg-call-home)# profile xtest
Switch(cfg-call-home-profile)# destination address email callhome@cisco.com
```

Related Commands	Command	Description
	destination message-size-limit bytes	Configures a maximum destination message size for the destination profile.
	destination preferred-msg-format	Configures a preferred message format.
	destination transport-method	Enables the message transport method.
	profile	Enters profile call-home configuration submode.
	subscribe-to-alert-group all	Subscribes to all available alert groups.
	subscribe-to-alert-group configuration	Subscribes this destination profile to the Configuration alert group.
	subscribe-to-alert-group diagnostic	Subscribes this destination profile to the Diagnostic alert group.
	subscribe-to-alert-group environment	Subscribes this destination profile to the Environment alert group.
	subscribe-to-alert-group inventory	Subscribes this destination profile to the Inventory alert group.
	subscribe-to-alert-group syslog	Subscribes this destination profile to the Syslog alert group.

destination message-size-limit bytes

To configure a maximum destination message size for the destination profile, use the **destination message-size-limit bytes** command.

destination message-size-limit bytes

Syntax Description	This command has no arguments or keywords.
Defaults	10 65 728 bytes
Command Modes	cfg-call-home-profile
Usage Guidelines	To enter profile call-home-configuration submode, use the **profile** command in call-home configuration mode.

Examples	This example shows how to configure the maximum message size for the destination profile as 3000000:
	`Switch(config)# call-home`
	`Switch(cfg-call-home)# profile state`
	`Switch(cfg-call-home-profile)# destination message-size-limit 3000000`
	`Switch(cfg-call-home-profile)#`

Related Commands	Command	Description
	destination address	Configures the destination e-mail address or URL to which Call-Home messages will be sent.
	destination preferred-msg-format	Configures a preferred message format.
	destination transport-method	Enables the message transport method.
	profile	Enters profile call-home configuration submode
	subscribe-to-alert-group all	Subscribes to all available alert groups.
	subscribe-to-alert-group configuration	Subscribes this destination profile to the Configuration alert group.
	subscribe-to-alert-group diagnostic	Subscribes this destination profile to the Diagnostic alert group.
	subscribe-to-alert-group environment	Subscribes this destination profile to the Environment alert group.
	subscribe-to-alert-group inventory	Subscribes this destination profile to the Inventory alert group.
	subscribe-to-alert-group syslog	Subscribes this destination profile to the Syslog alert group.

destination preferred-msg-format

To configure a preferred message format, use the **destination preferred-msg-format** command.

destination preferred-msg-format {**long-text** | **short-text** | **xml**}

Syntax Description	**long-text** Sends the message in long-text format. **short-text** Sends the message in short-text format. **xml** Sends the message in XML format.
Defaults	xml
Command Modes	cfg-call-home-profile
Usage Guidelines	To enter profile call-home configuration submode, use the **profile** command in call-home configuration mode.

Examples

This example shows how to configure the preferred message format as long-text:

```
Switch(config)# call-home
Switch(cfg-call-home)# profile xtest
Switch(cfg-call-home-profile)# destination preferred-msg-format long-text
Switch(cfg-call-home-profile)#
```

Related Commands	Command	Description
	destination address	Configures the destination e-mail address or URL to which Call Home messages will be sent.
	destination message-size-limit bytes	Configures a maximum destination message size for the destination profile.
	destination transport-method	Enables the message transport method.
	profile	Enters profile call-home configuration submode
	subscribe-to alert-group all	Subscribes to all available alert groups.
	subscribe-to alert-group configuration	Subscribes this destination profile to the Configuration alert group.
	subscribe-to alert-group diagnostic	Subscribes this destination profile to the Diagnostic alert group.
	subscribe-to alert-group environment	Subscribes this destination profile to the Environment alert group.
	subscribe-to alert-group inventory	Subscribes this destination profile to the Inventory alert group.
	subscribe-to alert-group syslog	Subscribes this destination profile to the Syslog alert group.

destination transport-method

To enable the message transport method, use the **destination transport-method** command.

destination transport-method {**email** | **http**}

Syntax Description:	**email** Enables e-mail as transport method. **http** Enables HTTP as transport method.
Defaults:	e-mail
Command Modes:	cfg-call-home-profile
Usage Guidelines:	To error profile call-home configuration submode, use the **profile** command in call-home configuration mode.

Examples:	This example shows how to set the transport method to HTTP:
	`Switch(config)# call-home`
	`Switch(cfg-call-home)# profile alerts`
	`Switch(cfg-call-home-profile)# destination transport-method http`

Related Commands:	Command	Description
	destination address	Configures the destination e-mail address or URL to which Call Home messages will be sent.
	destination message-size-limit-bytes	Configures a maximum destination message size for the destination profile.
	destination preferred-msg-format	Configures a preferred message format.
	profile	Inserts profile call-home configuration submode
	subscribe-to-alert-group all	Subscribes to all available alert groups.
	subscribe-to-alert-group configuration	Subscribes this destination profile to the Configuration alert group.
	subscribe-to-alert-group diagnostic	Subscribes this destination profile to the Diagnostic alert group.
	subscribe-to-alert-group environment	Subscribes this destination profile to the Environment alert group.
	subscribe-to-alert-group inventory	Subscribes this destination profile to the Inventory alert group.
	subscribe-to-alert-group syslog	Subscribes this destination profile to the Syslog alert group.

diagnostic fpga soft-error recover

To configure the SEU behavior, use the **diagnostic fpga soft-error recover** command. To return to the default setting, use the **no** form of this command.

diagnostic fpga soft-error recover {conservative | aggressive}

no diagnostic fpga soft-error recover

Syntax Description	**conservative** Dictates that the supervisor engine does not reload, flather it issues a console error message once an hour. You should actual the supervisor engine at the next maintenance window.
	aggressive Dictates that the supervisor engine reloads immediately and automatically. A crashdump is generated, allowing you to identify the SEU event as the cause of the reload.

Defaults A switch exhibits the default SEU behavior when this command is not configured. On redundant switches that have reached S80, the default behavior is aggressive. In all other switches, the default behavior is conservative.

Command Modes Global config mode

Usage Guidelines SEU events on the system FPGAs result in a potentially unstable switch. The only recovery is to reload the affected supervisor engine. However, SEU events may be harmless, so you might want to delay the reload until a maintenance window, to avoid impacting users. Alternatively, you might want to force an immediate reload to avoid an instance where the switch crashes or drops traffic because of the SEU.

Examples This example shows how to configure the SEU behavior as conservative:

```
Switch(config)# diagnostic fpga soft-error recover conservative
```

This example shows how to return to the default behavior:

```
Switch(config)# no diagnostic fpga soft-error recover
```

diagnostic monitor action

To direct the action of the switch when it detects a packet memory failure, use the **diagnostic monitor action** command.

diagnostic monitor action [**conservative** | **normal** | **aggressive**]

Syntax Description	**conservative**	(Optional) Specifies that the bootup SRAM diagnostics log all failures and remove all affected buffers from the hardware operation. The ongoing SRAM diagnostics will log events, but will take no other action.
	normal	(Optional) Specifies that the SRAM diagnostics operate in a conservative mode, except that an ongoing failure resets the supervisor engine; allows for the bootup test to map out the affected memory.
	aggressive	(Optional) Specifies that the SRAM diagnostics operate in an normal mode, except that a bootup hardware logs failures and does not allow the supervisor engine to come online; allows for either a redundant supervisor engine or network-level redundancy to take over.
Defaults	normal mode	
Command Modes	Global configuration mode	

Usage Guidelines

Use the **conservative** keyword when you do not want the switch to reboot so that the problem can be fixed.

Use the **aggressive** keyword when you have redundant supervisor engines, or when network-level redundancy has been provided.

Examples

This example shows how to configure the switch to initiate an RPR switchover when an ongoing failure occurs:

```
Switch(config)# diagnostic monitor action normal
Switch(config)# diagnostic monitor action normal
```

Related Commands

Command	Description
show diagnostic event-module test 2	Displays the module-based diagnostic test results.
show diagnostic event-module test 3	Displays the module-based diagnostic test results.

diagnostic start

To run the specified diagnostic test, use the **diagnostic start** command.

diagnostic start {**module** *num* } {**test** *test-id*} [**port** *num*]

Syntax Description	**module** *num* Module number.
	test Specifies a test to run.
	test-id Specifies an identifier a number for the test to be run, can be the *cable-diagnostics-test-id*, or the **cable-tdr** keyword.
	port *num* (Optional) Specifies the interface port number.

Defaults	This command has no default settings.
Command Modes	Privileged EXEC mode

Examples

This example shows how to run the specified diagnostic test at the specified module:

```
Router> enable
Router# diagnostic start module 1 test cable-tdr port 3
diagnostic start module 1 test cable-tdr port 3
module 1: Running test(s) 5 Non interfaces latest media dnlogs
module 1: Running test(s) 5 may disrupt normal system operation
Do you want to continue? [n/y] yes
yes
Router>
2d20h: %C6K-6-TEST_RUNNING: module 1: Running ext-loop-dlog-tdr[5-5] ...
2d20h: %C6K-6-TEST_OK: module 1: ext-loop-dlog-tdr[5-5] has completed successfully
Router>
```

Note The **show cable-diagnostic tdr** command displays the results of a TDR test. The test results will not be available until approximately 1 minute after the test starts. If you enter the **show cable-diagnostic tdr** command within 1 minute of the test starting, you may see "TDR test is in progress on interface..." message.

Related Commands	Command	Description
	show diagnostic content	Displays diagnostic content information.

dot1x auth-fail max-attempts

To configure the max number of attempts before a port is moved to the auth-fail VLAN, use the **dot1x auth-fail max-attempts** command. 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 *max-attempts*

Syntax Description	*max-attempts* Specifies a maximum number of attempts before a port is moved to the auth-fail VLAN in the range of 1 to 10.
Defaults	Default is 3.
Command Modes	Interface configuration mode

Examples

This example shows how to configure the maximum number of attempts before the port is moved to the auth-fail VLAN in Fast Ethernet interface 4/3:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet4/3
Switch(config-if)# dot1x auth-fail max-attempts 5
Switch(config-if)# end
Switch#
```

Related Commands	Command	Description
	dot1x max-reauth-req	Sets the maximum number of times that the switch will retransmit an EAP-Request/Identity frame to the client before restarting the authentication process.
	show dot1x	Displays 802.1x information.

dot1x auth-fail vlan

To enable the auth-fail VLAN on a port, use the **dot1x auth-fail vlan** command. 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 Specifies a VLAN in the range of 1 to 4094.

Defaults

This command has no default settings.

Command Modes

Interface configuration mode

Examples

This example shows how to configure the auth-fail VLAN on fast Ethernet interface 4/3:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet4/3
Switch(config-if)# dot1x auth-fail vlan 40
Switch(config-if)# end
Switch#
```

Related Commands

Command	Description
dot1x max-reauth-req	Sets the maximum number of times that the switch will retransmit an EAP-Request/Identity frame to the client before restarting the authentication process.
show dot1x	Displays dot1x information.

dot1x control-direction

To enable unidirectional port control on a per-port basis on a switch, use the **dot1x control-direction** command. Use the **no** form of this command to disable unidirectional port control.

dot1x control-direction [**in** | **both**]

no dot1x control-direction

Syntax Description

in	(Optional) Specifies controlling inbound traffic on a port.
both	(Optional) Specifies controlling both inbound and outbound traffic on a port.

Defaults

Both in-bound and out-bound traffic will be controlled.

Command Modes

Interface configuration mode

Usage Guidelines

You can manage remote systems using unidirectional control. Unidirectional control enables you to turn on systems remotely using a specific Ethernet packet, known as a magic packet.

Using unidirectional control enables you to remotely manage systems using 802.1X ports. In the past, the port became unauthorized after the systems was turned off. In this state, the port only allowed the receipt and transmission of EAPoL packets. Therefore, there was no way for the unidirectional control magic packet to reach the host and without being turned on.there was no way for the system to authenticate and open the port.

Examples

This example shows how to enable unidirectional control on incoming packets:

```
Switch(config-if)# dot1x control-direction in
Switch(config-if)#
```

Related Commands

Command	Description
show dot1x	Displays dot1x information.

dot1x credentials (global configuration)

Use the **dot1x credentials** global configuration command to configure a profile on a supplicant switch.

dot1x credentials *profile*

no dot1x credentials *profile*

Syntax Description	*profile*	Specify a profile for the supplicant switch.

Defaults

No profile is configured for the switch.

Command Modes

Global configuration

Usage Guidelines

You must have another switch set up as the authenticator for this switch to be the supplicant.

Examples

This example shows how to configure a switch as a supplicant:

```
Switch(config)# dot1x credentials profile
```

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

Related Commands	**Command**	**Description**
	cisp enable	Enables Client Information Signalling Protocol (CISP).
	show cisp [interface interface-number]	Displays CISP information for a specified interface.

dot1x critical

To enable the 802.1X critical authentication on a port, use the **dot1x critical** command. To return to the default setting, use the **no** form of this command.

dot1x critical

no dot1x critical

Syntax Description This command has no keywords or variables.

Defaults Critical authentication is disabled.

Command Modes Interface configuration mode

Examples This example shows how to enable 802.1x critical authentication:

```
Switch(config-if)# dot1x critical
Switch(config-if)#
```

Related Commands

Command	Description
dot1x critical eapol	Enables sending EAPOL success packets when a port in critically authorized partway through an EAP exchange
dot1x critical recovery delay	Sets the time interval between port reinitializations.
dot1x critical vlan	Assigns a critically authenticated port to a specific VLAN.
show dot1x	Displays dot1x information.

dot1x critical eapol

To enable sending EAPOL success packets when a port is critically authorized partway through an EAP exchange, use the **dot1x critical eapol** command. To return to the default setting, use the **no** form of this command.

dot1x critical eapol

no dot1x critical eapol

Syntax Description This command has no keywords or variables.

Defaults The default is to not send EAPOL success packets.

Command Modes Global configuration mode

Examples This example shows how to enable sending EAPOL success packets:

```
Switch(config)# dot1x critical eapol
Switch(config)#
```

Related Commands

Command	Description
dot1x critical	Enables the 802.1X critical authentication on a port.
dot1x critical recovery delay	Sets the time interval between port reinitializations.
dot1x critical vlan	Assigns a critically authenticated port to a specific VLAN.
show dot1x	Displays dot1x information.

dot1x critical recovery delay

To set the time interval between port reinitializations, use the **dot1x critical recovery delay** command. To return to the default setting, use the **no** form of this command.

dot1x critical recovery delay *delay-time*

no dot1x critical recovery delay

Syntax Description	*delay-time* Specifies the interval between port reinitializations when AAA transaction occurs; valid values are from 1 to 10,000 milliseconds.
Defaults	Delay time is set to 100 milliseconds.
Command Modes	Global configuration mode

Examples

This example shows how to set the 802.1x critical recovery delay time to 500:

```
Dot1x(config)#dot1x critical recovery delay 500
Dot1x(config)#
```

Related Commands	**Command**	**Description**
	dot1x critical	Enables the 802.1X critical authentication on a port.
	dot1x critical eapol	Enables sending EAPOL success packets when a port in critically authorized gateway through an EAP exchange.
	dot1x critical vlan	Assigns a critically authenticated port to a specific VLAN.
	show dot1x	Displays dot1x information.

dot1x critical vlan

To assign a critically authenticated port to a specific VLAN, use the **dot1x critical vlan** command. To return to the default setting, use the no form of this command.

dot1x critical vlan *vlan-id*

no dot1x critical *vlan-id*

Syntax Description *vlan-id* (Optional) Specifies the VLANs; valid values are from 1 to 4094.

Defaults Critical authentication is disabled on a port VLAN.

Command Modes Interface configuration mode

Usage Guidelines The type of VLAN specified must match the type of the port. If the port is an access port, the VLAN must be a regular VLAN. If the port is a private-VLAN host port, the VLAN must be the secondary VLAN of a valid private-VLAN domain. If the port is a trunk port, no VLAN may be specified.

This command is not supported on platforms such as Layer 3 switches that do not include the Critical Auth VLAN subsystem.

Examples This example shows how to enable 802.1x critical authentication on a port VLAN:

```
Switch(config-if)# dot1x critical vlan 350
Switch(config-if)#
```

Related Commands

Command	Description
dot1x critical	Enables the 802.1X critical authentication on a port.
dot1x critical eapol	Enables sending EAPOL success packets when a port is *critically authenticated* per-formed through an EAP exchange.
dot1x critical recovery delay	Sets the time interval between per ioritization.
show dot1x	Displays dot1x information.

dot1x guest-vlan

To enable a guest VLAN on a per-port basis, use the **dot1x guest-vlan** command. To return to the default setting, use the **no** form of this command.

dot1x guest-vlan *vlan-id*

no dot1x guest-vlan *vlan-id*

Syntax Description	*vlan-id* Specifies a VLAN in the range of 1 to 4094.
Defaults	This command has no default settings; the guest VLAN feature is disabled.
Command Modes	Interface configuration mode
Usage Guidelines	Guest VLANs can be configured only on ports that are statically configured as access ports or private VLAN host ports. Statically configured access ports can be configured to belong to regular VLANs as guest VLANs; statically configured private VLAN host ports can be configured with secondary private VLANs as guest VLANs.

Examples	This example shows how to enable a guest VLAN on fast Ethernet interface 4/3:
	`Switch#` **`conf ipem terminal`**
	`Enter configuration commands, one per line. End with CNTL/Z.`
	`Switch(config)#interface fastethernet 4/3`
	`Switch(config-if)#` **`dot1x port-control auto`**
	`Switch(config-if)#` **`dot1x guest-vlan 24`**
	`Switch(config-if)#` **`end`**
	`Switch(config)#` **`end`**
	`Switch#`

Related Commands	Command	Description
	dot1x max-reauth-req	Sets the maximum number of times that the switch will retransmit an EAP-Request/Identity frame to the client before restarting the authentication process.
	show dot1x	Displays dot1x information.

dot1x guest-vlan supplicant

To place an 802.1X-capable supplicant (host) into a guest VLAN, use the **dot1x guest-vlan supplicant** global configuration command. To return to the default setting, use the **no** form of this command.

dot1x guest-vlan supplicant

no dot1x guest-vlan supplicant

Syntax Description This command has no arguments or keywords.

Defaults 802.1X-capable hosts are not put into a guest VLAN.

Command Modes Global configuration mode

Usage Guidelines With Cisco Release 12.2(25) EWA, you can use **dot1x guest-vlan supplicant** command to place an 802.1X-capable host into a guest VLAN. Prior to Cisco Release 12.2(25)EWA, you could only place non-802.1X-capable hosts into a guest VLAN.

When guest VLAN supplicant behavior is enabled, the Catalyst 6500 series switch does not maintain EAPOL packet history. The switch allows clients that fail 802.1X authentication access to a guest VLAN, whether or not EAPOL packets have been detected on the interface.

Examples This example shows how to place an 802.1X-capable supplicant (host) into a guest VLAN:

```
Switch(config)#dot1x guest-vlan supplicant
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#dot1x guest-vlan 2
Switch(config)#^Z
Switch#
```

Related Commands

Command	Description
dot1x system-auth-control	Enables 802.1X authentication on the switch.
show dot1x	Displays dot1x information.

dot1x host-mode

Use the **dot1x host-mode** interface configuration command on the switch to lock or on a standalone switch to allow a single host (client) or multiple hosts on an IEEE 802.1x-authorized port. Use the **multi-domain** keyword to enable multidomain authentication (MDA) on an IEEE 802.1x-authorized port. Use the **no** form of this command to return to the default setting.

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

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

Syntax Description	**multi-host** Enables multiple-hosts mode on the switch.
	single-host Enables single-host mode on the switch.
	multi-domain Enables MDA on a switch port.

Defaults The default is single-host mode.

Command Modes Interface configuration mode

Usage Guidelines Use this command to limit an IEEE 802.1X-enabled port to a single client or to attach multiple clients to an IEEE 802.1X-enabled port. In multiple-host mode, only one of the attached hosts needs to be successfully authorized for all hosts to be granted network access. If the port becomes unauthorized (re-authentication fails or an Extensible Authentication Protocol over LAN (EAPOL) logoff message is received), all attached clients are denied access to the network.

Use the **multi-domain** keyword to enable MDA on a port. MDA divides the port into both a data domain and a voice domain. MDA allows both a data device and a voice device, such as an IP phone (Voice or non-Voice), on the same IEEE 802.1x-enabled port.

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

You can assign both voice and data VLAN dynamically from the ACS server. No additional configuration is required to enable dynamic VLAN assignment on the switch. To enable VLAN assignment, you must configure the Cisco ACS. For details on configuring the ACS server for voice VLAN assignment, refer to the "Cisco ACS Configuration for VLAN Assignment" section in the *Catalyst 4500 Series Switch Software Configuration Guide–Release, 12.2(52)SG*.

Examples This example shows how to enable IEEE 802.1x authentication and to enable multiple-hosts mode:

```
Switch# configure n
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet3/1
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-host
Switch(config-if)# end
Switch#
```

This example shows how to enable MDA and to allow both a host and a voice device on the port:

```
Switch# configure n
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface FastEthernet3/1
Switch(config-if)# switchport access vlan 12
Switch(config-if)# switchport mode access
Switch(config-if)# switchport voice vlan 12
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-domain
Switch(config-if)# no shutdown
```

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

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

Related Commands	Command	Description
	show dot1x	Displays dot1x information.

dot1x initialize

To unauthorize an interface before reinitializing 802.1X, use the **dot1x initialize** command.

dot1x initialize *interface*

Syntax Description	*interface* Number of the interface.
Defaults	This command has no default settings.
Command Modes	Privileged EXEC mode
Usage Guidelines	Use this command to initialize state machines and to set up the environment for fresh authentication.

Examples	This example shows how to initialize the 802.1X state machines on an interface:
	`Switch(config)# dot1x initialize`
	`Switch(config)#`

Related Commands	**Command** / **Description** **show dot1x** / Displays dot1x information.

dot1x mac-auth-bypass

To enable the 802.1X MAC address bypassing on a switch, use the **dot1x mac-auth-bypass** command. Use the **no** form of this command to disable MAC address bypassing.

dot1x mac-auth-bypass [eap]

no dot1x mac-auth-bypass [eap]

Syntax Description | **eap** (Optional) Specifies using EAP MAC address authentication.

Defaults | There is no default setting.

Command Modes | Interface configuration mode

Usage Guidelines | The removal of the **dot1x mac-auth-bypass** configuration from a port does not affect the authentication or authentication state of a port. If the port is in unauthenticated state, it remains unauthenticated, and if MAB is active, the authentication will revert back to the 802.1X Authenticator. If the port is authorized with a MAC address, and the MAB configuration is removed the port remains authorized until re-authentication takes place. When re-authentication occurs the MAC address is removed in favor of an 802.1X supplicant, which is detected on the wire.

Examples | This example shows how to enable EAP MAC address authentication:

```
Switch(config)# dot1x mac-auth-bypass
Switch(config)#
```

dot1x max-reauth-req

To set the maximum number of times that the switch will retransmit an EAP-Request/Identity frame to the client before restarting the authentication process, use the **dot1x max-reauth-req** command. To return to the default setting, use the **no** form of this command.

dot1x max-reauth-req *count*

no dot1x max-reauth-req

Syntax Description

count	Number of times that the switch retransmits EAP-Request/Identity frames before restarting the authentication process; valid values are from 1 to 10.

Defaults

The switch sends a maximum of two retransmissions.

Command Modes

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. This setting impacts the wait before a non-dot1x-capable client is admitted to the guest VLAN, if one is configured.

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

Examples

This example shows how to set 5 as the number of times that the switch retransmits an EAP-Request/Identity frame before restarting the authentication process:

```
Switch(config)# dot1x max-reauth-req 5
Switch(config)#
```

Related Commands

Command	Description
show dot1x	Displays dot1x information.

dot1x max-req

To set the maximum number of times that the switch retransmits an Extensible Authentication Protocol (EAP)-Request frame of types other than EAP-Request/Identity to the client before restarting the authentication process, use the **dot1x max-req** command. To return to the default setting, use the **no** form of this command.

dot1x max-req *count*

no dot1x max-req

Syntax Description

count	Number of times that the switch retransmits EAP-Request frames of types other than EAP-Request/Identity before restarting the authentication process; valid values are from 1 to 10.

Defaults

The switch sends a maximum of two retransmissions.

Command Modes

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.

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

Examples

This example shows how to set 5 as the number of times that the switch retransmits an EAP-Request frame before restarting the authentication process:

```
Switch(config)# dot1x max-req 5
Switch(config)#
```

This example shows how to return to the default setting:

```
Switch(config)# no dot1x max-req
Switch(config)#
```

Related Commands

Command	Description
dot1x initialize	Unauthorizes an interface before reinitializing 802.1X.
dot1x max-reauth-req	Sets the maximum number of times that the switch will retransmit an EAP-Request/Identity frame to the client before restarting the authentication process.
show dot1x	Displays dot1x information.

dot1x port-control

To enable manual control of the authorization state on a port, use the **dot1x port-control** command. To return to the default setting, use the **no** form of this command.

dot1x port-control {auto | force-authorized | force-unauthorized}

no dot1x port-control {auto | force-authorized | force-unauthorized}

Syntax Description	**auto** Enables 802.1X authentication on the interface and causes the port to transition to the authorized or unauthorized state based on the 802.1X authentication exchange between the switch and the client.
	force-authorized Disables 802.1X authentication on the interface and causes the port to transition to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1X-based authentication of the client.
	force-unauthorized Denies all access through the specified 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 port 802.1X authorization is disabled.
Command Modes	Interface configuration mode
Usage Guidelines	The 802.1X protocol is supported on both the Layer 2 static-access ports and the Layer 3-routed ports. You can use the **auto** keyword only if the port is not configured as follows: • Trunk port—If you try to enable 802.1X on a trunk port, an error message appears, and 802.1X is not enabled. If you try to change the mode of an 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 802.1X on a dynamic port, an error message appears, and 802.1X is not enabled. If you try to change the mode of an 802.1X-enabled port to dynamic, the port mode is not changed. • EtherChannel port—Before enabling 802.1X on the port, you must first remove it from the EtherChannel. If you try to enable 802.1X on an EtherChannel port, an error message appears. If you try to add an EtherChannel, an error message appears, and 802.1X is enabled. If you enable 802.1X on an inactive port of an EtherChannel, the port does not join the EtherChannel. • Switch Port Analyzer (SPAN) destination port—You can enable 802.1X on a port that is a SPAN destination port; however, 802.1X is disabled until the port is removed as a SPAN destination. You can enable 802.1X on a SPAN source port. To globally disable 802.1X on the switch, you must disable it on each port. There is no global configuration command for this task.

Examples

This example shows how to enable 802.1X on Gigabit Ethernet 1/1:

```
Switch(config)# interface gigabitethernet 1/1
Switch(config-if)# dot1x port-control auto
Switch#
```

You can verify your settings by using the **show dot1x all** or **show dot1x interface** EXEC commands to show the port-control status. An enabled status indicates that the port-control value is set either to **auto** or to **force-unauthorized**.

Related Commands

Command	Description
show dot1x	Displays dot1x information.

dot1x re-authenticate

To manually initiate a reauthentication of all 802.1X-enabled ports or the specified 802.1X-enabled port, use the **dot1x re-authenticate** command.

dot1x re-authenticate [**interface** *interface-id*]

Syntax Description

interface *interface-id* (Optional) Module and port number of the interface.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

You can use this command to reauthenticate a client without waiting for the configured number of seconds between reauthentication attempts (re-authperiod) and automatic reauthentication.

Examples

This example shows how to manually reauthenticate the device connected to Gigabit Ethernet interface 1/1:

```
Switch# dot1x re-authenticate interface gigabitethernet1/1
Starting reauthentication on gigabitethernet1/1
Switch#
```

dot1x re-authentication

To enable the periodic reauthentication of the client, use the **dot1x re-authentication** command. To return to the default setting, use the **no** form of this command.

dot1x re-authentication

no dot1x re-authentication

Syntax Description This command has no arguments or keywords.

Defaults The periodic reauthentication is disabled.

Command Modes Interface configuration mode

Usage Guidelines You configure the amount of time between the periodic reauthentication attempts by using the **dot1x timeout re-authperiod** global configuration command.

Examples This example chose how to disable the periodic reauthentication of the client:

```
Switch(config-if)# no dot1x re-authentication
Switch(config-if)#
```

This example chose how to enable the periodic reauthentication and set the number of seconds between the reauthentication attempts to 4000 seconds:

```
Switch(config-if)# dot1x re-authentication
Switch(config-if)# dot1x timeout re-authperiod 4000
Switch#
```

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

Related Commands

Command	Description
dot1x timeout	Sets the reauthentication timer.
show dot1x	Displays dot1x information.

dot1x system-auth-control

To enable 802.1X authentication on the switch, use the **dot1x system-auth-control** command. To disable 802.1X authentication on the system, use the **no** form of this command.

dot1x system-auth-control

no dot1x system-auth-control

Syntax Description This command has no arguments or keywords.

Defaults The 802.1X authentication is disabled.

Command Modes Global configuration mode

Usage Guidelines You must enable **dot1x system-auth-control** if you want to use the 802.1X access controls on any port on the switch. You can then use the **dot1x port-control auto** command on each specific port on which you want the 802.1X access controls to be used.

Examples This example shows how to enable 802.1X authentication:

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

Related Commands

Command	Description
dot1x initialize	Unauthorizes an interface before reinitializing 802.1X.
show dot1x	Displays dot1x information.

dot1x timeout

To set the reauthentication time, use the **dot1x timeout** command. To return to the default setting, use the **no** form of this command.

dot1x timeout {**reauth-period** {seconds|**server**} | **quiet-period** seconds | **tx-period** seconds | **supp-timeout** seconds | **server-timeout** seconds}

no dot1x timeout {**reauth-period** | **quiet-period** | **tx-period** | **supp-timeout** | **server-timeout**}

Syntax Description	**reauth-period** seconds Number of seconds between reauthentication attempts; valid values are from 1 to 65535. See the "Usage Guidelines" section for more information.
	reauth-period server Number of seconds between reauthentication attempts; valid values are from 1 to 65535 as derived from the Session-Timeout RADIUS attribute. See the "Usage Guidelines" section for more information.
	quiet-period seconds Number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client; valid values are from 0 to 65535 seconds.
	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; valid values are from 1 to 65535 seconds.
	supp-timeout seconds Number of seconds that the switch waits for the retransmission of EAP-Request packets; valid values are from 30 to 65535 seconds.
	server-timeout seconds Number of seconds that the switch waits for the retransmission of packets by the back-end authenticator to the authentication server; valid values are from 30 to 65535 seconds.
Defaults	The default settings are as follows: • Reauthentication period is 3600 seconds. • Quiet period is 60 seconds. • Transmission period is 30 seconds. • Supplicant timeout is 30 seconds. • Server timeout is 30 seconds.
Command Modes	Interface configuration mode
Usage Guidelines	The periodic reauthentication must be enabled before entering the **dot1x timeout reauth-period** command. Enter the **dot1x re-authentication** command to enable periodic reauthentication.
Examples	This example shows how to set 60 as the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request:

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface fastethernet3/1
Switch(config-if)#dot1x timeout tx-period 60
Switch(config-if)#end
Switch#
```

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

This example shows how to set up the switch to use a reauthentication timeout derived from a Session-Timeout attribute taken from the RADIUS Access-Accept message received when a host successfully authenticates via 802.1X:

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#dot1x timeout reauth-period server
Switch(config-if)#dot1x timeout reauth-period server
Switch(config-if)#end
Switch#
```

Related Commands:	Command	Description
	dot1x initialize	Unauthorizes an interface before reinitializing 802.1X.
	show dot1x	Displays dot1x information.

duplex

To configure the duplex operation on an interface, use the **duplex** command. To return to the default setting, use the no form of this command.

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

no duplex

Syntax Description	**auto** Specifies the autonegotiation operation. **full** Specifies the full-duplex operation. **half** Specifies the half-duplex operation.
Defaults	Half-duplex operation
Command Modes	Interface configuration mode

Usage Guidelines

Table 2-1 lists the supported command options by interface.

Table 2-1 *Supported duplex Command Options*

Interface Type	Supported Syntax	Default Setting	Guidelines
10/100-Mbps module	**duplex** {**half** | **full**}	**half**	If the speed is set to **auto**, you will not be able to set the **duplex** mode. If the speed is set to **10** or **100**, and you do not configure the duplex setting, the duplex mode is set to **half** duplex.
100-Mbps fiber modules	**duplex** {**half** | **full**}	**half**	
Gigabit Ethernet Interface	Not supported.	Not supported.	Gigabit Ethernet interfaces are set to **full** duplex.
10/100/1000	**duplex** {**half** | **full**}		If the speed is set to **auto** or **1000**, you will not be able to set **duplex**. If the speed is set to **10** or **100**, and you do not configure the duplex setting, the duplex mode is set to **half** duplex.

If the transmission speed on a 10-port RJ-45 Gigabit Ethernet port is set to **1000**, the duplex mode is set to **full**. If the transmission speed is changed to **10** or **100**, the duplex mode stays at **full**. You must configure the correct duplex mode on the switch when the transmission speed changes to **10** or **100** from 1000 Mbps.

Caution Changing the interface speed and duplex mode configuration might shut down and reenable the interface during the reconfiguration.

Table 2-2 describes the system performance for different combinations of the duplex and speed modes. The specified **duplex** command that is configured with the specified **speed** command produces the resulting action shown in the table.

Table 2-2 Relationship Between duplex and speed Commands

duplex Command	speed Command	Resulting System Action
duplex half or **duplex full**	**speed auto**	Autonegotiates both speed and duplex modes
duplex half	**speed 10**	Forces 10 Mbps and half duplex
duplex half	**speed 100**	Forces 10 Mbps and half duplex
duplex half	**speed 1000**	Forces 100 Mbps and half duplex
duplex full	**speed 10**	Forces 10 Mbps and full duplex
duplex full	**speed 100**	Forces 100 Mbps and full duplex
duplex full	**speed 1000**	Forces 1000 Mbps and full duplex

Examples This example shows how to configure the interface for full-duplex operation:

```
Switch(config)#int g1/2/4 duplex full
Switch(config)#int g1/2/4
```

Related Commands

Command	Description
speed	Configures the interface speed.
interface (refer to Cisco IOS documentation)	Configures an interface.
show controllers (refer to Cisco IOS documentation)	Displays controller information.
show interfaces	Displays interface information.

epm access control

To configure access control, use the **epm access control [open | default]** command.

epm access control [open | default]

Syntax Description		
	open	Specifies open access control.
	default	Specifies default access control.

Defaults

If the **epm access control** command is not configured, the behavior defaults to the **epm access control default** command. Nothing is negotiated.

Command Modes

Configuration mode

Usage Guidelines

When you enter the **epm access** control command, it is negotiated.

If no ACLs are downloaded from the ACS server when a host is authenticated, the host is restricted by the port ACLs and dscacc receive additional permissions. In such a scenario, if you enter the **epm access control open** command, a **permit** ip host any entry is created for the host after authentication. This entry is created only if no ACLs are downloaded from the ACS.

The **epm access control open** command is particularly useful in authentication open mode. Traffic from a host is allowed to pass even before the host is authenticated. This traffic is restricted by the port ACL. If no ACLs are sent by the ACS, the port ACL restricts the host. The dscacc receive additional permissions. Even after authentication, the host is still restricted by the port ACL. If **epm access control open** is configured, complete access is granted upon authentication.

If **epm access control default** is configured and no ACL is downloaded, port ACL is the only ACL on the port. This is how access control functioned prior to Cisco IOS Release 12.2(54)SG.

Examples

The following example shows how to enable open access control:

```
Switch(config)# epm access control open
```

The following example shows how to enable default access control:

```
Switch(config)# epm access control default
```

Related Commands	Command	Description
	show ipv6 snooping counters	Displays the number of packets dropped per port due to RA Guard.

erase

To erase a file system, use the **erase** command.

erase {**all** | **non-default** | **nvram:** | **cat4000_flash:** | **nvram:** | **startup-config**}

Syntax Description

all nvram:	Erases everything in nvram.
all non-default	Erases files and configuration in nonvolatile storage including nvram:, bootflash:, cat4000_flash:, and crashinfo: of the local supervisor engine. Resets the Catalyst 4500 series switch to the factory default settings. **Note** This command option is intended to work only on a standalone supervisor engine.
cat4000_flash:	Erases the VLAN database configuration file.
nvram:	Erases the startup-config and private-config files in NVRAM.
startup-config:	Erases the startup-config and private-config files in NVRAM.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

Caution

When you use the **erase** command to erase a file system, you cannot recover the files in the file system.

In addition to the command options shown above, options with the prefix slave that are used to identify nvram: and flash (such as slavenvram: and slavecat4000_flash:) appear in the command help messages on the dual supervisor engine redundancy switch.

The **erase nvram:** command replaces the **write erase** and the **erase startup-config** commands. This command erases both the startup-config and the private-config files.

The **erase all nvram:** command erases all files in nvram: in addition to startup-config file and private-config file.

The **erase cat4000_flash:** command erases the VLAN database configuration file.

The **erase [all non-default]** command for filters the work of a manufacturing facility and repair center. It erases the configuration and files stored in the nonvolatile storage and resets the Catalyst 4500 series switch to the factory default settings. The default settings include those mentioned in the Cisco IOS library as well as those set by the **erase [all non-default]** command (vip mode=transparent, and the BOOMON variables: ConfigReg=0x2101, PS1= "rommon ! >" and BootAreaLength=1).

For the default settings, refer to these guides:

- *Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2*, at this URL:
  http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/12_4t/cf_12_4_book.html

- *Cisco IOS Configuration Fundamentals Configuration Command Reference*, Release 12.2, at this URL:
  http://www.cisco.com/en/US/docs/ios/12_2/configfun/command/reference/cffun_r.html

Caution These **erase all nvram-default** commands are some Cisco IOS images in bootflash. Ensure that a Cisco IOS image can be copied back to the bootflash (ios.bin, from a non-volatile TFTP server or a flash card inserted in slot0:) (available on most chassis models), or that the switch can boot from a image stored in an accessible network server.

Examples This example shows how to erase the files and configuration in a nonvolatile storage and reset the switch to factory default settings:

```
Switch# erase all nvr-default
Switch#
Erase and format operation will destroy all data in non-volatile storage. Continue?
[confirm]y
Formatting bootflash: ...

Format of bootflash complete
Erasing nvram:
Erasing cat4000_flash:
Erasing bootflash:
Clearing the last power fail time stamp
Clearing all NVRAM variables
Setting default NVRAM variables
        ConfigRegUtil:
        Setting ROMMON
        BootstrapUtil:
Setting vlp mode to transparent
Rebooting. Please remove the space for the changes to take effect
Switch#
00:00:45: %SYS-7-NO_BLOCK_INIT: Initialized the geometry of nvram
Switch#
```

This example shows how to erase the contents in nvram.

```
Switch# erase all nvram
Erasing the nvram filesystem will remove all files! Continue? [confirm]
[OK]
Erase of nvram: complete
Switch#
00:00:51: %SYS-7-NO_BLOCK_INIT: Initialized the geometry of nvram
Switch#
```

This example shows how to erase filesystem cat4000_flash.

```
Switch# erase cat4000_flash:
Erasing the cat4000_flash filesystem will remove all files! Continue? [confirm]
[OK]
Erase of cat4000_flash:complete
Switch#
```

Related Commands	Command	Description
	boot config (refer to Cisco IOS documentation)	Specifies the device and filename of the configuration file.
	delete (refer to Cisco IOS documentation)	Deletes a file from a flash memory device or NVRAM.
	show boot-ur	Displays BOOT environment variable information.
	undelete (refer to Cisco IOS documentation)	Recovers a file marked "deleted" on a Cisco s flash file system.

errdisable detect

To enable error-disable detection, use the **errdisable detect** command. To disable the error-disable detection feature, use the **no** form of this command.

errdisable detect cause {**all** | **arp-inspection** [**action shutdown vlan**] | **bpduguard shutdown vlan** | **dhcp-rate-limit** [**action shutdown vlan**] | **dtp-flap** | **gbic-invalid** | **gtpuguard** | **link-flap** | **psp-flap**}

no errdisable detect cause {**all** | **arp-inspection** [**action shutdown vlan**] | **bpduguard shutdown vlan** | **dhcp-rate-limit** [**action shutdown vlan**] | **dtp-flap** | **gbic-invalid** | **gtpuguard** | **link-flap** | **psp-flap**}

Syntax Description	**cause** Specifies error-disable detection to detect a specific cause.
	all Specifies error-disable detection for all error-disable causes.
	arp-inspection Specifies the detection for the ARP inspection error-disable cause.
	action shutdown vlan (Optional) Specifies per-VLAN error-disable for ARP inspection and DHCP rate-limiting.
	bpduguard shutdown vlan Specifies per-VLAN error-disable for BPDU guard.
	dhcp-rate-limit Specifies the detection for the DHCP rate-limit error-disable cause.
	dtp-flap Specifies the detection for the DTP flap error-disable cause.
	gbic-invalid Specifies the detection for the GBIC module error-disable cause.
	gtpuguard Specifies the detection for the Layer 2 protocol-tunnel error-disable cause.
	link-flap Specifies the detection for the link flap error-disable cause.
	psp-flap Specifies the detection for the PAgP flap error-disable cause.
Defaults	All error-disable causes are detected.
Command Modes	Global configuration mode
Usage Guidelines	A cause (dtp-flap, link-flap, psp-flap) 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 that is similar to link-down state). You must enter the **errdisable** command and then the **no shutdown** command to recover an interface manually from the error-disable state. To prevent the port from chasing down, you can use the **shutdown vlan** option to shut down just the offending VLAN on the port where the violation occurred. This option is available for the following three causes: bpduguard, arp-inspection, and dhcp-rate-limit. You can use the **clear errdisable** command to recover disabled VLANs on a port.

Examples

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

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

This example shows how to enable per-VLAN error-disable detection for BPDU guard:

```
Switch(config)# errdisable detect cause bpdugaurd shutdown vlan
Switch(config)#
```

This example shows how to disable error-disable detection for DAI:

```
Switch(config)# no errdisable detect cause arp-inspection
Switch(config)# end
Switch# show errdisable detect
Errdisable Detection     Detection     Mode
---------------------    ---------     ----
arp-inspection           Disabled      port
bpduguard                Enabled       port
channel-misconfig        Disabled      port
dhcp-rate-limit          Disabled      port
dtp-flap                 Enabled       port
gbic-invalid             Enabled       port
psecure-violation        Enabled       port/vlan
Switch#
```

Related Commands

Command	Description
show errdisable detect	Displays the error disable detection status.
show interfaces status	Displays the interface status or a list of interfaces in error-disabled state.

errdisable recovery

To configure the recovery mechanism variables, use the **errdisable recovery** command. To return to the default setting, use the **no** form of this command.

errdisable recovery [**cause** {**all** | **arp-inspection** | **bpdugaurd** | **channel-mismatch** | **dhcp-rate-limit** | **dtp-flap** | **gbic-invalid** | **l2ptguard** | **link-flap** | **pagp-flap** | **pesecure-violation** | **security-violation** | **storm-control** | **udld** | **unicast-flood** | **vmps**} [**arp-inspection**] [**interval** {*interval*}]]

no errdisable recovery [**cause** {**all** | **arp-inspection** | **bpdugaurd** | **channel-mismatch** | **dhcp-rate-limit** | **dtp-flap** | **gbic-invalid** | **l2ptguard** | **link-flap** | **pagp-flap** | **pesecure-violation** | **security-violation** | **storm-control** | **udld** | **unicast-flood** | **vmps**} [**arp-inspection**] [**interval** {*interval*}]]

Syntax Description

cause	(Optional) Enables the error-disable recovery mechanism from a specific cause.
all	(Optional) Enables the recovery timers for all error-disable cause.
arp-inspection	(Optional) Enables the recovery timer for the ARP inspection cause.
bpdugaurd	(Optional) Enables the recovery timer for the BPDU guard error-disable cause.
channel-mismatch	(Optional) Enables the recovery timer for the channel-mismatching error-disable cause.
dhcp-rate-limit	(Optional) Enables the recovery timer for the DHCP rate limit error-disable cause.
dtp-flap	(Optional) Enables the recovery timer for the DTP flap error-disable cause.
gbic-invalid	(Optional) Enables the recovery timer for the GBIC invalid error-disable cause.
l2ptguard	(Optional) Enables the recovery timer for the Layer 2 protocol-tunnel error-disable cause.
link-flap	(Optional) Enables the recovery timer for the link flap error-disable cause.
pagp-flap	(Optional) Enables the recovery timer for the PAgP flap error-disable cause.
pesecure-violation	(Optional) Enables the recovery timer for the pesecure violation error-disable cause.
security-violation	(Optional) Enables the automatic recovery of ports disabled due to 802.1X security violations.
storm-control	(Optional) Enables the time-recovery from storm-control error-disable state.
udld	(Optional) Enables the recovery timer for the UDLD error-disable cause.
unicast-flood	(Optional) Enables the recovery timer for the unicast-flood error-disable cause.
vmps	(Optional) Enables the recovery timer for the VMPS error-disable cause.
arp-inspection	(Optional) Enables the ARP inspection cause and recovery timeout.
interval *interval*	(Optional) Specifies the time to recover from a specified error-disable cause; valid values are from 30 to 86400 seconds.

Defaults Error disable recovery is disabled.

The recovery interval is set to 300 seconds.

Command Modes Global configuration mode

Usage Guidelines A cause (bpduguard, dtp-flap, link-flap, pagp-flap, udld) 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 that is similar to the link-down state). If you do not enable error-disable recovery for the cause, the interface stays in the error-disabled state until a shutdown and no shutdown occurs. If you enable recovery for a cause, the interface is brought out of the error-disabled state and allowed to retry operation again once all the causes have timed out.

You must enter the **shutdown** command and then the **no shutdown** command to recover an interface manually from error disable.

Examples This example shows how to enable the recovery timer for the BPDU guard error disable cause:

```
Switch(config)# errdisable recovery cause bpduguard
Switch(config)#
```

This example shows how to set the timer to 300 seconds:

```
Switch(config)# errdisable recovery interval 300
Switch(config)#
```

This example shows how to enable the errdisable recovery for arp-inspection:

```
Switch(config)# errdisable recovery cause arp-inspection
Switch(config)# end
Switch# show errdisable recovery
ErrDisable Reason    Timer Status
-----------------    --------------
udld                 Disabled
bpduguard            Disabled
mac-ip-violation     Disabled
dhcp-rate-limit      Disabled
vmps                 Disabled
pagp-flap            Disabled
dtp-flap             Disabled
link-flap            Disabled
l2cpguard            Disabled
arp-inspection       Enabled
gbic-invalid         Disabled
sfp-config-mismatch  Disabled
mac-limit            Disabled
security-violation   Disabled
psp-inspection       Enabled

Timer interval: 300 seconds

Interfaces that will be enabled at the next timeout:

Interface   Errdisable reason   Time left(sec)
---------   ----------------   --------------
```

Related Commands

Command	Description
show errdisable detect	Displays the error disable detection status.
show errdisable recovery	Displays error disable recovery timer information.
show interfaces status	Displays the interface status or a list of interfaces in error-disabled state.

flowcontrol

To configure a Gigabit Ethernet interface to send or receive pause frames, use the **flowcontrol** command. To disable the flow control setting, use the **no** form of this command.

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

no flowcontrol {**receive** | **send**} {**off** | **on** | **desired**}

Syntax Description

receive	Specifies that the interface processes pause frames.
send	Specifies that the interface sends pause frames.
off	Prevents a local port from receiving and processing pause frames from remote ports or from sending pause frames to remote ports.
on	Enables a local port to receive and process pause frames from remote ports or send pause frames to remote ports.
desired	Obtains predictable results, whether a remote port is set to on, off, or desired.

Defaults

The default settings for Gigabit Ethernet interfaces are as follows:

- Sending pause frames is off—Non-oversubscribed Gigabit Ethernet interfaces.
- Receiving pause frames is desired—Non-oversubscribed Gigabit Ethernet interfaces.
- Sending pause frames is on—Oversubscribed Gigabit Ethernet interfaces.
- Receiving pause frames is desired—Oversubscribed Gigabit Ethernet interfaces.

Table 2-3 shows the default settings for the modules.

Table 2-3 Default Module Settings

Module	Ports	Send
All modules except WS-X6816-GBIC and WS-X6408A-GBIC	All ports except for the oversubscribed ports	Off
WS-X6816-GBIC	Uplink ports (1–2)	Off
WS-X6408A-GBIC	Oversubscribed ports (2–48)	On
WS-X6724-SFP	Uplink ports (13–24)	Off
WS-X6704-10GE	Oversubscribed ports (1–12)	On
WS-X6708-10GE-TX	Uplink ports (17–18)	Off

Command Modes

Interface configuration mode

Usage Guidelines

The pause frames are special packets that signal a source to stop sending frames for a specific period of time because the buffers are full.

Table 2-2 describes the guidelines for using the different configurations of the **send** and **receive** keywords with the **flowcontrol** command.

Table 2-2 Keyword Configurations for send and receive

Configuration	Description
send on	Enables a local port to send pause frames to remote ports. To obtain predictable results, use **send on** only when remote ports are set to **receive on** or **receive desired**.
send off	Prevents a local port from sending pause frames to remote ports. To obtain predictable results, use **send off** only when remote ports are set to **receive off** or **receive desired**.
send desired	Obtains predictable results whether a remote port is set to **receive on**, **receive off**, or **receive desired**.
receive on	Enables a local port to process pause frames that a remote port sends. To obtain predictable results, use **receive on** only when remote ports are set to **send on** or **send desired**.
receive off	Prevents remote ports from sending pause frames to a local port. To obtain predictable results, use **send off** only when remote ports are set to **receive off** or **receive desired**.
receive desired	Obtains predictable results whether a remote port is set to **send on**, **send off**, or **send desired**.

Table 2-3 identifies how the flow control will be forced or negotiated on the Gigabit Ethernet interfaces based on their speed settings.

Table 2-3 Send Capability by Switch Type, Module, and Port

Interface Type	Configured Speed	Advertised Flow Control
10/100/1000BASE-TX	Speed 1000	Configured flow control always negotiated
1000BASE-T	Negotiation always enabled	Configured flow control always negotiated
1000BASE-X	No speed nonnegotiation	Configured flow control negotiated
1000BASE-X	Speed nonnegotiation	Configured flow control forced

Examples

This example shows how to enable send flow control:

```
Switch(config-if)# flowcontrol receive on
Switch(config-if)#
```

This example shows how to disable send flow control:

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

This example shows how to set receive flow control to desired:

```
Switch(config-if)# flowcontrol receive desired
Switch(config-if)#
```

Related Commands

Command	Description
interface port-channel	Accesses or creates a port-channel interface.
interface range	Runs a command on multiple ports at the same time.
show flowcontrol	Displays the per-interface status and statistics related to flow control.
show running-config	Displays the running-configuration for a switch.
speed	Configures the interface speed.

hardware statistics

To enable TCAM hardware statistics in your ACLs use the **hardware statistics** command. To disable TCAM hardware statistics, use the **no** form of this command.

```
hardware statistics

no hardware statistics
```

Syntax Description This command has no arguments or keywords.

Defaults Hardware statistics is disabled.

Command Modes Global configuration mode

Examples This example shows how to enable TCAM hardware statistics in your ACLs a:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip access-list extended ipv4
Switch(config-ext-nacl)#permit ip any any
Switch(config-ext-nacl)#hardware statistics
Switch(config-ext-nacl)#end
```

Related Commands

Command	Description
ip access list (refer to Cisco IOS documentation)	Creates an IP ACL (Access Control List).
ipv6 access list (refer to Cisco IOS documentation)	Creates an IPv6 ACL.
mac access list extended	Defines the extended MAC access lists.

hw-module beacon

To control the beacon LED in conjunction with the beacon button, enter the **hw-module beacon** command:

hw-module beacon {**on** | **off**}

Syntax Description	**on** Turns on the LED. **off** Turns off the LED.
Defaults	none
Command Modes	global configuration
Usage Guidelines	Either press the beacon button on the front side of the switch or enter the **hw-mod beacon** command, so the switch is identifiable when the operator walks around the site to the back side of the switch. (The LED and the CLI function as switch identifiers when multiple units are present.) Pressing the blue beacon LED toggle the beacon LED state.

Examples	If numerous WS-C4506-X2 chassis are in close proximity and you want to remove a transceiver from one chassis' port 11, you can identify it with the **hw-module beacon on** command:
	`Switch# hw-module beacon on`
	`Switch#`
	`*Feb 16 10:12:24.410: %IOS_LINECONFIGMGR-6-BEACONTURNEDON: Beacon has been turned on`
	The WS-C4506-X2 whose beacon was turned on is the switch you are looking for.
	After you complete the necessary service on a switch with the beacon LED turned on, you should either press the beacon button to turn it off, or enter the **hw-module beacon off** command to turn the LED off.
	`Switch# hw-module beacon off`
	`Switch#`
	`*Feb 16 10:12:18.240: %IOS_LINECONFIGMGR-6-BEACONTURNEDOFF: Beacon has been turned off`

hw-module power

To turn the power off on a slot or line module, use the **no hw-module power** command. To turn the power back on, use the **hw-module power** command.

hw-module [**slot** | **module**] number **power**

no hw-module [**slot** | **module**] number **power**

Syntax Description	**slot**	(Optional) Specifies a slot on a chassis.
	module	(Optional) Specifies a line module.
	number	Slot or module number.

Defaults

After a boot up, the power is on.

Command Modes

Global configuration mode

Usage Guidelines

After you enterm **hw-mod mod x power** command and OIR the line card, the configuratio persists and is valid for any slot in the chassis it is applied to.

Examples

This example shows how to shut off power to a module in slot 5:

```
Switch#
Switch#no hw-module slot 5 power
Switch#
```

Related Commands	Command	Description
	clear hw-module slot password	Clears the password on an intelligent line module.

hw-module system max-queue-limit

To enable a user to change the queue limit for all interfaces globally use the **hw-module system max-queue-limit** command. To cancel the global setting, use the **no** form of the command.

hw-module system max-queue-limit *max-queue-limit*

no hw-module system max-queue-limit *max-queue-limit*

Syntax Description *max-queue-limit* Specifies the queue limit for all interface. Valid values are from 1024 to 8184. This parameter must be a multiple of 8.

Defaults Not enabled by default

Command Modes Global configuration mode

Usage Guidelines This command allows you to change the queue limit for all interfaces globally rather than apply a policy with a queue limit to all the interfaces.

This is a global configuration command. It can be overriden by the per port, per class, **queue-limit** command.

For a standalone supervisor engine, you must reboot the engine after applying this command. For a redundant supervisor engine, you must enter the **redundancy reload shelf** command to enforce a reboot on both the supervisor engines.

Examples This example shows how to set the queue limit globally to 1024:

```
Switch# enable
Switch# configure terminal
Switch(config)# hw-module system max-queue-limit 1024
Enter the reboot 'hw-module system max-queue-limit'
Switch(config)# exit
Switch# reload /bootdir(cisco supervisor)
Switch# redundancy reload shelf (for redundancy supervisors in IOS mode)
Switch# redundancy force-switchover (followed by another redundancy force-switchover, for
redundancy supervisors in ROM mode
```

instance

To map a VLAN or a set of VLANs to an MST instance, use the **instance** command. To return the VLANs to the common instance default, use the **no** form of this command.

instance *instance-id* {**vlan** *vlan-range*}

no instance *instance-id*

Syntax Description	*instance-id* MST instance in which the specified VLANs are mapped; valid values are from 0 to 15.
	vlan *vlan-range* Specifies the number of the VLANs to be mapped to the specified instance. The number is entered as a single value or a range; valid values are from 1 to 4094.
Defaults	Mapping is disabled.
Command Modes	MST configuration mode
Usage Guidelines	The mapping is incremental, not absolute. When you enter a range of VLANs, this range is added or removed to the existing ones. Any unmapped VLAN is mapped to the CIST instance.

Examples	This example shows how to map a range of VLANs to instance 2:
	`Switch(config-mst)# instance 2 vlan 1-100`
	`Switch(config-mst)#`
	This example shows how to map a VLAN to instance 5:
	`Switch(config-mst)# instance 5 vlan 1020`
	`Switch(config-mst)#`
	This example shows how to move a range of VLANs from instance 2 to the CIST instance:
	`Switch(config-mst)# no instance 2 vlan 40-60`
	`Switch(config-mst)#`
	This example shows how to move all the VLANs mapped to instance 2 back to the CIST instance:
	`Switch(config-mst)# no instance 2`
	`Switch(config-mst)#`

Related Commands

Command	Description
name	Sets the MST region name.
revision	Sets the MST configuration revision number.

Command	Description
show spanning-tree mst	Displays MST protocol information.
spanning-tree mst configuration	Enters the MST configuration submode.

interface

To select an interface to configure and to enter interface configuration mode, use the **interface** command.

interface *type number*

Syntax Description

type	Type of interface to be configured; see Table 2-6 for valid values.
number	Module and port number.

Defaults

No interface types are configured.

Command Modes

Global configuration mode

Usage Guidelines

Table 2-6 lists the valid values for *type*.

Table 2-6 Valid type Values

Keyword	Definition
ethernet	Ethernet IEEE 802.3 interface.
fastethernet	100-Mbps Ethernet interface.
gigabitethernet	Gigabit Ethernet IEEE 802.3z interface.
tengigabitethernet	10-Gigabit Ethernet IEEE 802.3ae interface.
gr-ws	Gigabit Ethernet WAN IEEE 802.3z interface; supported on Catalyst 4500 series switches that are configured with a Supervisor Engine 2 only.
pos	PacketOver SONET interface on Packet over SONET Interface Processor; supported on Catalyst 4500 series switches that are configured with a Supervisor Engine 2 only.
atm	ATM interface; supported on Catalyst 4500 series switches that are configured with a Supervisor Engine 2 only.
vlan	VLAN interface; see the **interface vlan** command.
port-channel	Port-channel interface; see the **interface port-channel** command.
null	Null interface; the valid value is **0**.

Examples

This example shows how to enter the interface configuration mode on the Fast Ethernet interface 2/4:

```
Switch(config)# interface fastethernet4/4
Switch(config-if)#
```

Related Commands

Command	Description
show interfaces	Displays interface information.

interface port-channel

To access or create a port-channel interface, use the **interface port-channel** command.

interface port-channel *channel-group*

Syntax Description:	*channel-group* Port-channel group number; valid values are from 1 to 64.
Defaults:	This command has no default settings.
Command Modes:	Global configuration mode

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 can also create the port channels by entering the **interface port-channel** command. This will create a Layer 3 port channel. To change the Layer 3 port channel into a Layer 2 port channel, use the **switchport** command before you assign the physical interfaces to the channel group. A port channel cannot be changed from Layer 3 to Layer 2 or vice versa when it contains member ports.

Only one port channel in a channel group is allowed.

Caution

The Layer 3 port-channel interface is the routed interface. Do not enable Layer 3 addresses on the physical Fast Ethernet interfaces.

If you want to use CDP, you must configure it only on the physical Fast Ethernet interface and not on the port-channel interface.

Examples:

This example creates a port-channel interface with a channel-group number of 64:

```
Switch(config)# interface port-channel 64
Switch(config)#
```

Related Commands:

Command	Description
channel-group	Assigns and configures an EtherChannel interface to an EtherChannel group.
show ether channel	Displays EtherChannel information for a channel.

interface range

To run a command on multiple ports at the same time, use the **interface range** command.

interface range {**vlan** *vlan_id*~*vlan_id*} {*port-range* | **macro** *macro*}

Syntax Description	**vlan** *vlan_id*~*vlan_id*	Specifies a VLAN range; valid values are from 1 to 4094.
	port-range	Port range; for a list of valid values for *port-range*, see the "Usage Guidelines" section.
	macro *macro*	Specifies the name of a macro.

Defaults	This command has no default settings.
Command Modes	Global configuration mode Interface configuration mode

Usage Guidelines

You can use the **interface range** command on the existing VLAN SVIs only. To display the VLAN SVIs, enter the **show running-config** command. The VLANs that are not displayed cannot be used in the **interface range** command.

The values that are entered with the **interface range** command are applied to all the existing VLAN SVIs.

Before you can use a macro, you must define a range using the **define interface-range** command.

All configuration changes that are made to a port range are saved to NVRAM, but the port ranges that are created with the **interface range** command do not get saved to NVRAM.

You can enter the port range in two ways:

- Specifying up to five port ranges
- Specifying a previously defined macro

You can either specify the ports or the name of a port-range macro. A port range must consist of the same port type, and the ports within a range cannot span the modules.

You can define up to five port ranges on a single command; separate each range with a comma.

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

```
interface range gigabitethernet 5/1 -10, gigabitethernet4/8 -20
```

Use these formats when entering the *port-range*:

- *interface-type {module}/{first-port} - {last-port}*
- *interface-type {module}/{first-port} - {last-port}*

Valid values for *interface-type* are as follows:

- **FastEthernet**
- **GigabitEthernet**

- **Vlan** *vlan_id*

You cannot specify both a macro and an interface-range in the same command. After creating a macro, you can enter additional ranges. If you have already entered an interface range, the CLI does not allow you to enter a macro.

You can specify a single interface in the *port-range* value. This makes the command similar to the **interface** *interface-number* command.

Examples

This example shows how to use the **interface range** command to interface to fE 5/18 - 20:

```
Switch(config)# interface range fastethernet 5/18 - 20
Switch(config-if)#
```

This command shows how to run a *port-range* macro:

```
Switch(config)# interface range macro macro1
Switch(config-if)#
```

Related Commands

Command	Description
define interface-range	Creates a macro of interfaces.
show running-config (refer to Cisco IOS Documentation)	Displays the running configuration for a switch.

interface vlan

To create or access a Layer 3 switch virtual interface (SVI), use the **interface vlan** command. To delete an SVI, use the **no** form of this command.

interface vlan *vlan_id*

no interface vlan *vlan_id*

Syntax Description	*vlan_id* Number of the VLAN; valid values are from 1 to 4094.
Defaults	Fast EtherChannel is not specified.
Command Modes	Global configuration mode

Usage Guidelines

The SVIs are created the first time that you enter the **interface vlan** *vlan_id* command for a particular VLAN. The value, *id* value corresponds to the VLAN tag that is associated with the data frames on an ISL or 802.1Q-encapsulated trunk or the VLAN ID that is configured for an access port. A message is displayed whenever a VLAN interface is newly created, so you can check that you entered the correct VLAN number.

If you delete an SVI by entering the **no interface vlan** *vlan_id* command, the associated interface is forced into an administrative down state and marked as deleted. The deleted interface will no longer be visible in a **show interface** command.

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.

Examples

This example shows the output when you enter the **interface vlan** *vlan_id* command for a new VLAN number:

```
Switch(config)# interface vlan 23
%LINEPROTO-5-UPDOWN: Line protocol
Switch(config)#
```

ip admission proxy http refresh-all

To ensure that you see a customized Web/Auth login page with the same name in the switch system directory as a same-named prior login page, use the **ip admission proxy http refresh-all** command.

ip admission proxy http [success | failure | refresh-all | login [required | page]]

Syntax Description

success	Successful authentication proxy.
failure	Failed authentication proxy.
refresh-all	Refresh all custom html pages.
login required	Specify required webpage.
login page	Specify customized login webpage.

Defaults

If you do not enter this command, if any of the customized web-based authentication page files with the file of same name have been changed, you see the old login page rather than the new file.

Command Modes

Global configuration mode

Usage Guidelines

You should enter this command whenever the customized web-based authentication page has been changed in the system directory.

Examples

This example shows how to enter this command:

```
Switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip admission proxy http [success | failure | refresh-all | login]
Switch(config)# end
Switch#
```

<The new final page is observed.>

ip arp inspection filter vlan

To permit ARPs from hosts that are configured for static IP when DAI is enabled and to define an ARP access list and apply it to a VLAN, use the **ip arp inspection filter vlan** command. To disable this application, use the **no** form of this command.

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	Access control list name.
vlan-range	VLAN number or range; valid values are from 1 to 4094.
static	(Optional) Specifies that the access control list should be applied statically.

Defaults

No defined ARP ACLs are applied to any VLAN.

Command Modes

Global configuration mode

Usage Guidelines

When an ARP access control list is applied to a VLAN for dynamic ARP inspection, the ARP packets containing only the IP-to-Ethernet MAC bindings are compared against the ACLs. All other packet types are bridged in the incoming VLAN without validation.

This command specifies that the incoming ARP packets are compared against the ARP access control list, and the packets are permitted only if the access control list permits them.

If the access control lists deny the packets because of explicit denies, the packets are dropped. If the packets are deny because of an implicit deny, they are then matched against the list of DHCP bindings, if the ACL is not applied statically.

Examples

This example shows how to apply the ARP ACL static hosts to VLAN 1 for DAI:

```
Switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip arp inspection filter static-hosts vlan 1
Switch(config)# end
Switch#
Switch# show ip arp inspection vlan 1
Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

Vlan     Configuration    Operation  ACL Match          Static ACL
----     -------------    ---------  ---------          ----------
   1     Enabled          Active     static-hosts       No

Vlan     ACL Logging      DHCP Logging
----     -----------      ------------
```

```
Jack-Switch#      Deny
Jack-Switch#
```

Related Commands	Command	Description
	ip arp inspection	Defines an ARP access list or adds clauses at the end of a predefined list.
	show ip arp inspection	Displays the status of dynamic ARP inspection for a specific range of VLANs.

ip arp inspection limit (interface)

To limit the rate of incoming ARP requests and responses on an interface and prevent DoS from consuming all of the system's resources in the event of a DoS attack, use the **ip arp inspection limit** command. To release the limit, use the **no** form of this command.

ip arp inspection limit {*rate pps* | **none**} [**burst interval** *seconds*]

no ip arp inspection limit

Syntax Description

rate pps	Specifies an upper limit on the number of incoming packets processed per second. The rate can range from 1 to 10000.
none	Specifies no upper limit on the rate of the incoming ARP packets that can be processed.
burst interval *seconds*	(Optional) Specifies the consecutive interval in seconds over which the interface is monitored for the high rate of the ARP packets. The interval is configurable from 1 to 15 seconds.

Defaults

The rate is set to 15 packets per second on the 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 the trusted interfaces.

The burst interval is set to 1 second by default.

Command Modes

Interface configuration mode

Usage Guidelines

The mode ports should be configured with higher rates to reflect their aggregation. When the rate of the incoming packets exceeds the user-configured rate, the interface is placed into an error-disabled state. The error-disable timeout feature can be used to remove the port from the error-disabled state. The rate limit is applied on the bundled channel ports and on the trunk ports. Rate limiting is applied on the channel ports in non-multicast DAI-enabled VLANs or as the **none** keyword is specified to make the rate unlimited.

The rate of the incoming ARP packets on the channel ports is equal to the sum of the incoming rate of packets from all the channel members. Configure the rate limit for the channel ports only after examining the rate of the incoming ARP packets on the channel members.

After a switch receives ninetieth the configured rate of packets every second consecutively over a period of burst seconds, the interface is placed into an error-disabled state.

Examples

This example shows how to limit the rate of the incoming ARP requests to 25 packets per second:

```
Switch#config terminal
Switch(config)# interface fa5/3
Switch(config-if)# ip arp inspection limit rate 25
Switch(config-if)# end
Switch# show ip arp inspection interfaces fa5/6|begin 6/3
Interface        Trust State       Rate (pps)
---------------  -----------       ----------
Fa5/3            Untrusted         25
Switch#
```

This example shows how to limit the rate of the incoming ARP requests to 20 packets per second and to set the interface monitoring interval to 5 consecutive seconds:

```
Switch# config terminal
Switch(config)# interface fa5/5
Switch(config-if)# ip arp inspection limit rate 20 burst interval 5
Switch(config-if)# end
```

Related Commands

Command	Description
show ip arp inspection	Displays the status of dynamic ARP inspection for a specific range of VLANs.

ip arp inspection log-buffer

To configure the parameters that are associated with the logging buffer, use the **ip arp inspection log-buffer** command. To disable the parameters, use the **no** form of this command.

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 from the logging buffer; the range is from 0 to 1024.
logs number	Number of entries to be logged in an interval; the range is from 0 to 1024. A 0 value indicates that entries should not be logged out of this buffer.
interval seconds	Logging rate; the range is from 0 to 86400 (1 day). A 0 value indicates an immediate log.

Defaults

When dynamic ARP inspection is enabled, denied, or dropped, the ARP packets are logged.

The number of entries is set to 32.

The number of logging entries is limited to 5 per second.

The interval is set to 1.

Command Modes

Global configuration mode

Usage Guidelines

The first dropped packet of a given flow is logged immediately. The subsequent packets for the same flow are expressed as are not logged immediately. Registering these packets is done in a log buffer that is shared by all the VLANs. Entries from this buffer are logged on a rate-controlled basis.

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
Switch(config)#show ip arp inspection log-buffer
Dropped Log Buffer Size : 45
Dynamic Log Buffer Size : 32
Syslog rate : 5 entries per 1 seconds.
No entries in log buffer.
Switch(config)#
```

This example shows how to configure the logging rate to 10 logs per 3 seconds:

```
Switch(config)#ip arp inspection log-buffer logs 10 interval 3
Switch(config)#exit
Switch#show ip arp inspection log
Dropped Log Buffer Size : 45
Dynamic Log Buffer Size : 32
Syslog rate : 10 entries per 3 seconds.
No entries in log buffer.
Switch#
```

Related Commands	Command	Description
	arp access-list	Defines an ARP access-list or adds clauses at the end of a predefined list.
	show ip arp inspection	Displays the status of dynamic ARP inspection for a specific range of VLANs.

ip arp inspection trust

To set a per-port configurable trust state that determines the set of interfaces where incoming ARP packets are inspected, use the **ip arp inspection trust** command. To make the interfaces untrusted, use the **no** form of this command.

ip arp inspection trust

no ip arp inspection trust

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Interface configuration mode

Examples This example shows how to configure an interface to be trusted:

```
Switch(config)# interface fastethernet 6/3
Switch(config-if)# ip arp inspection trust
Switch(config-if)# end
```

To verify the configuration, use the show form of this command:

```
Switch# show ip arp inspection interface fastethernet 6/3

Interface        Trust State    Rate (pps)    Burst Interval
---------------  -----------    ----------    --------------
Fa6/3            Trusted        None          1
Switch#
```

Related Commands	Command	Description
	show ip arp inspection	Displays the status of dynamic ARP inspection for a specific range of VLANs.

ip arp inspection validate

To perform specific checks for ARP inspection, use the **ip arp inspection validate** command. To disable checks, use the **no** form of this command.

ip arp inspection validate [**src-mac**] [**dst-mac**] [**ip**]

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

Syntax Description	**src-mac** (Optional) Checks the source MAC address in the Ethernet header against the sender's MAC address in the ARP body. This checking is done against both ARP requests and responses. **Note** When **src-mac** is enabled, packets with different MAC addresses are classified as invalid and are dropped. **dst-mac** (Optional) Checks the destination MAC address in the Ethernet header against the target MAC address in ARP body. This checking is done for ARP responses. **Note** When **dst-mac** is enabled, the packets with different MAC addresses are classified as invalid and are dropped. **ip** (Optional) Checks the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses. The sender IP addresses are checked in all ARP requests and responses and target IP addresses are checked only in ARP responses.
Defaults	Checks are disabled.
Command Modes	Global configuration mode
Usage Guidelines	When enabling the checks, specify at least one of the keywords (**src-mac**, **dst-mac**, and **ip**) on the command line. Each command overrides the configuration of the previous command. If a command enables **src** and **dst mac** validations, and a second command enables IP validation only, the **src** and **dst mac** validations are disabled as a result of the second command. The **no** form of this command disables only the specified checks. If none of the check options are enabled, all the checks are disabled.

Examples	This example shows how to enable the source MAC validation:
	`Switch(config)# ip arp inspection validate src-mac`
	`Switch(config)# exit`
	`Switch# show ip arp inspection vlan 1`
	`Source Mac Validation : Enabled`
	`Destination Mac Validation : Disabled`
	`IP Address Validation : Disabled`

```
Vlan     Configuration   Operation  ACL Match          Static ACL
----     -------------   ---------  ---------          ----------
   5     Enabled         Active
Vlan     ACL Logging     DHCP Logging
----     -----------     ------------
   5     Deny            Deny
Switch#
```

Related Commands	Command	Description
	arp access-list	Defines an ARP access list or adds clauses at the end of a predefined list.
	show ip arp inspection	Displays the status of dynamic ARP inspection for a specific range of VLANs.

ip arp inspection vlan

To enable dynamic ARP inspection (DAI) on a per-VLAN basis, use the **ip arp inspection vlan** command. To disable DAI, use the **no** form of this command.

ip arp inspection vlan *vlan-range*

no ip arp inspection vlan *vlan-range*

Syntax Description *vlan-range* VLAN number or range; valid values are from 1 to 4094.

Defaults ARP inspection is disabled on all VLANs.

Command Modes Global configuration mode

Usage Guidelines You must specify on which VLANs to enable DAI. DAI may not function on the configured VLANs if they have not been created or if they are private.

Examples This example shows how to enable DAI on VLAN 1:

```
Switch#configure terminal
Switch(config)# ip arp inspection vlan 1
Switch(config)#end
Switch#show ip arp inspection vlan 1

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
Vlan    Configuration    Operation   ACL Match          Static ACL
----    -------------    ---------   ---------          ----------
  1       Enabled         Active
Vlan    ACL Logging      DHCP Logging
----    -----------      ------------
  1       Deny             Deny

Switch#
```

This example shows how to disable DAI on VLAN 1:

```
Switch#configure terminal
Switch(config)# no ip arp inspection vlan 1
Switch(config)#
```

Related Commands

Command	Description
arp access-list	Defines an ARP access list or adds clauses at the end of a predefined list.
show ip arp inspection	Displays the status of dynamic ARP inspection for a specific range of VLANs.

ip arp inspection vlan logging

To control the type of packets that are logged, use the **ip arp inspection vlan logging** command. To disable this logging control, use the **no** form of this command.

ip arp inspection vlan *vlan-range* **logging** {**acl-match** | **matching**[*name*] | **dhcp-bindings** {**permit** | **all**[*name*]}

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

Syntax Description

vlan-range	Number of the VLANs to be mapped to the specified instance. The number is entered as a single value or a range; valid values are from 1 to 4094.
acl-match	Specifies the logging criteria for packets that are dropped or permitted based on ACL matches.
matching	Specifies the logging of packets matched against ACLs is controlled by the **matching** keyword in the permit and deny access control entries of the ACL. **Note** By default, the **matching** keyword is not available on the ACEs. Whether the keyword is used, denied packets are not logged. Packets are logged only when they match against an ACE that has the **matching** keyword.
name	Specifies that ACL matched packets are not logged.
dhcp-bindings	Specifies the logging criteria for packets dropped or permitted based on matches against the DHCP bindings.
permit	Specifies logging when permitted by DHCP bindings.
all	Specifies logging when permitted or denied by DHCP bindings.
name	Prevents all logging of packets permitted or denied by DHCP bindings.

Defaults

All denied or dropped packets are logged.

Command Modes

Global configuration mode

Usage Guidelines

The **acl-match** and **dhcp-bindings** keywords merge with each other. When you set an ACL match configuration, the DHCP bindings configuration is not disabled. You can use the **no** form of this command to reset some of the logging criteria to their defaults. If you do not specify either option, all the logging types are reset to log on when the ARP packets are denied. The two options that are available to you are as follows:

- **acl-match**—Logging on ACL matches is reset to log on deny
- **dhcp-bindings**—Logging on DHCP binding comparison is reset to log on deny

Examples

This examples shows how to configure an ARP inspection on VLAN 1 in addition to a log on matching against the ACLs with the **logging** keyword:

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

```
Switch(config)# ip arp inspection vlan 1 logging acl-match matchlog
Switch(config)# end
Switch# show ip arp inspection vlan 1

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

Vlan     Configuration    Operation   ACL Match          Static ACL
----     -------------    ---------   ---------          ----------
   1     Enabled          Active
Vlan     ACL Logging      DHCP Logging
----     -----------      ------------
   1     Acl-Match        Deny
Switch#
```

Related Commands	Command	Description
	arp access-list	Defines an ARP access list or adds clauses at the end of a predefined list
	show ip arp inspection	Displays the status of dynamic ARP inspection for a specific range of VLANs.

ip cef load-sharing algorithm

To configure the load-sharing hash function so that the source TCP/UDP port, the destination TCP/UDP port, or both ports can be included in the hash in addition to the source and destination IP addresses, use the **ip cef load-sharing algorithm** command. To revert back to the default, which does not include the ports, use the **no** form of this command.

ip cef load-sharing algorithm {**include-ports** {**source** *source*} {**destination** *dest*} | **original** | **tunnel** | **universal**}

no ip cef load-sharing algorithm {**include-ports** {**source** *source*} {**destination** *dest*} | **original** | **tunnel** | **universal**}

Syntax Description

include-ports	Specifies the algorithm that includes the Layer 4 ports.
source *source*	Specifies the source ports in the load-balancing hash function.
destination *dest*	Specifies the destination port in the load-balancing hash. Uses the source and destination in hash function.
original	Specifies the original algorithm; not recommended.
tunnel	Specifies the algorithm for use in tunnel-only environments.
universal	Specifies the default Cisco IOS load-sharing algorithm.

Defaults

Default load-sharing algorithm is disabled.

Note This option does not include the source or destination port in the load-balancing hash.

Command Modes

Global configuration mode

Usage Guidelines

The original algorithm, tunnel algorithm, and universal algorithm are created through the hardware. For software-routed packets, the algorithms are handled by the software. The **include-ports** option does not apply in the software-switched traffic.

Examples

This example shows how to configure the IP CEF load-balancing algorithm that includes Layer 4 ports:

```
Switch(config)# ip cef load-sharing algorithm include-ports
Switch(config)#
```

This example shows how to configure the IP CEF load-sharing algorithm that includes Layer 4 tunneling pads:

```
Switch(config)# ip ref load-sharing algorithm include-port tunnel
Switch(config)#
```

Related Commands	Command	Description
	show ip ref vlan	Displays the IP CEF VLAN interface status and configuration information.

ip device tracking maximum

To enable IP port security binding tracking on a Layer 2 port, use the **ip device tracking maximum** command. To disable IP port security on a routed Layer 2 interface, use the **no** form of this command.

ip device tracking maximum *{number}*

no ip device tracking maximum *{number}*

Syntax Description

number	Specifies the number of bindings created in the IP device tracking table for a port, valid values are from 0 to 20-48.

Defaults

This command has no default settings.

Command Modes

Interface configuration mode

Examples

This example shows how to enable IP port security with IP-MAC filters on a Layer 2 access port:

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip device tracking
Switch(config)# interface fastethernet 4/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 1
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 5
Switch(config-if)# ip verify source tracking port-security
Switch(config-if)# end
```

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

Related Commands

Command	Description
ip verify source	Enables IP source guard on untrusted Layer 2 interfaces.
show ip verify source	Displays the IP source guard configuration and filters on a particular interface.

ip dhcp snooping

To enable DHCP snooping globally, use the **ip dhcp snooping** command. To disable DHCP snooping, use the **no** form of this command.

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 mode

Usage Guidelines You must enable DHCP snooping globally before you can use DHCP snooping on a VLAN.

Examples This example shows how to enable DHCP snooping:

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

This example shows how to disable DHCP snooping:

```
Switch(config)# no ip dhcp snooping
Switch(config)#
```

Related Commands

Command	Description
ip dhcp snooping information option	Enables DHCP option 82 data insertion.
ip dhcp snooping limit rate	Configures the number of the DHCP messages that an interface can receive per second.
ip dhcp snooping trust	Enables DHCP snooping on a trusted VLAN.
ip dhcp snooping vlan	Enables DHCP snooping on a VLAN or a group of VLANs.
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.

ip dhcp snooping binding

To set up and generate a DHCP binding configuration to restore bindings across reboots, use the **ip dhcp snooping binding** command. To disable the binding configuration, use the **no** form of this command.

ip dhcp snooping binding *mac-address* **vlan** *vlan-#* *ip-address* **interface** *interface* **expiry** *seconds*

no ip dhcp snooping binding *mac-address* **vlan** *vlan-#* *ip-address* **interface** *interface*

Syntax Description	*mac-address*	Specifies a MAC address.
	vlan *vlan-#*	Specifies a valid VLAN number.
	ipaddr	Specifies an IP address.
	interface *interface*	Specifies an interface type and number.
	expiry *seconds*	Specifies the interval (in seconds) after which binding is no longer valid.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Usage Guidelines Whenever a binding is added or removed using this command, the binding database is marked as changed and a write is initiated.

Examples This example shows how to generate a DHCP binding configuration on interface gigabitethernet1/1 in VLAN 1 with an expiration time of 1000 seconds:

```
Switch> ip dhcp snooping binding 0001.1234.1234 vlan 1 172.20.50.5 interface gi1/1 expiry 1000
Switch>
```

Related Commands

Command	Description
ip dhcp snooping	Globally enables DHCP snooping.
ip dhcp snooping information option	Enables DHCP option 82 data insertion.
ip dhcp snooping trust	Enables DHCP snooping on a trusted VLAN.
ip dhcp snooping vlan	Enables DHCP snooping on a VLAN or a group of VLANs.
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.

ip dhcp snooping database

To store the bindings that are generated by DHCP snooping, use the **ip dhcp snooping database** command. To either reset the timeout, reset the write-delay, or delete the agent specified by the URL, use the no form of this command.

ip dhcp snooping database {*url* | **timeout** *seconds* | **write-delay** *seconds*}

no ip dhcp snooping database {**timeout** | **write-delay**}

Syntax Description

url	Specifies the URL in one of the following forms: • file:/<*base*>/<*filename*> • ftp://<*user*>:<*password*>@<*host*>/<*filename*> • rcp://<*user*>@<*host*>/<*filename*> • nvram:/<*filename*> • bootflash:/<*filename*>
timeout *seconds*	Specifies when to abort the database transfer process after a change to the binding database. The minimum value of the delay is 15 seconds. 0 is defined as an infinite duration.
write-delay *seconds*	Specifies the duration for which the transfer should be delayed after a change to the binding database.

Defaults

The timeout value is set to 300 seconds (5 minutes).

The write-delay value is set to 300 seconds.

Command Modes

Interface configuration mode

Usage Guidelines

You need to create an empty file at the configured URL on network-based URLs (such as TFTP and FTP) before the switch can write the set of bindings for the first time at the URL.

Note Because both NVRAM and bootflash have limited storage capacity, using TFTP or network-based files is recommended. If you use flash to store the database file, new updates (by the agent) result in the creation of new files in the flash (quickly). In addition, due to the nature of the file system used on the flash, a large number of files creates errors to be considerably slowed. When a file is stored in a remote location accessible through TFTP, or RPR/SSO stateful supervisor engine can take over the binding list when a switchover occurs.

Examples

This example shows how to store a database file with the IP address 10.1.1.1 within a directory called directory. A file name will be created in the TFTP server.

```
Switch# sockip terminal
Switch(config)# ip dhcp snooping database tftp://10.1.1.1/directory/file
Switch(config)# ^Z
Switch# show ip dhcp snooping database
Agent URL : tftp://10.1.1.1/directory/file
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : Not Running
Abort Timer Expiry : Not Running

Last Succeeded Time : None
Last Failed Time : None
Last Failed Reason : No failure recorded.

Total Attempts      :   1  Startup Failures :   0
Startup Failures    :   0  Successful Reads :   0
Successful Reads    :   0  Failed Reads     :   0
Successful Writes   :   0  Failed Writes    :   0
Media Failures      :   0

Switch#
```

Related Commands

Command	Description
ip dhcp snooping	Globally enables DHCP snooping.
ip dhcp snooping binding	Sets up and gives data a DHCP binding configuration to ensure bindings across reboots.
ip dhcp snooping information option	Enables DHCP option 82 data insertion.
ip dhcp snooping trust	Enables DHCP snooping on a trusted VLAN.
ip dhcp snooping vlan	Enables DHCP snooping on a VLAN or a group of VLANs.
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.

ip dhcp snooping information option

To enable DHCP option 82 data insertion, use the **ip dhcp snooping information option** command. To disable DHCP option 82 data insertion, use the **no** form of this command.

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

no ip dhcp snooping information option format remote-id [hostname | *string* [*word*]]

Syntax Description	**format**	Specifies the option 82 information format.
	remote-id	Specifies the remote ID for option 82.
	hostname	Specifies the user-configured hostname for the remote ID.
	string *word*	Specifies the user-defined string for the remote ID. The word string can be from 1 to63 characters long with no spaces.

Defaults DHCP option 82 data insertion is enabled.

Command Modes Global configuration mode

Usage Guidelines If the hostname is longer than 63 characters it is truncated to 63 characters in the remote ID.

Examples This example shows how to enable DHCP option 82 data insertion:

```
Switch(config)# ip dhcp snooping information option
Switch(config)#
```

This example shows how to disable DHCP option 82 data insertion:

```
Switch(config)# no ip dhcp snooping information option
Switch(config)#
```

This example shows how to configure the hostname as the remote ID:

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

The following example shows how to enable DHCP Snooping on VLAN 500 through 555 and option 82 remote ID:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 500 555
Switch(config)# ip dhcp snooping information option format remote-id string switch123
Switch(config)# interface GigabitEthernet 5/1
Switch(config-if)# ip dhcp snooping trust
Switch(config-if)# ip dhcp snooping limit rate 100
Switch(config)# ip dhcp snooping vlan 555 information option format-type circuit-id
string customer555
Switch(config-if)# interface FastEthernet 2/1
```

```
Switch(config)#ip dhcp snooping vlan 555 information option format-type circuit-id
string customer1
Switch(config)# end
Switch#show ip dhcp snooping
```

Related Commands

Command	Description
ip dhcp snooping	Globally enables DHCP snooping.
ip dhcp snooping binding	Sets up and gives arm a DHCP binding configuration to restore bindings across reboots.
ip dhcp snooping information option	Enables DHCP option 82 data insertion.
ip dhcp snooping limit rate	Configures the number of the DHCP messages that an interface can receive per second.
ip dhcp snooping trust	Enables DHCP snooping on a trusted VLAN.
ip dhcp snooping vlan	Enables DHCP snooping on a VLAN or a group of VLANs.
ip dhcp snooping vlan information option format-type circuit-id string	Enables create or to add option of DHCP snooping option-82) on a VLAN.
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.

ip dhcp snooping information option allow-untrusted

To allow DHCP packets with option 82 data inserted to be received from a snooping untrusted port, use the **ip dhcp snooping information option allow-untrusted** command. To disallow receipt of these DHCP packets, use the **no** form of this command.

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 DHCP packets with option 82 are not allowed on snooping untrusted ports.

Command Modes Global configuration mode

Examples This example shows how to allow DHCP packets with option 82 data inserted to be received from a snooping untrusted port:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip dhcp snooping information option allow-untrusted
Switch(config)# end
Switch#
```

Related Commands

Command	Description
ip dhcp snooping	Globally enables DHCP snooping.
ip dhcp snooping information option	Enables DHCP option 82 data insertion.
ip dhcp snooping limit rate	Configures the number of the DHCP messages that an interface can receive per second.
ip dhcp snooping trust	Enables DHCP snooping on a trusted VLAN.
ip dhcp snooping vlan	Enables DHCP snooping on a VLAN or a group of VLANs.
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.

ip dhcp snooping limit rate

To configure the number of the DHCP messages that an interface can receive per second, use the **ip dhcp snooping limit rate** command. To disable the DHCP snooping rate limiting, use the **no** form of this command.

ip dhcp snooping limit rate *rate*

no ip dhcp snooping limit rate

Syntax Description | *rate* Number of DHCP messages a switch can receive per second.

Defaults | DHCP snooping rate limiting is disabled.

Command Modes | Interface configuration mode

Usage Guidelines | Typically, the rate limit applies to the untrusted interfaces. If you want to set up rate limiting for the trusted interface, note that the trusted interfaces aggregate all DHCP traffic in the switch, and you will need to adjust the rate limit of the interfaces to a higher value.

Examples | This example shows how to enable the DHCP message rate limiting:

```
Switch(config)#int fa gi/0/1 ip dhcp snooping limit rate 150
Switch(config)#
```

This example shows how to disable the DHCP message rate limiting:

```
Switch(config)#int fa gi/0/1 no ip dhcp snooping limit rate
Switch(config)#
```

Related Commands:

Command	Description
ip dhcp snooping	Globally enables DHCP snooping.
ip dhcp snooping information option	Enables DHCP option 82 data insertion.
ip dhcp snooping trust	Enables DHCP snooping on a trusted VLAN.
ip dhcp snooping vlan	Enables DHCP snooping on a VLAN or a group of VLANs.
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.

ip dhcp snooping trust

To configure an interface as trusted for DHCP snooping purposes, use the **ip dhcp snooping trust** command. To configure an interface as untrusted, use the **no** form of this command.

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 mode

This example shows how to enable DHCP snooping trust on an interface:

```
Switch(config)# ip dhcp snooping trust
Switch(config)#
```

This example shows how to disable DHCP snooping trust on an interface:

```
Switch(config)# no ip dhcp snooping trust
Switch(config)#
```

Related Commands

Command	Description
ip dhcp snooping	Globally enables DHCP snooping.
ip dhcp snooping information option	Enables DHCP option 82 data insertion.
ip dhcp snooping limit rate	Configures the number of the DHCP messages that an interface can receive per second.
ip dhcp snooping vlan	Enables DHCP snooping on a VLAN or a group of VLANs.
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.

ip dhcp snooping vlan

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

ip dhcp snooping [**vlan** number]

no dhcp snooping [**vlan** number]

Syntax Description	**vlan** number (Optional) Single VLAN number or a range of VLANs; valid values are from 1 to 4094.
Defaults	DHCP snooping is disabled.
Command Modes	Global configuration mode
Usage Guidelines	DHCP snooping is enabled on a VLAN only if both global snooping and the VLAN snooping are enabled.

Examples	This example shows how to enable DHCP snooping on a VLAN:
	`Switch(config)# ip dhcp snooping vlan 10`
	`Switch(config)#`
	
	This example shows how to disable DHCP snooping on a VLAN:
	`Switch(config)# no ip dhcp snooping vlan 10`
	`Switch(config)#`
	
	This example shows how to enable DHCP snooping on a group of VLANs:
	`Switch(config)# ip dhcp snooping vlan 10 55`
	`Switch(config)#`
	
	This example shows how to disable DHCP snooping on a group of VLANs:
	`Switch(config)# no ip dhcp snooping vlan 10 55`
	`Switch(config)#`

Related Commands	Command	Description
	ip dhcp snooping	Globally enables DHCP snooping.
	ip dhcp snooping information option	Enables DHCP option 82 data insertion.
	ip dhcp snooping limit rate	Configures the number of the DHCP messages that an interface can receive per second.
	ip dhcp snooping trust	Enables DHCP snooping on a trusted VLAN.
	ip dhcp snooping vlan information option format-type circuit-id string	Enables circuit-id option delimiter of DHCP snooping option 82 on a VLAN.
	show ip dhcp snooping	Displays the DHCP snooping configuration.
	show ip dhcp snooping binding	Displays the DHCP snooping binding entries.

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

To enable circuit-id (a suboption of DHCP snooping option 82) on a VLAN, use the **ip dhcp snooping vlan information option format-type circuit-id string** command. To disable circuit-id on a VLAN, use the **no** form of this command.

ip dhcp snooping vlan *number* **information option format-type circuit-id** [*override*] *string*

no ip dhcp snooping vlan *number* **information option format-type circuit-id** [*override*] *string*

Syntax Description

number	Specifies single or range of VLANs; valid values are from 1 to 4094.
override	(Optional) Specifies an override string.
string	Specifies a user-defined string for the circuit ID (range of 3 to63 ASCII characters with no spaces).

Defaults

With VLAN-port, if DHCP snooping option-82 is disabled.

Command Modes

Interface configuration

Usage Guidelines

The circuit-id suboption of DHCP option82 is supported only when DHCP snooping is globally enabled and on VLANs using DHCP option 82.

This command allows you to configure a string of ASCII characters to be the circuit ID. When you want to override the vlan-mod-port format type and insend use the circuit-ID to define subscriber information, use the **override** keyword.

Examples

The following example shows how to enable DHCP snooping on VLANS500through 555 and option 82 circuit-id:

```
Switch#no snooping vlan500
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 500 555
Switch(config)# ip dhcp snooping information option format remote-id string switch123
Switch(config)# interface GigabitEthernet 3/4
Switch(config-if)# ip dhcp snooping trust
Switch(config-if)# ip dhcp snooping limit rate 100
Switch(config-if)# ip dhcp snooping vlan 555 information option format-type circuit-id
string customer-555
Switch(config)# interface FastEthernet 2/1
Switch(config-if)# ip dhcp snooping vlan 555 information option format-type circuit-id
string customer-555
Switch(config-if)# end
```

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

```
Switch(config)# ip dhcp snooping vlan 250 information option format-type circuit-id
string string hostname
```

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

Note The show **ip dhcp snooping** user EXEC command only displays the global command output, including a minimum-VID 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	Globally enables DHCP snooping.
	ip dhcp snooping information option	Enables DHCP option 82 data insertion.
	ip dhcp snooping limit rate	Configures the number of the DHCP messages that an interface can receive per second.
	ip dhcp snooping trust	Enables DHCP snooping on a trusted VLAN.
	ip dhcp snooping vlan	Enables DHCP snooping on a VLAN or a group of VLANs.
	show ip dhcp snooping	Displays the DHCP snooping configuration.
	show ip dhcp snooping binding	Displays the DHCP snooping binding entries.

ip igmp filter

To control whether all hosts on a Layer 2 interface can join one or more IP multicast groups by applying an IGMP profile to the interface, use the **ip igmp filter** command. To remove a profile from the interface, use the **no** form of this command.

ip igmp filter *profile number*

no ip igmp filter

Syntax Description	*profile number* IGMP profile number to be applied; valid values are from 1 to 4294967295.
Defaults	Profiles are not applied.
Command Modes	Interface configuration mode
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 interface only one profile applied to it.

Examples	This example shows how to apply IGMP profile 22 to an interface:
	`Switch(config)# interface gigabitethernet1/1`
	`Switch(config-if)# ip igmp filter 22`
	`Switch(config-if)#`

Related Commands	Command	Description
	ip igmp profile	Creates an IGMP profile.
	show ip igmp profile	Displays all configured IGMP profiles or a specified IGMP profile.

ip igmp max-groups

To set the maximum number of IGMP groups that a Layer 2 interface can join, use the **ip igmp max-groups** command. To set the maximum back to the default, use the **no** form of this command.

ip igmp max-groups *number*

no ip igmp max-groups

Syntax Description

number Maximum number of IGMP groups that an interface can join; valid values are from 0 to 4294967294.

Defaults

No maximum limit.

Command Modes

Interface configuration mode

Usage Guidelines

You can use the **ip igmp max-groups** command only on Layer 2 physical interfaces; you cannot set the IGMP maximum groups for the routed ports, the switch virtual interfaces (SVIs), or the ports that belong to an EtherChannel group.

Examples

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

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip igmp max-groups 25
Switch(config-if)#
```

ip igmp profile

To create an IGMP profile, use the **ip igmp profile** command. To delete the IGMP profile, use the **no** form of this command.

ip igmp profile *profile number*

no ip igmp profile *profile number*

Syntax Description	*profile number* IGMP profile number being configured; valid values are from 1 to 4294967295.
Defaults	No profile created.
Command Modes	Global configuration mode IGMP profile configuration
Usage Guidelines	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 3 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# conf ig 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`
	`Switch(config-igmp-profile)# exit`

Related Commands

Command	Description
ip igmp filter	Controls whether all hosts on a Layer 2 interface can join one or more IP multicast groups by applying an IGMP profile to the interface.
show ip igmp profile	Displays all configured IGMP profiles or a specified IGMP profile.

ip igmp query-interval

To configure the frequency that the switch sends the IGMP host-query messages, use the **ip igmp query-interval** command. To return to the default frequency, use the **no** form of this command.

ip igmp query-interval *seconds*

no ip igmp query-interval

Syntax Description

seconds	Frequency, in seconds, at which the IGMP host-query messages are transmitted; valid values depend on the IGMP snooping mode. See the "Usage Guidelines" section for more information.

Defaults

The query interval is set to 60 seconds.

Command Modes

Interface configuration mode

Usage Guidelines

If you use the default IGMP snooping configuration, the valid query interval values are from 1 to 65535 seconds. If you have change the default configuration to support CGMP as the IGMP snooping learning method, the valid query interval values are from 1 to 300 seconds.

The designated switch for a vlan is the only switch that sends the IGMP host-query messages. For IGMP version 1, the designated switch is elected according to the multicast routing protocol that runs on the LAN. For IGMP version 2, the designated querier is the lowest IP-addressed multicast switch on the subnet.

If no queries are heard for the timeout period (controlled by the **ip igmp query-timeout** command), the switch becomes the querier.

Note Changing the timeout period may severely impact multicast forwarding.

Examples

This example shows how to change the frequency at which the designated switch sends the IGMP host-query messages:

```
Switch(config)# int fa gigabitethernet 1/1
Switch(config-if)# ip igmp query-interval 120
Switch(config-if)#
```

Related Commands

Command	Description
ip igmp querier-timeout (refer to Cisco IOS documentation)	Configure the timeout period before the router takes over as the querier for the interface after the previous querier has stopped querying.

Command	Description
ip pim query-interval (refer to Cisco IOS documentation)	Configures the frequency of Protocol Independent Multicast (PIM) router query messages.
show ip igmp groups (refer to Cisco IOS documentation)	Displays the multicast groups with receivers that are directly connected to the router and that were learned through Internet Group Management Protocol (IGMP), use the **show ip igmp groups** command in EXEC mode.

ip igmp snooping

To enable IGMP snooping, use the **ip igmp snooping** command. To disable IGMP snooping, use the **no** form of this command.

ip igmp snooping [**tcn** [**flood query count** *count*| **query solicit**]]

no ip igmp snooping [**tcn** [**flood query count** *count*| **query solicit**]]

Syntax Description

tcn	(Optional) Specifies the topology change configuration.
flood	(Optional) Specifies to flood the spanning tree table to the network when a topology change occurs.
query	(Optional) Specifies the TCN query configuration.
count *count*	(Optional) Specifies how often the spanning tree table is flooded; valid values are from 1 to 10.
solicit	(Optional) Specifies an IGMP general query.

Defaults

IGMP snooping is enabled.

Command Modes

Global configuration mode

Interface configuration mode

Usage Guidelines

The **tcn flood** option applies only to Layer-2 switch ports and EtherChannels; it does not apply to routed ports, VLAN interfaces, or Layer-3 channels.

The **ip igmp snooping vlan mrouter** is disabled by default on multicast routers.

Note You can use the **tcn flood** option in interface configuration mode.

Examples

This example shows how to enable IGMP snooping:

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

This example shows how to disable IGMP snooping:

```
Switch(config)# no ip igmp snooping
Switch(config)#
```

This example shows how to enable the flooding of the spanning tree table to the network after nine topology changes have occurred:

```
Switch(config)# ip igmp snooping tcn flood query count 9
Switch(config)#
```

This example shows how to disable the flooding of the spanning tree table to the network:

```
Switch(config)# no ip igmp snooping vlan 41add
Switch(config)#
```

This example shows how to enable an IGMP general query:

```
Switch(config)# ip igmp snooping vlan query solicit
Switch(config)#
```

This example shows how to disable an IGMP general query:

```
Switch(config)# no ip igmp snooping vlan query solicit
Switch(config)#
```

Related Commands	Command	Description
	ip igmp snooping vlan immediate-leave	Enable IGMP immediate-leave processing.
	ip igmp snooping vlan mrouter	Configures a Layer 2 interface as a multicast router interface for a VLAN.
	ip igmp snooping vlan static	Configures a Layer 2 interface as a member of a group.

ip igmp snooping report-suppression

To enable report suppression, use the **ip igmp snooping report-suppression** command. To disable report suppression and forward the reports to the multicast devices, use **no** form of this command.

ip igmp snooping report-suppression

no igmp snooping report-suppression

Syntax Description This command has no arguments or keywords.

Defaults IGMP snooping report-suppression is enabled.

Command Modes Global configuration mode

Usage Guidelines If the **ip igmp snooping report-suppression** command is disabled, all the IGMP reports are forwarded to the multicast devices.

If the command is enabled, report suppression is done by IGMP snooping.

Examples This example shows how to enable report suppression:

```
Switch(config)# ip igmp snooping report-suppression
Switch(config)#
```

This example shows how to disable report suppression:

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

This example shows how to display the system status for report suppression:

```
Switch# show ip igmp snooping
vlan 1
--------
IGMP snooping is globally enabled
IGMP snooping TCN solicit query is globally disabled
IGMP snooping flood query count is 2 in vlan 1
IGMP snooping is enabled on this Vlan
IGMP snooping Immediate Leave is disabled on this Vlan
IGMP snooping mrouter learn mode is pim-dvmrp on this Vlan
IGMP snooping is running in IGMP_ONLY mode on this Vlan
IGMP snooping report suppression is enabled on this Vlan
Switch#
```

Related Commands	Command	Description
	ip igmp snooping vlan immediate-leave	Enable IGMP immediate-leave processing.
	ip igmp snooping vlan mrouter	Configures a Layer 2 interface as a multicast router interface for a VLAN.
	ip igmp snooping vlan static	Configures a Layer 2 interface as a member of a group.

ip igmp snooping vlan

To enable IGMP snooping for a VLAN, use the **ip igmp snooping vlan** command. To disable IGMP snooping, use the **no** form of this command.

ip igmp snooping vlan *vlan-id*

no ip igmp snooping vlan *vlan-id*

Syntax Description *vlan-id* Number of the VLAN; valid values are from 1 to 1001 and from 1006 to 4094.

Defaults IGMP snooping is disabled.

Command Modes Global configuration mode

Usage Guidelines This command is entered in VLAN interface configuration mode only.

The **ip igmp snooping vlan** command is disabled by default on multicast routers.

Examples This example shows how to enable IGMP snooping on a VLAN:

```
Switch(config)# ip igmp snooping vlan 250
Switch(config)#
```

This example shows how to disable IGMP snooping on a VLAN:

```
Switch(config)# no ip igmp snooping vlan 250
Switch(config)#
```

Related Commands

Command	Description
ip igmp snooping vlan immediate-leave	Enable IGMP immediate-leave processing.
ip igmp snooping vlan mrouter	Configures a Layer 2 interface as a multicast router interface for a VLAN.
ip igmp snooping vlan static	Configures a Layer 2 interface as a member of a group.

ip igmp snooping vlan explicit-tracking

To enable per-VLAN explicit host tracking, use the **ip igmp snooping vlan explicit-tracking** command. To disable explicit host tracking, use the **no** form of this command.

ip igmp snooping vlan *vlan-id* **explicit-tracking**

no ip igmp snooping vlan *vlan-id* **explicit-tracking**

Syntax Description

vlan_id	(Optional) Specifies a VLAN; valid values are from 1 to 4094 and from 4096 to 4094.

Defaults

Explicit host tracking is enabled.

Command Modes

Global configuration mode

Examples

This example shows how to disable IGMP explicit host tracking on interface VLAN 200 and how to verify the configuration:

```
Switch>(config)# no ip igmp snooping vlan 200 explicit-tracking
Switch>(config)# end
Switch# show ip igmp snooping vlan 200 | include explicit-tracking
Global IGMP Snooping Configuration:
---------------------------------
IGMP snooping              : Enabled
IGMPv3 snooping            : Enabled
Report suppression         : Enabled
TCN solicit query          : Disabled
TCN flood query count      : 2

Vlan 2:
------
IGMP snooping              : Enabled
IGMPv2 immediate leave     : Disabled
Explicit host tracking     : Disabled
Multicast router learning mode : pim-dvmrp
IP address for IGMP queries on this vlan : 1.1.1.1
Explicit host tracking     : Disabled
Switch#
```

Related Commands

Command	Description
ip igmp snooping vlan immediate-leave	Enables IGMP immediate-leave processing.
ip igmp snooping vlan mrouter	Configures a type-7 interface as a static mrouter interface for a VLAN.
ip igmp snooping vlan static	Configures a type-2 interface as a member of a group.
show ip igmp snooping membership	Displays host membership information.

ip igmp snooping vlan immediate-leave

To enable IGMP immediate-leave processing, use the **ip igmp snooping vlan immediate-leave** command. To disable immediate-leave processing, use the **no** form of this command.

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

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

Syntax Description	*vlan_num* Number of the VLAN; valid values are from 1 to 4094.
	immediate-leave Enables immediate-leave processing.
Defaults	Immediate-leave processing is disabled.
Command Modes	Global configuration mode
Usage Guidelines	You enter this command in global configuration mode only. Use the immediate-leave feature only when there is a single receiver for the MAC group for a specific VLAN. 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 4:
	`Switch(config)# ip igmp snooping vlan 4 immediate-leave`
	`Switch(config)#`
	This example shows how to disable IGMP immediate-leave processing on VLAN 4:
	`Switch(config)# no ip igmp snooping vlan 4 immediate-leave`
	`Switch(config)#`

Related Commands	Command	Description
	ip igmp snooping	Enables IGMP snooping.
	ip igmp snooping vlan mrouter	Configures a Layer 2 interface as a multicast router interface for a VLAN.
	ip igmp snooping vlan static	Configures a Layer 2 interface as a member of a group.
	show ip igmp interface	Displays the information about the IGMP interface status and configuration.
	show mac address-table multicast	Displays information about the multicast MAC address table.

ip igmp snooping vlan mrouter

To statically configure an Layer 2 interface as a multicast router interface for a VLAN, use the **ip igmp snooping vlan mrouter** command. To remove the configuration, use the **no** form of this command.

ip igmp snooping vlan *vlan-id* **mrouter** {**interface** {**fastethernet** *slot/port*} | **gigabitethernet** *slot/port*} | **tengigabitethernet** *slot/port*} | **port-channel** *number*}} | **learn** {**cgmp** | **pim-dvmrp**}}

no ip igmp snooping vlan *vlan-id* **mrouter** {**interface** {**fastethernet** *slot/port*} | **gigabitethernet** *slot/port*} | **tengigabitethernet** *slot/port*} | **port-channel** *number*}} | **learn** {**cgmp** | **pim-dvmrp**}}

Syntax Description

vlan *vlan-id*	Specifies the VLAN ID number to use in the command; valid values are from 1 to 4094.
interface	Specifies the next-hop interface to a multicast router.
fastethernet *slot/port*	Specifies the Fast Ethernet interface; number of the slot and port.
gigabitethernet *slot/port*	Specifies the Gigabit Ethernet interface; number of the slot and port.
tengigabitethernet *slot/port*	Specifies the 10-Gigabit Ethernet interface; number of the slot and port.
port-channel *number*	Port-channel number; valid values are from 1 to 64.
learn	Specifies the multicast switch learning method.
cgmp	Specifies the multicast switch snooping CGMP packets.
pim-dvmrp	Specifies the multicast switch snooping PIM-DVMRP packets.

Defaults

Multicast switch snooping PIM-DVMRP packets are specified.

Command Modes

Interface configuration mode

Usage Guidelines

Was enter this command in VLAN interface configuration mode only.

The interface to the switch must be in the VLAN where you are entering the command. It must be both administratively up and line protocol up.

The CGMP learning method can decrease control traffic.

The learning method that you configure is saved in NVRAM.

The static connections to multicast interfaces are supported only on switch interfaces.

Examples

This example shows how to specify the next-hop interface to a multicast switch:

```
Switch(config-if)# ip igmp snooping vlan2 mrouter interface fastethernet 5/6
Switch(config-if)#
```

This example shows how to specify the multicast switch learning method:

```
Switch(config)# ip igmp snooping 400 mrouter learn cgmp
Switch(config)#
```

Related Commands	Command	Description
	ip igmp snooping	Enables IGMP snooping.
	ip igmp snooping vlan immediate leave	Enables IGMP immediate leave processing.
	ip igmp snooping vlan static	Configures a Layer 2 interface as a member of a group.
	show ip igmp snooping	Displays information on dynamically learned and manually configured VLAN switch interfaces.
	show ip igmp snooping mrouter	Displays information on the dynamically learned and manually configured multicast switch interfaces.

ip igmp snooping vlan static

To configure a Layer 2 interface as a member of a group, use the **ip igmp snooping vlan static** command. To remove the configuration, use the **no** form of this command.

ip igmp snooping vlan *vlan_num* **static** *mac-address* {**interface** {**fastethernet** *slot/port*} | {**gigabitethernet** *slot/port*} | {**tengigabitethernet** *slot/port*} | {**port-channel** *number*}}

no ip igmp snooping vlan *vlan_num* **static** *mac-address* {**interface** {**fastethernet** *slot/port*} | {**gigabitethernet** *slot/port*} | {**tengigabitethernet** *mod/interface-number*} | {**port-channel** *number*}}

Syntax Description

vlan_num	Number of the VLAN.
mac-address	Group MAC address.
interface	Specifies the next-hop interface to multicast switch.
fastethernet *slot/port*	Specifies the Fast Ethernet interface, number of the slot and port.
gigabitethernet *slot/port*	Specifies the Gigabit Ethernet interface, number of the slot and port.
tengigabitethernet *slot/port*	Specifies the 10-Gigabit Ethernet interface, number of the slot and port.
port-channel *number*	Port-channel number; valid values are from 1 through 64.

Defaults

This command has no default settings.

Command Modes

Global configuration mode

Examples

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

```
Switch(config)# ip igmp snooping vlan 4 static 0100.5e01.0203 interface fastethernet 5/11
Configuring port FastEthernet5/11 on group 0100.5e01.0203 vlan 4
Switch(config)#
```

Related Commands

Command	Description
ip igmp snooping	Enable IGMP snooping.
ip igmp snooping vlan immediate-leave	Enable IGMP immediate-leave processing.
ip igmp snooping vlan mrouter	Configures a Layer 2 interface as a multicast router interface for a VLAN.
show mac-address-table multicast	Displays information about the multicast MAC address table.

ip local-proxy-arp

To enable the local proxy ARP feature, use the **ip local-proxy-arp** command. To disable the local proxy ARP feature, use the **no** form of this command.

ip local-proxy-arp

no ip local-proxy-arp

Syntax Description This command has no arguments or keywords.

Defaults Local proxy ARP is disabled.

Command Modes Interface configuration mode

Usage Guidelines Use this feature only on subnets where hosts are intentionally prevented from communicating directly to the switch on which they are connected.

ICMP redirect is disabled on interface where the local proxy ARP feature is enabled.

Examples This example shows how to enable the local proxy ARP feature:

```
Switch(config-if)# ip local-proxy-arp
Switch(config-if)#
```

ip mfib fastdrop

To enable MFIB fast drop, use the **ip mfib fastdrop** command. To disable MFIB fast drop, use the **no** form of this command.

ip mfib fastdrop

no ip mfib fastdrop

Syntax Description This command has no arguments or keywords.

Defaults MFIB fast drop is enabled.

Command Modes Privileged EXEC mode

Examples This example shows how to enable MFIB fast drops:

```
Switch(config)# ip mfib fastdrop
Switch(config)#
```

Related Commands

Command	Description
clear ip mfib fastdrop	Clears all the MFIB fast-drop entries.
show ip mfib fastdrop	Displays all currently active fast-drop entries and shows whether fast drop is enabled.

ip multicast multipath

To enable load-splitting of IP multicast traffic over Equal Cost Multipath (ECMP), use the **ip multicast multipath** command in global configuration mode. To disable this function, use the **no** form of this command.

ip multicast [*vrf vrf-name*] **multipath** [**s-g-hash** | **basic** | **next-hop-based**]

no ip multicast [*vrf vrf-name*] **multipath** [**s-g-hash** | **basic** | **next-hop-based**]

Syntax Description

vrf vrf-name	(Optional) Enables ECMP multicast load splitting for IP multicast traffic associated with the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
s-g-hash | **next-hop-based**	(Optional) Enables IS-IS multicast load splitting based on source and group address or on source, group, and next-hop address.
	The **basic** keyword enables a simple hash based on source and group address. This algorithm is referred to as the basic S-G-hash algorithm. The **next-hop-based** keyword enables a more complex hash based on source, group, and next-hop address. This algorithm is referred to as the next-hop-based S-G-hash algorithm.

Command Default If multiple equal-cost paths exist, multicast traffic will not be load-split across those paths.

Command Modes Global configuration (config)

Usage Guidelines The **ip multicast multipath** command does not work with bidirectional Protocol Independent Multicast (PIM).

Use the **ip multicast multipath** command to enable load splitting of IP multicast traffic across multiple equal-cost paths.

If two or more equal-cost paths from a source are available, unicast traffic will be load-split across those paths. However, by default, multicast traffic is not load-split across multiple equal-cost paths. In general, multicast traffic flows down from the reverse path forwarding (RPF) neighbor. According to the PIM specifications, this neighbor must have the highest IP address if more than one neighbor has the same metric.

When you configure load-splitting with the **ip multicast multipath** command, the system splits multicast traffic across multiple equal-cost paths based on source address using the S-hash algorithm. When the **ip multicast multipath** command is configured and multiple equal-cost paths exist, the path in which multicast traffic will travel is selected based on the source IP address. Multicast traffic from different sources will be load-split across the different equal-cost paths. Load splitting will not occur across equal-cost paths for multicast traffic from the same source sent to different multicast groups.

Note The **ip multicast multipath** command load splits the traffic but does not load balance the traffic. Traffic from a source will use only one path, even if the traffic greatly exceeds traffic from other sources.

If the **ip multicast multipath** command is configured with the **s-g-hash** keyword and multiple equal-cost paths exist, load splitting will occur across equal-cost paths based on source and group address or on source, group, and next-hop address. If you specify the optional **s-g-hash** keyword for load splitting, the router applies a hash-based algorithm used to calculate the equal-cost paths by specifying one of the following keywords:

- **basic**—The basic S-G-hash algorithm is predictable because no randomization is used in calculating the hash value. The basic S-G-hash algorithm, however, is subject to polarization because for a given source and group the same hash is always chosen irrespective of the router that the hash is being calculated on.
- **next-hop-based**—The next-hop-based S-G-hash algorithm is predictable because no randomization is used to determine the hash value. Unlike the S-G-hash and basic S-G-hash algorithm, the next-hop-based hash mechanism is not subject to polarization.

Examples

The following example shows how to enable ECMP multicast load splitting on a router based on source address using the S-hash algorithm:

```
Router(config)# ip multicast multipath
```

The following example shows how to enable ECMP multicast load splitting on a router based on source and group address using the basic S-G-hash algorithm:

```
Router(config)# ip multicast multipath s-g-hash basic
```

The following example shows how to enable ECMP multicast load splitting on a router based on source, group, and next-hop address using the next-hop-based S-G-hash algorithm:

```
Router(config)# ip multicast multipath s-g-hash next-hop-based
```

ip source binding

To add or delete a static IP source binding entry, use the **ip source binding** command. To delete the corresponding IP source binding entry, use the **no** form of this command.

ip source binding *ip-address mac-address* **vlan** *vlan-id* **interface** *interface-name*

no ip source binding *ip-address mac-address* **vlan** *vlan-id* **interface** *interface-name*

Syntax Description

ip-address	Binding IP address.
mac-address	Binding MAC address.
vlan *vlan-id*	VLAN number.
interface *interface-name*	Binding interface.

Defaults

This command has no default settings.

Command Modes

Global configuration mode

Usage Guidelines

The **ip source binding** command is used to add a static IP source binding entry only. These forms of this command delete the corresponding IP source binding entry. For the deletion to succeed, all required parameters must match.

Each static IP binding entry is keyed by a MAC address and VLAN number. If the CLI contains an existing MAC and VLAN, the existing binding entry will be updated with the new parameters; a separate binding entry will not be created.

Examples

This example shows how to configure the static IP source binding:

```
Switch(config)# ip source binding 10.0.0.1 0010.0026.0330 vlan 10 interface
fastethernet6/10
Switch(config)#
```

Related Commands

Command	Description
show ip source binding	Displays IP source bindings that are configured on the system.

ip sticky-arp

To enable sticky ARP, use the **ip sticky-arp** command. Use the **no** form of this command to disable sticky ARP.

ip sticky-arp

no ip sticky-arp

Syntax Description This command has no arguments or keywords.

Defaults Enabled

Command Modes Global configuration mode

Usage Guidelines This command is supported on PVLANs only.

ARP entries that are learned on Layer 3 PVLAN interfaces are sticky ARP entries. (You should display and verify ARP entries on the PVLAN interface using the **show arp** command).

For security reasons, sticky ARP entries on the PVLAN interface do not age out. Connecting new equipment with the same IP address generates a message and the ARP entry is not created.

Because the ARP entries on the PVLAN interface do not age out, you must manually remove ARP entries on the PVLAN interface if a MAC address changes.

Unlike static entries, sticky ARP entries are not stored and restored when you enter the **reload** and **restart** commands.

Examples This example shows how to enable sticky ARP:

```
Switch(config)#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#ip sticky-arp
Switch(config)#end
Switch#
```

This example shows how to disable sticky ARP:

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip sticky-arp
Switch(config)#end
Switch#
```

Related Commands	Command	Description
	arp (refer to Cisco IOS documentation)	Enables Address Resolution Protocol (ARP) entries for static routing over the Switched Multimegabit Data Service (SMDS) network.
	show arp (refer to Cisco IOS documentation)	Displays ARP information.

ip verify header vlan all

To enable IP header validation for Layer 2-switched IPv4 packets, use the **ip verify header vlan all** command. To disable the IP header validation, use the **no** form of this command.

ip verify header vlan all

no ip verify header vlan all

Syntax Description This command has no default settings.

Defaults The IP header is validated for bridged and routed IPv4 packets.

Command Modes Global configuration mode

Usage Guidelines This command does not apply to Layer 3-switched (routed) packets.

The Catalyst 4500 series switch checks the validity of the following fields in the IPv4 header for all switched IPv4 packets:

- The version must be 4.
- The header length must be greater than or equal to 20 bytes.
- The total length must be greater than or equal to four times the header length and greater than the Layer 2 packet size minus the Layer 2 encapsulation size.

If an IPv4 packet fails the IP header validation, the packet is dropped. If you disable the header validation, the packets with the invalid IP headers are bridged but are not routed even if routing was intended. The IPv4 access lists also are not applied to the IP headers.

Examples This example shows how to disable the IP header validation for the Layer 2-switched IPv4 packets:

```
Switch(config)# no ip verify header vlan all
Switch(config)# ip verify header vlan all
Switch(config)#^Z
Switch#
```

ip verify source

To enable IP source guard on untrusted Layer 2 interfaces, use the **ip verify source** command. To disable IP source guard on untrusted Layer 2 interfaces, use the **no** form of this command.

ip verify source [**vlan dhcp-snooping** | **tracking**] [**port-security**]

no ip verify source [**vlan dhcp-snooping** | **tracking**] [**port-security**]

Syntax Description

vlan dhcp-snooping	Enables IP source guard on untrusted Layer 2 DHCP snooping interfaces.
tracking	Enables IP port security tracks static IP address learning on a port.
port-security	Optionally filters both source IP and MAC addresses using the port security feature.

Defaults

IP source guard is disabled.

Command Modes

Global configuration mode

Examples

This example shows how to enable IP source guard on VLANs 10 through 20 on a per-port basis:

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip dhcp snooping
Switch(config)# interface range vlan 10 20
Switch(config-if-range)#switchport
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk native vlan 10
Switch(config-if)# switchport trunk allowed vlan 11-20
Switch(config-if)# ip dhcp snooping trust
Switch(config-if)# ip verify source vlan dhcp-snooping
Switch(config-if)# exit
Switch#show ip verify source interface fa3/1
Interface  Filter-type  Filter-mode  IP-address     Mac-address     Vlan
-----------------------------------------------------------------------
Fa3/1      ip-vlan      active       10.7.11.1       11-20
Fa3/1      ip-mac       active       deny-all        11-20
Switch#
```

This example shows how to enable IP port security with IP-MAC filters on a Layer 2 access port:

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip dhcp snooping
Switch(config)# interface fa6/5(access) a/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 6
Switch(config-if)# switchport access vlan mac 5
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 5
Switch(config-if)# ip verify source tracking port-security
Switch(config-if)# exit
```

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

Related Commands	Command	Description
	ip device tracking maximum	Enables IP port security binding tracking on a Layer 2 port.
	ip dhcp snooping	Globally enables DHCP snooping.
	ip dhcp snooping information option	Enables DHCP option 82 data insertion.
	ip dhcp snooping limit rate	Configures the number of the DHCP messages that an interface can receive per second.
	ip dhcp snooping trust	Enables DHCP snooping on a trusted VLAN.
	ip source binding	Adds or delete a static IP source binding entry.
	show ip dhcp snooping	Displays the DHCP snooping configuration.
	show ip dhcp snooping binding	Displays the DHCP snooping binding entries.
	show ip source binding	Displays IP source bindings that are configured on the system.
	show ip verify source	Displays the IP source guard configuration and filter on a particular interface.

ip verify unicast source reachable-via

To enable and configure unicast RPF checks on a IPv4 interface, use the **ip verify unicast source reachable-via** command. To disable unicast RPF, use the **no** form of this command.

ip verify unicast source reachable-via rx allow-default

no ip verify unicast source reachable-via

Syntax Description

rx	Verifies that the source address is reachable on the interface where the packet was received.
allow-default	Verifies that the default route matches the source address.

Defaults Disabled

Command Modes Interface configuration mode

Usage Guidelines

In basic RX mode, unicast RPF ensures a source address must be reachable on the arrival interface. For example, the source must be reachable without load balancing.

Note Unicast RPF is an input function and is applied only on the input interface of a router at the upstream end of a connection.

Do not use unicast RPF on internal network interfaces. Internal interfaces might have routing asymmetry, which means that there are multiple routes to the source of a packet. Apply unicast RPF only where there is natural or configured symmetry.

Examples

This example shows how to enable unicast RPF exists-only checking mode:

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface gigabitethernet1/1
Switch(config-if)#ip verify unicast source reachable-via rx allow-default
Switch(config-if)#end
Switch#
```

Related Commands

Command	Description
ip cef (refer to Cisco IOS documentation)	Enables Cisco Express Forwarding (CEF) on the switch.
show running-config	Displays the current running configuration for a switch.

ip wccp

To enable support of the specified Web Cache Communication Protocol (WCCP) service for participation in a service group, use the **ip wccp** command in global configuration mode. To disable the service group, use the **no** form of this command.

ip wccp {**web-cache** | *service-number*} [**accelerated**] [**group-address** *multicast-address*] [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** [**0** | **7**] *password*]

no ip wccp {**web-cache** | *service-number*} [**accelerated**] [**group-address** *multicast-address*] [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** [**0** | **7**] *password*]

Syntax Description

web-cache	Specifies the web-cache service. **Note** Web cache counts as one service. The maximum number of services, including those assigned with the *service-number* argument, are 8.
service-number	Dynamic service identifier, which means the service definition is dictated by the cache. The service number can be from the list 0–254. The maximum number of services, including those assigned with the **web-cache** keyword, are 8. **Note** If Cisco cache engines are being used in your service group, the reverse-proxy service is indicated by a value of 98.
accelerated	(Optional) Hardware acceleration for multicast packet acceleration exists. This keyword configures the service group to prevent a connection being formed with a cache engine unless the cache engine is capable of hardware acceleration. This allows redirection on the router to benefit from hardware acceleration.
group-address *multicast-address*	(Optional) Multicast IP address that communicates with the WCCP service group. The multicast address is used by the router to determine which cache engine should receive redirected messages.
redirect-list *access-list*	(Optional) Access list that controls traffic redirected to this service group. The access-list argument should consist of a string of no more than 64 characters (name or number) that specifies the access list.
group-list *access-list*	(Optional) Access list that determines which cache engines are allowed to participate in the service group. The access-list argument specifies either a standard access list number or name. The access-list argument.
password [**0**	**7**] *password*	(Optional) Message digest algorithm 5 (MD5) authentication for messages received from the service group. Messages that are not accepted by the authentication are discarded. The encryption type (as 0 or 7, with 0 specifying not yet encrypted and 7 for proprietary. The *password* argument can be up to eight characters in length.

Command Default WCCP services are not enabled on the router.

Command Modes Global configuration (config)

Usage Guidelines This command initiates a router to enable or disable the support for the specified service number or the well-known service name. A service number can be from 0 to 255. Once the service number or name is enabled, the router can participate in the establishment of a service group.

When **group-list** keyword is entered, the router initiates participation in the service group, multicasts space if none of the interfaces still has the service configured, and terminates the WCCP peers if no other services are configured.

The keywords following the **web-cache** keyword and the service-number argument are optional and may be specified in any order, but only may be specified once. The following sections outline the specific usage of each of the optional forms of this command:

ip wccp {**web-cache** | *service-number*} **group-address** *multicast-address*

A WCCP group address can be configured to set up a multicast address that cooperating routers and web caches can use to exchange WCCP protocol messages. If such an address is used, IP multicast routing must be enabled so that the messages that use the configured group (multicast) address are received correctly.

This option instructs the router to use the specified multicast IP address to coalesce the "I See You" responses for the "Here I Am" messages that it has received on this group/port/address. The response is sent to the group address as well. The default is for no group address to be configured, in which case all "Here I Am" messages are responded to with a unicast reply.

ip wccp {**web-cache** | *service-number*} **redirect-list** *access-list*

This option instructs the router to use an access list to control the traffic that is redirected to the web caches of the service group specified by the service-number. The access-list specification is a standard or extended access list, or a named or extended access list. The access-list can specify hosts which traffic is permitted to be redirected. The default is for no redirection. Only the configured of traffic is redirected.

WCCP requires that the following protocol and ports not be filtered by any access-list:

- User Datagram Protocol (UDP) protocol on ports 2048 and 2049. This port is used for control signaling. Blocking this type of traffic will prevent WCCP from establishing a connection between the router and a cache engine.

ip wccp {**web-cache** | *service-number*} **group-list** *access-list*

This option instructs the router to use an access list to control the cache engines that are allowed to participate in the specified service group. The access-list argument specifies either the number of a standard or extended access list or the name of any type of named access list. The access list itself specifies which cache engines are permitted to participate in the service group. The default is for no group list to be configured, in which case all cache engines may participate in the service group.

Tip Using **ip wccp** {**web-cache** | *service-number*} **group-list** command syntax resembles the **ip wccp** {**web-cache**| *service-number*} **group-listen** command, but these are entirely different commands. The **ip wccp group-listen** command is an interface configuration command used to configure an interface to listen for multicast notifications from a cache cluster. Refer to the description of the **wccp group-listen** command in the *Cisco IOS IP Application Services Command Reference*.

ip wccp {**web-cache** | *service-number*} **password** *password*

This option instructs the router to use MD5 authentication on the messages received from the service group specified by the service name given. Use the form of the command on both the router and on the routers. You must also configure the same password separately on each web cache. The password can be

up to a maximum of eight characters. Messages that do not authenticate when authentication is enabled on the router are discarded. The default is for no authentication password to be configured and for authentication to be disabled.

Examples

The following example shows how to configure a router to run WCCP reverse-proxy service, using the multicast address of 239.0.0.0:

```
Router(config)# ip multicast-routing
Router(config)# ip wccp 99 group-address 239.0.0.0
Router(config)# interface gigabitethernet 3/1
Router(config-if)# ip wccp 99 group-listen
```

The following example shows how to configure a router to redirect web-related packets without a destination of 10.168.196.51 to the web cache:

```
Router(config)# access-list 150 deny ip any host 10.168.196.51
Router(config)# access-list 150 permit ip any any
Router(config)# ip wccp web-cache redirect-list 150
Router(config)# interface gigabitethernet 3/1
Router(config-if)# ip wccp web-cache redirect out
```

Related Commands

Command	Description
ip wccp check service all	Enables all WCCP services.
ip wccp version	Specifies which version of WCCP you wish to use on your router.
show ip wccp	Displays global statistics related to WCCP.

ip wccp check services all

To enable all Web Cache Communication Protocol (WCCP) services, use the **ip wccp check services all** command in global configuration mode. To disable all services, use the **no** form of this command.

ip wccp check services all

no ip wccp check services all

Syntax Description This command has no arguments or keywords.

Defaults WCCP services are not enabled on the router.

Command Modes Global configuration (config)

Usage Guidelines With the **ip wccp check services all** command, WCCP can be configured to check all configured services for a match and perform redirection for those services if appropriate. The caches to which packets are redirected can be controlled by a redirect ACL access control list (ACL) as well as by the priority value of the service.

It is possible to configure an interface with more than one WCCP service. When more than one WCCP service is configured on an interface, the precedence of a service depends on the relative priority of the service compared to the priority of the other configured services. Each WCCP service has a priority value as part of its definition.

If no WCCP services are configured with a redirect ACL, the services are considered in priority order (highest priority first) and packets are redirected if they are not redirected by a higher priority service or redirected. If a service matches the packet and the service has a redirect ACL configured, then the IP packet will be checked against the ACL. If the packet is rejected by the ACL, the packet will not be passed down to lower priority services unless the **ip wccp check services all** command is configured. When the **ip wccp check services all** command is configured, WCCP will continue to attempt to match the packet against any remaining lower priority services configured on the interface.

Note The priority of a WCCP service group is determined by the web cache ip address. The priority of a WCCP service group cannot be configured via Cisco IOS software.

Note The **ip wccp check services all** command is a global WCCP command that applies to all services and is not associated with a single service.

Examples The following example shows how to configure all WCCP services:

```
Router(config)# ip wccp check services all
```

Related Commands	Command	Description
	ip wccp	Enables support of the specified WCCP service for participation in a service group.
	ip wccp group-listen	Configures an interface on a router to enable or disable the reception of IP multicast packets for Web Cache Communication Protocol (WCCP).
	ip wccp redirect	Enables (or let redirection on an inbound or outbound interface using Web Cache Communication Protocol (WCCP).
	ip wccp redirect exclude in	Configures an interface to exclude packets received on an interface from being checked for redirection.
	ip wccp version	Specifies which version of WCCP you wish to use on your router.

ip wccp group-listen

To configure an interface on a router to enable or disable the reception of IP multicast packets for Web Cache Communication Protocol (WCCP), use the **ip wccp group-listen** command in interface configuration mode. To disable the reception of IP multicast packets for WCCP, use the **no** form of this command.

ip wccp {**web-cache** | service-number} **group-listen**

no ip wccp {**web-cache** | service-number} **group-listen**

Syntax Description	**web-cache** The web cache service. *service-number* WCCP service number; valid values are from 0 to 254.
Defaults	This command is disabled by default.
Command Modes	Interface configuration (config-if)
Usage Guidelines	On routers that are to be members of a Service Group when IP multicast is used, the following configuration is required: • Configure the IP multicast address for use by the WCCP Service Group. • Configure the interfaces on which the router wishes to receive the IP multicast address with the **ip wccp** {**web-cache**	service-number} **group-listen** interface configuration command.

Examples	The following example shows how to enable the multicast packets for a web cache with a multicast address of 224.1.1.100:
	`Switch(config)#interface Vlan10`
	`Switch(config)#ip wccp web-cache group-address 224.1.1.100`
	`Switch(config)#interface gigabitethernet 3/1`
	`Switch(config-if)#ip wccp web-cache group-listen`

Related Commands	Command	Description
	ip wccp	Enables support of the WCCP server for participation in a service group.
	ip wccp check services all	Enables all Web Cache Communication Protocol (WCCP) services.
	ip wccp redirect	Enables WCCP redirection on an interface.
	ip wccp redirect	Enables packet redirection on an inbound or outbound interface using Web Cache Communication Protocol (WCCP).

Command	Description
ip wccp redirect exclude in	Configures an interface to exclude packets received on an interface from being checked for redirection.
ip wccp version	Specifies which version of WCCP you wish to use on your router.

ip wccp redirect

To enable packet redirection on an inbound or outbound interface using Web Cache Communication Protocol (WCCP), use the **ip wccp redirect** command in interface configuration mode. To disable WCCP redirection, use the **no** form of this command.

ip wccp {web-cache | service-number} redirect {in | out}

no ip wccp {web-cache | service-number} redirect {in | out}

Syntax Description	**web-cache** Enables the web cache service. *service-number* Identification number of the cache engine service group; valid values are from 0 to 254. If Cisco cache engines are used in the cache cluster, the reverse proxy service is indicated by a value of 99.
	in Specifies packet redirection on an inbound interface.
	out Specifies packet redirection on an outbound interface.
Command Default	Redirection checking on the interface is disabled.
Command Modes	Interface configuration (config-if)

Usage Guidelines

The **ip wccp {web-cache | service-number} redirect** in command allows you to configure WCCP redirection on an interface receiving inbound network traffic. When the command is applied to an interface, all packets arriving at that interface will be compared against the criteria defined by the specified WCCP service. If the packets match the criteria, they will be redirected.

Likewise, the **ip wccp {web-cache | service-number} redirect out** command allows you to configure the WCCP redirection check at an outbound interface.

Tips Be careful not to confuse the **ip wccp {web-cache | service-number} redirect {out | in}** interface configuration command with the **ip wccp redirect exclude in** interface configuration command.

Examples

The following example shows how to configure a session in which reverse proxy packets on Ethernet interface 3/1 are being checked for redirection and redirection is Cisco Cache Engine:

```
Router(config)# ip wccp 99
Router(config)# interface gigabitethernet 3/1
Router(config-if)# ip wccp 99 redirect out
```

The following example shows how to configure a session in which HTTP traffic arriving on GigabitEthernet interface 3/1 is redirected to a Cache Engine:

```
Switch(config)# ip wccp web-cache
Switch(config)# interface gigabitethernet 3/1
Switch(config-if)# ip wccp web-cache redirect in
```

Related Commands

Command	Description
ip wccp check services all	Configures an interface on a router to enable or disable the reception of IP multicast packets for Web Cache Communication Protocol (WCCP).
ip wccp group-listen	Configures an interface on a router to enable or disable the reception of IP multicast packets for Web Cache Communication Protocol (WCCP).
ip wccp redirect exclude in	Enables redirection exclusion on an interface.
show ip interface	Displays the usability status of interfaces that are configured for IP.
show ip wccp	Displays the WCCP global configuration and statistics.

p wccp redirect exclude in

To configure an interface to exclude packets received on an interface from being checked for redirection, use the **p wccp redirect exclude in** command in interface configuration mode. To disable the ability of a router to exclude packets from redirection check, use the **no** form of this command.

ip wccp redirect exclude in

no ip wccp redirect exclude in

Syntax Description This command has no arguments or keywords.

Command Default Redirection exclusion is disabled.

Command Modes Interface configuration (config-if)

Usage Guidelines This configuration command instructs the interface to exclude inbound packets from any redirection check. Note that the command is global to all the services and should be applied to any inbound interface that will be excluded from redirection.

This command is intended to be used to accelerate the flow of packets from a cache engine to the Internet as well as allow further use of the Web Cache Communication Protocol (WCCP) v2 packet return feature.

Examples In the following example, packets arriving on GigabitEthernet interface 3/1 are excluded from WCCP output redirection check:

```
Router(config)# interface gigabitethernet 3/1
Router(config-if)# ip wccp redirect exclude in
```

Related Commands

Command	Description
ip wccp	Enables support of the WCCP service for participation in a service group.
ip wccp redirect	Enables packet redirection on an inbound or outbound interface using Web Cache Communication Protocol (WCCP).
ip wccp redirect out	Configures redirection on an interface in the outgoing direction.
ip wccp check services all	Configures an interface or a router to enable or disable the reception of IP multicast packets for Web Cache Communication Protocol (WCCP).
ip wccp group-listen	Configures an interface or a router to enable or disable the reception of IP multicast packets for Web Cache Communication Protocol (WCCP).
ip wccp redirect exclude in	Enables redirection exclusion on an interface.
show ip interface	Displays the usability status of interfaces that are configured for IP.
show ip wccp	Displays the WCCP global configuration and statistics.

ipv6 mld snooping

To enable IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping globally or on the specified VLAN, use the **ipv6 mld snooping** command without keywords. To disable MLD snooping on a switch or the VLAN, use the **no** form of this command.

ipv6 mld snooping [**vlan** *vlan-id*]

no ipv6 mld snooping [**vlan** *vlan-id*]

Syntax Description

vlan *vlan-id* (Optional) Enables or disables IPv6 MLD snooping on the specified VLAN. The VLAN ID range is 1 to 4005 and 4006 to 4094.

Defaults

MLD snooping is globally disabled on the switch.

MLD snooping is enabled on VLANs. However, MLD snooping must be globally enabled before VLAN snooping can take place.

Command Modes

Global configuration mode

Usage Guidelines

When MLD snooping is globally disabled, it is disabled on all the existing VLAN interfaces. When you globally enable MLD snooping, it is enabled on all VLAN interfaces that are in the default state (enabled). VLAN configuration overrides global configuration on interfaces on which MLD snooping has been disabled.

If MLD snooping is globally disabled, you cannot enable it on a VLAN. If MLD snooping is globally enabled, you can disable it on individual VLANs.

VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in MLD snooping.

Examples

This example shows how to globally enable MLD snooping:

```
Switch(config)# ipv6 mld snooping
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# show ipv6 mld snooping
Switch(config)#
Switch#
```

This example shows how to disable MLD snooping on a VLAN:

```
Switch(config)# ipv6 mld snooping vlan 11
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# no ipv6 mld snooping vlan 11
Switch(config)# show ipv6 mld snooping vlan 11
Switch(config)#
Switch#
```

You can verify your settings by entering the **show ipv6 mld snooping** user EXEC command.

Related Commands	Command	Description
	show ipv6 mld snooping	Displays IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping configuration of the switch or the VLAN.

ipv6 mld snooping last-listener-query-count

To configure IP version 6 (IPv6) Multicast Listener Discovery Multicast Address Specific Queries (MASQ) that will be sent before aging out a client, use the **ipv6 mld snooping last-listener-query-count** command. To revert the query count to the default settings, use the **no** form of this command.

ipv6 mld snooping [**vlan** *vlan-id*] **last-listener-query-count** *integer_value*

no ipv6 mld snooping [**vlan** *vlan-id*] **last-listener-query-count**

Syntax Description	**vlan** *vlan-id* (Optional) Configures last-listener query count on the specified VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094.
	integer_value The integer range is 1 to 7.
Command Default	The default global count is 2. The default VLAN count is 0 (the global count is used).
Command Modes	Global configuration mode

Usage Guidelines

In MLD snooping, the IPv6 multicast switch periodically sends out queries to hosts belonging to the multicast group. If a host wants to leave a multicast group, it can silently leave or it can respond to the query with a Multicast Listener Done message (equivalent to an IGMP Leave message). When Immediate Leave is not configured (it should not be configured if multiple clients for a group exist on each port), or if the configured last-listener query count determines the number of MASQs that are sent before an MLD client is aged out.

When the last-listener query count is set for a VLAN, this count overrides the value configured globally. When the VLAN count is not configured (set to the default of 0), the global count is used.

VLAN numbers 1002 through 1005 are reserved for Token Ring and RSD VLANs and cannot be used in MLD snooping.

Examples

This example shows how to globally set the last-listener query count:

```
Switch#conf\term terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ipv6 mld snooping last-listener-query-count 3
Switch(config)# end
Switch#
```

This example shows how to set the last-listener query count for VLAN 10:

```
Switch#conf\term terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ipv6 mld snooping vlan 10 last-listener-query-count 3
Switch(config)# end
Switch#
```

You can verify your settings by entering the **show ipv6 mld snooping** [**vlan** *vlan-id*] user EXEC command.

Related Commands

Command	Description
ipv6 mld snooping last-listener-query-interval	Configures IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping last-listener query interval on the switch or on a VLAN.
show ipv6 mld snooping	Displays IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping configuration of the switch or the VLANs.
show ipv6 mld snooping querier	Displays IP version 6 (IPv6) ML Dsnoopingquerier-related information most recently received by the switch or the VLANs.

ipv6 mld snooping last-listener-query-interval

To configure IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping last-listener query interval on the switch or on a VLAN, use the **ipv6 mld snooping last-listener-query-interval** command. To reset the query time to the default settings, use the **no** form of this command.

ipv6 mld snooping [**vlan** *vlan-id*] **last-listener-query-interval** *integer_value*

no ipv6 mld snooping [**vlan** *vlan-id*] **last-listener-query-interval**

Syntax Description

vlan *vlan-id*	(Optional) Configures last-listener query interval on the specified VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094.
integer_value	Sets the time period (in thousandths of a second) that a multicast router must wait after sending a MASQ before deleting a port from the multicast group. The range is 100 to 32,768. The default is 1000 (1 second).

Command Default

The default global query interval (maximum response time) is 1000 (1 second).

The default VLAN query interval (maximum response time) is 0 (the global count is used).

Command Modes

Global configuration mode

Usage Guidelines

The last-listener-query-interval time is the maximum time that a multicast switch waits after issuing a Multicast Address Specific Query (MASQ) before deleting a port from the multicast group.

In MLD snooping, when the IPv6 multicast switch receives an MLD leave message, it sends out queries to hosts belonging to the multicast group. If there are no responses from a port to a MASQ for a length of time, the switch deletes the port from the membership database of the multicast address. The last listener query interval is the maximum time that the switch waits before deleting a nonresponsive port from the multicast group.

When a VLAN query interval is set, the global query interval is overrides. When the VLAN interval is set at 0, the global value is used.

VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs, and cannot be used in MLD snooping.

Examples

This example shows how to globally set the last-listener query interval to 2 seconds:

```
Switch(config)# ipv6 mld snooping last-listener-query-interval 2000
Switch(config)# ipv6 mld snooping vlan 1 last-listener-query-interval 3000
Switch(config)# ipv6 mld snooping last-listener-query-interval 2000
Switch(config)#
```

This example shows how to set the last-listener query interval for VLAN 1 to 5.5 seconds:

```
Switch(config)# ipv6 mld snooping vlan 1 last-listener-query-interval 5500
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ipv6 mld snooping vlan 1 last-listener-query-interval 5500
```

```
Switch(config)# end
Switch#
```

You can verify your settings by entering the **show ipv6 MLD snooping** [**vlan** *vlan-id*] user EXEC command.

Related Commands

Command	Description
ipv6 mld snooping last-listener-query-count	Configures IP version 6 (IPv6) Multicast Listener Discovery Multicast Address Specific Queries (MASQs) that will be sent before aging out a client.
show ipv6 mld snooping querier	Displays IP version 6 (IPv6) MLD Snooping querier-related information most recently received by the switch or the VLAN.

ipv6 mld snooping listener-message-suppression

To enable IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping listener message suppression, use the **ipv6 mld snooping listener-message-suppression** command. To disable MLD snooping listener message suppression, use the **no** form of this command.

ipv6 mld snooping listener-message-suppression

no ipv6 mld snooping listener-message-suppression

Command Default The default is for MLD snooping listener message suppression to be disabled.

Command Modes Global configuration mode

Usage Guidelines MLD snooping listener message suppression is equivalent to IGMP snooping report suppression. When it is enabled, received MLDv1 reports to a group are forwarded to IPv6 multicast routers only once in every report-forward time. This prevents the forwarding of duplicate reports.

Examples This example shows how to enable MLD snooping listener message suppression:

```
Switch# conf ipv6 terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ipv6 mld snooping listener-message-suppression
Switch(config)# end
Switch#
```

This example shows how to disable MLD snooping listener message suppression:

```
Switch# conf ipv6 terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# no ipv6 mld snooping listener-message-suppression
Switch(config)# end
Switch#
```

You can verify your settings by entering the **show ipv6 mld snooping [vlan** vlan-id] user EXEC command.

Related Commands

Command	Description
ipv6 mld snooping	Enables IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping globally or on the specified VLAN.
show ipv6 mld snooping	Displays IP version 6 (IPv6) MLD snooping configuration of the switch or the VLAN.

ipv6 mld snooping robustness-variable

To configure the number of IP version 6 (IPv6) Multicast Listener Discovery (MLD) queries that the switch sends before deleting a listener that does not respond, or to enter a VLAN ID to configure the number of queries per VLAN, use the **ipv6 mld snooping robustness-variable** command. To reset the variable to the default settings, see the **no** form of this command.

ipv6 mld snooping [**vlan** *vlan-id*] **robustness-variable** *integer_value*

no ipv6 mld snooping[**vlan** *vlan-id*] **robustness-variable**

Syntax Description	**vlan** *vlan-id* (Optional) Configures the robustness variable on the specified VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094.
integer_value	The robustness value integer from 1 to 3.

Command Default	The default global robustness variable (number of queries before deleting a listener) is 2. The default VLAN robustness variable (number of queries before aging out a multicast address) is 0, which means that the system uses the global robustness variable for aging out the listener.
Command Modes	Global configuration mode

Usage Guidelines

Robustness is measured by the number of MLDv1 queries sent with no response before a port is removed from a multicast group. A port is deleted when there are no MLDv1 reports received for the configured number of MLDv1 queries. The global value determines the number of queries that the switch sends before deleting a listener that does not respond, and it applies to all VLANs that do not have a VLAN value defined.

The robustness value configured for a VLAN overrides the global value. If the VLAN robustness value is 0 (the default), the global value is used.

VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in MLD snooping.

Examples

This example shows how to configure the global robustness variable so that the switch sends out three queries before it deletes a listener port that does not respond:

```
Switch(config)# ipv6 mld snooping robustness-variable 3
Switch(config)# end
Switch#show ipv6 mld snooping robustness-variable 3
Switch#
```

This example shows how to configure the robustness variable for VLAN 1. This value overrides the global configuration for the VLAN:

```
Switch(config)# ipv6 mld snooping vlan 1 robustness-variable 3
Switch(config)# end
Switch#show ipv6 mld snooping vlan 1 robustness-variable 3
```

```
Dot1x tcn-protect(tag)0 : end
Dot1x tcn-guard
```

You can verify your settings by entering the **show ipv6 MLD snooping** [**vlan** *vlan-id*] user EXEC command.

Related Commands	Command	Description
	ipv6 mld snooping last-listener-query-count	Configures IP version 6 (IPv6) Multicast Listener Discovery Multicast Address Specific Queries (MASQs) that will be sent before aging out a client.
	show ipv6 mld snooping	Displays IP version 6 (IPv6) MLD snooping configuration of the switch or the VLAN.

ipv6 mld snooping tcn

To configure IP version 6 (IPv6) Multicast Listener Discovery (MLD) Topology Change Notifications (TCNs), use the **ipv6 mld snooping tcn** commands. To revert the default settings, use the **no** form of the commands.

ipv6 mld snooping tcn [flood query count *integer_value* **| query solicit]**

no ipv6 mld snooping tcn [flood query count *integer_value* **| query solicit]**

Syntax Description		
	flood query count *integer_value*	Sets the flood query count, which is the number of queries that are sent before forwarding multicast data to only those ports requesting it. The range is 1 to 10.
	query solicit	Enables soliciting of TCN queries.

Command Default

TCN query soliciting is disabled.

When enabled, the default flood query count is 2.

Command Modes

Global configuration mode

Examples

This example shows how to enable TCN query soliciting:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ipv6 mld snooping tcn query solicit.
Switch(config)# end
Switch#
```

This example shows how to set the flood query count to 5:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ipv6 mld snooping tcn flood query count 5.
Switch(config)# end
Switch#
```

You can verify your settings by entering the **show ipv6 MLD snooping** [**vlan** *vlan-id*] user EXEC command.

Related Commands

Command	Description
show ipv6 mld snooping	Displays IP version 6 (IPv6) MLD snooping configuration of the switch or the VLAN.

ipv6 mld snooping vlan

To configure IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping parameters on the VLAN interface, use the **ipv6 mld snooping** vlan command. To reset the parameters to the default settings, use the no form of this command.

ipv6 mld snooping vlan *vlan-id* **[immediate-leave | mesonte interface** *interface-id* **| static** *ipv6-multicast-address* **interface** *interface-id*]

no ipv6 mld snooping vlan *vlan-id* **[immediate-leave | mesonte interface** *interface-id*| **static** *ipv6-address* **interface** *interface-id*]

Syntax Description	**vlan** *vlan-id* Specifies a VLAN number. The range is 1 to 1001 and 1006 to 4094.
	immediate-leave (Optional) Enables MLD Immediate-Leave processing on a VLAN interface. Use the **no** form of the command to disable the Immediate-Leave feature on the interface.
	mesonte interface (Optional) Configures a multicast switch port. The **no** form of the command disables the configuration.
	static *ipv6-multicast-address* Configures a multicast group with the specified IPv6 multicast address.
	interface *interface-id* Adds a static port to the group. The mesonte or static interface can be a physical port or a port-channel interface ranging from 1 to 48.
Command Default	MLD snooping Immediate-Leave processing is disabled. By default, there are no static IPv6 multicast groups. By default, there are no multicast switch ports.
Command Modes	Global configuration mode
Usage Guidelines	You should only configure the Immediate-Leave feature when there is only one receiver on every port in the VLAN. The configuration is saved in NVRAM. The **static** keyword is used for configuring the MLD member ports statically. The configuration and the static ports and groups are saved in NVRAM. VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs, and cannot be used in MLD snooping.

Examples	This example shows how to enable MLD Immediate-Leave processing on VLAN 1:
	`Switch(config)#ipv6 mld snooping vlan 1 immediate-leave`
	`Warning: enabling immediate leave processing may lead to loss of MLD data on ports.`
	`Switch(config)#ipv6 mld snooping vlan 1 immediate-leave`
	`Switch(config)#exit`
	`Switch#show ipv6 mld snooping vlan 1 ?`

This example shows how to disable MLD Immediate-Leave processing on VLAN 1:

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ipv6 mld snooping vlan 1 immediate-leave
Switch(config)# end
Switch#sh
```

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

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ipv6 mld snooping vlan 1 mrouter interface Gigabitethernet1/1
Switch(config)# end
Switch#sh
```

This example shows how to configure a static multicast group:

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ipv6 mld snooping vlan 1 static FF12::34 interface Gigabitethernet1/1
Switch(config)# end
Switch#sh
```

You can verify your settings by entering the **show ipv6 mld snooping vlan** vlan-id-one EXEC command.

Related Commands	Command	Description
	ipv6 mld snooping	Enables IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping globally or on the specified VLAN.
	show ipv6 mld snooping	Displays IP version 6 (IPv6) MLD snooping configuration of the switch or the VLAN.

issu abortversion

To cancel the ISSU upgrade or the downgrade process in progress and to restore the Catalyst 4500 series switch to its state before the start of the process, use the **issu abortversion** command.

issu abortversion *active-slot* [*active-image-new*]

Syntax Description	*active-slot* Specifies the slot number for the current standby supervisor engine. *active-image-new* (Optional) Name of the new image present in the current standby supervisor engine.
Defaults	There are no default settings.
Command Modes	Privileged EXEC mode

Usage Guidelines

You can use the **issu abortversion** command at any time to stop the ISSU process. To complete the process enter the **issu commitversion** command. Before any action is taken, a check ensures that both supervisor engines are either in the run version (RV) or load version (LV) state.

When the **issu abortversion** command is issued before the **issu runversion** command, the standby supervisor engine is reset to boot with the old image. When the **issu abortversion** command is entered after the **issu runversion** command, a change takes place and the new standby supervisor engine is reset and reloaded with the old image.

Examples

This example shows how you can reset and reload the standby supervisor engine:

```
Switch#issu abortversion 2
Switch#
```

Related Commands

Command	Description
issu acceptversion	Halts the rollback timer and ensures that the new Cisco IOS software image is not automatically stopped during the ISSU process.
issu commitversion	Loads the new Cisco IOS software image into the new standby supervisor engine.
issu loadversion	Starts the ISSU process.
issu runversion	Forces a change from the active supervisor engine to the standby supervisor engine and causes the newly active supervisor engine to run the new image specified.
show issu state	Displays the ISSU state and current booted image name during the ISSU process.

issu acceptversion

To halt the rollback timer and to ensure that the new Cisco IOS software image is not automatically stopped during the ISSU process, use the **issu acceptversion** command.

issu acceptversion *active-slot* [*active-image-new*]

Syntax Description	*active-slot*	Specifies the slot number for the currently active supervisor engine.
	active-image-new	(Optional) Name of the new image on the currently active supervisor engine.

Default Rollback timer resets automatically 45 minutes after you enter the **issu runversion** command.

Command Modes Privileged EXEC mode

Usage Guidelines After you are satisfied with the new image and have confirmed the new supervisor engine is reachable via the Cisco IOS software, you can halt the rollback timer and ensure that the new image is not stopped. If the **issu acceptversion** command is not entered within 45 minutes from the time the **issu runversion** command is entered, the entire ISSU process is automatically rolled back to the previous version of the software. The rollback timer starts immediately after you enter the **issu runversion** command.

If the rollback timer expires before the standby supervisor engine goes to a hot-standby state, the timer is automatically extended by up to 15 minutes. If the standby state goes to a hot-standby state within this extension time or the 15 minute extension expires, the switch aborts the ISSU process. A warning message that requires your intervention is displayed every 1 minute of the timer extension.

If the rollback timer is set to a long period of time, such as the default of 45 minutes, and the standby supervisor engine goes into the hot-standby state in 7 minutes, you have 38 minutes (45 minus 7) to roll back if necessary.

Use the **issu set rollback-timer** to configure the rollback timer.

Examples This example shows how to halt the rollback timer and allow the ISSU process to continue:

```
Router#issu acceptversion 2
```

Related Commands

Command	Description
issu abortversion	Cancels the ISSU upgrade or the downgrade process in progress and restores the switch to its state before the start of the process.
issu commitversion	Loads the new Cisco IOS software image into the new standby supervisor engine.
issu loadversion	Starts the ISSU process.

Command	Description
issu runversion	Forces a change from the active supervisor engine to the standby supervisor engine and causes the newly active supervisor engine to run the new image specified.
issu set rollback-timer	Configures the In Service Software Upgrade (ISSU) rollback timer value.
show issu state	Displays the ISSU state and current booted image name during the ISSU process.

issu commitversion

To load the new Cisco IOS software image into the new standby supervisor engine, use the **issu commitversion** command.

issu commitversion *standby-slot* [*standby-image-sw*]

Syntax Description	*standby-slot*	Specifies the slot number for the currently active supervisor engine.
	standby-image-sw	(Optional) Name of the new image on the currently active supervisor engine.

Defaults Enabled by default.

Command Modes Privileged EXEC mode

Usage Guidelines The **issu commitversion** command verifies that the standby supervisor engine has the new Cisco IOS software image in its file system and that both supervisor engines are in the ear version (EV) state. If these conditions are met, the following actions take place:

- The standby supervisor engine is reset and booted with the new version of Cisco IOS software.
- The standby supervisor engine moves into the Stateful Switchover (SSO) mode and is fully started for all clients and applications with which the standby supervisor engine is compatible.
- The supervisor engines are moved into final state, which is the same as initial state.

Entering the **issu commitversion** command completes the In-Service Software Upgrade (ISSU) process. This process cannot be stopped or reversed to its original state without starting a new ISSU process.

Entering the **issu commitversion** command without entering the **issu acceptversion** command is equivalent to entering both the **issu acceptversion** and the **issu commitversion** commands. Use the **issu commitversion** command if you do not intend to run in the current state for an extended period of time and are satisfied with the new software version.

Examples This example shows how you can configure the standby supervisor engine to be reset and reloaded with the new Cisco IOS software version:

```
Switch# issu commitversion 5
Switch#
```

Related Commands	**Command**	**Description**
	issu acceptversion	Halts the rollback timer and ensures that the new Cisco IOS software image is not automatically stopped during the ISSU process.
	issu commitversion	Loads the new Cisco IOS software image into the new standby supervisor engine.
	issu loadversion	Starts the ISSU process.

Command	Description
issu runversion	Forces a change from the active supervisor engine to the standby supervisor engine and causes the newly active supervisor engine to run the new image specified.
show issu state	Displays the ISSU state and current booted image name during the ISSU process.

issu loadversion

To start the ISSU process, use the **issu loadversion** command.

issu loadversion *active-slot active-image-new standby-slot standby-image-new* [**force**]

Syntax Description		
	active-slot	Specifies the slot number for the currently active supervisor engine.
	active-image-new	Specifies the name of the new image on the currently active supervisor engine.
	standby-slot	Specifies the standby slot on the networking device.
	standby-image-new	Specifies the name of the new image on the standby supervisor engine.
	force	(Optional) Overrides the automatic rollback when the new Cisco IOS software version is determined to be incompatible.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

The **issu loadversion** command causes the standby supervisor engine to be reset and booted with the new Cisco IOS software image specified by the command. If both the old image and the new image are ISSU capable, ISSU compatible, and have no configuration mismatches, the standby supervisor engine moves into Stateful Switchover (SSO) mode, and both supervisor engines move into the load version (LV) state.

It will take several seconds after the **issu loadversion** command is entered for Cisco IOS software to load into the standby supervisor engine and the standby supervisor engine to transition to SSO mode.

Examples

This example shows how to initiate the ISSU process:

```
Switch#issu loadversion 1 bootflash:new/image 2 slavebootflash:new/image
Switch#
```

Related Commands	Command	Description
	issu abortversion	Cancels the ISSU upgrade or the downgrade process in progress and restores the switch to its state before the start of the process.
	issu acceptversion	Halts the rollback timer and ensures that the new Cisco IOS software image is not automatically stopped during the ISSU process.
	issu commitversion	Loads the new Cisco IOS software image into the new standby supervisor engine.

Command	Description
issu runversion	Forces a change from the active supervisor engine to the standby supervisor engine and causes the newly active supervisor engine to run the new image specified.
show issu state	Displays the ISSU state and current booted image name during the ISSU process.

issu runversion

To force a change from the active supervisor engine to the standby supervisor engine and to cause the newly active supervisor engine to run the new image specified in the **boot bootvariable** command, use the **issu runversion** command.

issu runversion *standby-slot* [*standby-image-new*]

Syntax Description	*standby-slot*	Specifies the standby slot on the networking device.
	standby-image-new	(Optional) Specifies the name of the new image on the standby supervisor engine.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Usage Guidelines The **issu runversion** command changes the currently active supervisor engine to standby supervisor engine and the end-standby-supervisor engine is booted with the old image version following and resets the switch. As soon as the standby-supervisor engine moves into the active standby state, the rollback timer is started.

Examples This example shows how to force a change of the active-supervisor engine to standby-supervisor engine:

```
Switch# issu runversion 2
Switch#
```

Related Commands	Command	Description
	issu abortversion	Cancels the ISSU upgrade or the downgrade process in progress and restores the switch in its state before the start of the process.
	issu acceptversion	Halts the rollback timer and ensures that the new Cisco IOS software image is not automatically stopped during the ISSU process.
	issu commitversion	Loads the new Cisco IOS software image into the new standby supervisor engine.
	issu loadversion	Starts the ISSU process.
	show issu state	Displays the ISSU state and current booted image name during the ISSU process.

issu set rollback-timer

To configure the In Service Software Upgrade (ISSU) rollback timer value, use the **issu set rollback-timer** command.

issu set rollback-timer *seconds*

Syntax Description	*seconds* Specifies the rollback timer value, in seconds. The valid timer value range is from 0 to 7200 seconds (2 hours). A value of 0 seconds disables the rollback timer.
Defaults	Rollback timer value is 2700 seconds.
Command Modes	Global configuration mode

Usage Guidelines Use the **issu set rollback-timer** command to configure the rollback timer value. You can only enable this command when the supervisor engines are in the init state.

Examples This example shows how you can set the rollback timer value to 3600 seconds, or 1 hour:

```
Switch#show redundancy issu
Switch(config)#issu set rollback-timer 3600
Switch(config)#end
Switch#
```

Related Commands	Command	Description
	issu acceptversion	Halts the rollback timer and ensures that the new Cisco IOS software image is not automatically stopped during the ISSU process.
	issu set rollback-timer	Configures the In Service Software Upgrade (ISSU) rollback timer value.

l2protocol-tunnel

To enable protocol tunneling on an interface, use the **l2protocol-tunnel** command. You can enable tunneling for the Cisco Discovery Protocol (CDP), Spanning Tree Protocol (STP), or VLAN Trunking Protocol (VTP) packets. To disable tunneling on the interface, use the **no** form of this command.

l2protocol-tunnel [cdp | stp | vtp]

no l2protocol-tunnel [cdp | stp | vtp]

Syntax Description

cdp	(Optional) Enables tunneling of CDP.
stp	(Optional) Enables tunneling of STP.
vtp	(Optional) Enables tunneling of VTP.

Defaults

The default is that no Layer 2 protocol packets are tunneled.

Command Modes

Interface configuration mode

Usage Guidelines

You must enter this command, with or without protocol type, 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.

Examples

This example shows how to enable protocol tunneling for the CDP packets:

```
Switch(config)# int fa 5/1
Switch(config-if)# l2protocol-tunnel cdp
Switch(config-if)#
```

Related Commands

Command	Description
l2protocol-tunnel cos	Configures the class of service (CoS) value for all tunneled Layer 2 protocol packets.
l2protocol-tunnel drop-threshold	Sets a drop threshold for the maximum rate of Layer 2 protocol packets per second to be received before an interface drops packets.
l2protocol-tunnel shutdown-threshold	Configures the protocol tunneling encapsulation rate

l2protocol-tunnel cos

To configure the class of service (CoS) value for all tunneled Layer 2 protocol packets, use the **l2protocol-tunnel cos** command. To return to the default value of zero, use the **no** form of this command.

l2protocol-tunnel cos *value*

no l2protocol-tunnel cos

Syntax Description	*value* Specifies the CoS priority value for tunneled Layer 2 protocol packets. The range is 0 to 7, with 7 being the highest priority.
Defaults	The default is to use the CoS value that is configured for data on the interface. If no CoS value is configured, the default is 5 for all tunneled Layer 2 protocol packets.
Command Modes	Global configuration mode
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`
	`Switch(config)#`

Related Commands	Command	Description
	l2protocol-tunnel	Enables protocol tunneling on an interface.
	l2protocol-tunnel drop-threshold	Sets a drop threshold for the maximum rate of Layer 2 protocol packets per second to be received before an interface drops packets.
	l2protocol-tunnel shutdown-threshold	Configures the protocol tunneling encapsulation rate.

l2protocol-tunnel drop-threshold

To set a drop threshold for the maximum rate of Layer 2 protocol packets per second to be received before an interface drops packets, use the **l2protocol-tunnel drop-threshold** command. You can set the drop threshold for the Cisco Discovery Protocol (CDP), Spanning Tree Protocol (STP), or VLAN Trunking Protocol (VTP) packets. To disable the drop threshold on the interface, use the **no** form of this command.

l2protocol-tunnel drop-threshold {**cdp** | **stp** | **vtp**} *value*

no l2protocol-tunnel drop-threshold [**cdp** | **stp** | **vtp**] *value*

Syntax Description	**cdp** (Optional) Specifies a drop threshold for CDP. **stp** (Optional) Specifies a drop threshold for STP. **vtp** (Optional) Specifies a drop threshold for VTP. *value* Specifies a threshold on packets per second to be received for encapsulation before the interface shuts down, or specifies the threshold before the interface drops packets. The range is 1 to 4096. The default is no threshold.
Defaults	The default is no drop threshold for the number of the Layer 2 protocol packets.
Command Modes	Interface configuration mode

Usage Guidelines

The **l2protocol-tunnel drop-threshold** command controls 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 on the interface, the drop threshold value must be less than or equal to the shutdown threshold value.

When the drop threshold is reached, the interface drops the Layer 2 protocol packets until the rate at which they are received is below the drop threshold.

Examples

This example shows how to configure the drop threshold rate:

```
Switch(config)# int fa2/1
Switch(config-if)# l2protocol-tunnel drop-threshold cdp 50
Switch(config-if)#
```

Related Commands	**Command**	**Description**
	l2protocol-tunnel	Enables protocol tunneling on an interface.
	l2protocol-tunnel cos	Configures the class of service (CoS) value for all tunneled Layer 2 protocol packets.
	l2protocol-tunnel shutdown-threshold	Configures the protocol tunneling encapsulation rate.

l2protocol-tunnel shutdown-threshold

To configure the protocol-tunneling encapsulation rate, use the **l2protocol-tunnel shutdown-threshold** command. You can set the encapsulation rate for the Cisco Discovery Protocol (CDP), Spanning Tree Protocol (STP), or VLAN Trunking Protocol (VTP) packets. To disable the encapsulation rate on the interface, use the no form of this command.

l2protocol-tunnel shutdown-threshold [**cdp** | **stp** | **vtp**] *value*

no l2protocol-tunnel shutdown-threshold [**cdp** | **stp** | **vtp**] *value*

Syntax Description	**cdp** (Optional) Specifies a shutdown threshold for CDP.
	stp (Optional) Specifies a shutdown threshold for STP.
	vtp (Optional) Specifies a shutdown threshold for VTP.
	value Specifies a threshold in packets per second to be received for encapsulation before the interface shuts down. The range is 1 to 4096. The default is no threshold.

Defaults	The default is no shutdown threshold for the number of Layer 2 protocol packets.
Command Modes	Interface configuration mode

Usage Guidelines

The **l2protocol-tunnel shutdown-threshold** command controls the number of protocol packets per second that are received on an interface before it shuts down. When no protocol options specified with the keyword, the threshold is applied to each of the tunneled Layer 2 protocol types. If you also set a drop threshold on the interface, 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 l2protocol-tunnel**, the interface is brought out of the error-disabled state and allowed to attempt to work again. If all the causes have timed out, if the error-recovery feature generation is not enabled for **l2protocol**, the interface stays in the error-disabled state until you enter the **shutdown** and **no shutdown** commands.

Examples

This example shows how to configure the maximum rate:

```
Switch(config)#int fa6/1
Switch(config-if)# l2protocol-tunnel shutdown-threshold cdp 50
Switch(config-if)#
```

Related Commands	**Command**	**Description**
	l2protocol-tunnel	Enables protocol tunneling on an interface.

Command	Description
l2protocol-tunnel cos	Configures the class of service (CoS) value for all tunneled Layer 2 protocol packets.
l2protocol-tunnel drop-threshold	Sets a drop threshold for the maximum rate of Layer 2 protocol packets per second to be received before an interface drops packets.

lacp port-priority

To set the LACP priority for the physical interfaces, use the **lacp port-priority** command.

lacp port-priority *priority*

Syntax Description	*priority* Priority for the physical interfaces, valid values are from 1 to 65535.
Defaults	Priority is set to 32768.
Command Modes	Interface configuration mode
Usage Guidelines	You must assign exclusive to the switch a port priority that can be specified automatically or by entering the **lacp port-priority** command. The port priority is used with the port number to form the port identifier. The port priority is used to decide which ports should be put in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating. Although this command is a global configuration command, the priority value is supported only on port channels with LACP-enabled physical interfaces. This command is supported on LACP-enabled interfaces. When setting the priority, the higher numbers indicate lower priorities.

Examples	This example shows how to set the priority for the interface:
	`Switch(config)#int gi1/1/4 lacp port-priority 32768`
	`Switch(config)#int gi1/1/4`

Related Commands	Command	Description
	channel-group	Assigns and configures an EtherChannel interface to an EtherChannel group.
	channel-protocol	Restricts LACP or PAgP on an interface.
	lacp system-priority	Sets the priority of the system for LACP.
	show lacp	Displays LACP information.

lacp system-priority

To set the priority of the system for LACP, use the **lacp system-priority** command.

lacp system-priority *priority*

Syntax Description	*priority* Priority of the system; valid values are from 1 to 65535.

Defaults Priority is set to 32768.

Command Modes Global configuration mode

Usage Guidelines You must assign each switch that is running LACP a system priority that can be specified automatically or by entering the **lacp system-priority** command. The system priority is used with the switch MAC address to form the system ID and is also used during negotiation with other systems.

Although this command is a global configuration command, the *priority* value is supported on port channels with LACP-enabled physical interfaces.

When setting the priority, the higher numbers indicate lower priorities.

You can also enter the **lacp system-priority** command in interface configuration mode. After you enter the command, the system defaults to global configuration mode.

Examples This example shows how to set the system priority:

```
Switch(config)# lacp system-priority 32768
Switch(config)#
```

Related Commands	Command	Description
	channel-group	Assigns and configures an EtherChannel interface to an EtherChannel group.
	channel-protocol	Enables LACP or PAgP on an interface.
	lacp system-priority	Sets the priority of the system for LACP.
	show lacp	Displays LACP information.

lldp tlv-select power-management

To to enable power negotiation through LLDP, use the **lldp tlv-select power-management** interface command.

lldp tlv-select power-management

Syntax Description This command has no arguments or keywords.

Defaults Enabled on POEP ports

Command Modes Interface level

Command History

Release	Modification
12.2(52)SG	Support was introduced on the Catalyst 4500 series switch.

Usage Guidelines You need to disable this feature if you do not want to perform power negotiation through LLDP. This feature is not supported on non-POEP ports; the CLI is suppressed on such ports and TLV is not exchanged.

Examples This example shows how to enable LLDP power negotiation on interface Gigabit Ethernet 3/1:

```
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int gi 3/1
Switch(config-if)#lldp tlv-select power-management
```

Related Commands

Command	Description
lldp run	Cisco IOS Command Reference library.

logging event link-status global (global configuration)

To change the default switch-wide global link-status event messaging settings, use the **logging event link-status global** command. Use the **no** form of this command to disable the link-status event messaging.

```
logging event link-status global
no logging event link-status global
```

Syntax Description This command has no arguments or keywords.

Defaults The global link-status messaging is disabled.

Command Modes Global configuration mode

Usage Guidelines If link-status logging event is not configured at the interface level, this global link-status setting takes effect for each interface.

Examples This example shows how to globally enable link status message on each interface:

```
Switch# conf t terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# logging event link-status global
Switch(config)# end
Switch#
```

Related Commands	Command	Description
	logging event link-status (interface configuration)	Enables the link-status event messaging on an interface.

logging event link-status (interface configuration)

To enable the link-status event messaging on an interface, use the **logging event link-status** command. Use the **no** form of this command to disable link-status event messaging. Use the **logging event link-status use-global** command to apply the global link-status setting.

logging event link-status

no logging event link-status

logging event link-status use-global

Defaults Global link-status messaging is enabled.

Command Modes Interface configuration mode

Usage Guidelines To enable system logging of interface state-change events on a specific interface, enter the **logging event link-status** command in interface configuration mode.

To enable system logging of interface state-change events on all interfaces in the system, enter the **logging event link-status global** command in global configuration mode. All interfaces without the state change event configuration use the global setting.

Examples This example shows how to enable logging event state-change events on interface gi13/1:

```
Switch# conf t terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface gi13/1
Switch(config-if)# logging event link-status
Switch(config-if)# end
Switch#
```

This example shows how to turn off logging event link status regardless of the global setting:

```
Switch# conf t terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface gi13/1
Switch(config-if)# no logging event link-status
Switch(config-if)# end
Switch#
```

This example shows how to enable the global event link-status setting on interface gi13/1:

```
Switch# conf t terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface gi13/1
Switch(config-if)# logging event link-status use-global
Switch(config-if)# end
Switch#
```

Related Commands	Command	Description
	logging event link-status global (global configuration)	Changes the default switch-wide global link-status event messaging settings.

logging event trunk-status global (global configuration)

To enable the trunk-status event messaging globally, use the **logging event trunk-status global** command. Use the **no** form of this command to disable trunk-status event messaging.

logging event trunk-status global

no logging event trunk-status global

Syntax Description This command has no arguments or keywords.

Defaults Global trunk-status messaging is disabled.

Command Modes Global configuration mode

Usage Guidelines If trunk-status logging event is not configured at the interface level, the global trunk-status setting takes effect for each interface.

Examples This example shows how to globally enable link-status messaging on each interface:

```
Switch#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#logging event trunk-status global
Switch(config)#^Z
Switch#
```

Related Commands

Command	Description
logging event trunk-status global (global configuration)	Enables the trunk-status event messaging on an interface.

logging event trunk-status (interface configuration)

To enable the trunk-status event messaging on an interface, use the **logging event trunk-status** command. Use the **no** form of this command to disable the trunk-status event messaging. Use the **logging event trunk-status** *use-global* command to apply the global trunk-status setting.

logging event trunk-status

no logging event trunk-status

logging event trunk-status *use-global*

Defaults Global trunk-status messaging is enabled.

Command Modes Interface configuration mode

Usage Guidelines To enable system logging of interface state-change events on a specific interface, enter the **logging event trunk-status** command in interface configuration mode.

To enable system logging of interface state-change events on all interfaces in the system, enter the **logging event trunk-status** *use-global* command in global configuration mode. All interfaces without the state-change event configuration use the global setting.

Examples This example shows how to enable logging event state-change events on interface gi11/1:

```
Switch# conf t terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface gi11/1
Switch(config-if)# logging event trunk-status
Switch(config-if)# end
Switch#
```

This example shows how to turn off logging event trunk-status regardless of the global setting:

```
Switch# conf t terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface gi11/1
Switch(config-if)# no logging event trunk-status
Switch(config-if)# end
Switch#
```

This example shows how to enable the global event trunk-status setting on interface gi11/1:

```
Switch# conf t terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface gi11/1
Switch(config-if)# logging event trunk-status use-global
Switch(config-if)# end
Switch#
```

Related Commands	Command	Description
	logging trunk-status (global configuration)	Enables the trunk-status event messaging on an interface.

mab

To enable and configure MAC authentication bypass (MAB) on a port, use the **mab** command in interface configuration mode. To disable MAB, use the **no** form of this command.

mab [eap]

no mab [eap]

Note The **mab** command is totally independent of the effect of the **dot1x system-auth-control** command.

Syntax Description **eap** (Optional) Specifies that a Full-EAP conversation should be used, as opposed to standard RADIUS Access-Request, Access-Accept conversation.

Command Default Disabled

Command Modes Interface configuration mode

Usage Guidelines When a port is configured for MAB as a fallback method, it operates in a typical dot1X method until a configurable number of failed attempts to request the identity of the host. The authentic ator learns the MAC address of the host and uses that information to query an authentication server to see whether this MAC address will be granted access.

Examples The following example shows how to enable MAB on a port:

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

The following example shows how to enable and configure MAB on a port:

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

The following example shows how to disable MAB on a port:

```
Switch(config-if)# no mab
Switch(config-if)#
```

Related Commands

Command	Description
show authentication	Displays Authentication Manager information.
show mab	Displays MAB information.
show running-config	Displays the running configuration information.

mac access-list extended

To define the extended MAC access lists, use the **mac access-list extended** command. To remove the MAC access lists, use the **no** form of this command.

mac access-list extended *name*

no mac access-list extended *name*

Syntax Description	*name* ACL to which the entry belongs.
Defaults	MAC access lists are not defined.
Command Modes	Global configuration mode

Usage Guidelines

When you enter the ACL name, follow these naming conventions:

- Maximum of 31 characters long and can include a-z, A-Z, 0-9, the dash character (-), the underscore character (_), and the period character (.)
- Must start with an alpha character and must be unique across all ACLs of all types
- Case sensitive
- Cannot be a number
- Must not be a keyword; keywords to avoid are all, default-action, map, help, and editbuffer

When you enter the **mac access-list extended** name command, you use the following subnetcommands to create or delete entries in a MAC hyper access list:

[**no**] {**permit**| **deny**} {{*src-mac mask*} |**any**} {*dest-mac mask*} [**protocol-family** | **applyhcalc**] *aap-non-ipv4* | *decnet* | *ipx* | *ipvk* | *sna-ipv4* | *sna-non-ipv4* | *vines* | *xns*} [*<arbitrary ethertype> | name-called ethertype*].

Table 2-7 describes the syntax of the **mac access-list extended** subcommands.

Table 2-7 mac access-list extended Subcommands

Subcommand	Description
any	Specifies any source-host or destination-host.
arbitrary ethertype	(Optional) Specifies an arbitrary ethertype in the range 1536 to 65535 (Decimal or Hexadecimal).
deny	Prevents access if the conditions are matched.
dest-mac mask	(Optional) Specifies a destination MAC address of the form *dest-mac address dest-mac-address mask*.

Table 2-7 mac access-list extended Subcommands (continued)

Subcommand	Description
name *ether-type* *ether-type*	(Optional) Denotes a predefined name or hexadecimal number of an EtherType for common protocols: *aarp*—AppleTalk ARP *amber*—DEC-Amber *appletalk*—Apple Talk/Ether Talk *dec-spanning*—DEC-Spanning Tree *decnet-iv*—DECnet Phase IV *diagnostic*—DEC-Diagnostic *dsm*—DEC-DSM *etype-6000*—0x6000 *etype-8042*—0x8042 *lat*—DEC-LAT *lavc-sca*—DEC-LAVC-SCA *mop-console*—DEC-MOP Remote Console *mop-dump*—DEC-MOP Dump *msdos*—DEC-MSDOS *mumps*—DEC-MUMPS *netbios*—DEC-NETBIOS *protocol-family* An Ethernet protocol family *vines-echo*—VINES Echo *vines-ip*—VINES IP *xns-idp*—XNS IDP
lsap	(Optional) Defines a customer-form access list.
permit	Allows access if the conditions are matched.
protocol-family	(Optional) Name of the protocol family. Table 2-8 lists which packets are mapped to a particular protocol family.
src-mac mask	Source MAC address in the form: *source-mac-address source-mac-address-mask*.

Table 2-8 describes mapping an Ethernet packet to a protocol family.

Table 2-8 Mapping an Ethernet Packet to a Protocol Family

Protocol Family	Ethertype in Packet Header
Appletalk	0x809B, 0x80F3
Arp-Non-Ipv4	0x0806, and protocol header of Arp is a non-Ip protocol family
Decnet	0x6000-0x6009, 0x8038-0x8042
Ipx	0x8137-0x8138

Table 2-8 Mapping an Ethernet Packet to a Protocol Family

Protocol Family	Ethertype in Packet Header
Ipv4	0x0800
Rarp-Ipv4	0x8035 and protocol header of Rarp is Ipv4
Rarp-Non-Ipv4	0x8035 and protocol header of Rarp is a non-Ipv4 protocol family
Vines	0x0BAD, 0x0BAE, 0x0BAF
Xns	0x0600, 0x0807

When you enter the *src-mac mask* or *dst-mac mask* value, follow these guidelines:

- Enter the MAC address as three 4-byte values in dotted hexadecimal format such as 0030.96ZX.5B14.
- Enter the MAC address masks as three 4-byte values in dotted hexadecimal format. Use 1 bit as a wild card. For example, to match an address exactly, use 0000.0000.0000 (can be entered as 0.0.0).
- For the optional *protocol* parameter, you can enter either the EtherType or the keyword.
- Entries without a *protocol* parameter match any protocol.
- The access lists entries are scanned in the order that you enter them. The first matching entry is used. To improve performance, place the most commonly used entries near the beginning of the access list.
- An implicit **deny any any** entry exists at the end of an access list unless you include an explicit **permit any any** entry at the end of the list.
- All new entries to an existing list are placed at the end of the list. You cannot add entries to the middle of a list.

Examples

This example shows how to create a MAC layer access list named mac_layer that denies traffic from 0000.4700.0001, which is going to 0000.4700.0050, and permits all other traffic:

```
Switch(config)# mac access-list extended mac_layer
Switch(config-ext-mac)# deny 0000.4700.0001 0.0.0 0000.4700.0050 0.0.0 protocol-family
appletalk
Switch(config-ext-mac)# permit any any
Switch(config-ext-mac)# end
Switch#
```

Related Commands

Command	Description
show vlan access-map	Displays VLAN access map information.

mac-address-table aging-time

To configure the aging time for the entries in the Layer 2 table, use the **mac-address-table aging-time** command. To reset the seconds value to the default setting, use the **no** form of this command.

mac-address-table aging-time *seconds* [**vlan** *vlan_id*]

no mac-address-table aging-time *seconds* [**vlan** *vlan_id*]

Syntax Description	*seconds*	Aging time in seconds; valid values are 0 and from 10 to 1000000 seconds.
	vlan *vlan_id*	(Optional) Single VLAN number or a range of VLANs; valid values are from 1 to 4094.

Defaults

Aging time is set to 300 seconds.

Command Modes

Global configuration mode

Usage Guidelines

If you do not enter a VLAN, the change is applied to all routed-port VLANs.

Enter 0 seconds to disable aging.

Examples

This example shows how to configure the aging time to 400 seconds:

```
Switch(config)# mac-address-table aging-time 400
Switch(config)#
```

This example shows how to disable aging:

```
Switch(config)# mac-address-table aging-time 0
Switch(config)#
```

Related Commands

Command	Description
show mac-address-table aging-time	Displays MAC address table aging information.

mac-address-table dynamic group protocols

To enable the learning of MAC addresses include the "ip" and "other" protocol buckets, even though the incoming packet may belong to only one of the protocol buckets, use the **mac-address-table dynamic group protocols** command. To disable grouped learning, use the **no** form of this command.

mac-address-table dynamic group protocols {**ip** | **other**} {**ip** | **other**}

no mac-address-table dynamic group protocols {**ip** | **other**} {**ip** | **other**}

Syntax Description	**ip**	Specifies the "ip" protocol bucket.
	other	Specifies the "other" protocol bucket.

Defaults The group learning feature is disabled.

Command Modes Global configuration mode

Usage Guidelines The entries within the "ip" and "other" protocol buckets are created according to the protocol of the incoming traffic.

When you use the **mac-address-table dynamic group protocols** command, an incoming MAC address that might belong to either the "ip" or the "other" protocol bucket, is learned on both protocol buckets. Therefore, any traffic destined to this MAC address and belonging to any of the protocol buckets is unicasted to that MAC address, rather than flooded. This reduces the unicast Layer 2 flooding that might be caused if the incoming traffic from a host belongs to a different protocol bucket than the traffic that is destined to the sending host.

Examples This example shows that the MAC addresses are initially assigned to either the "ip" or the "other" protocol bucket:

```
Switch> show mac-address-table dynamic
Legend: Notice:an
 vLan  mac address     type        protocols       port
-----+---------------+--------+-------------+----------------------
   1   0000.0000.5000  dynamic  other       4d gabbit fc5/mod/1/1
   1   0000.0234.0d46  dynamic  ip          4d gabbit fc5/mod/1/1
   1   0000.2700.1a00  dynamic  ip assigned 4d gabbit fc5/mod/1/1
   1   0000.2700.1a46  dynamic  ip          4d gabbit fc5/mod/1/1
   1   0000.4726.0b70  dynamic  ip          4d gabbit fc5/mod/1/1
   1   0000.4726.7b00  dynamic  ip          4d gabbit fc5/mod/1/1
   1   0000.4700.4b46  dynamic  ip          4d gabbit fc5/mod/1/1
   1   0000.5a00.1d00  dynamic  ip          4d gabbit fc5/mod/1/1
   1   0000.5a00.1d46  dynamic  ip          4d gabbit fc5/mod/1/1
   1   0000.5b00.3a46  dynamic  ip          4d gabbit fc5/mod/1/1
   1   0000.5a00.5a00  dynamic  ip          4d gabbit fc5/mod/1/1
   1   0000.5a00.5a46  dynamic  ip          4d gabbit fc5/mod/1/1
   1   0004.5a0a.6a00  dynamic  ip          4d gabbit fc5/mod/1/1
   1   0004.5a0a.6a46  dynamic  ip          4d gabbit fc5/mod/1/1
```

show address-table dynamic group protocols

```
1    0014.5e00.0803   dynamic  ip                   Gigabit0/38/network/1.1
1    0014.5e00.0804   dynamic  ip                   Gigabit0/38/network/1.1
1    0014.5e00.0806   dynamic  ip                   Gigabit0/38/network/1.1
1    0014.5e00.0906   dynamic  ip                   Gigabit0/38/network/1.1
1    0014.5e00.0907   dynamic  ip                   Gigabit0/38/network/1.1
1    0014.5e00.0a03   dynamic  ip                   Gigabit0/38/network/1.1
1    0014.5e00.0a04   dynamic  ip                   Gigabit0/38/network/1.1
1    0014.5e00.0a06   dynamic  ip                   Gigabit0/38/network/1.1
1    0017.a907.7a04   dynamic  ip                   Gigabit0/38/network/1.1
1    0017.a907.7a06   dynamic  ip                   Gigabit0/38/network/1.1
1    0017.a907.7a14   dynamic  ip                   Gigabit0/38/network/1.1
1    0030.9734.2140   dynamic  ip                   Gigabit0/38/network/1.1
1    0030.9734.2146   dynamic  ip                   Gigabit0/38/network/1.1
1    0030.9734.2176   dynamic  ip                   Gigabit0/38/network/1.1
1    0032.7ba6.07fa   dynamic  mac-pseudo           Gigabit0/38/network/1.1
1    0032.a3b2.c572   dynamic  ip                   Gigabit0/38/network/1.1
1    0032.a3b2.c576   dynamic  ip                   Gigabit0/38/network/1.1
1    0032.d851.d5ad   dynamic  ip                   Gigabit0/38/network/1.1
1    0032.d851.f0c6   dynamic  ip                   Gigabit0/38/network/1.1
1    0032.d851.f0d6   dynamic  ip                   Gigabit0/38/network/1.1
1    0040.0407.d2ae   dynamic  ip                   Gigabit0/38/network/1.1
1    0040.0408.1c33   dynamic  ip                   Gigabit0/38/network/1.1
1    0040.0408.1c43   dynamic  mac-pseudo           Gigabit0/38/network/1.1
1    0040.0408.1c53   dynamic  ip                   Gigabit0/38/network/1.1
1    0040.0c7ba.da3d  dynamic  ip                   Gigabit0/38/network/1.1
1    0040.d179.2f0d   dynamic  ip                   Gigabit0/38/network/1.1
1    0040.d179.4f05   dynamic  ip                   Gigabit0/38/network/1.1
1    0040.d179.4f15   dynamic  ip                   Gigabit0/38/network/1.1
1    0040.d179.4f25   dynamic  ip                   Gigabit0/38/network/1.1
1    0040.d180.a8d2   dynamic  ip                   Gigabit0/38/network/1.1
1    0040.d180.a8d6   dynamic  ip                   Gigabit0/38/network/1.1
Switch#
```

This example shows how to assign MAC addresses that belong to either the "ip" or the "other" bucket to both buckets:

```
Switch(config)# mac-address-table dynamic group protocols ip other
Switch(config)# exit
Switch# show mac address-table dynamic
Unicast Entries
 vlan  mac address     type        protocols          port
-------+---------------+--------+---------+----------------------------------
 1     0001.0000.0000  dynamic  ip,other            Gigabit0/38/network/1.1
 1     0001.4244.5a00  dynamic  ip,other            Gigabit0/38/network/1.1
 1     0001.4700.2a41  dynamic  ip,other            Gigabit0/38/network/1.1
 1     0001.4700.4275  dynamic  ip,other            Gigabit0/38/network/1.1
 1     0001.4700.4a41  dynamic  ip,other            Gigabit0/38/network/1.1
 1     0001.4700.7a41  dynamic  ip,other            Gigabit0/38/network/1.1
 1     0001.4700.d6a3  dynamic  ip,other            Gigabit0/38/network/1.1
 1     0001.4700.d6a4  dynamic  ip,other            Gigabit0/38/network/1.1
 1     0001.4700.d6a6  dynamic  ip,other            Gigabit0/38/network/1.1
 1     0001.4701.3a41  dynamic  ip,other            Gigabit0/38/network/1.1
 1     0001.5204.2b14  dynamic  ip,other            Gigabit0/38/network/1.1
 1     0001.5a64.8b53  dynamic  ip,other            Gigabit0/38/network/1.1
 1     0001.5a64.8b54  dynamic  ip,other            Gigabit0/38/network/1.1
 1     0001.5a64.8b56  dynamic  ip,other            Gigabit0/38/network/1.1
 1     0001.5a64.8b5a  dynamic  ip,other            Gigabit0/38/network/1.1
 1     0001.5a64.8b7a  dynamic  ip,other            Gigabit0/38/network/1.1
 1     0001.5a64.8c13  dynamic  ip,other            Gigabit0/38/network/1.1
 1     0001.5a64.8c14  dynamic  ip,other            Gigabit0/38/network/1.1
 1     0001.5a64.8c16  dynamic  ip,other            Gigabit0/38/network/1.1
 1     0001.5a64.8c1a  dynamic  ip,other            Gigabit0/38/network/1.1
 1     0001.5a64.8c3d  dynamic  ip,other            Gigabit0/38/network/1.1
Switch#
```

```
1    0034.c14d.1b40   dynamic  ip,ipx,assigned     GigabitEthernet1/1
1    0034.c14d.1b41   dynamic  ip,ipx,assigned     GigabitEthernet1/1
1    0034.c14d.b400   dynamic  ip,ipx,assigned     GigabitEthernet1/1
1    0035.dbe5.7c0a   dynamic  ip,ipx,assigned     GigabitEthernet1/1
1    0037.a987.7a00   dynamic  ip,ipx,assigned     GigabitEthernet1/1
1    0037.a987.7a80   dynamic  ip,ipx,assigned     GigabitEthernet1/1
1    0037.e9a6.5a34   dynamic  ip,ipx,assigned     GigabitEthernet1/1
1    0038.df4b.4b00   dynamic  ip,ipx,assigned     GigabitEthernet1/1
1    0038.5054.2148   dynamic  ip,ipx,assigned     GigabitEthernet1/1
1    0038.5583.c480   dynamic  ip,ipx,assigned     GigabitEthernet1/1
1    0012.4140.c070   dynamic  ip,ipx,assigned     GigabitEthernet1/1
1    0050.5437.5fa0   dynamic  ip,ipx,assigned     GigabitEthernet1/1
1    0050.5437.5fb0   dynamic  ip,ipx,assigned     GigabitEthernet1/1
1    0050.8a6c.81c8   dynamic  ip,ipx,assigned     GigabitEthernet1/1
1    0050.8a6b.a837   dynamic  ip,ipx,assigned     GigabitEthernet1/1
1    0060.3e47.8f30   dynamic  ip,ipx,assigned     GigabitEthernet1/1
1    0060.5b56.2b48   dynamic  ip,ipx,assigned     GigabitEthernet1/1
1    0060.b771.c6be   dynamic  ip,ipx,assigned     GigabitEthernet1/1
1    0060.b7ed.7d7e   dynamic  ip,ipx,assigned     GigabitEthernet1/1
1    0060.b7ba.4bc0   dynamic  ip,ipx,assigned     GigabitEthernet1/1
1    0060.b7fb.2938   dynamic  ip,ipx,assigned     GigabitEthernet1/1
1    0060.b7ed.7d80   dynamic  ip,ipx,assigned     GigabitEthernet1/1
1    0060.b7fb.4240   dynamic  ip,ipx,assigned     GigabitEthernet1/1
1    0060.b0fb.093e   dynamic  ip,ipx,assigned     GigabitEthernet1/1
1    0060.b0fb.0940   dynamic  ip,ipx,assigned     GigabitEthernet1/1
1    0030.2041.b039   dynamic  ip,ipx,assigned     GigabitEthernet1/1
Total 1,000
```

mac address-table learning vlan

To enable MAC address learning on a VLAN, use the **mac address-table learning** global configuration command. Use the **no** form of this command to disable MAC address learning on a VLAN to control which VLANs can learn MAC addresses.

mac address-table learning vlan-list

no mac address-table learning vlan vlan-id

Syntax Description	vlan-id Specifies a single VLAN ID or a range of VLAN IDs (separated by a hyphen or comma. Valid VLAN IDs are 1 to 4094.

Defaults	Enabled on all VLANs.
Command Modes	Global configuration

Usage Guidelines

When you control MAC address learning on a VLAN, you can manage the available table space by controlling which VLANs, and which ports can learn MAC addresses.

You can disable MAC address learning on a single VLAN ID (for example, by entering **no mac address-table learning vlan 223**) or on a range of VL AN IDs (for example, by entering **no mac address-table learning vlan 1-20, 15**)

Before you disable MAC address learning, familiarize yourself with the network topology and the switch system configuration. If you disable MAC address learning on a VLAN, flooding may occur in the network. For example, if you disable MAC address learning on a VL AN with a configured switch virtual interface (SVI), the switch floods all IP packets in the Layer 2 domain. If you disable MAC address learning on a VLAN with a trunk port, flooding is sent to every port on the switch that could be part of that VLAN domain. Disable MAC address learning only on VL AN s that contain two ports. Use caution before disabling MAC address learning on a VLAN with an SVI.

You cannot disable MAC address learning on a VLAN that the switch uses internally. This action causes the switch to generate an error message and rejects the **mac address-table learning vlan** command. To view an internal VL AN, enter the **show vlan internal usage** privileged EXEC command.

If you disable MAC address learning on a VLAN configured as a PVLAN primary or a secondary VLAN, the MAC addresses are still learned on the VLAN (primary or secondary) associated with the PVLAN.

You cannot disable MAC address learning on an RSPAN VLAN. The configuration is not allowed.

If you disable MAC address learning on a VLAN that includes a secure port, MAC address learning is automatically also disabled on the secure port. If you enable port security on the interface, the disabled MAC address learning state is enabled.

To display the MAC address learning status of a specific VLAN or for all VLANs, enter the **show mac-address-table learning vlan** command.

Examples

This example shows how to disable MAC address learning on VLAN 2003:

```
Switch(config)# no mac address-table learning vlan 2003
```

Related Commands

Command	Description
show mac address-table learning	Displays the MAC address learning status on all VLANs or on the specified VLAN.

mac-address-table notification

To enable MAC address notification on a switch, use the **mac-address-table notification** command. To return to the default setting, use the no form of this command.

mac-address-table notification [{**change** [*history-size* | *hs_value*] | **interval** *intv_value*} | [**mac-source**] | [**threshold** [*limit percentage* | **interval** *time*]] | [**trunk-fail** [**interval** *time* | **limit** *trunk_fail*]]

no mac-address-table notification [{**change** [*history-size* | *hs_value*] | **interval** *intv_value*} | [**mac-source**] | [**threshold** [*limit percentage* | **interval** *time*]] | [**trunk-fail** [**interval** *time* | **limit** *trunk_fail*]]

Syntax Description

change	(Optional) Specifies enabling MAC change notification.
history-size *hs_value*	(Optional) Sets a maximum number of entries in the MAC change notification history table. The range is 0 to 500 entries.
interval *intv_value*	(Optional) Sets a notification trap interval: the set interval time between two consecutive traps. The range is 0 to 2147483647 seconds.
mac-source	(Optional) Specifies enabling MAC source notification.
threshold	(Optional) Specifies enabling MAC threshold notification.
limit *percentage*	(Optional) Specifies the percentage of MAT utilization threshold; valid values are from 1 to 100 percent.
interval *time*	(Optional) Specifies the time between MAC threshold notifications; valid values are given-time as equal to 120 seconds.
trunk-fail	(Optional) Specifies up/down(4) notifications of failures to install MAC addresses learned on unknown ports hardware. Disabled by default.
interval *time*	(Optional) Specifies the syslog interval between hardware MAC learning failure notifications. The default interval is 0 (forever). The range is between 1 to 100000 seconds.
limit *trunk_fail*	(Optional) Specifies the number of hardware MAC learning failures to be allowed in a notification interval.

Defaults

MAC address notification feature is disabled.

The default MAC change trap interval value is 1 second.

The default number of entries in the history table is 1.

MAC move notification is disabled.

MAC threshold monitoring feature is disabled.

The default limit is 50 percent.

The default time is 120 seconds.

Hardware MAC learning failure syslog notification is disabled.

The default limit is 1000.

The default interval is 150 seconds.

Command Modes Global configuration mode

Usage Guidelines You can enable the MAC change notification feature using the **mac-address-table notification change** command. If you do this, you must also enable MAC notification traps on an interface using the **snmp trap mac-notification change interface** configuration command and configure the switch to send MAC change traps to the NMS using the **snmp-server enable traps mac-notification** global configuration command.

When the history-size option is configured, the existing MAC change history table is deleted, and a new table is created.

Examples This example shows how to set the MAC address notification history table size to 300 entries:

```
Switch(config)# mac-address-table notification change history-size 300
Switch(config)#
```

This example shows how to set the MAC address notification interval time to 1250 seconds:

```
Switch(config)# mac-address-table notification change interval 1250
Switch(config)#
```

This example shows how to enable hardware MAC address learning failure syslog notification:

```
Switch(config)# mac address-table notification learn-fail
```

This example shows how to set the interval of hardware MAC address learning failure syslog notification to 30 seconds:

```
Switch(config)# mac address-table notification learn-fail interval 30
```

Related Commands

Command	Description
clear mac-address-table	Clears the global counter entries from the Layer 2 MAC address table.
mac-address-table notification	Enables MAC address notification on a switch.
snmp-server enable traps	Enables SNMP notifications.
snmp trap mac-notification change	Enables SNMP MAC address notifications.

mac-address-table static

To configure the static MAC addresses for a VLAN interface or drop unicast traffic for a MAC address for a VLAN interface, use the **mac-address-table static** command. To remove the static MAC address configuration, use the **no** form of this command.

mac-address-table static *mac-addr* | **vlan** *vlan-id* | **interface** *type* | **drop**

no mac-address-table static *mac-addr* | **vlan** *vlan-id* | **interface** *type* | **drop**

Syntax Description	*mac-addr* MAC address; optional when using the **no** form of this command. **vlan** *vlan-id* VLAN and valid VLAN number; valid values are from 1 to 4094. **interface** *type* Interface type and number; valid options are **FastEthernet** and **GigabitEthernet**. **drop** Drops all traffic received from and going to the configured MAC address in the specified VLAN.

Defaults

This command has no default settings.

Command Modes

Global configuration mode

Usage Guidelines

When a static MAC address is installed, it is associated with a port.

The output interface specified must be a Layer 2 interface and not an SVI.

If you do not enter a protocol type, an entry is automatically created for each of the four protocol types.

Entering the **no** form of this command does not remove the system MAC address.

When entering a MAC address, entering **interface** is optional. For unicast entries, the entry is restored automatically. For multicast entries, if you do not specify an interface, the entire entry is restored. You can specify the selected ports to be restored by specifying the interface.

Examples

This example shows how to add the static entries to the MAC address table:

```
Switch(config)# mac-address-table static 0050.3e8d.6400 vlan 100 interface fastethernet5/7
Switch(config)#
```

Related Commands	Command	Description
	show mac-address-table static	Displays the static MAC address table entries only.

macro apply cisco-desktop

To enable the Cisco-recommended features and settings that are suitable for connecting a switch port to a standard desktop, use the **macro apply cisco-desktop** command.

macro apply cisco-desktop *$AVID access_vlanid*

Syntax Description	**$AVID** *access_vlanid* Specifies an access VLAN ID.
Defaults	This command has no default settings.
Command Modes	Interface configuration mode
Usage Guidelines	This command can only be viewed and applied; it cannot be modified. Ensure that the existing configuration on the interface does not conflict with the intended macro configuration. Before you apply the macro, clear the configuration on the interface with the **default interface** command.

Examples	This example shows how to enable the Cisco-recommended features and settings on port fa2/1:
	`Switch(config)# interface FastEthernet2/1`
	`Switch(config-if)# **macro apply cisco-desktop $AVID 50**`
	`Switch(config-if)#`
	
	The contents of this macro are as follows:
	`# Basic interface - Enable data VLAN only`
	`# Recommended value for access vlan (AVID) should not be 1`
	`switchport access vlan $AVID [access_vlanid]`
	`switchport mode access`
	`# Enable port security limiting port to a single`
	`# MAC address - -that of desktop`
	`switchport port-security`
	`# Ensure port-security age is greater than one minute`
	`# and use inactivity timer`
	`switchport port-security aging time 2`
	`# Shut up in the config`
	`switchport port-security violation restrict`
	`switchport port-security aging inactivity`
	`switchport port-security aging type inactivity`
	`# Configure port as an edge network port`
	`spanning-tree portfast`
	`spanning-tree bpduguard enable`

Related Commands	Command	Description
	macro apply cisco-phone	Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a standard desktop and a Cisco IP phone.
	macro apply cisco-router	Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a router.
	macro apply cisco-switch	Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to another switch.

macro apply cisco-phone

To enable the Cisco-recommended features and settings that are suitable for connecting a switch port to a standard desktop and a Cisco IP phone, use the **macro apply cisco-phone** command.

macro apply cisco-phone SWID *access_vlanid* **DVID** *voice_vlanid*

Syntax Description	**SWID** *access_vlanid* Specifies an access VLAN ID. **DVID** *voice_vlanid* Specifies a voice VLAN ID.
Defaults	This command has no default settings.
Command Modes	Interface configuration mode
Usage Guidelines	This command can only be viewed and applied; it cannot be modified. Ensure that the existing configuration on the interface does not conflict with the intended macro configuration. Before you apply the macro, clear the configuration on the interface with the **default interface** command.

Examples	This example shows how to enable the Cisco-recommended features and settings on port fa2/1:
	
	`Switch(config)# interface fastethernet2/1`
	`Switch(config-if)# macro apply cisco-phone SWID 10 DVID 50`
	`Switch(config-if)#`
	
	The contents of this macro are as follows:
	
	`# VoIP enabled interface - Enable data VLAN`
	`# add voice VLAN`
	`switchport access vlan $DVID (access vlan $DVID should not be 1)`
	`switchport access vlan $SWID [access_vlan_id]`
	`switchport mode access`
	`switchport voice vlan $DVID (DVID value which should be`
	`# different from data VLAN`
	`# Recommended value for voice vlan (DVID) should not be 1`
	`switchport port-security maximum 2`
	`# Enable port security limiting port to a 2 MAC`
	`# addresses -- One for desktop and two for phone`
	`switchport port-security`
	`switchport port-security aging time 2`
	`# Enable port-security age to greater than one minute`
	`# and use inactivity timer`
	`switchport port-security violation restrict`
	`# Make violating packets get dropped`
	`switchport port-security aging type inactivity`
	`# Enable auto-qos to extend trust to attached Cisco phone`
	`mls qos trust device cisco-phone`
	`# Configure port as an edge network port`
	`spanning-tree portfast`
	`spanning-tree bpduguard enable`

Related Commands	Command	Description
	macro apply cisco-desktop	Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a standard desktop.
	macro apply cisco-router	Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a router.
	macro apply cisco-switch	Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to another switch.

macro apply cisco-router

To enable the Cisco-recommended features and settings that are suitable for connecting a switch port to a router, use the **macro apply cisco-router** command.

macro apply cisco-router SNVID *native_vlanid*

Syntax Description	**SNVID** *native_vlanid* Specifies a native VLAN ID.
Defaults	This command has no default settings.
Command Modes	Interface configuration mode
Usage Guidelines	This command can only be viewed and applied; it cannot be modified. Ensure that the existing configuration on the interface does not conflict with the intended macro configuration. Before entering the **macro apply cisco-router** command, clear the configuration on the interface with the **default interface** command.

Examples	This example shows how to enable the Cisco-recommended features and settings on port fa2/1:
	`Switch(config)# interface FastEthernet2/1`
	`Switch(config-if)# **macro apply cisco-router SNVID 80**`
	`Switch(config-if)#`
	
	The contents of this macro are as follows:
	`# Access Uplink to Distribution`
	`# Enable port security globally and on this port`
	`# Define unique Native VLAN on trunk ports`
	`# Recommended value for native vlan (NOTE: should not be 1)`
	`switchport trunk native vlan $native_vlan_id$`
	`# Update the allowed VLAN list to VLANs that exist in`
	`# management domain, voice and data VLANs`
	`# switchport trunk allowed vlan DVLANAME$[vlan_range]`
	`# Hardcode trunk and disable negotiation to`
	`# speed up convergence`
	`# Hardcode speed and duplex to router`
	`switchport mode trunk`
	`switchport nonegotiate`
	`speed 100`
	`duplex full`
	`# Configure qos to trust this interface`
	`auto qos voip trust`
	`qos trust dscp`
	`# Ensure fast access to the network when enabling the interface.`
	`# Ensure that switch devices cannot harass servers on the interface.`
	`spanning-tree portfast`
	`spanning-tree bpdugaard enable`

Related Commands	Command	Description
	macro apply cisco-desktop	Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a standard desktop.
	macro apply cisco-phone	Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a standard desktop and a Cisco IP phone.
	macro apply cisco-router	Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a router.
	macro apply cisco-switch	Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to another switch.

macro apply cisco-switch

To enable the Cisco-recommended features and settings that are suitable for connecting a switch port to another switch, use the **macro apply cisco-switch** command.

macro apply cisco-switch SSVID *native_vlanid*

Syntax Description	**SSVID** *native_vlanid* Specifies a native VLAN ID.
Defaults	This command has no default settings.
Command Modes	Interface configuration mode
Usage Guidelines	This command can only be viewed and applied; it cannot be modified. Ensure that the existing configuration on the interface does not conflict with the intended macro configuration. Before you apply this macro, clear the configuration on the interface with the **default interface** command.

Examples	This example shows how to enable the Cisco-recommended features and settings on port fa2/1:
	`Switch>enable Password:****`
	`Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z.`
	`Switch(config)# **macro apply cisco-switch SSVID 40**`
	`Switch(config-if)#`

The contents of this macro are as follows:

```
# Access Uplink to Distribution
# Enable port security globally
# Define unique Native VLAN on trunk ports
# Recommended value for native vlan (SSVID) should not be 1
switchport trunk native vlan $SSVID$ # native_vlan_id
# Update the allowed vlan range appropriately to meet their in
switchport trunk, voice and native VlAN
# switchport trunk allowed vlan ZZLAN$$
# Hardcode trunk and disable negotiation to
# speed up convergence
switchport mode trunk
switchport nonegotiate
# Port security feature on this interface
ssm qos vlq trust
# EOC.hr defines the link as pt-pt for rapid convergence
spanning-tree link-type point-to-point
```

Related Commands	Command	Description
	macro apply cisco-desktop	Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a standard desktop.
	macro apply cisco-phone	Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a standard desktop and a Cisco IP phone.
	macro apply cisco-router	Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a router.

macro auto device

Use the **macro auto device** command to simplify changing the parameters for a built-in function for a *device type*. Use the **no** form of this command to revert to the initial parameter values.

macro auto device *device_type* [*parameter value*]

no macro auto device *device_type* [*parameter value*]

Syntax Description	*device_type* Specifies the device type. • **phone**—Apply interface configs on detecting a phone • **switch**—Apply interface configs on detecting a switch • **router**—Apply interface configs on detecting a router • **ap**—Apply interface configs on detecting an ap • **bmp**—Apply interface configs on detecting a light weight ap • **dmp**—Apply interface configs on detecting a DMP • **ipvsc**—Apply interface configs on detecting a IPVSC
	parameter value (Optional) parameter=value—Replace default values that begin with it. Enter new values in the form of name value pair separated by a space (parameter1=value1 <space> parameter2=value2 <space>...). Default values are shown in parenthesis.

Command Modes Global configuration

Usage Guidelines Although you can use the **macro auto execute** command to produce the same effect as the **macro auto device** command, the latter is simpler.

Examples This example shows how to change the access VLAN and voice VLAN from their default value to user defined values for phone devices.

```
Switch(config)# macro auto device phone ACCESS_VLAN=45 VOICE_VLAN=20
```

Related Commands

Command	Description
macro auto execute (built-in function)	Enables a built-in function for a device, collects its environmental variables, assigns its parameters, and runs the parameterized macro.
macro auto execute (remotely-defined trigger)	Enables a remotely-defined trigger, collects its environmental variables, assigns its parameters, and runs the parameterized macro.
macro auto execute (user-defined function)	Enables a user-defined function, collects its environmental variables, assigns its parameters, and runs the parameterized macro.
macro auto global processing	Enables Auto Smartports on a switch.
macro auto processing	Enables Auto Smartports macros on a port-by-port basis.

Command	Description
show ip source binding	Displays static and dynamic entries from the IP source binding table.
show ip verify source	Displays the IP source guard configuration on interfaces.
shutdown vlan	Disables access and trunk traffic on specified VLANs.

macro auto execute (built-in function)

Use the **macro auto execute** configuration command to change built-in function default values or to map user-defined triggers to built-in functions and to pass the parameter values. Use the **no** form of this command to unmap the trigger.

macro auto execute *event_trigger* **builtin** *built_function* [*param name=value*]

no macro auto execute *event_trigger* **builtin***built_function* [*param name=value*]

Syntax Description	*event_trigger* Defines mapping from an event trigger to a built-in macro. Specify an *event trigger*: • CISCO_PHONE_EVENT • CISCO_SWITCH_EVENT • CISCO_ROUTER_EVENT • CISCO_WIRELESS_AP_EVENT • CISCO_WIRELESS_LIGHTWEIGHT_AP_EVENT • CISCO_DMP_EVENT • CISCO_IPVSC_EVENT • WOMD—Apply a user-defined event trigger.
	built_function Specifies a built-in macro name: • CISCO_PHONE_AUTO_SMARTPORT (Optional) Specify the parameter values: $ACCESS_VLAN=[1] and $VOICE_VLAN=[2]. • CISCO_SWITCH_AUTO_SMARTPORT (Optional) Specify the parameter values: $NATIVE_VLAN=[1]. • CISCO_ROUTER_AUTO_SMARTPORT (Optional) Specify the parameter values: $NATIVE_VLAN=[1]. • CISCO_AP_AUTO_SMARTPORT (Optional) Specify the parameter values: $NATIVE_VLAN=[1]. • CISCO_LWAP_AUTO_SMARTPORT (Optional) Specify the parameter values: $ACCESS_VLAN=[1]. • CISCO_DMP_AUTO_SMARTPORT • CISCO_IP_CAMERA_AUTO_SMARTPORT
	parameters=value [value2] (Optional) Specifies values for the parameters that are to be used in the function body.

Defaults Auto Smartports is disabled.

Command Modes Global configuration

Usage Guidelines

The switch automatically maps from built-in event triggers to built-in functions. The built-in functions are system-defined functions in the software image.

Use the **macro auto execute** global configuration command to replace the built-in function default values with values specific to your switch.

You can also create user-defined triggers and use this command to map the trigger to built-in functions.

You can create user-defined event triggers by entering the **built-trigger** global configuration command. Use the **show shell** privileged EXEC command to display the contents of the built-in and user-defined triggers and functions.

Examples

This example shows how to create two built-in macros for Smartports macros for connecting Cisco switches and Cisco IP phones to the switch. It modifies the default voice VLAN, access VLAN, and native VLAN for the trunk interface:

```
Switch# configure terminal
Switch(config)#[1] the next command modifies the access and voice vlan
Switch(config)#[2] macro auto execute AccessPort BUILTIN CISCO_PHONE_EVENT
Switch(config)#[3] macro auto execute CISCO_PHONE_EVENT built-in CISCO_PHONE_APPL_MODIFYAUDIO
AccESS_VLAN=10 VOICE_VLAN=20
Switch(config)#[4] exit
Switch(config)#[5] the next command modifies the native vlan
Switch(config)#[6] for the built-in switch auto smartport macro
Switch(config)#[7] macro auto execute mpSwitchport BUILTIN CISCO_SWITCH_APPL_SMARTPORT
NATIVE_VLAN=10
Switch(config)#[8] the next example creates a user-defined trigger and maps it to a
built-in function
Switch(config)#[9] built trigger mpSwitchport "sec=SmartPort"
Switch(config)#[10] macro auto execute mpSwitchport BUILTIN CISCO_SWITCH_APPL_SMARTPORT_ACCESSVLAN
vlan=vlan
Switch(config)#[11] the next command enables auto smart ports globally
Switch(config)#[12] macro auto global processing fallback CDP

Switch#[13] here's the running configuration of the interface connected
Switch#[14] to another Cisco Switch after the Macro is applied
Switch#[15] show
Switch#[16] show running-config interface gi1/0/1
Building configuration...

Current configuration : 1284 bytes

!
interface GigabitEthernet1/0/1
switchport trunk encapsulation dot1q
switchport trunk native vlan 10
switchport mode trust
switchport voice vlan vlan 10 40 20
queue-set 2
priority-queue out
mls qos trust cos
auto qos voip trust
macro description CISCO_SWITCH_EVENT
end
```

Related Commands	Command	Description
	macro auto device	Globally enables macros for automatic device detection on a switch port.
	macro auto execute (remotely-defined trigger)	Maps a trigger to a remotely-defined macro name.
	macro auto execute (user-defined function)	Maps a trigger to a user-defined function.
	macro auto global processing	Globally enables Auto Smartports on a switch.
	macro auto processing	Enables Auto Smartports macros on a switch port.
	macro auto sticky	Specifies not to remove configuration applied by Auto Smartports macros when macros unmatch.
	shell trigger	Creates a new shell trigger.

macro auto execute (remotely-defined trigger)

Use the **macro auto execute** configuration command to map a trigger to a remotely defined function. Use the **no** form of this command to unmap the trigger.

macro auto execute *trigger_name* **remote** *url*

no macro auto execute *trigger_name* **remote** *url*

trigger_name	Specifies the trigger name
url	Specifies the remotely-defined URL

Syntax Description

Defaults

None

Command Modes

Global configuration

Usage Guidelines

This command enables you to store shell functions in a central location and utilized by ASP on many switches. This alleviates the problem of updating functions on every switch for each modification.

Triggering of the remotely defined function requires network connectivity to the URL, which is accessed for each execution of the function.

Examples

This example shows how to map a trigger to the remotely defined function **myfunction** – the filename that contains the function body.

```
Switch(config)# macro auto execute myvlrtigger remote http://dlan.foflgbnm/myfunction
```

Related Commands

Command	Description
macro auto device	Enables macros for devices the monitoring for a built-in function for a Phone type.
macro auto execute (built-in function)	Changes built-in function default values or to define a different trigger to built-in function, and to pass the parameter values.
macro auto execute (user-defined function)	Maps a trigger to a user-defined function.
macro auto global processing	Enables Auto Smartports on a switch.
macro auto processing	Enables Auto Smartports macros on specific interfaces.
macro auto sticky	Specifies sticky Auto Smartports macros applied by ASP across link-down and link-up events.
shell trigger	Creates a user-defined trigger.

macro auto execute (user-defined function)

Use the **macro auto execute** configuration command to map a trigger to a user-defined function. Use the **no** form of this command to unmap the trigger.

macro auto execute *trigger_name* [*param_name*=*value*] [*function body*]

no macro auto execute *trigger_name* [*param_name*=*value*]

Syntax Description	*trigger_name*	Specifies the trigger name.
	param_name=*value*	(Optional) Specifies values for the parameters that are to be used in the function body.
	function_body	Shell functions with CLIs.

Defaults None

Command Modes Global configuration

Usage Guidelines Because the function defined in this command does not have a name, you cannot use it to map to another trigger. This is the only way that you can map a trigger to a user-defined function. Shell functions defined in the non-configure mode can not be used to map triggers.

Examples This example shows how to map the user-defined event trigger **Cisco-Digital Media Player** (DMP) to a user-defined macro.

a. Connect the DMP to an 802.1x or MAB-enabled switch port.

b. On the RADIUS server, set the attribute-value pair to **auto-smart-port**=*CISCO_DMP_EVENT*.

c. On the switch, create the event trigger *CISCO_DMP_EVENT*, and enter the user-defined macro commands.

d. The switch recognizes the attribute-value pair=*CISCO_DMP_EVENT* response from the RADIUS server and applies the macro associated with this event trigger.

```
Switch(config)# macro trigger CISCO_DMP_EVENT class-map DMP player
Switch(config)# macro auto execute CISCO_DMP_EVENT [
if [[ $LINKUP -eq YES ]]; then
conf t
interface $LINKPORT#
 macro description $TRIGGER#
 switchport access vlan 5
 switchport mode access
 switchport port-security
 switchport port-security maximum 1
 switchport port-security violation restrict
 switchport port-security aging time 2
 switchport port-security aging type inactivity
 spanning-tree portfast
 spanning-tree bpdufilter
```

```
        exit
}
d1
if [ $LINKUP -eq 0 ]; then
read a
interface $INTERFACE
    no macro description STATIC200
    no switchport access vlan 1
    if [ $AUDM_MAXLAN -eq 0 ]; then
    no switchport mode access
    fi
    no switchport port-security
    no switchport port-security maximum 1
    no switchport port-security violation restrict
    no switchport port-security aging time 2
    no switchport port-security aging type inactivity
    no switchport port-security
    no spanning-tree bpduguard enable
    exit
d1
}
Switch(config)# end
```

Related Commands	Command	Description
	macro auto device	Enables/disables the generation by default of macros for a device class.
	macro auto execute (built-in function)	Configure built-in functions (default values or no macro or default macro) to run when a link-up event occurs.
	macro auto execute (remote-defined-image)	Maps a trigger to a remote-defined function.
	macro auto global processing	Enables Auto Smartports on a switch.
	macro auto processing	Enables Auto Smartports macros on a specific interface.
	macro auto sticky	Specifies not to remove configurations applied by AAA access-lists, VLAN and device changes.
	show trigger	Displays macro and definitions.

macro auto global processing

Use the **macro auto global processing** global configuration command to enable Auto SmartPorts macros on the switch. Use the **no** form of this command to disable Auto SmartPorts (ASP) macros globally.

macro auto global processing [**cdp** | **lldp**]

no macro auto global processing [**cdp** | **lldp**]

Note Starting with Release 15.0(2)SG, the **lldp** keyword is not supported.

Syntax Description

cdp	Selects CDP as fallback mode.
lldp	Selects LLDP as fallback mode.

Defaults

Auto Smartports is disabled.

Command Modes

Global configuration

Usage Guidelines

Use the **macro auto global processing** global configuration command to globally enable Auto Smartports macros on the switch. To disable ASP macros on a specific port, use the **no macro auto processing** command in the interface mode before ASP is enabled globally.

Auto Smartports macros dynamically configure ports based on the device type detected on the port. When the switch detects a new device on a port it applies the appropriate ASP macro. When a link-down event occurs on a port, the switch removes the macros. For example, when you connect a Cisco IP phone to a port, ASP automatically applies the IP phone macro. The IP phone macro enables quality of service (QoS), security features, and a dedicated voice VLAN to ensure proper treatment of delay-sensitive voice traffic.

ASP uses event triggers to map devices to macros. The most common event triggers are based on Cisco Discovery Protocol (CDP) messages received from connected devices. The detection of a device results in CDP event trigger. Cisco IP phone, Cisco wireless access point, Cisco switch, or Cisco router. Other event triggers are MAC authentication bypass (MAB) and 802.1X authentication messages.

Use CDP if port authentication is enabled and the RADIUS server does not send an event trigger.

Select LLDP to apply auto configuration if authentication fails.

If authentication is enabled on a port, a switch ignores CDP and LLDP messages unless the **cdp** keyword is enabled.

When using 802.1X or MAB authentication, configure the RADIUS server to support the Cisco attribute-value (AV) pair **auto-smart-port** event trigger.

When CDP-identified devices advertise multiple capabilities, a switch chooses a capability in this priority order: switch, router, access point, lightweight access point, phone, host.

To verify that an ASP macro is applied to an interface, use the **show running-config** command.

The **macro auto global processing** and **macro auto global processing http** commands enables ASP globally if it is not already enabled, and set the fallback to CDP or LLDP, respectively. However, the **no macro auto global processing [{ip | http}]** command only removes the fallback mechanism. It does not disable ASP globally, only the **no macro auto global processing** command disables ASP globally.

The keywords **cdp** and **lldp** are also controlled at the interface level; by default, CDP is the fallback mechanism on interfaces. If you prefer LLDP, use the **macro auto processing** command, or use the **macro auto processing lldp** command.

If you want to activate both CDP and LLDP, you must enable them in sequence. For example, you would first enter the **macro auto processing cdp** command, then the **macro auto processing lldp** command.

Examples

This example shows how enable ASP on a switch and to disable the feature on Gi1/0/1:

```
Switch(config)# interface interface Gi1/0/1
Switch(config-if)# no macro auto processing
Switch(config)# no macro auto global processing
```

Related Commands

Command	Description
macro auto device	Enables ASP macros for a specific device type or disables ASP macros for a device type.
macro auto execute (built-in function)	Changes fallback function (if) for a macro or its mapping of built-in functions, and to pass the parameters values.
macro auto execute (remotely-defined trigger)	Maps a trigger to a remotely-defined macro.
macro auto execute (user-defined function)	Maps a trigger to a user-defined function.
macro auto processing	Enables ASP macros on a specific interface.
macro auto sticky	Enables a user to set remote configuration applied by ASP macros for both sticky and device removal.
shell trigger	Creates a user-defined trigger.

macro auto mac-address-group

Use the **macro auto mac-address-group** command to configure a group of MAC-address or OUIs as a trigger. Use the **no** form of this command to unconfigure the group.

macro auto mac-address-group *grp_name*

no macro auto mac-address-group *grp_name*

Syntax Description	*grp_name* Specifies the group name.
Command Modes	Global configuration
Usage Guidelines	This command changes the mode to config-mac-addr-grp, in which you can add or remove a MAC address or OUI from the group. You can specify a list of MACs or OUIs, or a range of OUIs (maximum of 5 in the range).

Examples	This example shows how to configure **testGroup** as a trigger:
	`Switch(config)# macro auto mac-address-group testGroup`
	`Switch(config-addr-grp-macro)# mac-address list 1111.1111.1111 2222.2222.2222`
	`Switch(config-addr-grp-macro)# exit`
	`Switch(config)#`

Related Commands	Command	Description
	macro auto monitor (built-in function)	Enables built-in function macros to monitor port status, port usage, port built-in trigger and port the monitor mode.
	macro auto execute (remotely-defined trigger)	Maps a trigger to a remotely-defined function.
	macro auto execute (locally-defined trigger)	Maps a trigger to a locally-defined function.
	macro auto system-mac	Enables Auto Smartports on a switch.
	macro auto global processing	Enables Auto Smartports macros on a switch.
	macro auto processing	Enables Auto Smartports macros on specific interfaces.
	macro auto sticky	Specifies not to remove configuration added by ASP macros, but keep the device attached.
	shell trigger	Creates a new shell trigger.

macro auto monitor

To enable the device classifier, use the **macro auto monitor** global configuration command. Use the **no** form of this command to disable the device classifier.

```
macro auto monitor

no macro auto monitor
```

Syntax Description This command has no arguments or keywords.

Command Default Device classifier is enabled.

Command Modes Global configuration

Usage Guidelines Use the **no macro auto monitor** global configuration command to disable the device classifier. You cannot disable the device classifier while it is being used by features such as ASP.

Examples This example shows how to enable the ASP device classifier on a switch:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# no macro auto monitor
Switch(config)# end
```

Related Commands

Command	Description
show macro auto monitor clients	Displays the clients using the device classifier facility on the switch.
show macro auto monitor device	Displays the devices connected to a switch, along with their properties and classifications.
show macro auto monitor type	Displays all the device types known to the device classification agent.

macro auto processing

Note Only use this command when Auto SmartPorts (ASP) is enabled globally, when ASP is disabled globally, interface-level control has no effect.

Use the **macro auto processing** interface configuration command to enable ASP macros on a specific interface. Use the **no** form of this command to disable ASP on a specific interface before ASP is enabled globally.

macro auto processing [fallback cdp] [fallback lldp]

no macro auto processing [fallback cdp] [fallback lldp]

Syntax Description	fallback cdp — Specifies as CDP as the fallback mechanism. fallback lldp — Specifies as LLDP as the fallback mechanism.
Defaults	fallback mechanism is CDP.
Command Modes	Interface level configuration

Usage Guidelines

The **no macro auto processing** command should be configured on all interfaces where ASP is not desirable (such as Layer 3 and EtherChannel interfaces) before ASP is enabled globally.

At the interface level, the default fallback mechanism is CDP. To change the mechanism to LLDP, enter the **no macro auto processing fallback cdp** command, followed by the **macro auto processing fallback lldp** command.

Examples

This example shows how to enable the feature on an interface:

```
Switch(config)# interface gi1/1
Switch(config-if)# macro auto processing
```

Related Commands

Command	Description
macro auto macam [built-in function]	Configures mapping from an event trigger to a built-in macro.
shell trigger	Creates a user defined trigger.
show shell functions	Displays configuration commands for all the built-in functions including user created and built-in functions.
show shell triggers	Displays detail for all supported user created and built-in triggers.
macro auto macam [built-in function]	Changes built-in function default values or re-map user defined triggers to built-in functions, and to pass the parameter values.

Command	Description
macro auto execute (remotely-defined trigger)	Maps a trigger to a remotely-defined functions.
macro auto execute (user-defined function)	Maps a trigger to a user-defined function.
macro auto global processing	Enables Auto Smartports on a switch.

macro auto sticky

Use the **macro auto sticky** configuration to specify not to remove configurations applied by ASP across link flaps and device reboot.

macro auto sticky

Syntax Description	This command has no arguments or keywords.
Defaults	Not sticky (macros are removed)
Command Modes	Global configuration
Usage Guidelines	This command enables you to avoid unnecessary removal of ASP configuration when a feature unnecessarily shuts down a link (like EnergyWise), which shuts down interface links to save energy. When such a feature is enabled, you don't want ASP macros to be applied and removed unnecessarily. So you configure the sticky feature.
Examples	This example shows how to specify not to remove configurations: `Switch(config)# macro auto sticky`
Related Commands	

Command	Description
macro auto execute (built-in function)	Adds a built-in macro to an interface or to a port or port-channel interface. Assigns a built-in function, and an optional parameter string.
macro auto execute (remotely-defined trigger)	Adds a trigger to a remotely-defined trigger.
macro auto execute (user-defined function)	Adds a trigger to a user-defined function.
macro auto global processing	Enables Auto Smartports on a switch.
macro auto processing	Enables Auto Smartports macros on a port or port-channel.
shell trigger	Creates a user-defined trigger.

macro global apply cisco-global

To apply the system-defined default template to the switch, use the **macro global apply cisco-global** global configuration command on the switch stack or on a standalone switch.

macro global apply cisco-global

Syntax Description This command has no keywords or variables.

Defaults This command has no default setting.

Command Modes Global configuration mode

Examples These examples show how to apply the system-defined default to the switch:

```
Switch(config)# macro global apply cisco-global
Switch(config)# macro name Cisco-global-default
Switch(config)#
```

macro global apply system-cpp

To apply the control plane policing default template to the switch, use the **macro global apply system-cpp** global configuration command on the switch stack or on a standalone switch.

macro global apply system-cpp

Syntax Description This command has no keywords or variables.

Defaults This command has no default setting.

Command Modes Global configuration mode

Examples This example shows how to apply the system-defined default to the switch:

```
Switch (config)# macro global apply system-cpp
Switch (config)#
```

Related Commands

Command	Description
macro global apply cisco-global	Applies the system-defined default template to the switch.
macro global description	Enters a description about the macros that are applied to the switch.

macro global description

To enter a description about the macros that are applied to the switch, use the **macro global description** global configuration command on the switch stack or on a standalone switch. Use the **no** form of this command to remove the description.

macro global description *text*

no macro global description *text*

Syntax Description	*text* Enters a description about the macros that are applied to the switch.
Defaults	This command has no default setting.
Command Modes	Global configuration mode
Usage Guidelines	This command associates continent 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.
Examples	This example shows how to add a description to a switch: `Switch(config)# macro global description wild aggressive mode enabled` You can verify your settings by entering the **show parser macro description** privileged EXEC command.
Related Commands	**Command** / **Description** **macro global apply** / Applies the system-defined/default template to the switch.

main-cpu

To enter the main CPU submode and manually synchronize the configurations on the two supervisor engines, use the **main-cpu** command.

```
main-cpu
```

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Redundancy mode

Usage Guidelines The main CPU submode is used to manually synchronize the configurations on the two supervisor engines. From the main CPU submode, use the **auto-sync** command to enable automatic synchronization of the configuration files in NVRAM.

Note Allow you enter the main CPU submode, you can use the **auto-sync** command to automatically synchronize the configuration between the primary and secondary route-processor based on the primary configuration. In addition, you can use *all* the redundancy commands that are applicable to the main CPU.

Examples This example shows how to enable the default automatic synchronization feature using the auto-sync standard command to synchronize the running-config and config-register configuration of the active supervisor engine with the standby supervisor engine. The updates for the boot variables are automatic and cannot be disabled.

```
Switch(config)# redundancy
Switch(config-red)# main-cpu
Switch(config-r-mc)# auto-sync standard
Switch(config-r-mc)# exit
Switch(config)# copy running-config startup-config
Switch#
```

Related Commands

Command	Description
auto-sync	Enables automatic synchronization of the configuration files in NVRAM.

match

To specify a match clause by selecting one or more ACLs for a VLAN access-map sequence, use the **match** subcommand. To remove the match clause, use the **no** form of this command.

match {ip address {*acl-number* | *acl-name*} | **[mac address** *acl-name*]

no match {ip address {*acl-number* | *acl-name*} | **[mac address** *acl-name*]

Note If a match clause is not specified, the action for the VLAN access-map sequence is applied to all packets. All packets are matched against the sequence in the access-map.

Syntax Description	**ip address** *acl-number* Selects one or more IP ACLs for a VLAN access-map sequence; valid values are from 1 to 199 and from 1300 to 2699.
	ip address *acl-name* Selects an IP ACL by name.
	mac address *acl-name* Selects one or more MAC ACLs for a VLAN access-map sequence.
Defaults	This command has no default settings.
Command Modes	VLAN access-map mode

Usage Guidelines

The match clause specifies the IP or MAC ACL for traffic filtering.

The MAC sequence is not effective for IP packets. IP packets should be access controlled by IP match clauses.

Refer to the *Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide* for additional configuration guidelines and restrictions.

Refer to the *Cisco IOS Command Reference* publication for additional **match** command information.

Examples

This example shows how to define a match clause for a VLAN access map:

```
Switch(config)# vlan access-map genaccess 10
Switch(config-access-map)# match ip address 13
Switch(config-access-map)#
```

Related Commands	Command	Description
	show vlan access-map	Displays the contents of a VLAN access map.
	vlan access-map	Enters VLAN access-map command mode to create a VLAN access map.

match (class-map configuration)

To define the match criteria for a class map, use the **match** class-map configuration command. To remove the match criteria, use the **no** form of this command.

match {**access-group** *acl-index-or-name* | **cos** *cos-list* | [**ip**] **dscp** *dscp-list* | [**ip**] **precedence** *ip-precedence-list* | **qos-group** *value* | **protocol** [**ip** | **ipv6**] | **vlan** *vlan-id*}

no match {**access-group** *acl-index-or-name* | **cos** *cos-list* | [**ip**] **dscp** *dscp-list* | [**ip**] **precedence** *ip-precedence-list* | **qos-group** *value* | **protocol** [**ip** | **ipv6**] | **vlan** *vlan-id*}

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.
	cos *cos-list*	Lists up to four Layer 2 class of service (CoS) values to match against a packet. Separate each value with a space. The range is 0 to 7.
	[**ip**] **dscp** *dscp-list*	(Optional) IP keyword. It specifies that the match is for IPv4 packets only. If not used, the match is for both IPv4 and IPv6 packets. Lists up to eight IP Differentiated Services Code Point (DSCP) values to match against a packet. 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*	(Optional) IP keyword. It specifies that the match is for IPv4 packets only. If not used, the match is for both IPv4 and IPv6 packets. Lists up to eight IP precedence values to match against a packet. Separate each value with a space. The range is 0 to 7. You also can enter a mnemonic name for a commonly used value.
	qos-group *value*	Specifies the internally generated qos-group value assigned to a packet on the input qos classification.
	protocol ip	Specifies IPv4 the Ethernet header. Though visible in the command-line help strings, the only protocol types supported are IP, IPv4, and ARP.
	protocol ipv6	Specifies IPv6 in the Ethernet header. Though visible in the command-line help strings the only protocol types supported are IP, IPv6, and ARP.
	protocol arp	Specifies ARP in the Ethernet header. Though visible in the command-line help strings the only protocol types supported are IP, IPv6, and ARP.

Defaults No match criteria are defined.

Command Modes Class-map configuration mode

Usage Guidelines

Before entering the **match** command, you must first enter the **class-map** global configuration command to specify the name of the class whose match criteria you want to modify. The **match** command is used to specify which fields in the packets are examined to classify the packets. If a packet matches the specified criteria, the packet is considered a member of the class and is forwarded according to the quality of service (QoS) specifications set in the traffic policy.

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 equivalent to entering the **match ip dscp 10** command. You can enter the **match ip precedence critical** command, which is equivalent to entering the **match ip precedence 5** command. For a list of supported mnemonics, enter the **match ip dscp ?** or the **match ip precedence ?** command in the command-line help strings.

To match only IPv6 packets, you must use the **match protocol ipv6** command. To match only IPv4 packets you can either specify the protocol or the protocol keyword.

To match only ARP packets, you must use the **match protocol arp** command.

You can configure the **match tcp** or **udp**, **match ip dscp** *dscp-list*, **match ip precedence** *ip-precedence-list* commands in a class map within a policy map.

The **match** *cos*, *dei* or *dei-cos* command applies only to Ethernet frames that carry a VLAN tag.

The **match qos-group** command is used by the class-map to identify a specific QoS group value assigned to a packet. The QoS group value is local to the switch and is associated with a packet on the input Qos classification.

Packets that do not meet any of the matching criteria are classified as members of the default traffic class. You configure it by specifying **class-default** as the class name in the **class** policy-map configuration command. For more information, see the "class" section on page 2-84.

Examples

This example shows how to create a class map called *class1*, which matches all the inbound traffic with DSCP values of 10, 11, and 12:

```
Switch# configure terminal
Switch(config)# class-map class1
Switch(config-cmap)# match ip dscp 10 11 12
Switch(config-cmap)# exit
Switch#
```

This example shows how to create a class map called *class1*, which matches all the inbound traffic with IP-precedence values of 5, 6, and 7 for both IPv4 and IPv6 traffic:

```
Switch# configure terminal
Switch(config)# class-map class1
Switch(config-cmap)# match ip precedence 5 6 7
Switch(config-cmap)# exit
Switch#
```

This example shows how to delete the IP-precedence match criteria and to classify traffic using *acl1*:

```
Switch# configure terminal
Switch(config)# class-map class1
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
Switch#
```

This example shows how to specify a class-map that applies only to IPv6 traffic on a Supervisor Engine 6-E:

```
Switch(config)# conf t
Switch(config)# class-map match-all ipv6 only
Switch(config-cmap)# match dscp af11
Switch(config-cmap)# match protocol ipv6
Switch(config-cmap)# exit
Switch(config)#
```

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 and to enter class-map configuration mode.
	show class-map	Displays class map information.

match flow ip

To specify match criteria to treat flows with a unique source or destination address as new flows, use the **match flow ip** command. To disable this function, use the **no** form of this command.

match flow ip {source-address | ip-destination-address | ip-protocol | l4 source-address | l4 destination-address} [destination-address]

no match flow ip {source-address | ip-destination-address | ip-protocol | l4 source-address | l4 destination-address} [destination-address]

Syntax Description	**source-address** Establishes a new flow from a flow with a unique IP source address. **ip destination-address** (Optional) Comprises the full flow keyword; treats each flow with unique IP source, destination, protocol, and Layer 4 source and destination address as a new flow. **ip-protocol** **l4 source-address** **l4 destination-address** **destination-address** Establishes a new flow from a flow with a unique IP destination address.
Defaults	This command has no default settings.
Command Modes	class-map configuration submode

Usage Guidelines

When you specify the source-address keyword, each flow with a unique source address is treated as a new flow.

When you specify the destination-address keyword, each flow with a unique destination address is treated as a new flow.

A policy image's *defined-flow-based* policy map when you configure the flow keywords on the class map that it uses. In attach a flow-based policy map as a child to an aggregate policy map, use the **service-policy** command.

Note The **match flow** command is available on the Catalyst 6500 series switch only when Supervisor Engine VI (WS-SUP10-10GE) is present.

Examples

This example shows how to create a flow-based class map associated with a source address:

```
Switch(config)# class-map match-all c1
Switch(config-cmap)# match flow ip source-address
Switch(config-cmap)# end
!
Switch# show class-map c1
Class Map match-all c1 (id 2)
  Match flow ip source-address
Switch#
```

This example shows how to create a flow-based class-map associated with a destination address:

```
Switch(config)# class-map match-all v1
Switch(config-cmap)# match flow ip destination-address
Switch(config-cmap)# end
Switch#
```

```
Switch# show class-map v1
Class Map match-all v1 (id 2)
    Match flow ip destination-address
Switch#
```

Assume there are two active flows on the Fast Ethernet interface 6/1 with source addresses 192.168.1.20.20 and 192.168.10.20. The following example shows how to maximum such flow to 1 Mbps with an allowed burst value of 9600 bytes:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# class-map v1
Switch(config-cmap)# match flow ip source-address
Switch(config-cmap)# exit
Switch(config)# policy-map p1
Switch(config-pmap)# class v1
Switch(config-pmap-c)# police 1000000 9600
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet6/1
Switch(config-if)# service-policy input p1
Switch(config-if)# end
Switch# write memory
```

```
Switch# show policy-map interface
FastEthernet6/1

  Service-policy input: p1

    Class-map: v1 (match-all)
      1963140 packets
      Match: flow ip source-address
      police: Percent(0)
        Conform: 1000000 bytes Exceed: 2370596424 bytes

    Class-map: class-default (match-any)
      0 packets,
      Match: any
      0 packets
Switch#
```

This example shows two active flows on the Fast Ethernet interface 6/1 with destination addresses of 192.168.20.20 and 192.168.30.20. The following example shows how to maximum such flow to 1 Mbps with an allowed burst value of 9600 bytes:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# class-map v1
Switch(config-cmap)# match flow ip destination-address
Switch(config-cmap)# exit
Switch(config)# policy-map p1
Switch(config-pmap)# class v1
Switch(config-pmap-c)# police 1000000 9600
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet6/1
Switch(config-if)# service-policy input p1
```

```
Switch(config)#[3] end
Switch# write memory
Switch# show policy-map interface
FastEthernet4/1
  service-policy input p1

    class-map: c1 (match-all)
      2968272 packets,
      Match: flow ip destination-address
      policy: Rate-Shaping
        [snipped: 4245632 bytes Normal: 4765952 bytes

    Class-map: class-default (match-any)
      0 packets,
      Match: any
      0 packets
Switch#
```

Assume there are two active flows as shown below on the Fast Ethernet interface 4/1:

Src Ip	Dst Ip	Sprtcp	Dprtcp	Datalen
192.168.10.10	192.168.20.20	20	6789	81
192.168.10.10	192.168.20.20	20	6789	31

With the following configuration, each flow is policed to a 1000000bps with an allowed 9000-byte burst value.

Note If you use the **match flow ip source-address|destination-address** command, these two flows are consolidated into one flow because they have the same source and destination address.

```
Switch# conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#[1] class c1
Switch(config-cmap)#[2] match flow ip source-address ip destination-address ip protocol 14
source-port 14 destination-port
Switch(config-cmap)#[3] exit
Switch(config)#[4] policy-map p1
Switch(config-pmap)#[5] class c1
Switch(config-pmap-c)#[6] police 1000000 9000
Switch(config-pmap-c)#[7] exit
Switch(config-pmap)#[8] exit
Switch(config)#[9] interface FastEthernet 4/1
Switch(config-if)#[10] service-policy input p1
Switch(config-if)#[11] end
Switch# write memory
Switch# show policy-map interface
FastEthernet4/1

  class-map c1
    match flow ip source-address ip destination-address ip protocol 14 source-port 14
    destination-port
  !
  policy-map p1
    class c1
      police 1000000 bps 9000 bytes conformed-action transmit exceed-action drop
  !
  interface FastEthernet 4/1
    service-policy input p1
```

```
Switch# show class-map c1
  Class Map match-all c1 (id 2)
    Match flow ip source-address ip destination-address ip protocol 14 source-port 14
destination-port

Switch# show policy-map p1
  Policy Map p1
    Class c1
      police 1000000 bps 9000 byte conform-action transmit exceed-action drop

Switch# show policy-map interface
  FastEthernet3/1:

    Service-policy input: p1

      Class-map: c1 (match-all)
        314231292 packets
        Match: flow ip source-address ip destination-address ip protocol 14 source-port 14
destination-port
        police: Per-interface:
          Conform: 142998434 bytes Exceed: 237299424 bytes

      Class-map: class-default (match-any)
        0 packets
        Match: any
        0 packets
Switch#
```

Related Commands	Command	Description
	service-policy (interface configuration)	Attaches a policy map to an interface.
	show class-map	Displays class map information.
	show policy-map	Displays information about the policy map.
	show policy-map interface	Displays the statistics and configuration of the input and output policies that are attached to an interface.

mdix auto

To enable the automatic medium-dependent interface crossover (auto-MDIX) feature on the interface, use the **mdix auto** command. When auto-MDIX is enabled, the interface automatically detects the required cable connection type (straight-through or crossover) and configures the connection appropriately. Use the **no** form of this command to disable auto-MDIX.

mdix auto

no mdix auto

Syntax Description This command has no arguments or keywords.

Defaults Auto-MDIX is enabled.

Command Modes Interface configuration mode

Usage Guidelines The following line cards support Auto-MDIX through the CLI on their copper media ports: WS-X4124-RJ45, WS-X4148-RJ45 (hardware revision .10 or higher), and WS-X4232-GB-RJ45 (hardware revision 1.4, or higher). WS-X4165-GE-RJ45, and WS-4648-RJ45V+E (Auto-MDIX support when inline power is disabled on the port).

Line cards that support auto-MDIX by default when port auto-negotiation enabled and cannot be turned off: WS-X4148-RJ45V, WS-X4224-GB-RJ45, WS-X4148-GB-RJ45, WS-X4148-GB-RJ45V, WS-X4248-GB-RJ45, and WS-X4232-GB-RJ45.

Line cards that cannot support auto-MDIX functionality, either by default or CLI commands, include: WS-X4148-RJ45V, WS-X4224-GB-RJ45V, WS-X4235-GB-T, WS-X4148-FX, WS-X4248-RJ21V, WS-X4248-RJ45V, WS-X4224-RJ45V, and WS-X4232-GB-RJ.

When you enable auto-MDIX on an interface, you must also set the interface speed to be autonegotiated so that the feature operates correctly.

When auto-MDIX (and autonegotiation of speed) is enabled on one or both of connected interfaces, link up occurs even if the cable type (straight-through or crossover) is incorrect.

Examples This example shows how to enable auto MDIX on a port:

```
Switch(config)# interface fastethernet
Switch(config)# interface FastEthernet0/1
Switch(config-if)# speed auto
Switch(config-if)# mdix auto
Switch(config-if)# end
```

Related Commands	Command	Description
	speed	Configures the interface speed.
	show interfaces	Displays traffic on a specific interface.

Command	Description
show interfaces capabilities	Displays the interface capabilities for an interface or for all the interfaces on a switch.
show interfaces status	Displays the interface status.

media-type

To select the connector for a dual-mode capable port, use the **media-type** command.

media-type {**rj45** | **sfp**}

Syntax Description	**rj45** Uses the RJ-45 connector.
	sfp Uses the SFP connector.

Defaults	**sfp**

Command Modes	Interface configuration mode

Usage Guidelines	This command is supported on all ports on the WS-X-6406-GB-T module and ports 1-16/1-48 on the WS-X-4948 chassis.
	Entering the **show interface capabilities** command provides the Multiple Media Types field, which displays the values **rj45** if a port is not dual-mode capable and lists the media types (**sfp** and **rj45**) for dual-mode capable ports.

Examples	This example shows how to configure port 1/-16 on a WS-X-48-48 chassis to use the RJ-45 connector:

```
Switch(config)# interface gigabitethernet 1/-16
Switch(config-if)# media-type rj45
```

mode

To set the redundancy mode, use the **mode** command.

mode {**rpr** | **sso** }

Syntax Description	**rpr** Specifies RPR mode.
	sso Specifies SSO mode.

Defaults

If you are upgrading the current supervisor engine from Cisco IOS Release 12.2(18)EW or an earlier release to 12.2(18)EWA, and the RPR mode has been stored in the startup configuration, both supervisor engines will continue to operate in RPR mode after the software upgrade. To use SSO mode, you must manually change the redundancy mode to SSO.

Command Modes

Redundancy configuration mode

Usage Guidelines

RPR and SSO modes are not supported on Catalyst 4500 series switches that are configured with Supervisor Engine 2.

The **mode** command can be entered only from within redundancy configuration mode.

Follow these guidelines when configuring your system to RPR or SSO mode:

- You must use identical Cisco IOS images and supervisor engines to support RPR and SSO mode. Redundancy may not work due to differences between the Cisco IOS release and supervisor engine capabilities.
- Any module that are not online at the time of a switchover are reset and reloaded on a switchover.
- If you perform an OIR of the module within 60 seconds before a stateful switchover, the module resets during the stateful switchover and the port states are recreated.
- The FIB tables are cleared on a switchover. Routed traffic is interrupted until route tables re-converge.

The redundant supervisor engine reloads on any mode change and begins to work in the current mode.

Examples

This example shows how to set the redundancy mode to SSO:

```
Switch(config)# redundancy
Switch(config-red)# mode sso
Switch(config-red)#
```

Related Commands

Command	Description
redundancy	Enters the redundancy configuration mode.
redundancy force-switchover	Forces a switchover from the active to the standby supervisor engine.

Command	Description
show redundancy	Displays redundancy facility information.
show running-config	Displays the running configuration of a switch.

monitor capture {access-list | class-map}

To specify an access list or class map as the core filter, use the **monitor capture** {**access-list** | **class-map**} command. To remove the filter, use the **no** form of this command.

monitor capture *name* {**access-list** *name*} | {**class-map** *name*}

no monitor capture *name* {**access-list** *name*} | {**class-map** *name*}

Syntax Description	*name* Specifies a capture point. **access-list** *name* Specifies access list name **class-map** *name* Specifies class map name
Defaults	None
Command Modes	Privileged EXEC mode
Usage Guidelines	The access list or class maps defined with configuration commands. The access list or class map should be defined prior to entering the **monitor capture** command. We can specify the core filter as a class map, access list, or as an explicit in-line filter. If the filter has already been specified when you enter the **monitor capture** command, it replaces the older one.
Examples	The following example shows how to define a core system filter using an existing ACL or class-map: Switch#: **monitor capture mycap filter access-list myacl** Switch#: **monitor capture mycap filter class-map mycm** Switch#: **no monitor capture mycap filter class-map mycm**

monitor capture [clear | export]

To clear capture buffer contents or to store the packets to a file, use the **monitor capture [clear | export** *filename*] command.

monitor capture *name* [**clear** | **export** *filename*]

Syntax Description	*name* Specifies a capture point.
	clear Clears all the packets in the capture buffer.
	export *filename* Store all the packets in capture buffer in a .pcap file.

Defaults	none

Command Modes	Privileged EXEC mode

Usage Guidelines	The **clear** option empties the capture buffer and the **export** option stores the packets in the capture buffer to the file. You should use these commands only when the storage destination is a capture buffer. These commands empty the buffer during capture or when it has stopped either because one or more stop conditions has been met or you entered the **stop** command. If you enter the **clear** command after the capture has stopped, further **export** (or **decode**) and **display** commands have no impact because the buffer has no packets.

Examples	The following example shows how to associate or disassociate a capture file:

```
Switch#monitor capture mycap export bootflash:mycap.pcap
Switch#monitor capture mycap clear
```

monitor capture [interface | vlan | control-plane]

To specify one or more attachment points with direction, use the **monitor capture [interface | vlan | control-plane]** command. To remove the attachment point, use the **no** form of the command.

monitor capture *name* [[**interface** *name* | **vlan** *num* | **control-plane**] [**in** | **out** | **both**]]

no monitor capture *name* [[**interface** *name* | **vlan** *num*| **control-plane**] [**in** | **out** | **both**]]

Syntax Description:	*name* — Specifies a capture point.
	interface *name* — Specifies an interface. Interface range is allowed.
	vlan *num* — Specifies a VLAN.
	control-plane — Specifies control plane.
	input	**output**	**both** — Specific traffic direction.

Defaults: None

Command Modes: Privileged EXEC mode

Usage Guidelines: Specifies one or more attachment points with direction. We can specify a range of interfaces also. The command can be repeated as many times as needed to add multiple attachment points.

We need to mention at least one attachment point. For VLAN, the direction has to be set to both.

Examples: The following example shows how to add an attachment point:

```
Switch# monitor capture mycap interface gigabitethernet 3/1 in
```

The following example shows how to remove an attachment point:

```
Switch# no monitor capture mycap interface gigabitethernet 3/1 in
```

monitor capture file location buffer-size

To specify the capture destination, use the **monitor capture** command. To remove the details, use the **no** form of this command.

monitor capture *name* [**file location** *filename* [**buffer-size** *{1-100}*] | **ring** *{2-10}*] [**size** *{1-10}*] [[**buffer** | **circular**] **size** *{1-100}*]

[**no monitor capture** *name* [**file** | **buffer**]

Syntax Description

file location *filename*	Specifies filename of location.
buffer-size *{1-100}*	Specifies buffer size in MB.
ring *{2-10}*	Specifies number of files.
size *{1-100}*	Specifies the file size.
buffer [**circular**	**size** *{1-100}*]	Specifies that the capture destination is a buffer. By default, the mode is linear. The keyword **circular** sets the buffer mode to circular. The keyword **size** specifies the buffer size.

Defaults

The default buffer size is one MB.

Command Modes

Privileged EXEC mode

Usage Guidelines

The capture destination can be a file in storage disk or a memory buffer. This command specifies the parameters related to packet storage.

The **file** option specifies that the packets must be stored in a file. To reduce or avoid any loss in packet capture, you can use the **buffer-size** option. The capture and store operations require more CPU, limiting the capture throughput.

You can increase the throughput by using **ring** *{2-10}* mode, wherein the packets are first captured in the buffer. Within this mode, the "duration" parameter defines the capture duration. Once the buffer is full or the duration closes, the buffer is written to the file, gracefully increasing the capture throughput. The lock-step mode is automatically triggered by specifying the buffer size to 32MB or higher.

The size of the capture file can be limited with the **size** option. The file location must one of the following:

- Internal bootflash (bootflash:)
- External flash (slot0:)
- USB (usb0:)

Do not specify any other devices.

The destination file can be a ring of files rather than a single file. The **ring** option specifies the number of files in the ring whose size specifies the total size of all the files. In ring file mode, when the file size limit has reached, it accommodates space for new packets by removing the oldest file.

If the capture destination is a buffer, you must use the **show** command to decode and display the packets from the buffer. If the capture destination is a pcfile, capture continues until you explicitly issue the **stop** command. If no space exists in the buffer, oldest packet(s) are removed to accommodate the new ones. If the **circular** option is not provided, newer packets are discarded when the capture buffer is full.

Examples

The following example snapes show how to specify a file or a ring of files as the capture destination:

```
Switch# monitor capture myexp asscrlan buffer circular 1000000file location
bootflash:myexp.pcap
Switch# monitor capture myexp file location bootflash:myexp.pcap size 40
Switch# monitor capture myexp file location bootflash:myexp.pcap ring 4 size 40
Switch# monitor capture myexp file location bootflash:myexp.pcap buffer-size 4
Switch# monitor capture myexp file location bootflash:myexp.pcap ring 4 size 40
buffer-size 16
Switch# no monitor capture myexp file
```

The following example shows how to snap capture in lock-step mode:

```
Switch# monitor capture myexp file location bootflash:myexp.pcap buffer-size 64
Switch# no monitor capture myexp file
```

The following example shows how to make a circular buffer as the capture destination and operate on the buffer:

```
Switch# monitor capture myexp buffer circular size 1
Switch# monitor capture myexp interface vlan 1
Switch# monitor capture myexp start
Switch# show monitor capture myexp buffer
0.000000 10.1.1.246 > 255.1.1.2  UDP Source port: 20000  Destination port: 20000
0.000000 10.1.1.246 > 255.1.1.2  UDP Source port: 20000  Destination port: 20000
0.000000 10.1.1.246 > 255.1.1.2  UDP Source port: 20000  Destination port: 20000
0.000000 10.1.1.246 > 255.1.1.2  UDP Source port: 20000  Destination port: 20000
0.000000 10.1.1.246 > 255.1.1.2  UDP Source port: 20000  Destination port: 20000
0.000000 10.1.1.246 > 255.1.1.2  UDP Source port: 20000  Destination port: 20000
0.000000 10.1.1.246 > 255.1.1.2  UDP Source port: 20000  Destination port: 20000
0.000000 10.1.1.172 > 255.1.1.2  UDP Source port: 20000  Destination port: 20000
0.000000 10.1.1.172 > 255.1.1.2  UDP Source port: 20000  Destination port: 20000
0.000000 10.1.1.172 > 255.1.1.2  UDP Source port: 20000  Destination port: 20000
0.000000 10.1.1.172 > 255.1.1.2  UDP Source port: 20000  Destination port: 20000
0.000000 10.1.1.172 > 255.1.1.2  UDP Source port: 20000  Destination port: 20000
Switch# show monitor capture myexp buffer detailed
Packet 1 : Length: 1000 Packet type: 0x0800 (IP) Protocol: 0x11 (UDP) Priority
Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00)
    Epoch Time: 1126245142.09980000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 252 bytes (2016 bits)
    Capture Length: 252 bytes (2016 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ip:udp:data]
Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 54:78:dc:4e:95:5f
(54:78:dc:4e:95:5f)
    Destination: 54:78:dc:4e:95:5f (54:78:dc:4e:95:5f)
        Address: 54:78:dc:4e:95:5f (54:78:dc:4e:95:5f)
                 .1. .... .... .... .... .... = Ig bit: Individual address (unicast)
                 ..0. .... .... .... .... .... = LG bit: Globally unique address (factory default)
```

```
    Source: 00:00:00:00:03:01 (00:00:00:00:00:01)
        address: 00:00:00:00:03:01 (00:00:00:00:00:01)
                 ..... ..... ..... = IG bit: Individual address (unicast)
                 ..... ..... ..... = LG bit: Globally unique address (factory default)
    Type: IP (0x0800)
Switch#sh monitor session mpsp buffer dump
  0.000000   16.1.1.164 -> 20.1.1.2   UDP Source port: 20001  Destination port: 20002

0000: 54 70 00 3a 00 5f 00 00 00 03 11 d6 00 d0 d0 d0  Tp..:._........
0010: 00 ee 00 00 00 00 4d 11 99 9e ba 01 01 ae ba 01  ......M.ž.ž.....
0020: 01 02 4e 24 4e 24 00 3a 00 00 4d 6f 6e 69 74 6f  ..N$N$.:..Monito
0030: 04 07 09 09 0a 0a 0c 0c 0e 0e 10 10 12 12 14 14  ................
0040: 16 16 18 18 1a 1a 1c 1c 1e 1e 20 20 22 22 24 24  .......... ..."".$$
0050: 26 26 28 28 2a 2a 2c 2c 2e 2e 30 30 32 32 34 34  &&((**,,..00224 4
0060: 36 36 38 38 3a 3a 3c 3c 3e 3e 40 40 42 42 45 45  6688:::<<>>@@BBEE
0070: 4d 4d 50 50 53 53 56 56 59 59 5c 5c 5f 5f 62 62  MMPPSSVVYY\\__bb
0080: 52 57 58 5a 5c 5e 60 62 64 66 68 6a 6c 6e 70 72  RWXZ\^`bdfhjln pr
0090: 64 67 69 6b 6d 6f 71 73 75 77 79 7b 7d 7f 81 83  dgijkmoqsuwy{}..
00a0: 85 87 89 8b 8d 8f 91 93 95 97 99 9b 9d 9f a1 a3  ................
00b0: a5 a7 a9 ab ad af b1 b3 b5 b7 b9 bb bd bf c1 c3  ................
00c0: c5 c7 c9 cb cd cf d1 d3 d5 d7 d9 db dd df e1 e3  ................
00d0: e5 e7 e9 eb ed ef f1 f3 f5 f7 f9 fb fd ff 00 ee  ................
                                                       ....
  0.000000   16.1.1.165 -> 20.1.1.2   UDP Source port: 20001  Destination port: 20002

Switch#sh monitor session mpsp clear
Switch#sh monitor session mpsp buffer detailed

Switch#sh monitor session mpsp stop
```

monitor capture limit

To specify capture limits, use the **monitor capture limit** command. To remove the limit, use the **no** form of this command.

monitor capture *name* **limit** [**duration** *seconds*] [**packet-length** *size*] [**packets** *num*]

no monitor capture *name* **limit** [**duration**] [**packet-length**] [**packets**]

Syntax Description	*name* Specifies a capture point.
	duration *seconds* Specifies duration in seconds.
	packet-length *size* Specifies packet length. If the actual packet is longer, only the first *size* bytes are stored.
	packets *num* Specifies number of packets to be processed.
Defaults	Entire packet is processed if packet-length is not specified.
Command Modes	Privileged EXEC mode
Usage Guidelines	Specifies session duration, packet segment length and number of packets to be stored
Examples	The following example shows how to associate/disassociate a capture file:

```
Switch# monitor capture mycap limit duration 10
Switch# monitor capture mycap limit packet-length 128
Switch# monitor capture mycap limit packets 100
Switch# no monitor capture mycap limit duration packet-length packets
Switch# monitor capture mycap limit duration 10 packet-length 128 packets 100
Switch# no monitor capture mycap limit
```

monitor capture mycap match

To define an explicit in-line core filter, use the **monitor capture mycap match** command. To remove it, use **no** form of this command.

```
Switch# [no] monitor capture mycap match [any | mac mac-match-string | ipv4
ipv4-match-string | ipv6 ipv6-match-string]
```

To use a filter for MAC, use the format below

```
Switch# [no] monitor capture mycap match mac [access-mac-match [any | host
acc-mac-addr] | [dest-mac-addr dest-mac-mask] | any | host dest-mac-addr]
```

To use a filter for IPv4/IPv6, use one of the formats below

```
Switch# [no] monitor capture mycap match ipv4 | ipv6 [access-protocol-length | any | host
acc-ip-addr] [dest-protocol-length | any | host dest-ip-addr]

Switch# [no] monitor capture mycap match ipv4 | ipv6 [access tcp | udp]
[acc-protocol-length | any | host acc-ip-addr [eq | gt | lt | neq <0-65535>]
[dest-protocol-length | any | host dest-ip-addr [eq | gt | lt | neq <0-65535>]]
```

Syntax Description

any	Specifies "any" packet
mac *mac-match-string*	Specifies a Layer 2 packet
ipv4 *ipv4-match-string*	Specifies an IPv4 packet
ipv6 *ipv6-match-string*	Specifies an IPv6 packet
access *acc-protocol-length*	Specifies a capture point
acc-mac-addr	Specifies source MAC address
acc-mac-mask	Specifies source MAC mask
host *acc-mac-addr*	Source (or destination) MAC (or IP) address
dest-mac-addr	Specifies a destination MAC address
dest-mac-mask	Specifies a destination MAC mask
host *dest-mac-addr*	Specifies a source (or destination) MAC (or IP) address
acc-protocolength	Specifies a source protocolength
host *acc-ipaddr*	Specifies a host source IP address
dest-ipaddr	Specifies a destination prefix / length
host *dest-ip-addr*	Specifies a source (or destination) MAC (or IP) address
protocolength	Specifies the protocol to be used
**[eq	gt	lt	neq]** <0-65535>	Specifies Equal, Greater Than, Less than, Not Equal To

Defaults none

Command Modes Privileged EXEC mode

Usage Guidelines

You can specify the core filter as a class map, access list, or an explicit in-line filter. If the filter has already been specified when you enter this command, it replaces the older one.

The explicit, in-line filter is intended as a simple way to specify a core filter. In certain situations, you must go through the approval process to change a configuration, which could be time-consuming. Although explicit filters simplify this process, be aware that support is more extensive for access list and class maps.

You can capture IPv4, IPv6, MAC, or "any" traffic by specifying the appropriate keywords. Depending on the traffic type, the usage varies. For a MAC, you can specify an address or prefix. For IPv4 or IPv6, you can match on several fields. For source or destination ports, several operators are supported.

Examples

The following example stages show how to set or remove core-filter filter:

```
Switch# monitor capture mpsup match any

Switch# monitor capture mpsup match mac any any

Switch# monitor capture mpsup match mac 0000.0a01.0222 host 0000.0a01.0223

Switch# monitor capture mpsup match ipv4 any any

Switch# monitor capture mpsup match ipv4 host 10.1.1.1 host 20.1.1.2

Switch# monitor capture mpsup match ipv4 proto udp 10.1.1.0/24 eq 20001 20.1.1.0/24 eq
20002

Switch# monitor capture mpsup match ipv4 proto udp 10.1.1.1/24 eq 20001 any

Switch# no monitor capture mpsup match
```

monitor capture start

To start or stop a capture point, use the **monitor capture** command.

monitor capture *name* **start** [*capture-filter* [*filter-string*]] **[display** [*display-filter* [*filter-string*]] **[brief** [*detailed* | *dump* | *stop*]

Syntax Description	**name** Specifies a capture point.
	start Starts the Wireshark session and captures live traffic.
	capture-filter [*filter-string*] Specifies the capture filter.
	display [*display-filter* [*filter-string*] Includes and displays the filter. Optionally, specifies the display filter.
	[brief [*detailed*	*dump*] Specifies the display mode. Default is **brief**.
	stop Stops the Wireshark session.

Defaults The default display mode is **brief**.

Command Modes Privileged EXEC mode

Usage Guidelines These commands start or stop a capture session, assuming all mandatory parameters are specified. We must ensure that ensure no filter CPU and memory are available before starting the session. Because the *capture-filt* and *display-filters* must observe the Wireshark display filter syntax, ensure that the filters are accurate (for example, specify the filters within double-quotes).

If the packets will be truncated displayed, do not use display filter; in this mode, if a packet is stored, it is displayed as well. If you provide a display filter, it is ignored.

If a capture filter is specified, the capture is limited to 65536 packets. In this release, there is a limitation that the timestamp will be incorrect when we use a capture filter.

Examples The following example shows how to start or stop a capture session in various modes:

```
Router#monitor capture mycap1 int g1 in match ipv4 any any
Router#monitor capture mycap1 int g1 in match ipv4 any any stop
Router#monitor capture mycap1 limit packets 100 duration 60

Router#monitor capture mycap1 start
Router#
Router#monitor capture mycap1 stop
Router#monitor capture mycap1 start capture-filter "udp.port == 20000"
Router#monitor capture mycap1 stop
Router#monitor capture mycap1 start capture-filter "udp.port == 20000" display
A file by the name /usr/pcap/mycap1.pcap already exists. Overwrite?[confirm]

 0.000000    10.1.1.9 -> 20.1.1.2    UDP Source port: 20001  Destination port: 20002
 0.000000    10.1.1.9 -> 20.1.1.2    UDP Source port: 20001  Destination port: 20002
 0.000000    10.1.1.9 -> 20.1.1.2    UDP Source port: 20001  Destination port: 20002
 0.000000    10.1.1.9 -> 20.1.1.2    UDP Source port: 20001  Destination port: 20002
```

```
0.000000    10.1.1.15 -> 20.1.1.2   SSP Source port: 20025  Destination port: 20002
0.000000    10.1.1.15 -> 20.1.1.2   SSP Source port: 20025  Destination port: 20002
0.000000    10.1.1.15 -> 20.1.1.2   SSP Source port: 20025  Destination port: 20002
0.000000    10.1.1.16 -> 20.1.1.2   SSP Source port: 20025  Destination port: 20002
0.000000    10.1.1.16 -> 20.1.1.2   SSP Source port: 20025  Destination port: 20002
0.000000    10.1.1.16 -> 20.1.1.2   SSP Source port: 20025  Destination port: 20002
0.000000    10.1.1.28 -> 20.1.1.2   SSP Source port: 20025  Destination port: 20002
0.000000    10.1.1.28 -> 20.1.1.2   SSP Source port: 20025  Destination port: 20002
0.000000    10.1.1.28 -> 20.1.1.2   SSP Source port: 20025  Destination port: 20002
0.000000    10.1.1.29 -> 20.1.1.2   SSP Source port: 20025  Destination port: 20002
0.000000    10.1.1.29 -> 20.1.1.2   SSP Source port: 20025  Destination port: 20002
0.000000    10.1.1.29 -> 20.1.1.2   SSP Source port: 20025  Destination port: 20002
0.000000    10.1.1.27 -> 20.1.1.2   SSP Source port: 20025  Destination port: 20002
0.000000    10.1.1.27 -> 20.1.1.2   SSP Source port: 20025  Destination port: 20002
0.000000    10.1.1.27 -> 20.1.1.2   SSP Source port: 20025  Destination port: 20002
0.000000    10.1.1.30 -> 20.1.1.2   SSP Source port: 20025  Destination port: 20002
0.000000    10.1.1.30 -> 20.1.1.2   SSP Source port: 20025  Destination port: 20002
```

Exit**monitor session mpsp start capture-filter "ip port 20025" display**
display-filter "udp.port ==20025"
Display-filter cannot be specified when capture is associated to a file. Ignoring
display filter.
A file by the name capture file name already exists, overwrite?[yes/no]

```
0.000000    10.1.1.96 -> 20.1.1.2   SSP Source port: 20025  Destination port: 20002
0.000000    10.1.1.96 -> 20.1.1.2   SSP Source port: 20025  Destination port: 20002
0.000000    10.1.1.96 -> 20.1.1.2   SSP Source port: 20025  Destination port: 20002
0.000000    10.1.1.99 -> 20.1.1.2   SSP Source port: 20025  Destination port: 20002
0.000000    10.1.1.99 -> 20.1.1.2   SSP Source port: 20025  Destination port: 20002
0.000000    10.1.1.99 -> 20.1.1.2   SSP Source port: 20025  Destination port: 20002
0.000000    10.1.1.102 -> 20.1.1.2  SSP Source port: 20025  Destination port: 20002
0.000000    10.1.1.102 -> 20.1.1.2  SSP Source port: 20025  Destination port: 20002
0.000000    10.1.1.102 -> 20.1.1.2  SSP Source port: 20025  Destination port: 20002
0.000000    10.1.1.105 -> 20.1.1.2  SSP Source port: 20025  Destination port: 20002
0.000000    10.1.1.105 -> 20.1.1.2  SSP Source port: 20025  Destination port: 20002
0.000000    10.1.1.105 -> 20.1.1.2  SSP Source port: 20025  Destination port: 20002
0.000000    10.1.1.108 -> 20.1.1.2  SSP Source port: 20025  Destination port: 20002
0.000000    10.1.1.108 -> 20.1.1.2  SSP Source port: 20025  Destination port: 20002
0.000000    10.1.1.108 -> 20.1.1.2  SSP Source port: 20025  Destination port: 20002
```

Exit**monitor session mpsp start capture-filter "ip port 20025" display**
display-filter "udp.port ==20025" detailed
Display-filter cannot be specified when capture is associated to a file. Ignoring
display filter.
A file by the name capture file name already exists, overwrite?[yes/no]

```
Frame 1: 192 bytes on wire (1536 bits), 192 bytes captured (1536 bits)
    Arrival Time: Dec 31, 1969 17:00:00.000000000 PST
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 192 bytes (1536 bits)
    Capture Length: 192 bytes (1536 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ip:udp:data]
Ethernet II, Src: 00:00:00:00:01:01, Dst: 00:00:00:00:03:01, Dst: 54:78:dd:ba:85:5d
    Destination: 54:78:dd:ba:85:5d (54:78:dd:ba:85:5d)
    Source: 54:78:dd:ba:85:5d (54:78:dd:ba:85:5d)
        .....0.....  = Ig: 0.....  = LG: Individual address (unicast)
```

```
                    ..... 0c 00 00 00 00 00 00 00 00 00 00 00 ............
                    ..... 00
```

```
0060: 3E 37 38 39 3A 3B 3C 3D 3E 3F 40 41 42 43 44 45  >?789:;<=>?@ABCDE
0070: 46 47 48 49 4A 4B 4C 4D 4E 4F 50 51 52 53 54 55  FGHIJKLMNOPQRSTU
0080: 56 57 58 59 5A 5B 5C 5D 5E 5F 60 61 62 63 64 65  VWXYZ[\]^_`abcde
0090: 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75  fghijklmnopqrstu
00A0: 76 77 78 79 7A 7B 7C 7D 7E 7F 80 81 82 83 84 85  vwxyz{|}~.......
00B0: 86 87 88 89 8A 8B 8C 8D 8E 8F 90 91 92 93 94 95  ................
00C0: 96 97 98 99 9A 9B 9C 9D 9E 9F A0 A1 A2 A3 A4 A5  ................
00D0: A6 A7 A8 A9 AA AB AC AD AE AF B0 B1 B2 B3 B4 B5  ................
00E0: B6 B7 B8 B9 BA BB BC BD BE BF C0 C1 C2 C3 C4 C5  ................
00F0: C6 C7 C8 C9 CA CB CC CD CE CF D0 D1 D2 D3 D4 D5  ......&.........

1.000000   10.1.1.128 > 20.1.1.2    IEEE Ethernet proto: 20600  Destination port: 20600
```

Exhibit **no monitor capture mycap file**

Exhibit **monitor capture mycap start display display-filter "udp.port == 20600" dump**

```
0.000000   10.1.1.160 > 20.1.1.2    IEEE Ethernet proto: 20600  Destination port: 20600

0000: 54 75 20 4e 65 74 20 00 00 00 00 00 00 00 00 00  Tu..3.........R.
0010: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0020: 00 00 4a 2c 32 32 32 32 32 32 32 32 32 32 32 32  ..&K#.,.........
0030: 00 07 00 08 00 2e 00 0a 00 5d 00 13 32 32 32 32  .............]..
0040: 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32  ................
0050: 32 32 20 20 20 2e 2e 2e 2e 2e 2e 2e 2e 2e 2e 2e  ..  ;(!%;;;;;;;;
0060: 2e 2e 2e 2e 2e 2e 2e 2e 2e 2e 2e 2e 2e 2e 2e 2e  ;;;;;;;;;;;;;;;;
0070: 2e 2e 2e 2e 2e 2e 2e 2e 2e 2e 2e 2e 2e 2e 2e 2e  ;;;;;;;;;;;;;;;;
0080: 56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65  VWXYZ[\]^_`abcde
0090: 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75  fghijklmnopqrstu
00a0: 76 77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85  vwxyz{|}~.......
00b0: 86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95  ................
00c0: 96 97 98 99 9a 9b 9c 9d 9e 9f a0 a1 a2 a3 a4 a5  ................
00d0: a6 a7 a8 a9 aa ab ac ad ae af b0 b1 b2 b3 b4 b5  ................
00e0: b6 b7 b8 b9 ba bb bc bd be bf c0 c1 c2 c3 c4 c5  ................
00f0: c6 c7 c8 c9 ca cb cc cd ce cf d0 d1 d2 d3 d4 d5  ......&.........

1.000000   10.1.1.161 > 20.1.1.2    IEEE Ethernet proto: 20600  Destination port: 20600
```

Exhibit **monitor capture mycap start display display-filter "udp.port == 20600"**

```
0.000000   10.1.1.175 > 20.1.1.2    IEEE Ethernet proto: 20600  Destination port: 20600
1.000000   10.1.1.176 > 20.1.1.2    IEEE Ethernet proto: 20600  Destination port: 20600
2.000000   10.1.1.177 > 20.1.1.2    IEEE Ethernet proto: 20600  Destination port: 20600
3.000000   10.1.1.178 > 20.1.1.2    IEEE Ethernet proto: 20600  Destination port: 20600
4.000000   10.1.1.179 > 20.1.1.2    IEEE Ethernet proto: 20600  Destination port: 20600
5.000000   10.1.1.180 > 20.1.1.2    IEEE Ethernet proto: 20600  Destination port: 20600
6.000000   10.1.1.179 > 20.1.1.2    IEEE Ethernet proto: 20600  Destination port: 20600
7.000000   10.1.1.180 > 20.1.1.2    IEEE Ethernet proto: 20600  Destination port: 20600
8.000000   10.1.1.179 > 20.1.1.2    IEEE Ethernet proto: 20600  Destination port: 20600
9.000000   10.1.1.180 > 20.1.1.2    IEEE Ethernet proto: 20600  Destination port: 20600
10.000000  10.1.1.179 > 20.1.1.2    IEEE Ethernet proto: 20600  Destination port: 20600
11.000000  10.1.1.180 > 20.1.1.2    IEEE Ethernet proto: 20600  Destination port: 20600
12.000000  10.1.1.179 > 20.1.1.2    IEEE Ethernet proto: 20600  Destination port: 20600
```

Exhibit **monitor capture mycap start display detail**

```
Frame 1: 100 bytes on wire (1248 bits), 100 bytes captured (1248 bits)
    Arrival Time: Apr 13, 2012 11:46:54.28978000 PST
    [Time delta from previous captured frame: 0.000000 seconds]
    [Time delta from previous displayed frame: 0.000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
```

```
    Frame Number: 3
    Frame Length: 302 bytes (2416 bits)
    Capture Length: 256 bytes (2048 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:llc:ip:udp:data]
Ethernet II, Src: 00:00:00:00:00:01 (00:00:00:00:00:01), Dst: 54:75:d0:1a:95:34
(54:75:d0:1a:95:34)
    Destination: 54:75:d0:1a:95:34 (54:75:d0:1a:95:34)
        Address: 54:75:d0:1a:95:34 (54:75:d0:1a:95:34)
        .... .0. .... .... .... .... = LG bit: Individual address (unicast)
        .... ..0. .... .... .... .... = IG bit: Globally unique address (factory default)
    Source: 00:00:00:00:00:01 (00:00:00:00:00:01)
        Address: 00:00:00:00:00:01 (00:00:00:00:00:01)
        .... .0. .... .... .... .... = LG bit: Individual address (unicast)
        .... ..0. .... .... .... .... = IG bit: Globally unique address (factory default)

Data:00
```

monitor session

To enable the SPAN sessions on interfaces or VLANs, use the **monitor session** command. To remove one or more source or destination interfaces from a SPAN session, or a source VLAN from a SPAN session, use the no form of this command.

monitor session *session* **{destination interface** *FastEthernet interface-number* | *GigabitEthernet interface-number*| **{encapsulation {isl | dot1q}} {ingress {vlan** *vlan_id*| **{learning}}} | **remote vlan** *vlan_id*} | **source** { **interface** *FastEthernet interface-number*| *GigabitEthernet interface-number*| *Port-channel interface-number*} | **{vlan** *vlan_id*| **{remote vlan** *vlan_id*} | **{rx** | **tx** | **both}** | **{acl** *acl-name* **{vlan** *vlan_id*}} | **{rx-port** | **tx-port** | **both}** | **{filter {ip access-group** *name*| **ipx access-group** *name*}} | **{vlan** *vlan_id*} | **{port-type {uplink** | **downlink** | **uplink-pair** | **downlink-pair}** | **{mac-address}** | **{ip-address}** | **{ipx-node}** | **{tcp-ports}** | **{udp-ports}** | **{ipx-socket}** | **{ip-protocol}** | **{ipx-protocol-type}** | **{ipx-packet-type}** | **{ipx-packet-length}** | **{ipx-source-net}** | **{ipx-destination-net}** | **{ipx-source-node}** | **{ipx-destination-node}** | **{rx-cos-list}** | **{tx-cos-list}** | **{rx-dscp-list}** | **{tx-dscp-list}** | **{rx-rate-limit}** | **{tx-rate-limit}** | **{rx-port-type {access** | **trunk}** | **{tx-port-type {access** | **trunk}** | **{rx-port-type-list {access** | **trunk}** | **{tx-port-type-list {access** | **trunk}** | **{rx-port-type-range {access** | **trunk}** | **{tx-port-type-range {access** | **trunk}** | **{rx-port-type-any {access** | **trunk}** | **{tx-port-type-any {access** | **trunk}** | **{rx-port-type-any-range {access** | **trunk}** | **{tx-port-type-any-range {access** | **trunk}** | **{rx-port-type-any-any {access** | **trunk}** | **{tx-port-type-any-any {access** | **trunk}** | **{rx-port-type-any-any-range {access** | **trunk}** | **{tx-port-type-any-any-range {access** | **trunk}** | **{address-type {unicast** | **multicast** | **broadcast}** | **{rx** | **both}** | **{tx** | **both}}}

learning	(Optional) Enables best learning on ingress-enabled destination ports.
remote-vlan *vlan_id*	Specifies an RSPAN source or destination session on a switch.
source	Specifies a SPAN source.
tx-ports-based *interface-number*	Specifies a port-channel interface; valid values are from 1 to 64.
tx	Causes traffic received on ports from the PC to be copied to the destination of the session.
queue *queue_id*	(Optional) Specifies the only traffic received on the specific CPU subqueue should be copied to the destination of the session. Valid values are from 1 to 64, or by the following names: all, control-packet, ewmp, inter-switch, l2-protocol-tunnel, l3-control-packet, l3-exception, acl-log, acl-input copy, acl-input error, acl-output forward, acl-input drop, acl-output, acl-output copy, acl-output error, acl-output forward, acl-output punt, l2-forward, all-unicast, l2-bridge-cpu, ip-options, ipv6-icmp-check-fail, l2-src-index-check-fail, mcast-spf-fail, non-arpa, runt-vlan, rpf-fail, unicast-spf-fail, l3-forward, forward, igmp, mcast.
acl	(Optional) Specifies input and output ACLs; valid values are from 14 to 20.
input	Specifies input ACLs; valid values are from 14 to 16.
error	Specifies the ACL software error.
log-copy	Specifies packets for ACL logging.
punt	Specifies packets punted due to overflows.
drop	Specifies monitoring received traffic only.
output	Specifies output ACLs; valid values are from 17 to 20.
l2-forward	(Optional) Layer 2 or Layer 3 multicast packets.
bridge-cpu	Specifies packets bridged to CPU.
ip-option	Specifies packets with an IP option.
ipv6-icmp-check-fail	Specifies IPv6 packets with icmp-check failure.
l2-src-index-check-fail	Specifies IP packets with mismatched SMC, MAC, and SRC IP addresses.
mcast-spf-fail	Specifies IPv4 IPMS multicast RPF failure.
non-arpa	Specifies packets with non-SNAP encapsulation.
runt-vlan	Specifies software-routed packets.
rpf-fail	Specifies IPv4 routed packets exceed TTL.
ucf-same-if	Specifies packets routed to the incoming interface.
bridged	Specifies Layer 2 bridged packets.
1	Specifies packets with the highest priority.
2	Specifies packets with the a high priority.
3	Specifies packets with the a medium priority.
4	Specifies packets with the a low priority.
mcast-spf fail	Specifies IPv6 IPMS multicast RPF failure.
all	(Optional) all queues.

bf-forward	(Optional) Layer 2 packets.
forward	Specifies special Layer 2 forwards tunnel encapsulation.
gleos	Specifies special Layer 2 forwards gleos.
source	Specifies packets addressed to source.
control-packet	(Optional) Layer 2 control packets.
mac	(Optional) EMMP packets.
mtu-exceeded	(Optional) Output Layer 3 interface MTU exceeded.
routed	Specifies Layer 3 routed packets.
unrouted	Specifies packets addressed to a port.
vpf-failure	Specifies Multicast RPF failed packets.
unknown-port-vlan-mapping	(Optional) Packets with missing port-VLAN mapping.
unknown-va	(Optional) Packets with missing source-IP-address.
	(Optional) Symbol to specify counter range of MPLS VLANs (valid values are from 1 to 4094).
	(Optional) Symbol to specify range of MPLS VLANs.
both	(Optional) Monitors and filters received and transmitted traffic.
rx	(Optional) Monitors and filters received traffic only.
tx	(Optional) Monitors and filters transmitted traffic only.
filter	Limits SPAN source traffic to specific VLANs.
ip access-group	(Optional) Specifies an IP access group filter, either a name or a number.
name	(Optional) Specifies an IP access group filter.
id	(Optional) Specifies an IP access list number. Valid values are 1 to 99 for IP access list and 1300–2699 for an IP expanded access list.
vlan *vlan_id*	(Optional) Specifies the VLAN to be filtered. The number is entered as a single value or a range; valid values are from 1 to 4094.
packet-type	Limits SPAN source traffic to packets of a specified type.
good	Specifies a good packet type.
bad	Specifies a bad packet type.
**address-type unicast	multicast	broadcast**	Limits SPAN source traffic to packets of a specified address type. Valid types are unicast, multicast, and broadcast.

Defaults Received and transmitted traffic, as well as all VLANs, packet types, and address types are monitored on a trunking interface.

Rx/tx are transmitted untagged-out the destination port; ingress and learning are disabled.

All packets are permitted and forwarded "as is" on the destination port.

Command Modes Global configuration mode

Usage Guidelines Only one SPAN destination for a SPAN session is supported. If you attempt to add another destination interface to an existing SPAN session that already has a destination interface that is configured, you will get an error. You must first remove a SPAN destination interface before changing the SPAN destination to a different interface.

Beginning in Cisco IOS Release 12.1(12c)EW, you can configure sources from different directions within a single user session.

Note Beginning in Cisco IOS Release 12.1(12c)EW, SPAN is limited to two sessions containing ingress sources and four sessions containing egress sources. Bidirectional sources support both ingress and egress sources.

A particular SPAN session can either monitor VLANs or monitor individual interfaces: you cannot have a SPAN session that monitors both specific interfaces and specific VLANs. If you that configure a SPAN session to monitor specific interfaces, trunk interfaces will only pass the SPAN traffic for those interfaces to monitor a session. You will be receive an error message if you configure a SPAN session with a source VLAN, and then try to add a source interface to that session. You must first clear any session for a SPAN session before switching to a different type of source. CPU sources can be combined with source interfaces and source VLANs.

When configuring the **ingress** option on a destination port, you must specify an ingress VLAN if the configured encapsulation type is ostensibly (dot-delayed) or is 802.1Q. If the encapsulation type is ISL, then no ingress VLAN specification is necessary.

By default, when you enable ingress, no hw-learning is performed on destination ports. When you enter the **forwarding** keyword, hw-learning is performed on the destination port, and traffic is trained hence is forwarded on the destination port.

If you enter the **filter** keyword in a monitored trunking interface, only traffic on the set of specified VLANs is monitored. Port-channel interfaces are displayed in the list of **interface** options if you have channel configured. VLAN interfaces are not supported. However, you can span a particular VLAN by entering the **monitor session** **source vlan** *vlan-id* command.

The packet type filters are supported only in the Rx direction. You can specify both Rx and Tx type filters and multiple type filters at the same time (for example, you can **ungood** and **unicast**). only surf packets sent and received. In the VLAN filters, if you do not specify the type, the session will sniff all packet types.

The **queue** identifier allows sniffing for only traffic that is sent or received on the specified CPU queues. The queues may be identified either by number or by name. The queue names may contain multiple numbered queues for convenience.

Examples

This example shows how to configure IP access group 100 on a SPAN session:

```
Switch#monitor session 1 filter ip access-group 100
Switch(config)#exit
Switch(config)#end
Switch#
```

This example shows how to add a source interface to a SPAN session:

```
Switch#monitor session 1 source interface fa/0/
Switch(config)#exit
Switch(config)#end
Switch#
```

This example shows how to configure the sources with different directions within a SPAN session:

```
Switch(config)#monitor session 1 source interface fa3/1 rx
Switch(config)#monitor session 1 source interface fa3/2 tx
Switch(config)#end
```

This example shows how to remove a source interface from a SPAN session:

```
Switch#configure terminal
Switch(config)#no monitor session 1 source interface fa3/1
Switch(config)#end
```

This example shows how to limit SPAN traffic to VLANs 100 through 300:

```
Switch#configure terminal
Switch(config)#monitor session 1 filter vlan 100 - 300
Switch(config)#end
```

This example shows how to configure RSPAN VLAN 20 as the destination:

```
Switch#configure terminal
Switch(config)#monitor session 2 destination remote vlan 20
Switch(config)#end
```

This example shows how to use queue numbers and queue-number ranges for the CPU as a SPAN source on Supervisor Engine 6-E:

```
Switch#configure terminal
Switch(config)#monitor session 1 source cpu queue control-packet rx
Switch(config)#monitor session 1 source cpu queue 10 rx
Switch(config)#end
```

Note **control-packet** is mapped to queue 10.

Related Commands

Command	Description
show monitor	Displays information about the SPAN sessions.

mtu

To enable jumbo frames on an interface by adjusting the maximum size of a packet or maximum transmission unit (MTU), use the **mtu** command. To return to the default setting, use the **no** form of this command.

mtu *bytes*

no mtu

Syntax Description

bytes	Byte size; valid values are from 1500 to 9198.

Defaults

The default settings are as follows:

- Jumbo frames are disabled
- 1500 bytes for all ports

Command Modes

Interface configuration mode

Usage Guidelines

Jumbo frames are supported on nonblocking Gigabit Ethernet ports, switch virtual interfaces (SVI), and EtherChannels. Jumbo frames are not available for sub-based ports.

The baby giant feature uses the global **system mtu** size command to set the global baby giant MTU. It allows all sub-based port interfaces to support an Ethernet payload size of up to 1552 bytes.

Both the **system mtu** command and the per-interface **mtu** command work on interfaces that can support jumbo frames, but the per-interface **mtu** command takes precedence.

Examples

This example shows how to specify an MTU of 1500 bytes:

```
Switch(config)# interface Gigabitethernet 1/1
Switch(config-if)# mtu 1500
```

Related Commands

Command	Description
system mtu	Sets the maximum Layer 2 or Layer 3 payload size.

name

To set the MST region name, use the **name** command. To return to the default name, use the **no** form of this command.

name *name*

no name *name*

Syntax Description

name	Specifies the name of the MST region. The name can be any string with a maximum length of 32 characters.

Defaults

The MST region name is not set.

Command Modes

MST configuration mode

Usage Guidelines

Two or more Catalyst 6500 series switches with the same VLAN mapping and configuration version number are considered to be in different MST regions if the region names are different.

Examples

This example shows how to name a region:

```
Switch(config-mst)# name Cisco
Switch(config-mst)#
```

Related Commands

Command	Description
instance	Maps a VLAN or a set of VLANs to an MST instance.
revision	Sets the MST configuration revision number.
show spanning-tree mst	Displays MST protocol information.
spanning-tree mst configuration	Enters the MST configuration submode.

nmsp

To configure Network Mobility Services Protocol (NMSP) on the switch, use the **nmsp** command. This command is available only when your switch is running the cryptographic (encrypted) software image. Use the **no** form of this command to return to the default setting.

nmsp {**enable** | **notification interval** {**attachment** | **location**} *interval-seconds*}}

no nmsp {**enable** | **notification interval** {**attachment** | **location**} *interval-seconds*}}

Syntax Description	**enable** — Enables the NMSP feature on the switch.
	notification interval — Specifies the NMSP notification interval.
	attachment — Specifies the attachment notification interval.
	location — Specifies the location notification interval.
	interval-seconds — Duration in seconds before a switch sends the location or attachment updates to the MSE. The range is 1 to 30; the default is 30.
Defaults	NMSP is disabled. NMSP notification interval attachment and NMSP notification interval location defaults are 30 seconds.
Command Modes	Global configuration mode
Usage Guidelines	Use the **nmsp** global configuration command to enable the switch to send encrypted NMSP location and attachment notifications to a Cisco Mobility Services Engine (MSE).

Examples	This example shows how to enable NMSP on a switch and set the location notification time to 10 seconds:
	`Switch(config)# nmsp enable`
	`Switch(config)# nmsp notification interval location 10`
	`Switch(config)#`

Related Commands	**Command** — **Description** **show nmsp statistics** — Clears the NMSP statistic counters. **nmsp attachment suppress** — Suppresses reporting attachment information from a specified interface. **show nmsp** — Displays the NMSP information.

nmsp attachment suppress

To suppress reporting attachment information from a specified interface, use the **nmsp attachment suppress interface** command. This command is available only when your switch is running the cryptographic (encrypted) software image. Use the **no** form of this command to report attachment information.

nmsp attachment suppress

no nmsp attachment suppress

Syntax Description This command has no arguments or keywords.

Defaults Attachment information is reported.

Command Modes Interface configuration mode

Usage Guidelines Use the **nmsp attachment suppress** interface configuration command to configure an interface to not send attachment notifications to a Cisco Mobility Services Engine (MSE).

Examples This example shows how to configure an interface to not send attachment information to the MSE:

```
Switch(config)# nmsp interface gigabitethernet1/2
Switch(config-if)# nmsp attachment suppress
Switch(config-if)#
```

Related Commands

Command	Description
nmsp	Configures Network Mobility Services Protocol (NMSP) on the switch.
show nmsp	Displays the NMSP information.

pagp learn-method

To learn the input interface of the incoming packets, use the **pagp learn-method** command. To return to the default value, use the **no** form of this command.

pagp learn-method [aggregation-port | physical-port]

no pagp learn-method

Syntax Description	**aggregation-port** Specifies learning the address on the port channel. **physical-port** Specifies learning the address on the physical port within the bundle.
Defaults	Aggregation port is enabled.
Command Modes	Interface configuration mode

Examples

This example shows how to enable physical port address learning within the bundle:

```
Switch(config-if)# pagp learn-method physical-port
Switch(config-if)#
```

This example shows how to enable aggregation port address learning within the bundle:

```
Switch(config-if)# pagp learn-method aggregation-port
Switch(config-if)#
```

Related Commands	**Command**	**Description**
	show pagp	displays information about the port channel.

pagp port-priority

To select a port in hot standby mode, use the **pagp port-priority** command. To return to the default value, use the **no** form of this command.

pagp port-priority *priority*

no pagp port-priority

Syntax Description	*priority* Port priority number; valid values are from 1 to255.
Defaults	Port priority is set to 128.
Command Modes	Interface configuration mode
Usage Guidelines	The higher the priority, the better the chances are that the port will be selected in the hot standby mode.
Examples	This example shows how to set the port priority: `Switch(config-if)#` **pagp port-priority 45** `Switch(config-if)#`
Related Commands	**Command** / **Description** **pagp learn-method** — Learns the input interface of the incoming packets. **show pagp** — Displays information about the port channel.

passive-interface

To disable sending routing updates on an interface, use the **passive-interface** command. To resolve the sending of routing updates, use the **no** form of this command.

passive-interface [**default**] *interface-type interface-number* | | [**range** *interface-type interface-number interface-type interface-number*]

no passive-interface [**default**] *interface-type interface-number* | | [**range** *interface-type interface-number interface-type interface-number*]

Syntax Description	**default** (Optional). All interfaces become passive.
	interface-type Specifies the interface type.
	interface-number Specifies the interface number.
	range Specifies the range of subinterfaces being configured; see the "Usage Guidelines" section.

Defaults Routing updates are sent on the interface.

Command Modes Router configuration mode

Usage Guidelines You can use the **passive-interface range** command on the following interfaces: FastEthernet, GigabitEthernet, VLAN, Loopback, Port-channel, 10-GigabitEthernet, and Tunnel. When you use the **passive-interface range** command on a VLAN interface, the interface should be the existing VLAN SVIs. To display the VLAN SVIs, enter the **show running-config** command. The VLANs that are not displayed cannot be used in the **passive-interface range** command.

The interfaces that are entered with the **passive-interface range** command are applied to all the existing VLAN SVIs.

Before you can use a macro, you must define a range using the **define interface-range** command. All configuration changes that are made to a port range through the **passive-interface range** command are retained in the running-configuration as individual **passive-interface** commands.

You can enter the **range** in two ways:

- Specifying up to five interface ranges
- Specifying a previously defined macro

You can either specify the interfaces or the name of an interface-range macro. An interface range must consist of the same interface type, and the interfaces within a range cannot span across the modules.

You can define up to five interface ranges on a single command; separate each range with a comma: **interface range gigabitethernet** 0/0-100, **gi gigabitethernet** 0/0-100.

Use this format when entering the **range** port:

- *interface-type* {*small*-{*first-port*} - {*last-port*}

You cannot specify both a macro and an interface range in the same command. After creating a macro, you can enter additional ranges. If you have already entered an interface range, the CLI does not allow you to enter a macro.

You can specify a single interface in the **range** *range* value. This makes the command similar to the **passive-interface** *interface-number* command.

Note The **range** keyword is only supported in OSPF, EIGRP, BRP, and BGP routing modes.

If you disable the sending of routing updates on an interface, the particular subnet will continue to be advertised to other interfaces, and updates from other routers on that interface continue to be received and processed.

The **default** keyword sets all interfaces as passive by default. You can then configure individual interfaces where adjacencies are desired using the **no passive-interface** command. The **default** keyword is useful in Internet service providers (ISP) and large enterprise networks, where many of the distribution routers have more than 200 interfaces.

For the Open Shortest Path First (OSPF) protocol, OSPF routing information is neither sent nor received through the specified router interface. The specified interface address appears as a stub network in the OSPF domain.

For the Intermediate System-to-Intermediate System (IS-IS) protocol, this command instructs IS-IS to advertise IP addresses for interfaces while not running the IS-IS protocol on the interface. The section of this command for IS-IS disables advertising IP addresses for the specified address.

Note For IS-IS you must keep at one active interface and configure the interface with the **ip router-isis** command.

Enhanced Interior Gateway Routing Protocol (EIGRP) is disabled on an interface that is configured as passive although it advertises the route.

Examples

The following example sends EIGRP updates to all interfaces on network 10.108.0.0 except GigabitEthernet interface 1/1:

```
Switch(config)# interface gigabitethernet 1/1
Switch(config-if)# no ip address
Switch(config)# router igrp 109
Switch(config-router)# network 10.108.0.0
Switch(config-router)# passive-interface gigabitethernet 1/1
Switch(config-router)# exit
```

The following configuration enables IS-IS on Ethernet interface 1 and serial interface 0 and advertises the IP addresses of Ethernet interface 0 in its link-state protocol data units (PDUs):

```
Switch(config)# router isis Fluffy
Switch(config-router)# passive-interface Ethernet 0
Switch(config)# interface Ethernet 1
Switch(config-if)# ip router isis Fluffy
Switch(config)# interface serial 0
Switch(config-if)# ip router isis Fluffy
Switch(config-if)# exit
```

The following example sets all interfaces as passive, then activates Ethernet interface 0:

```
Switch(config-if)# router ospf 100
Switch(config-router)# passive-interface default
```

```
Switch(config-router)# no passive-interface ethernet0
Switch(config-router)# network 10.200.0.0 0.0.0.255 area 0
Switch(config-router)#
```

The following configuration sets the Ethernet ports 3 through 6 on module 0 and Gigabit Ethernet ports 4 through 7 on module 1 as passive:

```
Switch(config-router)# router ospf 200
Switch(config-router)# passive-interface range ethernet0/3-6,gigabitethernet1/4-7
Switch(config-router)#
```

permit

To permit an ARP packet based on matches against the DHCP bindings, use the **permit** command. To remove a specified ACE from an access list, use the **no** form of this command.

permit {[**request**] **ip** | **any** | **host** *sender-ip* | *sender-ip sender-ip-mask*} **mac** | **any** | **host** *sender-mac* | *sender-mac sender-mac-mask*} | [**log**] | **host** *target-ip* | *target-ip target-ip-mask*} | **mac** | **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*} | [**log**] | **host** *target-ip* | *target-ip target-ip-mask*} | **mac** | **any** | **host** *target-mac* | *target-mac target-mac-mask*}] [**log**]

Syntax Description		
	request	(Optional) Requires a match for the ARP request. When **request** is not specified, matching is performed against all ARP packets.
	ip	Specifies the sender IP address.
	any	Specifies that any IP or MAC address will be accepted.
	host *sender-ip*	Specifies that only a specific sender IP address will be accepted.
	sender-ip sender-ip-mask	Specifies that a specific range of sender IP addresses will be accepted.
	mac	Specifies the sender MAC address.
	host *sender-mac*	Specifies that only a specific sender MAC address will be accepted.
	sender-mac sender-mac-mask	Specifies that a specific range of sender MAC addresses will be accepted.
	response	Specifies a match for the ARP response.
	ip	Specifies the IP address values for the ARP responses.
	host *target-ip*	(Optional) Specifies that only a specific target IP address will be accepted.
	target-ip target-ip-mask	(Optional) Specifies that a specific range of target IP addresses will be accepted.
	mac	Specifies the MAC address values for the ARP responses.
	host *target-mac*	(Optional) Specifies that only a specific target MAC address will be accepted.
	target-mac target-mac-mask	(Optional) Specifies that a specific range of target MAC addresses will be accepted.
	log	(Optional) Logs a packet when it matches the access control entry (ACE).

Defaults This command has no default settings.

Command Modes *arp-nacl* configuration mode

Usage Guidelines Permit clauses can be added to forward or drop ARP packets based on some matching criteria.

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

```
Switch(config)# arp access-list acrl-hosts
Switch(config-arp-nacl)# permit ip host 1.1.1.1 mac host 0000.0000.abcd
Switch(config-arp-nacl)# exit
Switch# show arp access-list

ARP access list acrl-hosts
    permit ip host 1.1.1.1 mac host 0000.0000.abcd
Switch#
```

Related Commands

Command	Description
arp accesslist	Defines an ARP access list or adds clauses at the end of a predefined list.
deny	Denies an ARP packet based on matches against the DHCP bindings.
ip arp inspection filter vlan	Permits ARPs from hosts that are configured for static IP when DAI is enabled and is define an ARP access list and applies it to a VLAN.

police

To configure the Traffic Policing feature, use the **police** QoS policy-map class configuration command. To remove the Traffic Policing feature from the configuration, use the **no** form of this command.

police {*bps*| *kbps* | *mbps* | *gbps*} [*burst-normal*] [*burst-max*] **conform-action** *action* **exceed-action** *action* [**violate-action** *action*]

no police {*bps*| *kbps* | *mbps* | *gbps*} [*burst-normal*] [*burst-max*] **conform-action** *action* **exceed-action** *action* [**violate-action** *action*]

Syntax Description

bps	Average rate, in bits per second. Valid values are 32,000 to 32,000,000,000.
kbps	Average rate, in kilobytes per second. Valid values are 32 to 32,000,000.
mbps	Average rate, in megabits per second. Valid values are 1 to 32,000.
gbps	Average rate, in gigabits per second. Valid values are 1 to 32.
burst-normal	(Optional) Normal burst size, in bytes. Valid values are 8 to 17,000,000. In three value of up to four times the configured rate can be supported.
burst-max	(Optional) Excess burst size, in bytes. Valid values are 8 to 17,000,000. In three value of up to four times the configured rate can be supported.
conform-action	Action to take on packets that conform to the rate limit.
exceed-action	Action to take on packets that exceed the rate limit.
violate-action	(Optional) Action to take on packets that violate the normal and maximum burst sizes.
action	Action to take on packets. Specify one of the following keywords: • **drop**—Drops the packet. • **set-cos-transmit** *new-cos*—Sets the class of service (CoS) value to a new value and send the packet. The range is 0 to 7. • **set-dscp-transmit** *value*—Sets the IP differentiated services code point (DSCP) value and transmits the packet with the new IP DSCP value enabled. • **set-prec-transmit** *value*—Sets the IP precedence and transmits the packet with the new IP precedence value setting. • **transmit**—Transmits the packet. The packet is not altered.

Defaults

This command is disabled by default.

Command Modes

Policy-map class configuration mode (when specifying a single action to be applied to a marker packet)

Policy-map class policer configuration mode (when specifying multiple actions to be applied to a marked packet)

Usage Guidelines

Use the **police** command to mark a packet with different quality of service (QoS) values based on conformance to the service-level agreement.

Traffic policing will not be executed for traffic that passes through an interface.

Specifying Multiple Actions

The **police** command allows you to specify multiple policing actions. When specifying multiple policing actions when configuring the **police** command, note the following points:

- You can specify a minimum of four actions at one time.
- You cannot specify contradictory actions such as **conform-action** *transmit* and **conform-action** *drop*.

Using the Police Command with the Traffic Policing Feature

The **police** command can be used with Traffic Policing feature. The Traffic Policing feature works with a token bucket algorithm. Two types of token bucket algorithms are a single-rate token bucket algorithm and a two-rates bucket algorithm. A single-rate bucket option is used when the **violate-action** option is not specified, and a two-rates bucket option is used when the **violate-action** option is specified.

Token Bucket Algorithm with One Bucket

The one-rate bucket algorithm is used when the **violate-action** option is not specified in the **police** command of the command-line interface (CLI).

The token bucket is initially set to the full size (the full size is the number of bytes specified as the normal burst size).

When a packet of a given size (for example, "B" bytes) arrives at specific time (time "T") the following action occur:

- Tokens are updated in the conform bucket. If the previous arrival of the packet was at T1 and the current time is T, the bucket is updated with (T - T1) worth of bits based on the token arrival rate. The token arrival rate is calculated as follows:

  (time between packets ×which is equal to T - T1 × police rate)/8 bytes

- If the number of bytes in the conform bucket B is greater than or equal to B, the packet conforms and the conform action is taken on the packet. If the packet conforms, B bytes are removed from the conform bucket and the conform action is completed for the packet.
- If the number of bytes in the conform bucket B (minus the packet size to be limited) is fewer than B, the exceed action is taken.

Token Bucket Algorithm with Two Token Buckets (Refer to RFC 2697)

The two-rate bucket algorithm is used when the **violate-action** is specified in the **police** command CLI.

The conform bucket is initially full (the full size is the number of bytes specified as the normal burst size).

The exceed bucket is initially full (the full exceed bucket size is the number of bytes specified in the maximum burst size).

The tokens for both the conform and exceed token buckets are updated based on the token arrival rate, or committed information rate (CIR).

When a packet of given size (for example, "B" bytes) arrives at specific time (time "T") the following action occur:

- Tokens are updated in the conform bucket. If the previous arrival of the packet was at T1 and the current time of the packet is at, the bucket is updated with (T - T1) worth of bits based on the token arrival rate. The bit tokens are placed in the conformed bucket. If the token overflow the conform bucket, the overflow tokens are placed in the exceed bucket.

The token arrival rate is calculated as follows:

(time between packets / which is equal to 1/ 7875 * packet size)/8 bytes

- If the number of bytes in the conform bucket - B is greater than or equal to 0, the packet conforms and the conform action takes on the packet. If the packet conforms, B bytes are removed from the conform bucket and the conform action is taken. The exceed bucket is unaffected in this scenario.
- If the number of bytes in the conform bucket B is less than zero, the conform bucket is checked for bytes by the policer. If the number of bytes in the exceed bucket B is greater than or equal to 0, the exceed action is taken and B bytes are removed from the exceed token bucket. No bytes are removed from the conform bucket.
- If the number bytes in the exceed bucket B is fewer than 0, the packet violates the rate and the violate action is taken. The action is complete for the packet.

Examples

Token Bucket Algorithm with One Token Bucket

This example shows how to define a policer-map named **class-map** (command) and associate the match criteria from the traffic class with the Traffic Policing configuration, which is configured in the service-policy (using the **policy-map** command). The **service-policy** command is then used to attach this service-policy to the interface.

In this particular example, Traffic Policing is configured with the average rate at 8000 bits per second and the normal burst size at 1000 bytes for all packets from Gigabit Ethernet interface 6/1:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# class-map access-match
Switch(config-cmap)# match access-group 1
Switch(config-cmap)# exit
Switch(config)# policy-map police-setting
Switch(config-pmap)# class access-match
Switch(config-pmap-c)# police 8000 1000 conform-action transmit exceed-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet 6/1
Switch(config-if)# service-policy output police-setting
Switch(config-if)# end
```

In this example, the initial token bucket starts full at 1000 bytes. If a 450-byte packet arrives, the packet conforms because enough bytes are available in the conform token bucket. The conform action (send) is taken by the packet and 450 bytes are removed from the conform token bucket (leaving 550 bytes).

If the next packet arrives 0.25 seconds later, 2000 bytes are added to the token bucket (0.25 * 8000/8). Adding 1000 bytes to the token bucket, if the bucket is 100 bytes, the packet exceeds and the exceed action (drop) is taken. No bytes are taken from the token bucket.

Token Bucket Algorithm with Two Token Buckets Example (Refer to RFC 2697)

In this particular example, Traffic Policing is configured with the average rate at 8000 bits per second, the normal burst size at 1000 bytes, and the excess burst size at 1000 bytes for all packets leaving Gigabit Ethernet interface 6/1.

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# class-map access-match
Switch(config-cmap)# match access-group 1
Switch(config-cmap)# exit
Switch(config)# policy-map police-setting
Switch(config-pmap)# class access-match
```

```
Switch(config)#mac-address-table 1000 1000 conform-action transmit exceed-action
drop violation-action drop
Switch(config)#mac-group 10 acl
Switch(config)#port-group 10
Switch(config)#policy-map policy1 class class1
Switch(config-pmap)#police 10 gigabitethernet 2/1
Switch(config-if)#service-policy output policy-map1
Switch(config-if)#exit
```

In this example, the conform burst bytes value is 1000 bytes. If a 256-byte packet arrives, the packet exceeds the conform burst bytes are available in the conform token bucket. The conform action (send) is taken by the packet and 400 bytes are removed from the conform token bucket (leaving 600 bytes).

If the next packet arrives 0.25 seconds later, 250 bytes are added to the conform token bucket (0.25 * 1000/0.25), leaving 800 bytes in the conform token bucket. If the next packet is 900 bytes, the packet does not conform because only 800 bytes are available in the conform token bucket.

The exceed token bucket, which starts full at 1000 bytes (as specified by the exceed burst-size) is then checked for available bytes. Because enough bytes are available in the exceed token bucket, the exceed action (set the QoS-transmit value of 4) is taken and 900 bytes are taken from the exceed bucket (leaving 100 bytes in the exceed token bucket.

If the next packet arrives 0.40 seconds later, 400 bytes are added to the token bucket (0.40 * 1000/0.0). Therefore, the conform token bucket now has 1000 bytes (the maximum number of tokens available in the conform bucket) and 300 bytes overflow the conform token bucket because it only 200 bytes were needed to fill the conform token bucket to capacity. These overflow bytes are placed in the exceed token bucket, giving the exceed token bucket 300 bytes.

If the arriving packet is 1000 bytes, the packet conforms because enough bytes are available in the conform token bucket. The conform action (transmit) is taken by the packet and 1000 bytes are removed from the conform token bucket (leaving 0 bytes).

If the next packet arrives 0.20 seconds later, 200 bytes are added to the token bucket (0.20 * 1000/0.0). Therefore, the conform bucket now has 200 bytes. If the arriving packet is 400 bytes, the packet does not conform because only 200 bytes are available in the conform bucket. Similarly, the packet does not exceed because only 300 bytes are available in the exceed bucket. Therefore, the packet violates and the violate action (drop) is taken.

Related Commands	Command	Description
	police (percent)	Configures traffic policing on the basis of a percentage of bandwidth available on an interface.
	police (bps [burst])	Configures traffic policing using two rates, the committed information rate (CIR) and the peak information rate (PIR).
	policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.
	service-policy (policy-map class)	Creates a service policy that is a quality of service (QoS) policy within a policy map.
	show policy-map	Displays information about the policy map.
	show policy-map interface	Displays the statistics and configurations of the input and output policies that are attached to an interface.

police (percent)

To configure traffic policing on the basis of a percentage of bandwidth available on an interface, use the **police** command in Qos policy-map class configuration mode. To remove traffic policing from the configuration, use the **no** form of this command.

police cir *percent* **pir** *percent* [**conform-burst** *in-msec*] [**pir-percent** *percentage*] [**be** *peak-burst-msec*]

no police cir percent *percent* [**be** *conform-burst-in-msec*] [**pir-percent** *percentage*] [**be** *peak-burst-msec*]

Syntax Description

cir	Committed information rate. Indicates that the CIR will be used for policing traffic.
percent	Specifies that a percentage of bandwidth will be used for calculating the CIR.
percent	Specifies the bandwidth percentage. Valid range is a number from 1 to 100.
bc	(Optional) Conform-burst (bc) size used by the first token bucket for policing traffic.
conform-burst-in-msec	(Optional) Specifies the bc value in milliseconds. Valid range is a number from 1 to 2000.
pir	(Optional) Peak information rate (PIR). Indicates that the PIR will be used for policing traffic.
percent	(Optional) Specifies that a percentage of bandwidth will be used for calculating the PIR.
percent	(Optional) Specifies the bandwidth percentage. Valid range is a number from 1 to 100.
be	(Optional) Peak-burst (be) size used by the second token bucket for policing traffic.
peak-burst-in-msec	(Optional) Specifies the be size in milliseconds. Valid range is a number from 1 to 2000.
action	Action to take on packets. Specify one of the following keywords: • **drop**—Drops the packet. • **set-cos-transmit** *new-cos*—Sets the class of services (CoS) value to a new value and send the packet. The range is 0 to 7. • **set-dscp-transmit** *value*—Sets the IP differentiated services code point (DSCP) value and transmit the packet with the new IP DSCP value setting. • **set-prec-transmit** *value*—Sets the IP precedence and transmits the packet with the new IP precedence value setting. • **transmit**—Transmits the packet. The packet is not altered.

Command Default

This command is disabled by default.

Command Modes Policy-map class configuration mode

Usage Guidelines This command calculates the CIR and PIR on the basis of a percentage of the maximum amount of bandwidth available on the interface. When a policy map is attached to the interface, the equivalent CIR and PIR values in bits per second (bps) are calculated on the basis of the interface bandwidth and the percent value entered with this command. The **show policy-map interface** command can then be used to verify the bps rate calculated.

The calculated CIR and PIR bps rates must be in the range of 32,000 and 32,000,000,000 bps. If the rates are outside this range, the associated policy map cannot be attached to the interface. If the interface bandwidth changes (for example, more is added), the bps values of the CIR and the PIR are recalculated automatically on the basis of the new bandwidth. If a policy map is attached to an interface and after the policy map is attached to the interface, the bps values of the CIR and PIR are recalculated.

This command also allows you to specify the values for the conform burst rize and the peak burst rize in milliseconds. If you want bandwidth to be calculated as a percentage, the conform burst rize and the peak burst rize must be specified in milliseconds (ms).

Examples This example shows how to configure traffic policing using a CIR and a PIR based on a percentage of bandwidth on Gigabit interface 6/2. In this example, a CIR of 20 percent and a PIR of 40 percent have been specified. Additionally, exceptional by value and tw value (200 ms and 400 ms, respectively) have been specified.

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# policy-map policy1
Switch(config-pmap)# class-map class1
Switch(config-pmap-c)# police cir percent 20 br 3 ms pir percent 40 be 1 ms
Switch(config-pmap-c)# exit
Switch(config)# interface gigabitethernet 6/2
Switch(config-if)# service-policy output policy
Switch(config-if)# end
```

police rate

To configure single-or dual-rate policer, use the **police rate** command in policy-map configuration mode. To remove traffic policing from the configuration, use the **no** form of this command.

Syntax for Bytes Per Second

police *rate-action* **bps** [*burst-bytes-in-bytes-bytes*] [**peak-rate** *peak-rate-in-bps-bps*] [**peak-burst** *peak-burst-in-bytes-bytes*]

no police *rate-action* **bps** [*burst-bytes-in-bytes-bytes*] [**peak-rate** *peak-rate-in-bps-bps*] [**peak-burst** *peak-burst-in-bytes-bytes*]

Syntax for Percent

police *rate-action* **percent** *percentage* [**burst** *ms-ms*] [**peak-rate** *percent percentage*] [**peak-burst** *ms-ms*]

no police *rate-action* **percent** *percentage* [**burst** *ms-ms*] [**peak-rate** *percent percentage*] [**peak-burst** *ms-ms*]

Syntax Description	*action* Specifies the traffic policer rate-in bits per second. Valid range is 32,000 to 2,000,000,000.
	bps (Optional) Bits per second (bps) will be used to determine the rate at which traffic is policed.
	Note If *action* is not specified, traffic is policed via bps.
	burst *burst-in-bytes-bytes* (Optional) Specifies the burst size, in bytes, will be used for policing traffic. Valid range is from 64 to 2,500,625,536.
	peak-rate *peak-rate-in-bps-bps* (Optional) Specifies the peak burst value, in bytes, for the peak rate. Valid range is from 32,000 to 32,000,000,000.
	peak-burst *peak-burst-in-bytes-bytes* (Optional) Specifies the peak burst value, in bytes, will be used for policing traffic. If the police rate is specified in bps, the valid range of values is 64 to 2,500,625,536.
	percent (Optional) A percentage of interface bandwidth will be used to determine the rate at which traffic is policed.
	percentage (Optional) Bandwidth percentage. Valid range is a number from 1 to 100.
	burst *ms-ms* (Optional) Burst size, in milliseconds, will be used for policing traffic. Valid range is a number from 1 to 2,000.
	peak-rate *percent percentage* (Optional) Peak burst size, in percentage of interface bandwidth will be used to determine the PIR. Valid range is a number from 1 to 100.
	peak-burst *ms-ms* (Optional) Peak burst size, in milliseconds, will be used for policing traffic. Valid range is a number from 1 to 2,000.

Command Default This command is disabled by default.

Command Modes Policy-map configuration mode

Usage Guidelines Use the **police rate** command to limit traffic on the basis of pps, bps, or a percentage of interface bandwidth.

If the **police rate** command is issued, but the a rate is not specified, traffic that is destined will be policed on the basis of bps.

Examples This example shows how to configure policing on a class to limit traffic to an average rate of 1,500,000 bps:

```
Switch(config)# class-map c1
Switch(config-cmap)# match access-group 140
Switch(config-cmap)# exit
Switch(config)# policy-map p1
Switch(config-pmap)# class c1
Switch(config-pmap-c)# police rate 1500000 burst 500000
Switch(config-pmap-c)# exit
```

Related Commands

Command	Description
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.
show policy-map	Displays information about the policy map.

police (two rates)

To configure traffic policing using two rates, the committed information rate (CIR) and the peak information rate (PIR), use the **police** command in policy-map configuration mode. To remove two-rate traffic policing from the configuration, use the **no** form of this command.

police *cir* [**bc** *conform-burst*] *pir pir* [**be** *peak-burst*] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]]

no police *cir cir* [**bc** *conform-burst*] *pir pir* [**be** *peak-burst*] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]]

Syntax Description

cir	Committed information rate (CIR) at which the first token bucket is updated. Specifies the CIR value in bits per second. The value is a number from 32,000 to 32,000,000.0000.
bc	(Optional) Conform burst (bc) (or used by the first token bucket for policing).
conform-burst	(Optional) Specifies the bc value in bytes. The value is a number from 64 to 2,096,128.256.
pir	Peak information rate (PIR) at which the second token bucket is updated.
pir	Specifies the PIR value in bits per second. The value is a number from 32,000 to 32,000,000.0000.
be	(Optional) Peak burst (be) (or used by the second token bucket for policing).
peak-burst	(Optional) Specifies the peak burst (be) in bytes. The value is a number from 64 to 2,096,128.256.
conform-action	(Optional) Action to take on packets that conform to the CIR and PIR.
exceed-action	(Optional) Action to take on packets that conform to the PIR but not the CIR.
violate-action	(Optional) Action to take on packets exceed the PIR.
action	(Optional) Action to take on packets. Specify one of the following keywords:
	• **drop**—Drops the packet.
	• **set-cos-transmit** *new-cos*—Sets the class of services (CoS) value to a new value and send the packet. The range is 0 to 7.
	• **set-dscp-transmit** *new-dscp*—Sets the DF differentiated services code point (DSCP) value and sends the packet with the new DF DSCP value paired.
	• **set-prec-transmit** *new-prec*—Sets the IP precedence and sends the packet with the new IP precedence value setting.
	• **transmit**—Sends the packet with no alteration.

Command Default This command is disabled by default.

Command Modes Policy-map configuration mode

Usage Guidelines

Refer to RFC 2698-Two Rate Three Color Marker.

Two-rate traffic policing uses two token buckets—Tc and Tp—for policing traffic at two independent rates. Note the following points about the two token buckets:

- The Tc token bucket is updated at the CIR value each time a packet arrives at the two-rate policer. The Tc token bucket can contain up to the confirm burst (Bc) value.
- The Tp token bucket is updated at the PIR value each time a packet arrives at the two-rate policer. The Tp token bucket can contain up to the peak burst (Be) value.

Updating Token Buckets

The following scenario illustrates how the token buckets are updated:

A packet of 80 bytes arrives at time t. The last packet arrived at time t1. The CIR and the PIR token buckets at time t are represented by Tc(t) and Tp(t), respectively. Using these values and its time variation, the token buckets are updated as follows:

$$Tc(t) = min(CBR * (t-t1) + Tc(t1), Bc)$$

$$Tp(t) = min(PBR * (t-t1) + Tp(t1), Be)$$

Marking Traffic

The two-rate policer marks packets as either conforming, exceeding, or violating a specified rate. The following points (using a packet of 8 bytes) illustrate how a packet is marked:

- If B > Tp(t), the packet is marked as violating the specified rate.
- If B > Tc(t), the packet is marked as exceeding the specified rate, and the Tp(t) token bucket is updated as Tp(t) = Tp(t) - B.

Otherwise, the packet is marked as conforming to the specified rate, and both token buckets—Tc(t) and Tp(t)—are updated as follows:

$$Tp(t) = Tp(t) - B$$

$$Tc(t) = Tc(t) - B$$

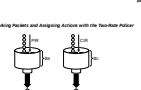
For example, if the CIR is 100 kbps, the PIR is 200 kbps, and a data stream with a rate of 250 kbps arrives at the two-rate policer, the packet would be marked as follows:

- 100 kbps would be marked as conforming to the rate.
- 100 kbps would be marked as exceeding the rate.
- 50 kbps would be marked as violating the rate.

Marking Packets and Assigning Actions Hierarchy

The flowchart in Figure 2-1 illustrates how the two-rate policer marks packets and assigns a corresponding action (that is, violate, exceed, or conform) to the packet.

Figure 2-1 Marking Packets and Assigning Actions with the Two-Rate Policer


PIR
CIR
PBR
CBR
B > TP
B > TC
Yes
No
Yes
No
Packet of size B
Yes
No
Violate
Exceed
Conform
Action
Action
Action
Action
2
3
1
2
3
1
2
3
1

```
Switch#show policy-map=- policy1

  Class-map: police (match all)
    0 packets, 0 bytes, 0 bytes
    30 seconds offered rate 1248000 bps, drop rate 248000 bps
    Match: access-group 101
    police:
        cir 500000 bps, conform-burst 10000, pir 1000000, peak-burst 130000
        conformed 39938 packets, 14248248 bytes; action: transmit
        exceeded 39938 packets, 14248248 bytes; action: set-prec-transmit 2
        violated 39731 packets, 7313824 bytes; action: drop
        conformed 499800 bps, exceed 500000 bps violate 248000 bps

  Class-map: class-default (match-any)
    0 packets, 0 bytes, 0 bytes
    30 seconds offered rate 0 bps, drop rate 0 bps
    Match: any
Switch#
```

The two-rate policer marks 500 kbps of traffic as conforming, 500 kbps of traffic as exceeding, and 250 kbps of traffic as violating the specified rate. Packets marked as conforming to the rate will be sent as is, and packets marked as exceeding the rate will be marked with IP Precedence 2 and then sent. Packets marked as violating the rate are dropped.

policy-map

To create or modify a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode, use the **policy-map** global configuration command. To delete an existing policy map and to return to global configuration mode, use the **no** form of this command.

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.	
Command Modes	Global configuration mode	

Usage Guidelines

Before configuring 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 or modified. After you enter the **policy-map** command, the switch enters policy-map configuration mode. You can configure or modify the class policies for that policy map and decide how to treat the classified traffic.

These configuration commands are available in policy-map configuration mode:

- **class**—Defines the classification match criteria for the specified class map. For more information, see the "class" section on page 2-64.
- **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.

To return to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

You can configure class policies in a policy map only if the classes have match criteria defined for them. To configure the match criteria for a class, use the **class-map** global configuration and **match** class-map configuration commands.

Examples

This example shows how to configure multiple classes in a policy map called policymap2:

```
Switch(config)#policy-map policymap2
Enter policy-map name(policymap2)
Switch(config-pmap)#class class1
Switch(config-pmap-c)#police 48000 2048 exceed-action
Switch(config-pmap-c)#set ip dscp 3
Switch(config-pmap-c)#set cos-transmit 5
Switch(config-pmap-c)#exit
Switch(config-pmap)#class class2
Switch(config-pmap-c)#police cir 128000 pir 256000 conform-action transmit exceed-action
Switch(config-pmap-c)#set dscp-transmit cs1 violate-action drop
```

```
Switch(config)#policy-map pm1a
Switch(config-pm)#class class1
Switch(config-pm-c)#no dump cos0
Switch(config-pm-c)#exit
Switch#
```

This example shows how to delete the policy-map called policymap2:

```
Switch#configure terminal
Switch(config)# no policy-map policymap2
Switch#
```

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

Related Commands	Command	Description
	class	Specifies the name of the class whose traffic policy you want to create or change.
	class-map	Creates a class map to be used for matching packets to the class whose name you specify and to enter class-map configuration mode.
	policy-map	Creates or modifies a policy map that can be attached to one or more ports to specify a service policy and to enter policy-map configuration mode.
	service-policy (interface configuration)	Attaches a policy map to an interface or applies different QoS policies on VLANs that an interface belongs to.
	show policy-map	Displays information about the policy map.

port-channel load-balance

To set the load-distribution method among the ports in the bundle, use the **port-channel load-balance** command. To reset the load distribution to the default, use the **no** form of this command.

port-channel load-balance *method*

no port-channel load-balance

Syntax Description	*method* Specifies the load distribution method. See the "Usage Guidelines" section for more information.
Defaults	Load distribution on the source XOR destination IP address is enabled.
Command Modes	Global configuration mode

Usage Guidelines

The following values are valid for the load-distribution method:

- **dst ip**—Load distribution on the destination IP address
- **dst mac**—Load distribution on the destination MAC address
- **dst port**—Load distribution on the destination TCP/UDP port
- **src dst ip**—Load distribution on the source XOR destination IP address
- **src dst mac**—Load distribution on the source XOR destination MAC address
- **src dst port**—Load distribution on the source XOR destination TCP/UDP port
- **src ip**—Load distribution on the source IP address
- **src mac**—Load distribution on the source MAC address
- **src port**—Load distribution on the source port

Examples

This example shows how to set the load-distribution method to the destination IP address:

```
Switch(config)# port-channel load-balance dst-ip
Switch(config)#
```

This example shows how to set the load-distribution method to the source XOR destination IP address:

```
Switch(config)# port-channel load-balance src-dst-port
Switch(config)#
```

Related Commands

Command	Description
interface port-channel	Accesses or creates a port-channel interface.
show etherchannel	Displays EtherChannel information for a channel.

port-channel standalone-disable

To disable the EtherChannel standalone option in a port channel, use the **port-channel standalone-disable** command in interface configuration mode. To enable this option, use the no form of this command.

port-channel standalone-disable

no port-channel standalone-disable

Syntax Description This command has no arguments or keywords.

Defaults The standalone option is disabled.

Command Modes Interface configuration mode

Usage Guidelines This command can only be used when the port channel protocol type is Link Aggregation Control Protocol (LACP). It allows you to change the current behavior when a physical port cannot bundle with an LACP EtherChannel.

Examples The following example shows how to enable the EtherChannel standalone option in a port channel:

```
Switch(config)# no port-channel standalone-disable
```

Related Commands

Command	Description
show etherchannel	Displays EtherChannel information for a channel.

port-security mac-address

To configure a secure address on an interface for a specific VLAN or VLAN range, use the **port-security mac-address** command.

port-security mac-address *mac_address*

Syntax Description	*mac_address* The MAC address that needs to be secured.
Command Modes	VLAN-range interface submode
Usage Guidelines	Layer 2 interfaces can be part of multiple VLANs (for example, a typical trunk port). In conjunction with the **vlan** command, you can use the **port-security mac-address** command to specify different addresses on different VLANs.
Examples	This example shows how to configure the secure address 1.1.1 on interface Gigabit Ethernet 1/1 for VLANs 2-3:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport port-security maximum dotq
Switch(config-if)# switchport mode trunk
Switch(config-if)# vlan 2-3
Switch(config-if-vlan-range)# port-security mac-address 1.1.1
Switch(config-if-vlan-range)# end
Switch#
```

Related Commands	Command	Description
	port-security mac-address sticky	Configures a sticky address on an interface for a specific VLAN or VLAN range.
	port-security maximum	Configures the maximum number of addresses on an interface for a specific VLAN or VLAN range.

port-security mac-address sticky

To configure a sticky address on an interface for a specific VLAN or VLAN range, use the **port-security mac-address sticky** command.

port-security mac-address sticky *mac_address*

Syntax Description	*mac_address* The MAC address that needs to be secured.

Command Modes VLAN-range interface submode

Usage Guidelines The Sticky feature must be enabled on an interface before you can configure the **port-security mac-address sticky** command.

Usage Guidelines Layer 2 interfaces can be part of multiple VLANs (for example, a typical trunk port). In conjunction with any **vlan** command, you can use the **port-security mac-address sticky** command to specify different sticky addresses on different VLANs.

The Sticky feature must be enabled on an interface before you can configure the **port-security mac-address sticky** command.

Sticky MAC addresses are addresses that persist across switch reboots and link flaps.

Examples This example chees how to configure the sticky address 1.1.1 on interface Gigabit Ethernet 1/1 for VLANs 2-5:

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# vlan 2-5
Switch(config-if-vlan-range)# port-security mac-address sticky 1.1.1
Switch(config-if-vlan-range)# end
Switch#
```

Related Commands	**Command**	**Description**
	port-security mac-address	Configures a secure address on an interface for a specific VLAN or VLAN range.
	port-security maximum	Configures the maximum number of addresses on an interface for a specific VLAN or VLAN range.

port-security maximum

To configure the maximum number of addresses on an interface for a specific VLAN or VLAN range, use the **port-security maximum** command.

port-security maximum *max_value*

Syntax Description	*max_value* The maximum number of MAC addresses.
Command Modes	VLAN-range interface submode
Usage Guidelines	Layer 2 interfaces can be part of multiple VLANs (for example, a trunk port). In conjunction with the **switchport port-security maximum** command to specify the maximum number of secure addresses on different VLANs. If a specific VLAN on a port is not configured with a maximum value, the maximum configured for the port applies for that VLAN. In this situation, the number of MAC addresses that can be secured on that VLAN is limited to the maximum value configured on the port. Each VLAN can be configured with a maximum value that is greater than the value configured on the port. In this case, the port can accommodate secure addresses on the VLAN up to the maximum configured for the port. In either of these situations, the number of MAC addresses secured on each VLAN is limited to the lesser of the VLAN configuration maximum and the port configuration maximum.

Examples	This example shows how to configure a maximum number of addresses (5) on interface Gigabit Ethernet 3/1 in VLANs 2-5:
	`Switch#configure terminal`
	`Enter configuration commands, one per line. End with CNTL/Z.`
	`Switch(config)#interface gig3/1`
	`Switch(config-if)#switchport trunk encapsulation dot1q`
	`Switch(config-if)#switchport mode trunk`
	`Switch(config-if)#vlan 2-5`
	`Switch(config-if-vlan-range)#port-security maximum 5`
	`Switch(config-if-vlan-range)#end`
	`Switch#`

Related Commands	Command	Description
	port-security max-address	Configures a secure address on an interface for a specific VLAN or VLAN range.
	port-security max-address sticky	Configures a sticky address on an interface for a specific VLAN or VLAN range.

power dc input

To configure the power DC input parameters on the switch, use the **power dc input** command. To return to the default power settings, use the **no** form of this command.

power dc input *watts*

no power dc input

Syntax Description

watts	Sets the total capacity of the external DC source in watts; valid values are from 200 to 8500.

Defaults

DC power input is 2500 W.

Command Modes

Global configuration mode

Usage Guidelines

If your interface is not capable of supporting Power over Ethernet, you will receive this message:

```
Power over Ethernet not supported on interface admin
```

Examples

This example shows how to set the total capacity of the external DC power source to 5000 W:

```
Switch(config)# power dc input 5000
Switch(config)#
```

Related Commands

Command	Description
show power	Displays information about the power status.

power efficient-ethernet auto

To enable EEE, use the **power efficient-ethernet auto** command. To disable EEE, use the **no** form of this command.

power efficient-ethernet auto

no power efficient-ethernet auto

Syntax Description This command has no arguments or keywords.

Defaults EEE is disabled

Command Modes Global configuration mode

Usage Guidelines EEE is supported on WS-X4748-UPOE+E and WS-X4748-RJ45-E.

EEE defines support for physical layer devices (PHYs) to operate in Low Power Idle (LPI) mode. When enabled, EEE supports QUIET times during low link utilization allowing both sides of a link to disable portions of each PHY operating circuitry and save power. This functionality is provided per port and is not enabled by default. To avoid issues with EEE functionality on any port during run-time, Cisco provides the **power efficient-ethernet auto** command to enable or disable EEE.

Because EEE relies on Auto Negotiation prior to determine whether to activate EEE, the port must initially enable auto negotiation. Furthermore, EEE is the correct action provided the speed is auto 1000M, auto 100M, or auto 10M and 100M. 10M (either auto or forced mode) does not require EEE for power saving.

Examples This example shows how to enable EEE:

```
Switch(config)# conf t
Switch(config)# interface gigabitethernet 1/1
Switch(config-if)# power efficient-ethernet auto
Switch(config-if)# exit
```

power inline

Toset the inline-power state for the inline-power-capable interfaces, use the **power inline** command. To return to the default values, use the **no** form of this command.

power inline {**auto** | **static** *milliwatt*} | **never** | **static** [**max** *milliwatt*] | **consumption** *milliwatt*}

no power inline

Syntax Description

auto	Sets the Power over Ethernet state to *auto mode for inline-power-capable* interfaces.
max *milliwatt*	(Optional) Sets the maximum power that the equipment can consume; valid range is from 2000 to 15400 mW for classic modules. For the WS-X6848-RJ45V-E, the maximum is 20000. For the WS-X6848-RJ45V-E, the maximum is 30000.
never	Disables both the detection and power for the inline-power-capable interfaces.
static	Allocates power statically.
consumption *milliwatt*	Sets power allocation per interface; valid range is from 4000 to 15400 for classic modules. Any non-default value disables automatic adjustment of power allocation.

Defaults

The default settings are as follows:

- Auto mode for Power over Ethernet is set.
- Maximum mW mode is set to 15400. For the WS-X6848-RJ45V-E, the maximum mW is set to 20000. For the WS-X6848-RJ45V-E, the maximum mW is set to 30000.
- Default allocation is set is 15400.

Command Modes

Interface configuration mode

Usage Guidelines

If your interface is not capable of supporting Power over Ethernet, you will receive this message:

```
Power over Ethernet not supported on interface admin
```

Examples

This example shows how to set the inline-power detection and power for the inline-power-capable interfaces:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet 4/5
Switch(config-if)# power inline auto
Switch(config-if)# exit
Switch#
```

This example shows how to disable the inline-power detection and power for the inline-power-capable interface:

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface fastethernet 4/1
Switch(config-if)#no power inline never
Switch(config-if)#no shut
Switch#
```

This example shows how to set the permanent Power over Ethernet allocation to 8000 mW for Fast Ethernet interface 4/1 regardless what is mandated either by the 802.3af class of the discovered device or by any CDP packet that is received from the powered device:

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface fastethernet 4/1
Switch(config-if)#power inline consumption 8000
Switch(config-if)#no shut
Switch#
```

This example shows how to pre-allocate Power over Ethernet to 16500 mW for Gigabit Ethernet interface 2/1 regardless of what is mandated either by the 802.3af class of the discovered device or by any CDP packet that is received from the powered device:

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface gigabitethernet 2/1
Switch(config-if)#power inline static max 16500
Switch(config-if)#no shut
Switch#
```

Related Commands	Command	Description
	show power	Displays information about the power inline.

power inline consumption

Text the default power that is allocated to an interface for all the inline-power-capable interfaces on the switch, use the **power inline consumption** command. To return to the default values, use the **no** form of this command.

power inline consumption default *milliwatts*

no power inline consumption default

Syntax Description	**default**	Specifies the switch to use the default allocation.
	milliwatts	Sets the default power allocation in milliwatts; the valid range is from 4000 to 15,399. Any non-default value disables automatic adjustment of power allocation.

Defaults

Milliwatt mode is set to 15400.

Command Modes

Global configuration mode

Usage Guidelines

The **inline power consumption** command overrides the power allocated to the port through IEEE Class power discovery and CDP/LLDP power negotiation. To guarantee safe operation of the system, ensure that the value configured here is no less than the actual power requirement of the attached device. If the power drawn by the inline powered devices exceeds the capability of the power supply, it could trip the power supply.

If your interface is not capable of supporting Power over Ethernet, you will receive this message:

```
Power over Ethernet not supported on interface inline
```

Examples

This example shows how to set the Power over Ethernet allocation to use 8000 mW, regardless of any CDP packet that is received from the powered device:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# power inline consumption default 8000
Switch(config)# end
Switch#
```

Related Commands

Command	Description
power inline	Sets the inline-power state for the inline-power-capable interfaces.
show power	Displays information about the power status.

power inline four-pair forced

To automatically enable power on both signal and spare pairs from a switch port, provided the end-device is PoE-capable on both signal and spare pairs but does not support the CDP or LLDP extensions required for UPOE, use the **power inline four-pair forced** command.

power inline four-pair forced

Syntax Description This command has no arguments or keywords.

Defaults None

Command Modes Interface configuration mode

Usage Guidelines Although IEEE 802.3af only provides for power up to 30W per port, the WS-X4748-UPOE+E module can provide up to 60W using the spare pair of an RJ45 cable (wires 4,5,7,8) with the signal pair (wires 1,2,3,6). Power on the spare pair is enabled when the switch port and end-device mutually identify themselves as UPOE-capable using CDP or LLDP and the end-device requests for power on the spare pair to be enabled. When the spare pair is powered, the end-device can negotiate up to 60W power from the switch using CDP or LLDP.

If the end-device is PoE-capable on both signal and spare pairs but does not support the CDP or LLDP extensions required for UPOE, then the following configuration auto-matically enables power on both signal and spare pairs from the switch port

Examples The following example shows how to automatically enable power on both signal and spare pairs from switch port gigabitethernet 2/1:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet 2/1
Switch(config-if)# power inline four-pair forced
Switch(config-if)# exit
Switch(config-if)# no shutdown
Switch(config-if)# end
Switch#
```

Do not enter this command if the end-device is incapable of sourcing inline power on the spare pair or if the end-device supports the CDP or LLDP extensions for UPOE.

power inline logging global

To enable console messages that show when a PoE device has been detected and to show when a PoE device has been removed, use the **power inline logging global** command.

power inline logging global

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Global configuration mode

Usage Guidelines Be aware of the potential for console flooding if this command is used on a switch connected to several PoE devices.

Examples This example shows how to globally enable PoE status messaging on each interface:

To enable PoE event logging, you set the **logging event poe-status global** command:

```
Switch# conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# power inline logging global
Switch(config)# log pilgrim(config)# 5/5
Switch(config-if)# shut
Switch(config-if)# no shut
%PM-5-LINEON:Gi1/5/5: LEGACYDEVICE DETECTED:Interface Gi1/5/5: PD removed
Switch(config-if)# no shut
Switch(config-if)# no shut
%PM-5-LINEON:Gi1/5/5: LEGACYDEVICE DETECTED:Interface Gi1/5/5: Power Inline detected: IEEE PD
```

Related Commands

Command	Description
logging event link-status global (global configuration)	Changes the default switch-wide global link-status event messaging settings.

power inline police

To configure Power over Ethernet policing on a particular interface, use the **power inline police** command. The **no** form of the command disables PoE policing on an interface.

power inline police [**action**] [**evoidable** | **log**]

no power inline police [**action**] [**evoidable** | **log**]

Syntax Description	**action** (Optional) Specifies the action to take on the port when a PoE policing fault occurs (the device evacuates power from it's allocated). **evoidable** (Optional) Enables PoE policing on the interface and places the port in an evoidable state when a PoE policing fault occurs. **log** (Optional) Enables PoE policing on the interface and, if a PoE policing fault occurs, shuts, restarts the port, and logs an error message.
Defaults	PoE policing is disabled.
Command Modes	Interface configuration mode

Usage Guidelines

If a port is in the evoidable state because of a PoE policing fault, enter the **shut** command followed by a **no shut** on the interface to make the port operational again.

You can also configure inline-power evoidable autorecovery so that an evoidable interface is automatically revived when the evoidable autorecovery timer expires.

Examples

This example shows how to enable PoE policing and configure a policing action:

```
Switch>enable|0 | sw pipg6ch10ethernet 2/2
Switch>enable|0 | power inline police
Switch>enable|0 | sw show power inline police pipg6ch10ethernet 2/2
Available:147.0(w)  Used:0(w)  Remaining:147.0(w)

Interface Admin  Oper       Admin   Oper       Cutoff  Oper
          Status Priority    Police  Police     Power   Power
--------- ------ --------    ------  ------     ------  ------
Gi2/1     auto   on          evoidable ok       17.4    7.4

Switch>enable|0 | power inline police action log
Available:147.0(w)  Used:0(w)  Remaining:147.0(w)

Interface Admin  Oper       Admin   Oper       Cutoff  Oper
          Status Priority    Police  Police     Power   Power
--------- ------ --------    ------  ------     ------  ------
Gi2/1     auto   on          log     ok         17.4    8.4
```

Related Commands	Command	Description
	errdisable recovery	Enables errdisable autorecovery; the port automatically reinstates itself after going to the errdisable state after its errdisable autorecovery timer expires.
	show power inline police	Displays the PoE policing status of an interface, module, or chassis.

power redundancy-mode

To configure the power settings for the chassis, use the **power redundancy-mode** command. To return to the default setting, use the **default** form of this command.

power redundancy-mode {**redundant** | **combined**}

default power redundancy-mode

Syntax Description

redundant	Configures the switch to redundant power management mode
combined	Configures the switch to combined power management mode

Defaults

Redundant power management mode

Command Modes

Global configuration mode

Usage Guidelines

The two power supplies must be the same type and wattage.

Caution If you have power supplies with different types or wattages installed in your switch, the switch will not recognize one of the power supplies. A switch set to redundant mode will not have power redundancy. A switch set to combined mode will use only one power supply.

In redundant mode, the power from a single power supply must provide enough power to support the switch configuration.

Table 2-9 lists the maximum available power for chassis and Power over Ethernet for each power supply.

Table 2-9 Available Power

Power Supply	Redundant Mode (W)	Combined Mode (W)
1000 W AC	System[1] = 1000 Inline = 0	System = 1667 Inline = 0
2800 W AC	System = 1360 Inline = 1400	System = 2473 Inline = 2333

1. The system power includes power for the supervisor engines, all modules, and the fan tray.

Examples

This example shows how to set the power management mode to combined:

```
Switch(config)# power redundancy-mode combined
Switch(config)#
```

Related Commands

Command	Description
show power	Displays information about the power status.

pppoe intermediate-agent (global)

To enable the PPPoE Intermediate Agent feature on a switch, use the **pppoe intermediate-agent** global configuration command. To disable the feature, use the **no** form of this command.

pppoe intermediate-agent

no pppoe intermediate-agent

Syntax Description This command has no arguments or keywords.

Defaults disabled

Command Modes Global configuration mode

Usage Guidelines You must enable PPPoE Intermediate Agent globally on a switch before you can use PPPoE Intermediate Agent on an interface or interface VLAN.

Examples This example shows how to enable PPPoE Intermediate Agent on a switch:

```
Switch(config)# pppoe intermediate-agent
```

This example shows how to disable PPPoE Intermediate Agent on a switch:

```
Switch(config)# no pppoe intermediate-agent
```

Related Commands

Command	Description
pppoe intermediate-agent (global)	Sets the access node identifier, generic error message, and circuit/remote string for a switch.

pppoe intermediate-agent (interface)

Note This command takes effect only if you enable the **pppoe intermediate-agent** global command.

To enable the PPPoE Intermediate Agent feature on an interface, use the **pppoe intermediate-agent** command. To disable the feature, use the **no** form of this command.

pppoe intermediate-agent

no pppoe intermediate-agent

Syntax Description This command has no arguments or keywords.

Defaults Disabled on all interfaces.

Command Modes Interface configuration mode

Usage Guidelines PPPoE Intermediate Agent is enabled on an interface provided the PPPoE Intermediate Agent is enabled both on the switch and the interface.

Examples This example shows how to enable the PPPoE Intermediate Agent on an interface:

```
Switch(config-if)# pppoe intermediate-agent
```

This example shows how to disable the PPPoE Intermediate Agent on an interface:

```
Switch(config-if)# no pppoe intermediate-agent
```

Related Commands

Command	Description
pppoe intermediate-agent format-type (interface)	Sets circuit ID or remote ID for an interface.
pppoe intermediate-agent limit-rate	Limits the rate of the PPPoE Discovery packets coming on an interface.
pppoe intermediate-agent trust	Sets the trust configuration of an interface.
pppoe intermediate-agent vendor-tag strip	Enables vendor-tag stripping on PPPoE Discovery packets from PPPoE Server (or BRAS).

pppoe intermediate-agent (interface vlan-range)

Note This command takes effect only if you enable the **pppoe intermediate-agent** global command.

To enable PPPoE Intermediate Agent on an interface VLAN range, use the **pppoe intermediate-agent** global command. To disable the feature, use the **no** form of this command.

```
pppoe intermediate-agent
no pppoe intermediate-agent
```

Syntax Description This command has no arguments or keywords.

Defaults Disabled on all VLANs on all interfaces

Command Modes Interface vlan-range configuration mode

Usage Guidelines Although this command takes effect irrespective of the **pppoe intermediate-agent** (interface configuration mode) command, you must enable the **pppoe intermediate-agent** (global configuration mode) command.

Examples This example shows how to enable PPPoE Intermediate Agent on a range of VLANs:

```
Switch(config)# int vlan-range 147-148
Switch(config-if-vlan-range)# pppoe intermediate-agent
```

This example shows how to disable PPPoE Intermediate Agent on a single VLAN:

```
Switch(config)# int vlan-range 210
Switch(config-if-vlan-range)# no pppoe intermediate-agent
```

Related Commands

Command	Description
pppoe intermediate-agent (interface)	Enables the PPPoE Intermediate Agent feature on an interface.

pppoe intermediate-agent format-type (global)

To set the access-node identifier, generic error message, and identifier string for the switch, use the **pppoe intermediate-agent format-type (global)** command. To disable the feature, use the **no** form of this command:

pppoe intermediate-agent format-type access-node-identifier *string string*

pppoe intermediate-agent format-type generic-error-message *string string*

pppoe intermediate-agent format-type identifier-string *string* **option** {*type*|*type*} **delimiter** {,|;|:|#}

no pppoe intermediate-agent format-type {**access-node-identifier** | **generic-error-message** | **identifier-string**}

Syntax Description

access-node-identifier *string string*	ASCII string literal value for the access-node-identifier.
generic-error-message *string string*	ASCII string literal value for the generic-error-message.
identifier-string *string string*	ASCII string literal value for the identifier-string.
option {*type*|*type*}	Options: **up** = slot + port **vs** = slot + VLAN **pv** = port + VLAN **spv** = slot + port + VLAN
delimiter {,|;|:|#}	Delimiter between the port/VLAN portions of **option**.

Defaults

access-node-identifier has a default value of 0.0.0.0.

generic-error-message, **identifier-string**, **option**, and **delimiter** have no default values.

Command Modes

Global configuration mode

Usage Guidelines

Use the **access-node-identifier** and **identifier-string** commands to enable the switch to generate the circuit-id parameters automatically.

The **no** form of **identifier-string** command unsets the option and delimiter.

Use the **generic-error-message** command to set an error message notifying the sender that the PPPoE Discovery packet was too large.

Examples

This example shows how to set an access-node-identifier:

```
Switch(config)# pppoe intermediate-agent format-type access-node-identifier string
switch-alec-123
```

This example shows how to enter a generic-error-message:

```
Switch(config)# no pppoe intermediate-agent format-type generic-error-message
```

Related Commands

Command	Description
show pppoe intermediate-agent interface	Displays the PPPoE Intermediate Agent configuration and statistics. (packet counters).

pppoe intermediate-agent format-type (interface)

Note This command takes effect only if you enable the **pppoe intermediate-agent** interface configuration command.

To set circuit-id or remote-id for an interface, use the **pppoe intermediate-agent format-type** command. To unset the parameters, use the **no** form of this command.

pppoe intermediate-agent format-type {**circuit-id** | **remote-id**} **string** *string*

no pppoe intermediate-agent format-type {**circuit-id** | **remote-id**} **string** *string*

Syntax Description

circuit-id string *string*	ASCII string literal value for circuit-id.
remote-id string *string*	ASCII string literal value for remote-id.

Defaults

No default values for circuit-id and remote-id.

Command Modes

Interface-configuration mode

Usage Guidelines

Use the **pppoe intermediate-agent format-type** command to set interface-specific circuit-id and remote-id values. If an interface-specific circuit-id is not set, the system's automatic generated circuit-id value is used.

Examples

This example shows how to set remote-id for an interface:

```
Switch(config)# pppoe intermediate-agent format-type remote-id string name0001
```

This example shows how to unset circuit-id for an interface:

```
Switch(config)# no pppoe intermediate-agent format-type circuit-id
```

Related Commands

Command	Description
pppoe intermediate-agent (interface)	Enables the PPPoE Intermediate Agent feature on an interface.
pppoe intermediate-agent (interface vlan-range)	Sets the circuit-id or remote-id for an interface vlan-range.

pppoe intermediate-agent format-type (interface vlan-range)

Note This command takes effect only if you enable the **pppoe intermediate-agent** interface vlan-range configuration mode command.

To set circuit-id or remote-id for an interface vlan-range, use the **pppoe intermediate-agent format-type** interface vlan-range mode command. To unset the parameters, use the **no** form of this on command.

pppoe intermediate-agent format-type {circuit-id | remote-id} string

no pppoe intermediate-agent format-type {circuit-id | remote-id} string

circuit-id string	ASCII string literal value to be set for circuit-id.
remote-id string	ASCII string literal value to be set for remote-id.

Syntax Description

Defaults No default values for circuit-id and remote-id.

Command Modes Interface vlan-range configuration mode

Usage Guidelines Use these commands to set circuit-id or remote-id on an interface vlan-range. If the circuit-id is not set, the system's automatically generated circuit-id is used.

Examples This example shows how to set remote-id on an interface VLAN:

```
Switch(config)# int vlan-range 20
Switch(config-if-vlan-range)#
pppoe intermediate-agent format-type remote-id string user001@040-vmblade
```

This example shows how to unset circuit-id on an interface vlan-range:

```
Switch(config)# int vlan-range 167-168
Switch(config-if-vlan-range)# no pppoe intermediate-agent format-type circuit-id
```

Related Commands

Command	Description
pppoe intermediate-agent (interface vlan-range)	Enables PPPoE Intermediate Agent on an interface VLAN range.

pppoe intermediate-agent limit rate

To limit the rate of the PPPoE Discovery packets arriving on an interface, use the **pppoe intermediate-agent limit rate** command. To disable the feature, use the **no** form of this command.

pppoe intermediate-agent limit rate *number*

no pppoe intermediate-agent limit rate *number*

Syntax Description	*number*	Specifies the threshold rate of PPPoE Discovery packets received on this interface in packets-per-second.

Defaults

This command has no default settings.

Command Modes

Interface configuration mode

Usage Guidelines

If this command is used and the PPPoE Discovery packets that are received exceeds the rate set, the interface will be error-disabled (shutdown).

Examples

This example shows how to set a rate limit for an interface:

```
Switch(config-if)# pppoe intermediate-agent limit rate 50
```

This example shows how to disable rate limiting for an interface:

```
Switch(config-if)# no pppoe intermediate-agent limit rate
```

Related Commands	Command	Description
	pppoe intermediate-agent (interface)	Enables the PPPoE Intermediate Agent feature on an interface

pppoe intermediate-agent trust

To set the trust configuration of an interface, use the **pppoe intermediate-agent trust** global command. To unset the trust parameter, use the **no** form of this command.

pppoe intermediate-agent trust

no pppoe intermediate-agent trust

Syntax Description This command has no arguments or keywords.

Defaults All interfaces are untrusted.

Command Modes Interface configuration mode

Usage Guidelines At least one trusted interface must be present on the switch for PPPoE Intermediate Agent feature to work.

Set the interface connecting the switch to the PPPoE Server (or BRAS) as trusted.

Examples This example shows how to set an interface as trusted:

```
Switch(config-if)# pppoe intermediate-agent trust
```

This example shows how to disable the trust configuration for an interface:

```
Switch(config-if)# no pppoe intermediate-agent trust
```

Related Commands

Command	Description
pppoe intermediate-agent vendor-tag strip	Enables vendor-tag stripping on PPPoE Discovery packets from a PPPoE Server (or BRAS).

pppoe intermediate-agent vendor-tag strip

Note This command takes effect only if you enable the **pppoe intermediate-agent** interface configuration command and the **pppoe intermediate-agent trust** command.

To enable vendor-tag stripping on PPPoE Discovery packets from PPPoE Server (or BRAS), use the **pppoe intermediate-agent vendor-tag strip** command. To disable this setting, use the **no** form of this command.

pppoe intermediate-agent vendor-tag strip

no pppoe intermediate-agent vendor-tag strip

Syntax Description This command has no arguments or keywords.

Defaults vendor-tag stripping is turned off.

Command Modes Interface configuration mode

Usage Guidelines This command has no effect on untrusted interfaces.

Use this command on a PPPoE Intermediate Agent trusted interface to strip off the vendor-specific tags in PPPoE Discovery packets that arrive downstream from the PPPoE Server (or BRAS), if any.

Examples This example shows how to set vendor-tag stripping on an interface:

```
Switch(config-if)# pppoe intermediate-agent vendor-tag strip
```

This example shows how to disable vendor-tag stripping on an interface:

```
Switch(config-if)# no pppoe intermediate-agent vendor-tag strip
```

Related Commands	Command	Description
	pppoe intermediate-agent (interface)	Enables the PPPoE Intermediate Agent feature on an interface.
	pppoe intermediate-agent trust	Sets the trust configuration of an interface.

priority

To enable the strict priority queue (low-latency queueing [LLQ]) and to give priority to a class of traffic belonging to a policy map attached to a physical port, use the **priority** policy-map class configuration command. To return to the default setting, use the **no** form of this command.

priority

no priority

Syntax Description This command has no arguments or keywords.

Defaults The strict priority queue is disabled.

Command Modes Policy-map class configuration mode

Usage Guidelines Use the **priority** command only in a policy map attached to a physical port. You can use this command only in class-level classes, you cannot use this command in class-default.

This command configures LLQ and provides strict-priority queueing. Strict-priority queueing enables delay-sensitive data, such as voice, to be sent before packets in other queues are sent. The priority queue is serviced first until it empty.

You cannot use the **bandwidth**, **dbl**, and the **shape** policy-map class configuration commands with the **priority** policy-map class configuration command in the same class within the same policy map. However, you can use these commands in the same policy map.

You can use **police** or set class configuration commands with the **priority** policy-map class configuration command.

If the priority queueing class is not rate limited, you cannot use the bandwidth command, you can use the bandwidth remaining percent command instead.

Examples This example shows how to enable the LLQ for the policy map called policy1:

```
Switch(config)#interface gigabitethernet 2/1
Switch(config-if)#service-policy output policy1
Switch(config)#policy-map policy1
Switch(config-pmap)# class voice
Switch(config-pmap-c)# priority
```

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

Related Commands

Command	Description
bandwidth	Specifies or modifies the minimum bandwidth pass-thru to a class belonging to a policy map attached to a physical port.
class	Specifies the name of the class whose traffic policy you want to create or change.
dbl	Enables dynamic buffer limiting for traffic hitting this class.
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.
service-policy (policy-map class)	Creates a service policy that is a quality of service (QoS) policy within a policy map.
shape (class-based queueing)	Enables traffic shaping a class of traffic in a policy map attached to a physical port.
show policy-map	Displays information about the policy map.

private-vlan

To configure private VLANs and the association between a private VLAN and a secondary VLAN, use the **private-vlan** command. To return to the default value, use the **no** form of this command.

private-vlan {**isolated** | **community** | **twoway-community** | **primary**}

private-vlan association *secondary-vlan-list* [**add** *secondary-vlan-list* | **remove** *secondary-vlan-list*]

no private-vlan {**isolated** | **community** | **twoway-community** | **primary**}

no private-vlan association

Syntax Description:	**isolated** Designates the VLAN as an isolated private VLAN.
	community Designates the VLAN as the community private VLAN.
	twoway-community Designates the VLAN as a bare port that belongs to a twoway-community secondary VLAN.
	primary Designates the VLAN as the primary private VLAN.
	association Creates an association between a secondary VLAN and a primary VLAN.
	secondary-vlan-list Specifies the number of the secondary VLAN. The list can contain only one isolated VLAN ID; it can also contain multiple community or twoway-community VLAN IDs.
	add (Optional) Associates a secondary VLAN to a primary VLAN.
	remove (Optional) Clears the association between a secondary VLAN and a primary VLAN.

Defaults: Private VLANs are not configured.

Command Modes: VLAN configuration mode

Usage Guidelines: You cannot configure VLANs 1 or VLANs 1001 to 1005 as private VLANs.

VTP does not support private VLANs. You must configure private VLANs on each device where you want private VLAN ports.

The *secondary_vlan_list* parameter cannot contain spaces; it can contain multiple comma-separated items. Each item can be a single private VLAN ID or a range of private VLAN IDs separated by hyphens.

The *secondary_vlan_list* parameter can contain multiple community VLAN IDs.

The *secondary_vlan_list* parameter can continuously use isolated VLAN ID. A private VLAN is defined as a set of private ports characterized by a common set of VLAN number pairs: each pair is made up of at least two special uninfected VLANs and is used by isolated ports or by a community of ports to communicate with the rest.

An isolated VLAN is a VLAN that is used by the isolated ports to communicate with the promiscuous ports. The isolated VLAN traffic is blocked on all other private ports in the same VLAN and can be received only by the standard trunking ports and the promiscuous ports that are assigned to the corresponding primary VLAN.

A community VLAN is the VLAN that carries the traffic among the community ports and from the community ports to the promiscuous ports on the corresponding primary VLAN. A community VLAN is not allowed on a private VLAN trunk.

A promiscuous port is a private port that is assigned to a primary VLAN.

A primary VLAN is a VLAN that is used to convey the traffic from the switches to the customer end stations on the private ports.

You can specify only one isolated vlan-id value, while multiple community VLANs are allowed. You can only associate isolated and community VLANs to one VLAN. The associated VLAN list may not contain primary VLANs. Similarly, a VLAN that is already associated to a primary VLAN cannot be configured as a primary VLAN.

The **private-vlan** commands do not take effect until you exit the config VLAN submode.

If you delete either the primary or secondary VLAN, the ports that are associated with the VLAN become inactive.

Refer to the *Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide* for additional configuration guidelines.

Examples

This example shows how to configure VLAN 202 as a primary VLAN and verify the configuration:

```
Switch(config)#vlan 202
Switch(config-vlan)#private-vlan primary
Switch(config-vlan)# end
Switch# show vlan private-vlan
Primary Secondary Type              Interfaces
------- --------- ----------------- ------------------------------------------
202     -         primary
```

This example shows how to configure VLAN 303 as a community VLAN and verify the configuration:

```
Switch(config)#vlan 303
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# end
Switch# show vlan private-vlan

Primary Secondary Type              Interfaces
------- --------- ----------------- ------------------------------------------
202     -         primary
        303       community
```

This example shows how to configure VLAN 440 as an isolated VLAN and verify the configuration:

```
Switch(config)# vlan 440
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# end
Switch# show vlan private-vlan

Primary Secondary Type              Interfaces
------- --------- ----------------- ------------------------------------------
202     -         primary
```

```
                 303      community
                 440      isolated
```

This example shows how to create a private VLAN relationship among the primary VLAN 14, the isolated VLAN 19, and community VLANs 20 and 21:

```
Switch(config)# vlan 14
Switch(config-vlan)# exit
Switch(config)# vlan 19 private-vlan isolated
Switch(config-vlan)# exit
Switch(config)# vlan 20 private-vlan primary
Switch(config)# vlan 21 private-vlan association 19
```

This example shows how to remove a private VLAN relationship and delete the primary VLAN. The associated secondary VLANs are not deleted.

```
Switch(config-vlan)# no private-vlan 14
Switch(config-vlan)#
```

This example shows how to configure VLAN 510 as a twoway-community VLAN and verify the configuration:

```
Switch(config)# vlan 510
Switch(config-vlan)# vlan 510
Switch(config-vlan)# private-vlan twoway-community
Switch(config-vlan)# end
Switch# show vlan private-vlan

Primary Secondary Type            Interfaces
------- --------- ----------------- ------------------------------------------
510     -         primary
        303       community
        440       isolated
        502       twoway-community
```

This example shows how to associate community VLANs 303 through 307 and 309 and isolated VLAN 440 with primary VLAN 202 and verify the configuration:

```
Switch# configure terminal
Switch(config)# vlan 202
Switch(config-vlan)# private-vlan association 303-307,309,440
Switch(config-vlan)# end
Switch# show vlan private-vlan

Primary Secondary Type            Interfaces
------- --------- ----------------- ------------------------------------------
202     303       community
202     304       community
202     305       community
202     306       community
202     307       community
202     309       community
202     440       isolated
        510       community
```

Note The secondary VLAN 303 has an associated primary VLAN.

This example shows how to remove an isolated VLAN from the private VLAN association:

```
Switch(config)# vlan 14
Switch(config-vlan)# private-vlan association remove 19
Switch(config-vlan)#
```

This example shows how to configure interface FastEthernet 5/1 as a PVLAN host port and verify the configuration:

```
Switch# configure terminal
Enter configuration commands one per line.
Switch(config)# interface fastethernet 5/1
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 202 440
Switch(config-if)# end
Switch# show interface fastethernet 5/1 switchport
Name: Fa5/1
Switchport: Enabled
Administrative Mode: private-vlan host
Operational Mode: private-vlan host
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Appliance trust: none
Administrative Private-vlan
  Host associations: 202 (VLAN0202) 440 (VLAN0440)
  Primary Mapping: none
  Trunk encapsulation : dot1q
  Trunk private vlans:
Operational private-vlan(s):
  Trunk private vlans: (VLAN0440)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
```

Related Commands	Command	Description
	show vlan	Displays VLAN information.
	show vlan private-vlan	Displays private VLAN information.

private-vlan mapping

To create a mapping between the primary and the secondary VLANs so that both share the same primary VLAN SVI, use the **private-vlan mapping** command. To remove all PVLAN mappings from an SVI, use the **no** form of this command.

private-vlan mapping *primary-vlan-id* {[*secondary-vlan-list*] [**add** *secondary-vlan-list*] | **remove** *secondary-vlan-list*}

no private-vlan mapping

Syntax Description	*primary-vlan-id* VLAN ID of the primary VLAN of the PVLAN relationship.
	secondary-vlan-list (Optional) VLAN ID of the secondary VLANs to map to the primary VLAN.
	add (Optional) Maps the secondary VLAN to the primary VLAN.
	remove (Optional) Removes the mapping between the secondary VLAN and the primary VLAN.

Defaults All PVLAN mappings are removed.

Command Modes Interface configuration mode

Usage Guidelines The *secondary_vlan_list* parameter cannot contain spaces. It can contain multiple, comma-separated items. Each item can be a single PVLAN ID or a range of PVLAN IDs separated by hyphens.

This command is valid in the interface configuration mode of the primary VLAN.

The SVI of the primary VLAN is created in Layer 3.

The traffic that is received on the secondary VLAN is routed by the SVI of the primary VLAN.

The SVIs of the existing secondary VLANs do not function and are considered down after this command is entered.

A secondary SVI can be mapped to only one primary SVI. If the configured PVLAN association is different from what is specified in this command (if the specified primary-vlan-id is configured as a secondary VLAN), all the SVIs that are specified in this command are brought down.

If you configure a mapping between two VLANs that do not have a valid Layer 2 association, the mapping configuration does not take effect.

Examples This example shows how to map the interface of VLAN 20 to the SVI of VLAN 18:

```
Switch(config)# interface vlan 18
Switch(config-if)# private-vlan mapping 18 20
Switch(config-if)#
```

This example shows how to permit the routing of the secondary VLAN ingress traffic from PVLANs 303 through 307, 309, and 440 and how to verify the configuration:

```
Switch(config)# interface vlan 18
```

```
Switch(config)# interface vlan 20
Switch(config-if)# private-vlan mapping add 303-307,309,440
Switch(config-if)# end
Switch#sh show interfaces private-vlan mapping
Interface Secondary VLAN Type
--------------------------------------------------
vlan202  303    isolated
vlan202  304    isolated
vlan202  305    isolated
vlan202  306    isolated
vlan202  307    isolated
vlan202  309    isolated
vlan202  440    isolated

Switch#sh
```

This example shows the displayed message that you will see if the VLAN that you are adding is already mapped to the SVI of VLAN 20. You must delete the mapping from the SVI of VLAN 10 first.

```
Switch(config)# interface vlan 10
Switch(config-if)# private-vlan mapping 10 add 21
  Command rejected: The interface for VLAN 21 is already mapped as a secondary.
Switch(config-if)#
```

This example shows how to remove all PVLAN mappings from the SVI of VLAN 10:

```
Switch(config)# interface vlan 10
Switch(config-if)# no private-vlan mapping
Switch(config-if)#
Switch#sh configure terminal
Switch(config)# interface vlan 202
Switch(config-if)# private-vlan mapping add 303-307,309,440
Switch(config-if)# end
Switch#sh show interfaces private-vlan mapping
Interface Secondary VLAN Type
--------------------------------------------------
vlan202  303    community
vlan202  304    community
vlan202  305    community
vlan202  306    community
vlan202  307    community
vlan202  309    community
vlan202  440    isolated

Switch#sh
```

Related Commands	Command	Description
	show interfaces private-vlan mapping	Displays PVLAN mapping information for VLAN SVIs.
	show vlan	Displays VLAN information.
	show vlan private-vlan	Displays private VLAN information.

private-vlan synchronize

To map the secondary VLANs in the same instance as the primary VLAN, use the **private-vlan synchronize** command.

private-vlan synchronize

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes MST configuration mode

Usage Guidelines If you do not map the VLANs in the same instance as the associated primary VLANs when you exit the MST configuration submode, a warning message displays and lists the secondary VLANs that are not mapped to the same instance as the associated primary VLANS. The **private-vlan synchronize** command automatically maps all secondary VLANs to the same instance as the associated primary VLANs.

Examples This example shows how to initialize PVLAN synchronization:

```
Switch(config-mst)# private-vlan synchronize
Switch(config-mst)#
```

This example assumes that a primary VLAN 2 and a secondary VLAN 3 are associated to VL ASN 2, and that all VLANs are mapped to the CIST instance 1. This example also shows the output if you try to change the mapping for the primary VLAN 2 only:

```
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# instance 1 vlan 2
Switch(config-mst)# exit
These secondary vlans are not mapped to the same instances as their primary:
->3
Switch(config)#
```

Related Commands

Command	Description
show spanning-tree mst	Displays MST protocol information.

profile

To enter profile call-home configuration submode, use the **profile** command in call-home configuration mode, use the **profile** command.

profile *profile_name*

Syntax Description

profile_name	Specifies the profile name.

Defaults

This command has no default settings.

Command Modes

cfg-call-home

Usage Guidelines

When you enter the **profile** *profile_name* command in call-home mode, the prompt changes to Switch(cfg-call-home-profile)#, and you have access to the following profile configuration commands:

- **active**
- **destination address**
- **destination message-size-limit bytes**
- **destination preferred-msg-format**
- **destination transport-method**
- **end**
- **exit**
- **subscribe-to-alert-group all**
- **subscribe-to-alert-group configuration**
- **subscribe-to-alert-group diagnostic**
- **subscribe-to-alert-group environment**
- **subscribe-to-alert-group inventory**
- **subscribe-to-alert-group syslog**

Examples

This example shows how to create and configure a user-defined call-home profile:

```
Switch(config)# call-home
Switch(cfg-call-home)# profile user
Switch(cfg-call-home-profile)# destination transport-method http
Switch(cfg-call-home-profile)# destination address http
Switch(cfg-call-home-profile)# destination message-size-limit 3000000
Switch(cfg-call-home-profile)# subscribe-to-alert-group configuration
Switch(cfg-call-home-profile)# subscribe-to-alert-group diagnostic severity minor
Switch(cfg-call-home-profile)# subscribe-to-alert-group environment severity warning
Switch(cfg-call-home-profile)# subscribe-to-alert-group syslog severity notification
pattern *SNMA*
Switch(cfg-call-home-profile)# subscribe-to-alert-group inventory periodic daily 21:02
```

Related Commands

Command	Description
destination address	Configures the destination e-mail address or URL to which Call Home messages will be sent.
destination message-size-limit bytes	Configures a maximum destination message size for the destination profile.
destination preferred-msg-format	Configures a preferred message format.
destination transport-method	Enables the message transport method.
subscribe to alert group all	Subscribes to all available alert groups.
subscribe to alert group configuration	Subscribes this destination profile to the Configuration alert group.
subscribe to alert group diagnostic	Subscribes this destination profile to the Diagnostic alert group.
subscribe to alert group environment	Subscribes this destination profile to the Environment alert group.
subscribe to alert group inventory	Subscribes this destination profile to the Inventory alert group.
subscribe to alert group syslog	Subscribes this destination profile to the Syslog alert group.

qos account layer-all encapsulation

To account for Layer 3 header length of 20 bytes in QoS policing features, use the **qos account layer-all encapsulation** command. To disable the use of additional bytes, use the **no** form of this command.

qos account layer-all encapsulation

no qos account layer-all encapsulation

Syntax Description This command has no arguments or keywords.

Defaults Policers account only for the Layer 2 header length in policing features. In contrast, shapers account for header length as well as IPG in rate calculation.

Command Modes Global configuration

Usage Guidelines Supervisor Engine 6-E, Supervisor Engine 6L-E, Catalyst 4900M, and Catalyst 4948E use the **qos account layer-all encapsulation** command to account for Layer 1 header of 20 bytes (preamble + IPG) and Layer 2 header in policing features. When this command is configured, policer statistics (in bytes) observed in the output of the **show policy-map interface** command reflect the Layer 1 header length as well (20 bytes per packet).

Examples This example shows how to shows how to include IPG in policing:

```
Switch(config)# conf t
Switch(config)# qos account layer-all encapsulation
Switch(config)# end
Switch#
```

Related Commands

Command	Description
show policy-map interface	Displays policer statistics on a specific interface.

qos account layer2 encapsulation

To include additional bytes to be accounted by the QoS features, use the **qos account layer2 encapsulation** command. To disable the use of additional bytes, use the **no** form of this command.

qos account layer2 encapsulation {**arpa** | **dot1q** | **isl** | **length** *bytes*}

no qos account layer2 encapsulation [**arpa** | **dot1q** | **isl**] **length** *bytes*]

Syntax Description

arpa	Specifies the account length of the Ethernet ARPA-encapsulated packet (18 bytes).
dot1q	Specifies the account length of the 802.1Q-encapsulated packet (22 bytes).
isl	Specifies the account length of the ISL-encapsulated packet (48 bytes).
length *bytes*	Specifies the a additional packet length account for, the valid range is from 0 to 64 bytes.

Defaults

The length that is specified in the Ethernet header is considered for both IP and non-IP packets. The Layer 2 length includes the VLAN tag overhead.

Command Modes

Global configuration mode

Usage Guidelines

Shaping and sharing always use Ethernet ARPA length to which 20 bytes of IPv6 overhead is always added for policing. However, only Layer 2 length including VLAN tag overhead is considered.

Note The given length is included when policing all IP packets irrespective of the encapsulation with which it was received. When **qos account layer2 encapsulation** is not configured, a fixed length of 18 bytes is included when policing all IP packets, not only those IP packets that are received with ISL encapsulation.

Sharing and shaping use the length that is specified in the Layer 2 header.

Examples

This example shows how to include an additional 18 bytes when policing IP packets:

```
Switch# conf t
Switch(config)# qos account layer2 encapsulation length 18
Switch(config)# end
Switch#
```

This example shows how to disable the consistent accounting of the Layer 2 encapsulation by the QoS features:

```
Switch# conf t
Switch(config)# no qos account layer2 encapsulation
Switch(config)# end
Switch #
```

Related Commands

Command	Description
show interfaces	Displays traffic on a specific interface.
switchport	Modifies the switching characteristics of a Layer 2 switch interface.
switchport block	Prevents the unknown multicast or unicast packets from being forwarded.

qos trust

To set the trusted state of an interface (for example, whether the packets arriving at an interface are trusted to carry the correct CoS, ToS, and DSCP classifications), use the **qos trust** command. To set an interface to the untrusted state, use the **no** form of this command.

qos trust {**cos** | *device cisco-phone* | **dscp** | **extend** [**cos** *priority*]}

no qos trust {**cos** | *device cisco-phone*| **dscp** | **extend** [**cos** *priority*]}

Syntax Description

cos	Specifies that the CoS bits in incoming frames are trusted and derives the internal DSCP value from the CoS bits.
device cisco-phone	Specifies the Cisco IP phone as the trust device for a port.
dscp	Specifies that the ToS bits in the incoming packets contain a DSCP value.
extend	Specifies to extend the trust to Port VL-AN ID (PVID) packets coming from the PC.
cos *priority*	(Optional) Specifies that the CoS priority value is set to PVID packets; valid values are from 0 to 7.

Defaults

The default settings are as follows:

- If global QoS is enabled, trust is disabled on the port.
- If global QoS is disabled, trust DSCP is enabled on the port.
- The CoS priority level is 0.

Command Modes

Interface configuration mode

Usage Guidelines

This command is not supported on the Supervisor Engine 6-E and Catalyst 4500M chassis.

You can only configure the trusted state on physical LAN interfaces.

By default, the trust state of an interface when QoS is enabled is untrusted; when QoS is disabled on the interface, the trust state is reset to trust DSCP.

When the interface trust state is **qos trust cos**, the transmit CoS is always the incoming packet CoS (or the default CoS for the interface, if the packet is untagged).

When the interface trust state is **qos trust dscp**, the security and QoS ACL classification will always use the internal DSCP derived from the incoming packet DSCP.

Trusted boundary should not be configured on the ports that are part of an EtherChannel (that is, a port channel).

Examples

This example shows how to set the trusted state of an interface to CoS:

```
Switch(config)#int gi1/0/1
Switch(config-if)#qos trust cos
Switch(config-if)#int
```

This example shows how to set the trusted state of an interface to DSCP:

```
Switch(config-if)# qos trust dscp
Switch(config-if)#
```

This example shows how to set the PVID CoS level to 6:

```
Switch(config-if)# qos trust extend cos 6
Switch(config-if)#
```

This example shows how to set the Cisco phone as the trust device:

```
Switch(config-if)# qos trust device cisco-phone
Switch(config-if)#
```

Related Commands

Command	Description
qos cos limit	Defines per-VLAN QoS for a Layer 2 interface.
show qos interface	Displays QoS information for an interface.

queue-limit

To specify or modify the maximum number of packets the queue can hold for a class policy configured in a policy map, use the **queue-limit** command. To remove the queue packet limit from a class, use the nofoorm of this command.

queue-limit *number-of-packets*

no queue-limit *number-of-packets*

Syntax Description	*number-of-packets* Number of packets that the queue for this class can accumulate; valid range is 16 to65 536. This number must be a multiple of 8.
Defaults	By default, each physical interface on a Catalyst 6500 switch has a default queue based on the number of slots in a chassis and the number of ports on the line cards.
Command Modes	QoS policy-map class configuration mode
Usage Guidelines	By default, each physical interface on a Catalyst 6500 switch comes up with a default queue. The size of this queue is based on the number of slots in a chassis as well as the number of ports on the line card that is in the switch. The queue is 256 queue entries of which 100 fit are set aside as a common shardm pool. The remaining 156 fit are equally distributed among the slots. Each slot further divides its allocated queue space into 32 queues. CBQ creates a queue for every class for which a class-map is defined. Packets satisfying the match criterion for a class accumulate in the queue reserved for the class until they are sent, which occurs when the queue is serviced by the fair queuing process. When the maximum packet threshold you defined for the class is reached, queuing of any further packets to the class queue causes tail drop or, if DBL is configured for the class policy, packet drop to take place.
Note	The queue-limit command is supported only after you first configure a scheduling action, such as bandwidth, or priority, except when you configure queue-limit in the class-default class of an output QoS policy-map.

Examples	This example shows how to configure a policy-map called policy11 to contain policy for a class called ac2003. Policy for this class is set so that the queue reserved for it has a maximum packet limit of 40:
	`Router(config)#policy-map policy11`
	`Router(config-pmap)#class ac2003`
	`Router(config-pmap-c)#bandwidth 2000`
	`Router(config-pmap-c)#queue-limit 40`
	`Router(config-pmap-c)#exit`
	`Router(config)`

Related Commands

Command	Description
bandwidth	Specifies or modifies the minimum bandwidth provided to a class belonging to a policy map attached to a physical port.
class	Specifies the name of the class whose traffic policy you want to create or change.
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.
shape (class-based queuing)	Enables traffic shaping a class of traffic on a policy map attached to a physical port.

redundancy

To enter the redundancy configuration mode, use the **redundancy** command in the global configuration mode.

redundancy

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Global configuration mode

Usage Guidelines The redundancy configuration mode is used to enter the main CPU submode.

To enter the main CPU submode, use the **main-cpu** command in the redundancy configuration mode.

The main CPU submode is used to manually synchronize the configurations on the two supervisor engines.

From the main CPU submode, use the **auto-sync** command to enable automatic synchronization of the configuration files in NVRAM.

Use the **no** command to disable redundancy. If you disable redundancy, then rerouting redundancy, the switch reverts to default redundancy settings.

Use the **exit** command to exit the redundancy configuration mode.

Examples This example shows how to enter redundancy mode:

```
Dak(config)#redundancy
Dak(config-red)#exit
Dak(config)#
```

This example shows how to enter the main CPU submode:

```
Dak(config)#redundancy
Dak(config-red)#main-cpu
Dak(config-r-cpu)#
```

Related Commands

Command	Description
auto-sync	Enables automatic synchronization of the configuration files in NVRAM.
main-cpu	Enters the main CPU submode and manually synchronize the configurations on the two supervisor engines.

redundancy config-sync mismatched-commands

To remove the active supervisor engine into the Mismatched Command List (MCL) and resets the standby supervisor engine, use the **redundancy config-sync mismatched-commands** command.

If your active and standby supervisor engines are running different versions of Cisco IOS, some of their CLIs will not be compatible. If such commands are already present in the running configuration of the active supervisor engine and the syncs-check for the command fails at the standby supervisor engine while it is booting, you must move the active supervisor engine into the Mismatched Command List (MCL).

redundancy config-sync {ignore | validate} mismatched-commands

Syntax Description	**ignore**	Ignore the mismatched command list.
	validate	Revalidate the mismatched command list with the modified running-configuration.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

The following is a log-entry example for mismatched commands:

```
00:00:01: Config Sync: Bulk-sync failure due to Servicing Incompatibility. Please check
full list of mismatched commands via:
  show redundancy config-sync failures mcl
Mismatched commands on slot 5/0 rejected from active peer:
interface Gigabitethernet1/1
! rudundant "interface"
! ip address 1.2.3.4 255.0.0.0
! no shutdown
```

To display all mismatched commands, use the **show redundancy config-sync failures** mcl command.

To clean the MCL, remove all mismatched commands from the active supervisor engine's running configuration, revalidate the MCL with a modified running configuration using the **redundancy config-sync validate mismatched-commands** command, then reload the standby supervisor engine.

You could also ignore the MCL by entering the **redundancy config-sync ignore mismatched-commands** command and rebooting the standby supervisor engine; the system changes to SSO mode.

Note If you ignore the mismatched commands, the *out-of-sync* configuration at the active supervisor engine and the standby supervisor engine will exists.

You can verify the ignored MCL with the **show redundancy config-sync ignored mcl** command.

If SSO mode cannot be established between the active and standby supervisor engines because of an incompatibility in the configuration file, a mismatched command list (MCL) is generated at the active supervisor engine and a reload into RPR mode is forced for the standby supervisor engine. Subsequent attempts to reload the standby supervisor engine into SSO mode are suspended and rebooting the standby supervisor engine with the exact same image, might cause the
C6K_REDUNDANCY-2-IOS_VERSION_CMDCK_FAIL and
RMI-3-PEER_IMAGE_INCOMPATIBLE messages to appear because the peer image is listed as incompatible. If the configuration problem can be corrected, you can clear the peer image from the incompatible list with the **redundancy config-sync ignore mismatched-commands** EXEC command while the peer is in a standby cold (RPR) state. This action allows the standby supervisor engine to boot in standby hot (SSO) state when it reloads.

Examples

This example shows how to validate removal of routes from the MCL:

```
Router(config)# redundancy config-sync validate mismatched-commands
Router(config)#
```

Related Commands

Command	Description
show redundancy config-sync	Displays an IOS *c*onfig-*s*ync failure or the *i*gnored *m*ismatched command list (MCL).

redundancy force-switchover

To force a switchover from the active to the standby supervisor engine, use the **redundancy force-switchover** command.

redundancy force-switchover

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Usage Guidelines Before using this command, refer to the "Performing a Software Upgrade" section of the Catalyst 4500 Series Swift Cisco IOS Software Configuration Guide for additional information.

The **redundancy force-switchover** command conducts a manual switchover to the redundant supervisor engine. The redundant supervisor engine becomes the new active supervisor engine running the Cisco IOS image. The modules are reset.

The old active supervisor engine reboots with the new image and becomes the standby supervisor engine.

Examples This example shows how to switch over manually from the active to the standby supervisor engine:

```
Router#redundancy force-switchover
Router#
```

Related Commands

Command	Description
redundancy	Enters the redundancy configuration mode.
show redundancy	Displays redundancy facility information.

redundancy reload

To force a reload of one or both supervisor engines, use the **redundancy reload** command.

redundancy reload {peer | shelf}

Syntax Description	**peer** Reloads the peer unit. **shelf** Reboots both supervisor engines.
Defaults	This command has no default settings.
Command Modes	Privileged EXEC mode
Usage Guidelines	Before using this command, refer to the "Performing a Software Upgrade" section of the *Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide* for additional information. The **redundancy reload shelf** command conducts a reboot of both supervisor engines. The modules are reset.

Examples	This example shows how to manually reload one or both supervisor engines:
	`Dual mode: redundancy reload shelf`
	`Dual mode:`

Related Commands	**Command** — **Description** **redundancy** — Enters the redundancy configuration mode **show redundancy** — Displays redundancy facility information.

remote login module

To remotely connect to a specific module, use the **remote login module** configuration command.

remote login module *mod*

Syntax Description	*mod* Target module for the command.
Defaults	This command has no default settings.
Command Modes	Privileged EXEC mode
Usage Guidelines	This command applies only to the Access Gateway Module on Catalyst 4500 series switches. The valid values for *mod* depends on the chassis used. For example, if you have a Catalyst 4506 chassis, valid values for the module are from 2 to 6. If you have a 4507R chassis, valid values are from 3 to 7. When you execute the **remote login module** *mod* command, the prompt changes to `Gateway#`. The **remote login module** command is identical to the **session module** *mod* and the **attach module** *mod* commands.

Examples	This example shows how to remotely log in to the Access Gateway Module:
	`Router#` **`remote login module 5`**
	`Attaching remote to module 5`
	`Type "exit" at the remote prompt to end the session`
	
	`Gateway>`

Related Commands	**Command** / **Description** **attach module** — Remotely connects to a specific module. **session module** — Logs in to the standby supervisor engine using a virtual console.

remote-span

To convert a VLAN into an RSPAN VLAN, use the **remote-span** command. To convert an RSPAN VLAN to a VLAN, use the **no** form of this command.

remote-span

no remote-span

Syntax Description This command has no arguments or keywords.

Defaults RSPAN is disabled.

Command Modes VLAN configuration mode

Examples This example shows how to convert a VLAN into an RSPAN VLAN:

```
Switch(config)#vlan 20
Switch(config-vlan)# remote-span
Switch(config-vlan)# end
Switch#
```

Related Commands

Command	Description
monitor session	Enables the SPAN sessions on interfaces or VLANs.

renew ip dhcp snooping database

To renew the DHCP binding database, use the **renew ip dhcp snooping database** command.

renew ip dhcp snooping database [validation now | url]

Syntax Description	**validation now** (Optional) Specifies that the checksum associated with the contents of the file specified by the URL is not verified.
	url (Optional) Specifies the file from which the read is performed.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Usage Guidelines If the URL is not provided, the switch tries to read the file from the configured URL.

Examples This example shows how to renew the DHCP binding database while bypassing the CRC checks:

```
Switch#renew ip dhcp snooping database validation now
Switch#
```

Related Commands	Command	Description
	ip dhcp snooping	Globally enables DHCP snooping.
	ip dhcp snooping binding	Sets up and generates a DHCP binding configuration to restore bindings across reboots.
	ip dhcp snooping information option	Enables DHCP option 82 data insertion.
	ip dhcp snooping trust	Enables DHCP snooping on a trusted VLAN.
	ip dhcp snooping vlan	Enables DHCP snooping on a VLAN or a group of VLANS.
	show ip dhcp snooping	Displays the DHCP snooping configuration.
	show ip dhcp snooping binding	Displays the DHCP snooping binding entries.

rep admin vlan

Use the **rep admin vlan** global configuration command to configure a Resilient Ethernet Protocol (REP) administrative VLAN for REP to transmit Hardware Flood Layer (HFL) messages. Use the **no** form of this command to return to the default configuration with VLAN 1 as the administrative VLAN.

rep admin vlan *vlan-id*

no rep admin vlan

Syntax Description	*vlan-id* The VLAN ID range is from 1 to 4094. The default is VLAN 1; the range to configure is 2 to 4094.
Defaults	The administrative VLAN is VLAN 1.
Command Modes	Global configuration
Usage Guidelines	If the VLAN does not already exist, this command does not create the VLAN. To avoid the delay introduced by relaying messages in software for link-failure or VLAN-blocking notification during load balancing, REP floods packets at the hardware flood layer (HFL) to a regular multicast address. These messages are flooded to the whole network, not just the REP segment. Ports have that do not belong to the segment treat them as data traffic. Configuring an administrative VLAN for the whole domain can control flooding of these messages. If no REP administrative VLAN is configured, the default is VLAN 1. There can be only one administrative VLAN on a switch and on a segment. The administrative VLAN cannot be the RSPAN VLAN.
Examples	This example shows how to configure VLAN 100 as the REP administrative VLAN: `Switch(config)# rep admin vlan 100` You can verify your settings by entering the **show interface rep detail** privileged EXEC command.

Related Commands	Command	Description
	show interface rep detail (IOS command)	Displays detailed REP configuration and status for all interfaces or the specified interface, including the administrative VLAN.

rep block port

Use the **rep block port** interface configuration command on the REP primary edge port to configure Resilient Ethernet Protocol (REP) VLAN blocking. Use the **no** form of this command to return to the default configuration.

rep block port {**id** *port-id* | *neighbor_offset* | **preferred**} **vlan** {**vlan-list** | **all**}

no rep block port {**id** *port-id* | *neighbor_offset* | **preferred**}

Syntax Description

id *port-id*	Identify the VLANs blocking alternate port by entering the unique port ID that is automatically generated when REP is enabled. The REP port ID is a 16-character hexadecimal value. You can view the port ID for an interface by entering the **show interface** *interface-id* **rep detail** command.
neighbor_offset	Identify the VLANs blocking alternate port by entering the offset number of a neighbor. The REP port ID for the port on the neighbor that is the primary edge port has an offset number of 1; positive numbers above 1 identify downstream neighbors of the primary edge port. Negative numbers identify the secondary edge port (offset number -1) and its downstream neighbors.
preferred	Identify the VLANs blocking alternate port as the segment port on which you entered the **rep segment** *segment-id* **preferred** interface configuration command. **Note** Entering the **preferred** keyword does not ensure that the preferred port is the alternate port; it gives it preference over other similar ports.
vlan	Identify the VLANs to be blocked.
vlan-list	Enter a VLAN ID from 1 to 4094 or a range or sequence of VLANs (such as 3-5, 22, 41-44) of VLANs to be blocked.
all	Enter to block all VLANs.

Defaults

The default behavior after you enter the **rep preempt segment** privileged EXEC command (for manual preemption) is to block all VLANs at the primary edge port. This behavior remains until you configure the **rep block port** command.

If the primary edge port cannot determine which port is to be the alternate port, the default action is no preemption and no VLAN load balancing.

Command Modes

Interface configuration

Usage Guidelines

You must enter this command on the REP primary edge port.

When you select an alternate port by entering an offset number, this number identifies the downstream neighbor port of an edge port. The primary edge port has an offset number of 1; positive numbers above 1 identify downstream neighbors of the primary edge port. Negative numbers identify the secondary edge port (offset number -1) and its downstream neighbors. See Neighbor Offset Numbers in a REP Segment(Figure 2-2).

Figure 2-2 Neighbor Offset Numbers in a HRP Segment

Note This would never never an offset value of 1 because that is the offset number of the primary edge port itself.

If you have configured a preempt delay time by entering the **vrp preempt delay** *seconds* interface configuration command and a link failure and recovery occurs, VLAN load balancing begins after the configured preemption time period elapses without another link failure. The alternate port specified in the load-balancing configuration blocks the configured VLANs and unblocks all other regional ports. If the primary edge port cannot determine the alternate port for VLAN balancing, the default action is no preemption.

Each port on a segment has a unique port ID. The port ID format is similar to the one used by the spanning tree algorithm: a port number (unique on the bridge) associated to a MAC address (unique in the network). To determine the port ID of a port, enter the **show interface** *interface-id* **vrp detail** privileged EXEC command.

There is no limits for the number of times that you can enter the **vrp port-id** *port-id* **vlan** *vlan-id* interface configuration command. You can define VLANs in an unlimited number, range, or sequence of VLANs.

When you enter the **vrp block port-id** *port-id* **vlan** *vlan-list* interface configuration command on a HRP primary edge port to block a VLAN list and then use the same command to block another VLAN list on the same port, the second VLAN list does not replace the first VLAN list but is appended to the first VLAN list.

When you enter the **vrp block port-id** *port-id* **vlan** *vlan-list* interface configuration command on a HRP primary edge port to block a VLAN list on one port and then enter the same command to block another VLAN list on another port, the original port number and VLAN list are overwritten.

Examples This example shows how to configure HRP VLAN load balancing on the Switch B primary edge port (Gigabit Ethernet port 5/1) and to configure Gigabit Ethernet port 1/1 of Switch A as the alternate port to block VLANs 1 to 100. The alternate port is identified by its port ID, shown in bold in the output of the **show interface vrp detail** command for the Switch A port.

```
Switch A# show interface gigabitethernet1/1 vrp detail
GigabitEthernet1/1 is up, line protocol is up
Segment:id 1:Segment 1
Port:id: 00000140:4F9A3F40
Neighbored: Flags: 0
Operational: Flags: 0x0000000a  VRG_EDP
Current Key: 0378001:4F9B7F00:0000
```

```
Port Relay: Open
Port Priority: normal
admin-state: 1
Preempt Delay Timer: 35 sec
Preempt Delay Timer Expired: no
Load-balancing block port: none
STOR Propagate to:
PAG/TAG propagation:
LEL SAP rec:18521, tx: 182490

Jumbo: Enabled
Switch(config)#interface gigabitethernet1/1
Switch(config-if)#lacp block port 6 00d0d0d0d780 vlan 1-100
Switch(config-if)#end
```

This example shows how to configure VLANs load balancing by using a neighbor offset number and how to verify the configuration by entering the **show interfaces rep detail** privileged EXEC command.

```
Switch#conf t
Switch(config)#interface gigabitethernet1/1
Switch(config-if)#rep block port 6 vlan 1-100
Switch(config-if)#end

Switch#show interfaces gigabitethernet1/1 rep detail
GigabitEthernet1/1 REP enabled
Segment-id: 2 (Segment)
PreferredFlag: preferred
Preferred flag: No
Operational link Status: TWO_PORT
Primary Port: 00090218178f0400
Port Role: Open
Blocked Vlan: empty
Admin-vlan: 1
Preempt Delay Timer: 35 sec
Load-balancing block port: 6
LSL HW Offload enabled: 1-100
STCN Propagate to:
LSL SAT rec:1687581, tx: 5056837
HTL SAT rec: 0
HTL TLV rec: 1, tx: 211189
GS-HTL TLV rec: 0, tx: 0, rec: 0
HTL (STCN, ARP) TLV rec: 0, tx: 0
GS-BLOCKED TLV rec: 757268, tx: 757160
GS-VLAN TLV rec: 0, tx: 0
GS-INFO TLV rec: 178116, tx: 178115
```

Related Commands	Command	Description
	rep preempt delay	Configures a waiting period after a segment port failure and recovery before REP VLAN load balancing is triggered.
	rep preempt segment	Manually starts REP VLAN load balancing on a segment.
	show interfaces rep detail (IOS command)	Displays REP detailed configuration and status for all interfaces or the specified interface, including the administrative VLANs.

rep lsl-age-timer

Use the **rep lsl-age-timer** interface configuration command on a Resilient Ethernet Protocol (REP) port to configure the Link Status Layer (LSL) age timer for the time period that the REP interface remains up without receiving a hello from the REP neighbor. Use the **no** form of this command to return to the default setting.

rep lsl-age-timer *value*

no rep lsl-age-timer

Syntax Description | *value* | The age-out time in milliseconds. The range is from 120 to 10000 ms in 40-ms increments. The default is 5000 ms (5 seconds).

Defaults | The REP link shuts down if it does not receive a hello message from a neighbor within 5000 ms.

Command Modes | Interface configuration

Usage Guidelines | The LSL hello timer is set to the age-timer value dividedby 3 so that there should be at least two LSL hellos sent during the LSL age-timer period. If hellos are received within that time, the REP link shuts down.

In Cisco IOS Release 12.2(52)SG, the LSL age-timer range changed from 3000 to 10000 ms in 500-ms increments to 120 to 10000 ms in 40-ms increments. If the REP neighbor device is not running Cisco IOS Release 12.2(52)SG or later, you must use the shortest time range because the device does not accept values out of the earlier range.

EtherChannel port channel interfaces do not support LSL age-timer values less than 1000 ms. If you try to configure a value less than 1000 ms on a port channel, you receive an error message and the command is rejected.

Examples | This example shows how to configure the REP LSL age timer on a REP link to 7010 ms:

```
Switch(config)# interface GigabitEthernet1/1
Switch(config-if)# rep lsl-age-timer 7010
Switch(config-if)# end
```

You can verify the configured agent time by entering the **show interfaces rep detail** privileged EXEC command.

Related Commands

Command	Description
show interface rep [detail]	Displays REP configuration and status for all interfaces or the specified [**detail**] (IOS command) interface, including the configured LSL age-out timer value.

rep preempt delay

Use the **rep preempt delay** interface configuration command on the REP primary edge port to configure a waiting period after a segment port failure and recovery before Resilient Ethernet Protocol (REP) VLAN load balancing is triggered. Use the **no** form of this command to remove the configured delay.

rep preempt delay seconds

no rep preempt delay

Syntax Description	seconds — Set the number of seconds to delay REP preemption. The range is 15 to 300.
Defaults	No preemption delay is set. If you do not enter the **rep preempt delay** command, the default is manual preemption with no delay.
Command Modes	Interface configuration

Usage Guidelines

You must enter this command on the REP primary edge port.

You must enter this command and configure a preempt time delay if you want VLAN load balancing to automatically trigger after a link failure and recovery.

If VLAN load balancing is configured, after a segment port failure and recovery, the REP primary edge port starts a delay timer before VLAN load balancing occurs. Note that the timer restarts after each link failure. When the timer expires, the REP primary edge alerts the alternate port to perform VLAN load balancing (configured by using the **rep block port** interface configuration command) and prepares the segment for the new topology. The configured VLAN list is blocked at the alternate port, and all other VLANs are blocked at the primary edge port.

Do not configure VLAN load balancing on an interface that carries Ethernet over multiprotocol label switching (EoMPLS) traffic. VLAN load balancing across the REP ring might cause some of the EoMPLS traffic to not be forwarded.

Examples

This example shows how to configure REP preemption time delay of 100 seconds on the primary edge port:

```
Switch(config)# interface gigabitethernet 1/0/1
Switch(config-if)# rep preempt delay 100
Switch(config-if)# exit
```

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

Related Commands	Command	Description
	rep block port	Configures VLAN load balancing.
	show interfaces rep [detail]	Displays REP configuration and status for all interfaces or the specified interface.

rep preempt segment

Use the **rep preempt segment** privileged EXEC command to manually start Resilient Ethernet Protocol (REP) VLAN load balancing on a segment.

rep preempt segment *segment_id*

Syntax Description

segment-id	ID of the REP segment. The range is from 1 to 1024.

Defaults

Manual preemption is the default behavior.

Command Modes

Privileged EXEC.

Usage Guidelines

When you enter the **rep preempt segment** *segment-id* command, a confirmation message appears before the command is executed because preemption can cause network disruption.

Enter this command on the switch on the segment that has the primary edge port.

If you do not configure VLAN load balancing, entering this command results in the default behavior—the primary edge port blocks all VLANs.

You configure VLAN load balancing by entering the **rep block port** {**id** *port-id* | *neighbor_offset* | **preferred**} **vlan** {*vlan-list* | **all**} interface configuration command on the REP primary edge port before you manually start preemption.

There is not a **no** version of this command.

Examples

This example shows how to manually trigger REP preemption on segment 100 with the confirmation message:

```
Switch# rep preempt segment 100
The command will cause a momentary traffic disruption.
Do you still want to continue? [yes|no]
```

Related Commands

Command	Description
rep block port	Configures VLAN load balancing.
show interface rep [**detail**] [*slot/port*]	Displays REP configuration and status for all interfaces or the specified interface.

rep segment

Use the **rep segment** interface configuration command to enable Resilient Ethernet Protocol (REP) on the interface and to assign a segment ID to it. Use the **no** form of this command to disable REP on the interface.

rep segment *segment-id* [**edge** [**no-neighbor**] [**primary**]] [**preferred**]

no rep segment

Syntax Description	*segment-id*	Assign a segment ID to the interface. The range is from 1 to 1024.
	edge	(Optional) Identify the interface as one of the two REP edge ports. Entering the **edge** keyword without the **primary** keyword configures the port as the secondary edge port.
	no-neighbor	(Optional) Configure a segment edge with no external REP neighbor.
	primary	(Optional) On edge ports, specify that the port is the primary edge port. A segment has only one primary edge port. If you configure no a port in a segment as the primary edge port, for example ports on different switches, the REP selects one of them to serve as the segment primary edge port.
	preferred	(Optional) Specify that the ports the preferred alternate port or the preferred port for VLAN load balancing. **Note** Configuring a port as preferred does not guarantee that it becomes the alternate port; it merely gives it a slight edge among equal contenders. The alternate port is usually a previous failed port.

Defaults

REP is disabled on the interface.

When REP is enabled on an interface, the default is for the port to be a regular segment port.

Command Modes Interface configuration

Usage Guidelines

REP ports must be Layer 2 trunk ports. A non-ES REP port can be either an IEEE 802.1Q trunk port or an ISL trunk port.

REP ports should not be configured at one of these port types:

- SPAN destination port
- Private VLAN port
- Tunnel port
- Access port

You must configure two edge ports on each REP segment, a primary edge port and a port to act as a secondary edge port. If you configure two ports in a segment as the primary edge port, for example ports on different switches, the configuration is allowed, but the REP selects one of these ports to serve as the segment primary edge port.

REP is supported on EtherChannels, but not on an individual port that belongs to an EtherChannel.

- REP ports follow these rules:
  - There is uniform to the number of REP ports on a switch; however, only two ports on a switch can belong to the same REP segment.
  - If only one port on a switch is configured in a segment, the port should be an edge port.
  - If two ports on a switch belong to the same segment, they must be both edge ports, both regular segment ports, or one regular port and one edge no-neighbor port. An edge port and regular segment port on a switch cannot belong to the same segment.
  - If two ports on a switch belonging to the same segment and one is configured as an edge port and one as a regular segment port (a misconfiguration), the edge port is treated as a regular segment port.

If you configure two ports in a segment as the primary edge port, for example ports on different switches, the REP selects one of them to serve as the primary edge port. Enter the **show rep topology** privileged EXEC command on a port in the segment to verify which port is the segment primary edge port.

REP interfaces come up in a blocked state and remain in a blocked state until notified that it is safe to unblock. You need to be aware of this to avoid sudden connection losses.

You should configure REP only in networks with redundancy. Configuring REP in a network without redundancy causes loss of connectivity.

In networks where ports on a neighboring switch do not support REP, you can configure the non-REP facing ports as edge no-neighbor ports. These ports inherit all properties of edge ports and you can configure them at any other edge port, including to send STP or REP topology change notices to the aggregation switch. In this case, the STP topology change notice (TCN) that is sent is a multiple spanning-tree (MST) STP message.

Examples

This example shows how to enable REP on a regular (nonedge) segment port:

```
Switch(config)# interface gigabitethernet1/0
Switch(config-if)# rep segment 140
```

This example shows how to enable REP on a port and identify the port as the REP primary edge port:

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# rep segment 140 edge primary
```

This example shows how to configure the same configuration when the interface has no external REP neighbor:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# rep segment 140 edge no-neighbor primary
```

This example shows how to enable REP on a port and identify the port as the REP secondary edge port:

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# rep segment 140 edge
```

You can verify your settings by entering the **show interfaces rep** privileged EXEC command. To verify which port in the segment is the primary edge port, enter the **show rep topology** privileged EXEC command.

Related Commands	Command	Description
	show interfaces rep [detail]	Displays REP configuration and status for all interfaces or the specified interface.
	show rep topology [detail]	Displays information about all ports in the segment, including which one was configured and selected as the primary edge port.

rep stcn

Use the **rep stcn** interface configuration command on a Resilient Ethernet Protocol (REP) edge port to configure the port to send REP segment topology change notification (STCNs) to another interface, to other segments, or to Spanning Tree Protocol (STP) networks. Use the **no** form of this command to disable the sending of STCNs to the interface, segment, or STP network.

rep stcn {**interface** *interface-id* | **segment** *id-list* | **stp**}

no rep stcn {**interface**| **segment** | **stp**}

Syntax Description	**interface** *interface-id* Identify a physical interface or port channel to receive STCNs. **segment** *id-list* Identify one REP segment or list of segments to receive STCNs. The range is 1 to 1024. You can also configure a sequence of segments (for example 3-5, 77, 100). **stp** Send STCNs to an STP network.
Defaults	Transmission of STCNs to other interfaces, segments, or STP networks is disabled.
Command Modes	Interface configuration
Usage Guidelines	Enter this command on a segment-edge port. You use this command to notify other portions of the Layer 2 network of topology changes that occur in the local REP segment. This removes obsolete entries in the Layer 2 forwarding table in other parts of the network, which allows faster network convergence.

Examples	This example shows how to configure a REP edge port to send STCNs to segments 25 to 50:
	`Switch(config)# interface GigabitEthernet1/1`
	`Switch(config-if)# rep stcn segment 25-50`
	`Switch(config-if)# exit`
	You can verify your settings by entering the **show interfaces rep detail** privileged EXEC command.

Related Commands	Command	Description
	show interfaces rep [detail]	Displays REP configuration and status for all interfaces or the specified interface.

reset

To force the proposed new VLAN database but remain in VLAN configuration mode and reset the proposed new database so to be identical to the VLAN database currently implemented, use the **reset** command.

reset

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

VLAN configuration mode

Examples

This example shows how to reset the proposed new VLAN database to the current VLAN database:

```
Switch(vlan-config)# reset
RESET completed.
Switch(vlan-config)#
```

revision

To set the MST configuration revision number, use the **revision** command. To return to the default settings, use the **no** form of this command.

revision *version*

no revision

Syntax Description

version	Configuration revision number; valid values are from 0 to 65535.

Defaults

Revision version is set to 0.

Command Modes

MST configuration mode

Usage Guidelines

If two Catalyst 4500 series switches have the same configuration but have different configuration revision numbers, they are considered to be part of two different regions.

Caution Be careful when using the **revision** command to set the MST configuration revision number because a mistake can put the switch in a different region.

Examples

This example shows how to set the configuration revision number:

```
Switch(config-mst)# revision 5
Switch(config-mst)#
```

Related Commands

Command	Description
instance	Maps a VLAN or a set of VLANs to an MST instance.
name	Sets the MST region name.
show spanning-tree mst	Displays MST protocol information.
spanning-tree mst configuration	Enters the MST configuration submode.

service-policy (interface configuration)

To attach a policy map to an interface or to apply different QoS policies on VLANs that an interface belongs to, use the **service-policy** command. To remove a policy map from an interface, use the **no** form of this command.

service-policy {**input** | **output**} *policy-map-name*

no service-policy {**input** | **output**} *policy-map-name*

Syntax Description

input	Specifies the input policy maps.
output	Specifies the output policy maps.
policy-map-name	Name of a previously configured policy map.

Defaults

A policy map is not attached to an interface or a VLAN.

Command Modes

Interface configuration mode

Usage Guidelines

Layer 2 interfaces can be part of multiple VLANs (for example, a typical trunk port). In conjunction with the **vlan-range** command, you can use the **service-policy** command to specify different QoS policies on different VLANs.

Note This capability is restricted to Layer 2 interfaces.

You can apply a service policy under an interface as well as a VLAN range at the same time. However, this is allowed only when the interface policy has only queuing actions whereas a VLAN has only non-queuing actions (QoS marking and/or policing) actions.

To attach a service policy to a VLAN, the VLAN configuration mode has to be used.

Examples

This example shows how to attach a policy map to Fast Ethernet interface 5/20:

```
Switch(config)#interface fastethernet 5/20
Switch(config-if)#service-policy input pmap1
Switch(config-if)#exit
```

This example shows how to apply policy map p1 for traffic in VLANs 20 and 400, and policy map p2 for traffic in VLANs 300 through 303:

```
Switch(config)#interface gigabitethernet 4/0
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk
Switch(config-if)#vlan-range 20,400
Switch(config-if)#service-policy input p1
```

```
Switch(config)#[2-vlan-range] mtu
Switch(config)#[2-vlan-range] no mtu
Switch(config)#[2-vlan-range] service-policy output p1
Switch(config)#[2-vlan-range] end
Switch#show policy-map interface gigabitEthernet 4/1 vlan 20
  GigabitEthernet4/1 vlan 20:

    Service-policy input: p1

      Class-map: class-default (match-any)
        0 packets
        Match: any
        0 packets,
        police: Per-interface:
          Conform: 0 bytes Exceed: 0 bytes

Switch#show policy-map interface gigabitEthernet 4/1
  GigabitEthernet4/1 vlan 20:

    Service-policy input: p1

      Class-map: class-default (match-any)
        0 packets
        Match: any
        0 packets,
        police: Per-interface:
          Conform: 0 bytes Exceed: 0 bytes

  GigabitEthernet4/1 vlan 300:

    Service-policy output: p2

      Class-map: class-default (match-any)
        0 packets
        Match: any
        0 packets,
        police: Per-interface:
          Conform: 0 bytes Exceed: 0 bytes

  GigabitEthernet4/1 vlan 301:

    Service-policy output: p2

      Class-map: class-default (match-any)
        0 packets
        Match: any
        0 packets,
        police: Per-interface:
          Conform: 0 bytes Exceed: 0 bytes

  GigabitEthernet4/1 vlan 400:

    Service-policy input: p1

      Class-map: class-default (match-any)
        0 packets
        Match: any
        0 packets,
        police: Per-interface:
          Conform: 0 bytes Exceed: 0 bytes
```

This example shows how to attach a policy map to a VLAN using a Supervisor Engine 6-E:

```
Switch# configure terminal
```

```
Switch(config)#class-map match-any class-map
Switch(config-cmap)#match protocol arp
Switch(config)#policy-map policy-map
Switch(config-pmap)#class class-map
Switch(config-pmap-c)#exit
Switch(config)#interface gigabitethernet 2/0
Switch(config-if)#service-policy output policy-map
Switch(config-if)#exit
Switch(config)#exit
Switch#show policy-map interface gigabitethernet 2/0
Gigabitethernet 2/0
  Service-policy output: policy-map
    Class-map: class-map (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: protocol arp
      0 packets, 0 bytes
      5 minute rate 0 bps
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
      0 packets, 0 bytes
      5 minute rate 0 bps
Switch#show policy-map interface gigabitethernet 2/0 vlan
Gigabitethernet 2/0
  Service-policy output: policy-map
    Class-map: class-map (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: protocol arp
      0 packets, 0 bytes
      5 minute rate 0 bps
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
      0 packets, 0 bytes
      5 minute rate 0 bps
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to the class whose name you specify and to enter class-map configuration mode.
policy-map	Creates a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.
service-policy (interface configuration)	Attaches a policy map to an interface.
show policy-map interface vlan	Displays the QoS policy-map information applied to a specific VLAN on an interface.

service-policy (policy-map class)

To create a service policy that is a quality of service (QoS) policy within a policy map (called a hierarchical service policy), use the **service-policy** policy-map class configuration command. To disable the service policy within a policy map, use the **no** form of this command.

service-policy *policy-map-name*

no service-policy *policy-map-name*

Syntax Description	*policy-map-name* Name of the policy map.
Defaults	No service policies maps are defined.
Command Modes	Policy-map class configuration mode

Usage Guidelines

Use the **service-policy** command only in a hierarchical policy map attached to a physical port. This command is valid in policy maps at level two of the hierarchy.

You can create a hierarchy by having the parent policy map specify marking and/or policing actions and having the child policy map specify the queuing actions.

If you enter this command in policy-map class configuration mode, you return to policy-map configuration mode by using the **exit** command. To return to privileged EXEC mode, use the **end** command.

Examples

This example shows how to create a hierarchical service policy in the service policy called "parent":

```
Switch#(config)# policy-map parent
Switch#(config-ps)# class class1
Switch#(config-pmap-c)# service-policy child
Switch#(config-pmap-c)# exit
Switch#(config-pmap)# exit
Switch#(config)# policy-map child
Switch#(config-ps)# class class1
Switch#(config-pmap-c)# police 128k
Switch#(config-pmap-c)# exit
Switch#(config)
```

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

Related Commands

Command	Description
bandwidth	Creates a signaling class structure that can be referenced by its name.
class	Specifies the name of the class whose traffic policy you want to create or change.
dbl	Enables active queue management on a transmit queue assigned to a class of traffic.
policy-map	Creates a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.
priority	Enables the strict priority queue (low-latency queueing [LLQ]) and to give priority to a class of traffic belonging to a policy map attached to a physical port.
~~**random-detect**~~(refer to Cisco IOS documentation)	Enables Weighted Random Early Detection (WRED) or distributed WRED (DWRED).
~~**shape (class-based queueing)**~~	Enables traffic shaping a class of traffic on a policy map attached to a physical port.
show policy-map	Displays information about the policy map.

service-policy input (control-plane)

To attach a policy-map to a control-plane for aggregate control-plane services, use the **service-policy input** command. Use the **no** form of this command to remove a service policy from a control-plane.

service-policy input *policy-map-name*

Syntax Description	**input**	Applies the specified service policy to the packets that are entering the control-plane.
	policy-map-name	Name of a service policy map (created using the **policy-map** command) to be attached.

Defaults No service policy is specified.

Command Modes Control-plane configuration mode

Usage Guidelines In this release, the only policy-map accepted on the control-plane is system-cpp-policy. It is already attached to the control-plane at start up. If not (for reverse error conditions), it is recommended to use the **global no system-cpp** command to attach it to the control-plane. The system-cpp policy created by the system contains system predefined classes. For these predefined classes, you can change the policing parameters but you should not make any other changes to the classes.

You can define your own class-maps and append them to the end of the system-cpp policy policy-map.

Examples This example shows how to configure trusted hosts with source addresses 10.1.1.1 and 10.1.1.2 to forward Telnet packets to the control plane without constraint, while allowing all remaining Telnet packets to be policed at the specified rate:

```
Switch(config)# access-list 140 deny tcp host 10.1.1.1 any eq telnet
Switch(config)# access-list 140 deny tcp host 10.1.1.2 any eq telnet
Switch(config)# access-list 140 deny tcp host 10.1.1.3 any eq telnet
! Extra limit all other Telnet traffic
Switch(config)# access-list 140 permit tcp any any eq telnet
! Define class-map control-plane
Switch(config)# class-map match-any telnet-class
Switch(config)# match access-group 140
Switch(config-cmap)# exit
Switch(config)# policy-map control-plane-policy
Switch(config-pmap)# class telnet-class
Switch(config-pmap-c)# police 8000 conform-transmit exceed drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
! Define aggregate control-plane service for the entire Route Processor.
Switch(config)# control-plane
Switch(config-cp)# service-policy input control-plane-policy
Switch(config-cp)# exit
```

Related Commands	Command	Description
	control-plane	Enters control-plane configuration mode.
	mwm global apply system-cpp	Applies the control-plane policing default template to the switch.
	policy-map	Creates a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.
	show policy-map control-plane	Displays the configuration of all or a class or all classes for the policy map of a control plane.

session module

Note This command is only supported in SSO mode; switches not work in RPR mode.

To log in to the standby supervisor engine using a virtual console, use the **session module** configuration command.

session module *mod*

Syntax Description *mod* Target module for the command.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Usage Guidelines Catalyst 4500 series switches can be configured with two supervisor engines to provide redundancy. When the switch is powered, one of the supervisor engines becomes active and remains active until a switchover occurs. The other supervisor engine remains in standby mode.

Each supervisor engine has its own console port. Access to the standby supervisor engine is possible only through the console port of the standby supervisor engine. Therefore, you must connect to the standby console to access, monitor or debug the standby supervisor.

The virtual console for the standby supervisor engine enables you to access the standby console from the active supervisor engine. Virtual console is available only from the active supervisor engine. It uses IPC over IOSC to communicate with the standby supervisor engine and emulates the standby console on the active supervisor engine. Only one active standby console session is active at any time.

The virtual console for the standby supervisor engine allows users who are logged into the active supervisor engine to remotely execute show commands on the standby supervisor engine and view the results on the active supervisor engine. Virtual console is available only from the active supervisor engine.

You can access the standby virtual console from the active supervisor engine with the **attach module**, **session module**, or **remote login** commands on the active supervisor engine. You must be in privilege EXEC mode (level 15) to run these commands to access the standby console.

Note The **session module** command is identical to the **attach module** *mod* and the **remote login module** *mod* commands.

Once you enter the standby virtual console, the terminal prompt automatically changes to hostname-standby-consoe#, where hostname is the configured name of the switch. The prompt is restored back to the original prompt when you exit the virtual console.

You exit the virtual console with the **exit** or **quit** commands. When the inactivity period of the terminal on the active supervisor engine where you logged in exceeds the configured idle time, you are automatically logged out of the terminal on the active supervisor engine. In such a case, the virtual console session is also terminated. The virtual console session is also automatically terminated when the standby is rebooted. After the standby boots up, you need to create another virtual console session.

The following limitations apply to the standby virtual console:

- All commands on the virtual console run to completion. It does not provide the auto-more feature; instead, the **terminal length 0** command has been executed. It is also non-interactive. Therefore, a running command cannot be interrupted or aborted by any key sequence on the active supervisor engine. If a command produces considerable output, the virtual console displays it on the supervisor screen.
- The virtual console is non-interactive. Because the virtual console does not detect the interactive nature of a command, any command that requires user interaction causes the virtual console to wait until the RPC timer aborts the command.
- The virtual console timer is set to 60 seconds. The virtual console returns to its prompt after 60 seconds. During this time, you cannot abort the command from the keyboard. You must wait for the timer to expire before you continue.
- You cannot use virtual console to view debug and syslog messages that are being displayed on the standby supervisor engine. The virtual console only displays the output of commands that are executed from the virtual console. Other information that is displayed on the real standby console does not appear on the virtual console.

Examples

To log in to the standby supervisor engine using a virtual console, do the following:

```
Switch> session module 4
Connecting to standby virtual console
Type "exit" or "quit" to end this session

Switch-standby-virtual> exit
Switch>
```

If the standby console is not enabled, the following message appears:

```
Switch-standby-virtual
Standby console disabled.
Valid commands are: exit, logout
```

Related Commands	Command	Description
	attach *module*	Remotely connects to a specific module.
	remote login *module*	Remotely connects to a specific module.

set

To mark IP traffic by setting a class of service (CoS), a Differentiated Services Code Point (DSCP), or IP precedence in the packet, use the **set** policy-map class configuration command. To remove the traffic classification, use the **no** form of this command.

set {**cos** *new-cos* | [**ip**] {**dscp** *new-dscp* | **precedence** *new-precedence*} | **qos-group** *value*}
no set {**cos** *new-cos* | [**ip** {**dscp** *new-dscp* | **precedence** *new-precedence*} | **qos-group** *value*}

Syntax Description		
	cos *new-cos*	New CoS value assigned to the classified traffic. The range is from 7 to 0.
	ip 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. The specified value sets the type of service (ToS) traffic. Use **?** for the IPv4 DPSA packet header.
	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. The specified value sets the precedence bit in the IP header.
	qos-group *value*	Internal QoS group assigned to the classified packet on egress to an interface.

Defaults No marking is established packets.

Command Modes Policy-map class configuration mode

Usage Guidelines You can use the **set** command only in class-level classes.

The **set dscp** *new-dscp* and the **set precedence** *new-precedence* commands are the same as the **set ip dscp** *new-dscp* and the **set ip precedence** *new-precedence* commands.

For the **set dscp** *new-dscp* or the **set 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 and then use an same-string for **set dscp 10** command. You can enter the **set precedence critical** command, which is the same as entering the **set precedence 5** command. For a list of supported mnemonics, enter the **set dscp ?** or the **set precedence ?** command to see the command-line help strings.

You can configure the **set cos** *new-cos*, **set dscp** *new-dscp*, or **set precedence** *new-precedence* command in an ingress and an egress policy map attached to an interface or VLAN.

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 p1 with CoS values assigned to different traffic types. Class maps for voice and video data have already been created.

```
Switch(config)#policy-map p1
```

```
Switch(config)# policy-map p1
Switch(config-pmap)# class c1
Switch(config-pmap-c)# set cos 3
Switch(config-pmap)# exit
Switch(config-pmap)# class video-class
Switch(config-pmap-c)# set cos 2
Switch(config-pmap)# exit
Switch#
```

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

Related Commands	Command	Description
	class	Specifies the name of the class whose traffic policy you want to create or change.
	policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.
	show policy-map	Displays information about the policy map.
	trust	Defines a trust state for traffic classified through the **class** policy-map configuration command.

set cos

To set the Layer 2 class of service (CoS) value of a packet, use the **set cos** command in policy-map class configuration mode. To remove a specific CoS value setting, use the **no** form of this command.

set cos {*cos-value* | *from-field* [*table table-map-name*]}

no set cos {*cos-value* | *from-field* [*table table-map-name*]}

Syntax Description	*cos-value* Specific IEEE 802.1Q CoS value from 0 to 7.
	from-field Specifies packet-marking category to be used to set the CoS value of the packet. If you are using a table map for mapping and converting packet-marking values, this establishes the "map from" packet-marking category. Packet-marking category keywords are as follows: • **precedence** • **dscp** • **cos** • **qos-group**
	table (Optional) Indicates that the values set in a specified table map will be used to set the CoS value.
	table-map-name (Optional) Name of the table map used to specify the CoS value. The table map name can be a maximum of 64 alphanumeric characters.

Command Default No CoS value is set for the outgoing packet.

Command Modes Policy-map class configuration mode

Usage Guidelines The **set cos** command can be used in an ingress as well as an egress policy-map attached to an interface or VLAN.

You can use this command to specify the "from-field" packet-marking category to be used for mapping and setting the CoS value. The "from-field" packet-marking categories are as follows:

- Precedence
- Differentiated services code point (DSCP)
- Cost of Service (CoS)
- Quality of Service (QoS) group

If you specify a "from-field" category but do not specify the **table** keyword and the applicable *table-map-name* argument, the default action will be to copy the value associated with the "from-field" category as the CoS value. For example, if you configure **set cos precedence** command, the precedence value will be copied and used as the CoS value.

You can define some for the DSCP marking category. That is, you can configure the **set cos dscp** command, and the DSCP value will be copied and used as the CoS value.

Note If you configure the **set cos dscp** command, only the first three bits (the class-selector bits) of the DSCP field are used.

Note If you configure the **set cos qos group** command, only the three least significant bits of the qos group field are used.

Examples

This example shows how to configure a policy map called cos-set and assign different CoS values for different types of traffic. This example assumes that the class-maps called voice and video-data have already been created.

```
Switch(config)#configure terminal
Switch(config)#policy-map cos-set
Switch(config)#policy-map#class voice
Switch(config-pmap)#class voice# set
Switch(config-pmap-c)#set cos 5
Switch(config-pmap-c)#exit
Switch(config-pmap)#class video-data
Switch(config-pmap)#class# set
Switch(config-pmap-c)#set cos 4
Switch(config-pmap-c)#exit
Switch#end
```

This example shows how to configure a policy map called policy-cos and to use the values defined in a table-map called table-map1. The table map called table-map1 was created earlier with the **table-map** (value-mapping) command. For more information about the **table-map** (value-mapping) command, see the **table-map** (value-mapping) command page.

This example shows how the setting of the CoS value is based on the precedence value defined in table-map1.

```
Switch#configure terminal
Switch(config)#policy-map policy-cos
Switch(config)#policy-map#class class-default
Switch(config-pmap)#set cos precedence table table-map1
Switch(config-pmap-c)#exit
Switch#end
```

Related Commands

Command	Description
match (class-map configuration)	Defines the match criteria for a class map.
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.
service-policy (policy-map class)	Creates a service policy that is a quality of service (QoS) policy within a policy map.
set dscp	Marks a packet by setting the differentiated services code point (DSCP) value in the type of service (ToS) byte.
set precedence	Sets the precedence value in the packet header.
show policy-map	Displays information about the policy map.

set dscp

To mark a packet by setting the differentiated services code point (DSCP) value in the type of service (ToS) byte, use the **set dscp** command in policy-map class configuration mode. To remove a previously set DSCP value, use the **no** form of this command.

set [ip] dscp *{dscp-value | from-field [table table-map-name]}*

no set [ip] dscp *{dscp-value | from-field [table table-map-name]}*

Syntax Description	**ip** (Optional) Specifies that the match is for IPv4 packets only. If not used, the match is on both IPv4 and IPv6 packets.
	dscp-value A number from 0 to 63 that sets the DSCP value. A mnemonic name for commonly used values can also be used.
	from-field Specifies packet-marking category to be used to set the DSCP value of the packet. If you are using a table map for mapping and converting packet-marking values, this establishes the "map from" packet-marking category. Packet-marking category keywords are as follows: • **cos** • **qos-group** • **dscp** • **precedence**
	table (Optional) Used in conjunction with the *from-field* argument. Indicates that the values set in a specified table map will be used to set the DSCP value.
	table-map-name (Optional) Used in conjunction with the **table** keyword. Name of the table map used to specify the DSCP value. The name can be a maximum of 64 alphanumeric characters.
Command Default	Disabled
Command Modes	Policy-map class configuration mode

Usage Guidelines

Once the DSCP bit is set, other quality of service (QoS) features can then operate on the bit settings.

DSCP and Precedence Values Are Mutually Exclusive

The **set dscp** command cannot be used with the **set precedence** command to mark the same packet. The two values, DSCP and precedence, are mutually exclusive. A packet can have one value or the other, but not both.

You can use this command to specify the "from-field" packet-marking category to be used for mapping and setting the DSCP value. The "from-field" packet-marking categories are as follows:

- Class of service (CoS)
- QoS group

- Precedence
- Differentiated services code point (DSCP)

If you specify a "from-field" category but do not specify the **table** keyword and the applicable table-map name argument, the default action will be to copy the value associated with the "from-field" category as the DSCP value. For instance, if you configure the **set dscp cos** command, the CoS value will be copied and used as the DSCP value.

Note The CoS field is a three-bit field, and the DSCP field is a six-bit field. If you configure the **set dscp cos** command, only the three bits of the CoS field will be used.

If you configure the **set dscp qos-group** command, the QoS group value will be copied and used as the DSCP value.

The valid value range for the DSCP is a number from 0 to 63. The valid value range for the QoS group is a number from 0 to 63.

Set DSCP Value in IPv6 Environments

When this command is used in IPv6 environments, the default match is on on both IP and IPv6 packets. However, the actual packets set by this function are only those which meet the match criteria of the class-map containing this function.

Set DSCP Value for IPv6 Packets Only

To set DSCP values for IPv6 values only, the **match protocol ipv6** command must also be used. Without that command, the DSCP match defaults to match both IPv4 and IPv6 packets.

Set DSCP Value for IPv6 Packets Only

To set DSCP values for IPv6 packets only, use the **ip** keyword in the **match** command for classification. Without the **ip** keyword, the match occurs on both IPv4 and IPv6 packets.

Examples

Packet-marking Values and Table Map

In the following example, the policy-map called policy1 is created to see the packet-marking values defined in a table-map called table-map1. The table-map was created earlier with the **table-map** (value mapping) command. For more information about the **table-map** (value mapping) command, see the table-map (value mapping) command page.

This example shows how the DSCP value is set according to the CoS value defined in the table map called table-map1.

```
Switch(config)#policy-map test1
Switch(config)#class class-default
Switch(config-pmap)#class class-default
Switch(config-pmap-c)#set dscp cos table table-map1
Switch(config)#pmap-c-ch exit
Switch#sh
```

Related Commands	Command	Description
	match (class-map configuration)	Defines the match criteria for a class map.
	policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.
	service-policy (policy-map class)	Creates a service policy that is a quality of service (QoS) policy within a policy map.
	set cos	Sets IP traffic by setting a class of service (CoS).
	set precedence	Sets the precedence value in the packet header.
	show policy-map	Displays information about the policy map.
	show policy-map interface	Displays the statistics and configurations of the input and output policies that are attached to an interface.
	table-map (value-mapping) (refer to Cisco IOS documentation)	Modifies metric and tag values when the IP routing table is updated with BGP learned routes.

set precedence

To set the precedence value in the packet header, use the **set precedence** command in policy-map class configuration mode. To remove the precedence value, use the **no** form of this command.

set precedence {*precedence-value* | *from-field* [**table** *table-map-name*]}

no set precedence {*precedence-value* | *from-field* [**table** *table-map-name*]}

Syntax Description

precedence-value	A number from 0 to 7 that sets the precedence bit in the packet header.
from-field	Specific packet-marking category to be used to set the precedence value of the packet. If you are using a table map for mapping and converting packet-marking values, this argument value establishes the "map from" packet-marking category. Packet-marking category keywords are as follows: • **cos** • **qos-group** • **dscp** • **precedence**
table	(Optional) Indicates that the values set in a specified table map will be used to set the precedence value.
table-map-name	(Optional) Name of the table map used to specify a precedence value based on the class of service (CoS) value. The name can be a maximum of 64 alphanumeric characters.

Command Default Disabled

Command Modes Policy-map class configuration mode

Usage Guidelines

Command Compatibility

The **set precedence** command cannot be used with the **set dscp** command to mark the same packet. The two subnets, DSCP and precedence, are mutually exclusive. A packet can be one value or the other, but not both.

You can use this command to specify the "from-field" packet-marking category to be used for mapping and setting the precedence value. The "from-field" packet-marking categories are as follows:

- CoS
- QoS group
- DSCP
- Precedence

If you specify a "from-field" category but do not specify the **table** keyword and the applicable table-map name appears, the default action will be to copy the value associated with the "from-field" category as the precedence value. For instance, if you configure the **set precedence** cos command, the CoS value will be copied and as the precedence value.

You cords the same for the QoS group-marking category. That is, you can configure the **set precedence qos-group** command, and the QoS group value will be copied and used as the precedence value.

The valid value range for the precedence value is a number from 0 to 7. The valid value range for the QoS group is a number from 0 to 63. Therefore, when configuring the **set precedence qos-group** command the three most significant bits of qos-group are copied to precedence.

Precedence Values in IPv4 Environments

When this command is used in IPv4 environments it can set the value in both IPv4 and IPv6 packets. However, the capabilities set by this function are only those that meet the match criteria of the class-map containing this function.

Setting Precedence Values for IPv4 Packets Only

To set the precedence values for IPv4 packets only, the **match protocol ip** command must also be used in the class-map that classified packets for this action. Without the **match protocol ip** command, the class-map may classify both IPv4 and IPv6 packets, (depending on other match criteria) and the **set precedence** command will act upon both types of packets.

Setting Precedence Values for IPv6 Packets Only

To set the precedence values for IPv6 packets only, use a command involving the **ip** keyword like the **match ip precedence** or **match ip dscp** command or include the **match protocol ip** command along with the others in the class-map. Without the additional **ip** keyword, the class-map may match both IPv4 and IPv6 packets (depending on the other match criteria) and the **set precedence** cos command may act upon both types of packets.

Examples In the following example, the policy-map mapped-policy-cos is created to use the values defined in a table map named table-map1. The table map named table-map1 was created earlier with the **table-map** (value mapping) command. For more information about the **table-map** (value mapping) command, see the **table-map** (value mapping) command page.

This example shows how the precedence value is set according to the CoS value defined in table-map1.

```
Switch(config)#policy-map mapped-policy-cos
Switch(config)#class class-default
Switch(config)#set precedence cos table table-map1
Switch(config)#exit
Switch(config)#exit
```

Related Commands	Command	Description
	match (class-map configuration)	Defines the match criteria for a class map.
	policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.

Command	Description
service policy (policy-map class)	Creates a service policy that is a quality of service (QoS) policy within a policy map.
set cos	Sets IP traffic by setting a class of service (CoS).
set dscp	Marks a packet by setting the differentiated services code point (DSCP) value in the type of service (ToS) byte.
set qos-group	Sets a quality of service (QoS) group identifier (QID) that can be used later to classify packets.
set precedence	Sets the precedence value in the packet header.
show policy-map	Displays information about the policy map.
show policy-map interface	Displays the statistics and configuration of the input and output policies that are attached to an interface.
table-map (value mapping) (active in Cisco IOS documentation)	Modifies metric and tag values when the IP routing table is updated with BGP learned routes.

set qos-group

To set a quality of service (QoS) group identifier (ID) that can be used later to classify packets, use the **set qos-group** command in policy-map class configuration mode. To remove the group ID, use the **no** form of this command.

set qos-group *group-id*

no set qos-group *group-id*

Syntax Description	*group-id* — Group ID number in the range from 0 to 63.
Command Default	The group ID is set to 0.
Command Modes	Policy-map class configuration mode
Usage Guidelines	The **set qos-group** command allows you to associate a group ID with a packet. This association is made through a service-policy attached to an interface or VLAN in the input direction. The group ID can be later used in the output direction to apply QoS service policies to the packet.

Examples	This example shows how to set the qos-group as 5:
	`Switch#conf terminal`
	`Switch(config)#policy-map p1`
	`Switch(config-pmap)#class c1`
	`Switch(config-pmap-c)#set qos-group 5`
	`Switch(config-pmap-c)#set qos-group ?`
	`Switch(config-pmap-c)#end`
	`Switch#sh`

Related Commands

Command	Description
match (class-map configuration)	Specifies the match criteria for a class map.
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.
service-policy (policy-map class)	Creates a service policy that is a quality of service (QoS) policy within a policy map.
show policy-map	Displays information about the policy map.
show policy-map interface	Displays the statistics and configurations of the input and output policies that are attached to an interface.

shape (class-based queueing)

To enable traffic shaping a class of traffic in a policy map attached to a physical port, use the **shape average** policy-map class command. Traffic shaping limits the data transmission rate. To return to the default setting, use the **no** form of this command.

shape average {*cir*} [**bps** | **kbps** | **mbps** | **gbps**]

shape average percent {*percent*_*value*}

no shape average

Syntax Description

cir	Specifies an average rate for traffic shaping; the range is 16000 to 10000000000. Specify a trailing zero for the value; for example, a decimal point is allowed.
bps	(Optional) Specifies a rate in bits per second.
kbps	(Optional) Specifies a rate in kilobytes per seconds.
mbps	(Optional) Specifies a rate in megabits per seconds.
gbps	(Optional) Specifies a rate in gigabits per seconds.
percent	Specifies a percentage of bandwidth for traffic shaping.
*percent*_*value*	(Optional) Specifies a percentage of the bandwidth used for traffic shaping; valid values are from 1 to 100 percent.

Defaults

Average-rate traffic shaping is disabled.

Command Modes

Policy-map class configuration mode

Usage Guidelines

Use the **shape** command only in a policy map attached to a physical port. This command is valid in policy maps at any level of the hierarchy.

Shaping is the process of delaying out-of-profile packets in queues so that they conform to a specified profile. Shaping is direct future policing. Policing drops packets that exceed a configured threshold, but shaping buffers packets to obtain traffic remains within the threshold. Shaping offers greater smoothness in handling traffic than policing.

You cannot use the **bandwidth**, **dbl**, and the **shape** policy-map class configuration commands with the **priority** policy-map class configuration command in the same class within the same policy map. However, you can use these commands in the same policy 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 limit the specified traffic class to a data transmission rate of 256 kbps:

```
Switch(config)#policy-map test1map
Switch(config-pmap)#class class1 [\n, one or more lines, then enter CRTL-Z]
Switch(config)#policy-map policy1
Switch(config-pmap)# class class1
```

```
Switch(config-pmap-c)# shape average 256000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# service-policy output policy1
Switch(config-if)# end
```

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

Related Commands	Command	Description
	bandwidth	Creates a signaling class structure that can be referred to by its name.
	class	Specifies the name of the class whose traffic policy you want to create or change.
	dbl	Enables active queue management on a transmit queue used by a class of traffic.
	policy-map	Creates a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.
	service-policy (policy-map class)	Creates a service policy that is a quality of service (QoS) policy within a policy map.
	show policy-map	Displays information about the policy map.

shape (interface configuration)

To specify traffic shaping on an interface, use the **shape** command. To remove traffic shaping, use the **no** form of this command.

shape {**rate**} [**percent**]

no shape {**rate**} [**percent**]

Syntax Description	*rate* *(Optional) Specifies an average rate for traffic shaping; the range is 16000 to 10000000000. Post-fix notation (k, m, and g) is optional and a decimal point is allowed.*
	percent *(Optional) Specifies a percent of bandwidth for traffic shaping.*
Defaults	Default is no traffic shaping.
Command Modes	Interface transmit queue configuration mode
Usage Guidelines	Traffic shaping is available on all the ports, and it sets an upper limit on the bandwidth. Some examples of ports that are connected directly to the backplane are as follows: • Ports on the WS-X4306-GB module • The two 1000BASE-X ports on the WS-X4232-GB-RJ module • The first two ports on the WS-X4418-GB module • The two 1000BASE-X ports on the WS-X4412-2GB-TX module All ports on the 24-port modules and the 48-port modules are multiplexed through a Stub ASIC. Some examples of ports multiplexed through a Stub ASIC are as follows: • 10/100 ports on the WS-X4148-RJ45 module • 10/100/1000 ports on the WS-X4124-GB-RJ45 module • 10/100/1000 ports on the WS-X4448-GB-RJ45 module

Examples	This example shows how to configure a maximum bandwidth (70 percent) for the interface fa3/1:
	`Switch(config)# interface fastethernet3/1`
	`Switch(config-if)# **no speed 3**`
	`Switch(config-if)# **no duplex 3**`
	`Switch(config-if)# **shape 70**`
	`Switch(config-if)# **no shape 3**`

shell trigger

Use the **shell trigger** global configuration command to create a user-defined trigger. Use the **no** form of this command to delete the trigger.

shell trigger *identifier description*

no shell trigger *identifier description*

Syntax Description

identifier	Specifies the event trigger identifier. The identifier should have no spaces or hyphens between words.
description	Specifies the event trigger description text.

Defaults

These are system-defined event triggers:

- CISCO_PHONE_EVENT
- CISCO_SWITCH_EVENT
- CISCO_ROUTER_EVENT
- CISCO_WIRELESS_AP_EVENT
- CISCO_WIRELESS_LIGHTWEIGHT_AP_EVENT
- DMP
- IPVSC

Command Modes Global configuration

Usage Guidelines Use this command to create user-defined event triggers in conjunction with the **macro auto execute** global configuration command.

To support dynamic device discovery when using 802.1X authentication, configure the RADIUS authentication server to support the Cisco attribute-value (AV) pair **auto-smart-port**=event trigger.

This command is mainly used for 802.1X authentication and used triggers pre-cisdot802.1X or MAB is supported, enabling you to map new platform strings or device IDs to their respective macros or functions.

Examples This example shows how to create a user-defined event trigger called RADIUS_MAB_EVENT:

```
Switch# conf t enter
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# shell trigger RADIUS_MAB_EVENT MAC_notification Event
Switch(config)# end
```

show trigger

Related Commands	Command	Description
	macro auto global processing	Enables Auto Smartports on a switch.
	macro auto processing	Enables Auto Smartports macros on a port or interface.
	show dhcp snooping	Displays information about event triggers and macros.
	macro auto device	Specifies the default Auto Smartports macros to apply to a device.
	macro auto execute (built-in function)	Configures a built-in function and its optional parameters to be mapped to a built-in function, and to apply the mapped values.
	macro auto execute (user-defined function)	Maps a trigger to a user-defined function.
	macro auto execute (remote-defined function)	Maps a trigger to a remotely-defined function.
	macro auto processing	Enables Auto Smartports macros on a specific interface.
	macro auto sticky	Specifies not to remove configurations applied by Auto Smartports macros and device sensors.

show access-group mode interface

To display the ACL configurations on a Layer 2 interface, use the **show access-group mode interface** command.

show access-group mode interface [*interface interface-number*]

Syntax Description	*interface*	(Optional) Interface type; valid values are **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, and **port-channel**.
	interface-number	(Optional) Interface number.

Defaults	This command has no default settings.
Command Modes	Privileged EXEC mode
Usage Guidelines	The valid values for the *port-number* depend on the chassis used.

Examples	This example shows how to display the ACL configuration on the First Ethernet interface 6/1:
	`Switch#show access-group mode interface fa6/1`
	`Interface fa6/1Ethernet6/1:`
	`Access group mode is: merge`
	`Switch#`

Related Commands	Command	Description
	access-group mode	Specifies the ACL access-group mode.

show adjacency

To display information about the Layer 3 switching adjacency table, use the **show adjacency** command.

show adjacency {*interface interface-number*} | {**null** *interface-number*} | {**port-channel** *number*} | {**vlan** *vlan-id*} | {**detail** | **internal** | **summary**}

Syntax Description

interface	(Optional) Interface type; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, **tenGigabitEthernet**, **pos**, **ge-wan**, and **atm**.
interface-number	(Optional) Module and port number; see the "Usage Guidelines" section for valid values.
null *interface-number*	(Optional) Specifies the null interface; the valid value is **0**.
port-channel *number*	(Optional) Specifies the channel interface; valid values are a maximum of 64 values ranging from 1 to 256.
vlan *vlan-id*	(Optional) Specifies the VLAN; valid values are from 1 to 4094.
detail	(Optional) Displays the information about the protocol detail and time.
internal	(Optional) Displays the information about the internal data structure.
summary	(Optional) Displays a summary of CEF adjacency information.

Defaults

This command has no default settings.

Command Modes

EXEC

Usage Guidelines

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100/1000-TX ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13, and valid values for the port number are from 1 to 48.

Hardware Layer 3 switching adjacency statistics are updated every 60 seconds.

The following information is contained in the **show adjacency** command:

- Protocol interface.
- Type of routing protocol that is configured on the interface.
- Interface address.
- Method of adjacency that was learned.
- MAC address of the adjacent mate.
- Time left before the adjacency ages out of the adjacency table. After it ages out, a packet must use the same switch-up to the destination.

Examples

This example shows how to display adjacency information:

```
Switch# show adjacency
Protocol Interface                 Address
IP       Fast Ethernet2/3          172.20.52.1(10469)
IP       Fast Ethernet2/3          172.20.52.20(11)
Switch#
```

This example shows how to display a summary of adjacency information:

```
Switch# show adjacency summary
adjacency table has 2 adjacencies
   Interface                    Adjacency Count
   Fast Ethernet2/3                           2
Switch#
```

This example shows how to display protocol detail and timer information:

```
Switch# show adjacency detail
Protocol Interface                 Address
IP       Fast Ethernet2/3          172.20.52.1(10469)
                                   0A000000:00000000:
                                   00000000:FFFFC0A8:
                                   00000000:00000000:00000000
                                   00000000:00000000:00000000
                                   00000000:00000000:00000000
                                   00010190:00020000FF960800
                                   ARP     03:08:24
IP       Fast Ethernet2/3          172.20.52.20(11)
                                   0A000000:00000000:
                                   00000000:FFFFC0A8:
                                   00000000:00000000:00000000
                                   00000000:00000000:00000000
                                   00010190:00020000FF960800
                                   ARP     03:08:24
Switch#
```

This example shows how to display adjacency information for a specific interface:

```
Switch# show adjacency fastethernet2/3
Protocol Interface                 Address
IP       Fast Ethernet2/3          172.20.52.1(10469)
IP       Fast Ethernet2/3          172.20.52.20(11)
Switch#
```

Related Commands

Command	Description
debug adjacency	Displays information about the adjacency debugging.

show ancp multicast

To display multicast streams activated by Access Node Control Protocol (ANCP), use the **show ancp multicast** command.

show ancp multicast [**group** *groupaddr*] [**source** *sourceaddr*] | [| **interface** *interfacename*]

Syntax Description	**group** *groupaddr* (Optional) Specifies a multicast group address. **source** *sourceaddr* (Optional) Specifies a multicast source address. **interface** *interfacename* (Optional) Specifies a multicast flowing on a specific interface.
Defaults	Displays all the multicast streams activated with ANCP.
Command Modes	Privileged EXEC
Examples	This example shows how to display multicast streams activated by ANCP:

```
ANCP-Client# show ancp mcl
ANCP Multicast Streams
Interfaces Vlan Interface Joined on
Group 238.2.2.1
0a010600000a0000 116 Fa7/6 18:27:05 UTC Sat Sep 13 2008
0a010600000a0000 116 Fa7/5 18:27:05 UTC Sat Sep 13 2008
0a010600000a0000 116 Fa7/4 18:27:05 UTC Sat Sep 13 2008
0a010600000a0000 116 Fa7/6 18:26:41 UTC Sat Sep 13 2008
Group 238.2.2.2
0a010600000a0000 116 Fa7/6 18:27:07 UTC Sat Sep 13 2008
0a010600000a0000 116 Fa7/5 18:27:07 UTC Sat Sep 13 2008
0a010600000a0000 116 Fa7/4 18:26:43 UTC Sat Sep 13 2008
0a010600000a0000 116 Fa7/6 18:26:43 UTC Sat Sep 13 2008
ANCP-Client#
```

show arp access-list

To display detailed information on an ARP access list, use the **show arp** command.

show arp access-list

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes EXEC

Examples This example shows how to display the ARP ACL information for a switch:

```
Switch# show arp access-list
arp access-list mac-arp
    permit ip 10.101.1.1 0.0.0.255 mac any
    permit ip 10.1.1.0 0.0.0.255 mac any
```

Related Commands	Command	Description
	access-group mode	Specifies the override modes (for example, VACL-override PACL) and the non-override modes (for example, merge or strict mode).
	arp access-list	Defines an ARP access list or adds clauses at the end of a predefined list.
	ip arp inspection filter vlan	Permits ARPs from hosts that are configured for static IP when DAI is enabled, defines an ARP access list, and applies the access list to a VLAN.

show authentication

To display the Auth Manager information, use the **show authentication** command in EXEC or Privileged EXEC mode.

show authentication [**interface** *interface*] [**registration** [**sessions** [**session-id** *session-id*] [**handle** *handle*] [**interface** *interface*] [**mac** *mac*] [**method** *method*] [**interface** *interface* [**details** | **policy**]]

Syntax Description

interface *interface*	Displays all of the Auth Manager details associated with the specified interface.
registrations	Displays details of all methods registered with the Auth Manager.
sessions	Displays details of the current Auth Manager sessions (for example, client devices). If you do not enter any optional specifiers, all current active sessions are displayed. You can enter the specifiers singly or in combination to display a specific session (or group of sessions).
session-id *session-id*	(Optional) Specifies an Auth Manager session.
handle *handle*	(Optional) Specifies the particular handle for which Auth Manager information is displayed. Range is 1 to 4294967295.
mac *mac*	(Optional) Displays Auth Manager session information for a specified MAC address.
method *method*	(Optional) Displays all clients authorized by a specified authentication method. Valid values are as follows: • **dot1x** • **mab** • **webauth**
interface *interface* **details**	(Optional) Displays detailed information.
interface *interface* **policy**	(Optional) Displays policies applied on the interface.

Command Default This command has no default settings.

Command Modes EXEC

Usage Guidelines Table 2–10 describes the significant fields shown in the show authentication display.

Note The possible values for the status of sessions are given below. For a session in terminal state, "Auths Success" or "Auths Failed" are displayed. "No method" is displayed if no method has provided a result.

Table 2-22 *show authentication Command Output*

Field	Description
Idle	The session has been initialized and no methods have ran yet.
Running	A method is running for this session.
No methods	No method has provided a result for this session.
Authc Success	A method has resulted in authentication success for this session.
Authc Failed	A method has resulted in authentication fail for this session.
Authz Success	All features have been successfully applied for this session.
Authz Failed	A feature has failed to be applied for this session.

Table 2-11 lists the possible values for the state of methods. For a session in terminal state, "Authc Success," "Authc Failed," or "Failed over" are displayed if the latter indicates a method and failed over is the next method which did not provide a result. "Not run" is displayed in the case of sessions that are synchronized on standby.

Table 2-23 *State Method Values*

Method State	State Level	Description
Not run	Terminal	The method has not run for this session.
Running	Intermediate	The method is running for this session.
Failed over	Terminal	The method has failed and the next method is expected to provide a result.
Authc Success	Terminal	The method has provided a successful authentication result for the session.
Authc Failed	Terminal	The method has provided a failed authentication result for the session.

Examples

The following example shows how to display authentication methods registered with Auth Manager:

```
Switch# show authmanager registered-methods
Auth Methods registered with the Auth Manager:
Handle Priority Name
2 0 dot1x
3 1 mab
5 2 webauth
4 3 dot1x_vlan
```

The following example shows how to display Auth Manager details for a specific interface:

```
Switch# show authmanager interface gigabitethernet1/23
Idle
Interface Domain Status Handle Interface
GDia Full UNAUTH 0x1a000c00 GigabitEthernet1/0/23
Available methods list:
Handle Priority Name
```

```
3 0 dot1x
Normalmib methods list:
Handle Security Name
3 0 dot1x
Switch#
```

The following example shows how to display all Auth-Manager sessions on the switch:

```
Switch#show authentication sessions
Interface MAC Address   Method  Domain  Status     Session ID
Gi1/1/10  0000.0000.0000 dot1x  DATA    Authz Fail 0A0A0A0A0000000B0B9B6D9D
Gi1/1/10  (unknown)     N/A     DATA    Auth Fail  0A0A0A0A0000000C0B9B6D7C
```

The following example shows how to display all Auth-Manager sessions on an interface:

```
Switch#show authentication sessions int gi 1/48
            Interface:  GigabitEthernet1/48
              MAC Address:  Unknown
               IP Address:  Unknown
                   Status:  Authz Success
                   Domain:  DATA
     Oper host-mode:  multi-host
   Oper control-dir:  both
     Authorized By:  Guest Vlan
        Vlan Group:  Vlan: 2
  Session timeout:  N/A
     Idle timeout:  N/A
  Common Session ID:  0A0A0A0A0000000E0B9B7274
        Acct Session ID:  0x00000006
                 Handle:  0x00000008
Normalmib methods list:
    Method   State
    dot1x    Failed over
```

The following example shows how to display Auth Manager session for a specified MAC address:

```
Switch#show authentication sessions mac 000a.8ad.0f86
            Interface:  GigabitEthernet1/23
              MAC Address:  000a.8ad.0f86
               Status:  Authz Success
               Domain:  DATA
     Oper host-mode:  single-host
   Authorized By:  Authentication Server
        Vlan Group:  N/A
          Handle:  0x88000003
Normalmib methods list:
    Method   State
    dot1x    Authz Success
Switch#show authentication sessions mac 000a.8ad.0f86 detail
            Interface:  GigabitEthernet1/23
              MAC Address:  000a.8ad.0f86
               Status:  Authz Success
               Domain:  DATA
     Oper host-mode:  single-host
   Authorized By:  Authentication Server
        Vlan Group:  N/A
          Handle:  0x88000003
Runnable methods list:
    Method   State
    dot1x    Authz Success
Switch#
```

The following example shows how to display all clients authorized via a specified auth-method:

```
Switch#show authentication sessions method mab
No Auth Manager contexts match supplied criteria
Switch#show authentication sessions method dot1x
MAC Address Domain Status Handle Interface
000a.8ad.0f86 DATA Authz Success 0x88000003 GigabitEthernet1/23
Switch#
```

The following example shows the policies applied on interface *ethr*:

```
Switch#show authentication sessions interface ethr policy
            Interface:  Ethernet0/0
              MAC Address:  aabb.cc00.0100
```

```
                IPv6 Address:  Unknown
                  Port Number:  1812
                  User-Name:    pagar
                  Status:       Authorized
                  Method:       dot1x
                Security Policy:  Should Secure
                Security Status:  Unsecure
                Open Edge:        Disabled
                Power Down:       Disabled
                Restart Count:    0-0-0
                Common Session ID:  C0A16301000000040013284
                Acct Session ID:  Unknown
                  Handle:         0x66000006
                  Current Policy:  POLICY_DOT1X

        Local Policies:
                  Template: DOT_1  (priority 10)
                    Idle timeout:  900 sec
                                   Type:  idle
                  URL Redirect:  www.a.com
                URL Redirect ACL:  a

                  Template: DOT_2  (priority 20)
                    Idle timeout:  180 sec
                                   Type:  idle
                  URL Redirect:  www.b.com
                URL Redirect ACL:  b

        Server Policies:
                    Idle timeout:  800 sec

        Resultant policies:
                    Idle timeout:  180 sec
                                   Type:  idle
                  URL Redirect:  www.a.com
                URL Redirect ACL:  a
                                   Type:  idle

        Method status list:
                  Method          State
                  dot1x           Author Success
```

Related Commands:	Command	Description
	authentication control-direction	Changes the port control to unauthorized or bidirectional.
	authentication critical recovery delay	Configures the 802.1X critical authentication parameters.
	authentication event	Configures the actions for authentication events.
	authentication fallback	Enables the Webauth fallback and specifies the fallback profile to use when failing over to Webauth.
	authentication host-mode	Defines the classification of a session that will be used to apply the access-policies using the host-mode configuration.
	authentication open	Enables open access on this port.
	authentication order	Specifies the order in which authentication methods should be attempted for a client on an interface.

Command	Description
authentication periodic	Enables reauthentication for this port.
authentication port-control	Configures the port-control value.
authentication priority	Specifies the priority of authentication methods on an interface.
authentication timer	Configures the authentication timer.
authentication violation	Specifies the action to be taken when a security violation exists on a port.

show auto install status

To display the status of an automatic installation, use the **show auto install status** command.

show auto install status

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Examples This example shows how to display the IP address of the TFTP server and to display whether or not the switch is currently acquiring the configuration file on the TFTP server:

```
Switch# show auto install status

Status                  : Downloading config file
DHCP Server             : 20.0.0.1
TFTP Server             : 20.0.0.1
Config File Fetched     : Undetermined
```

The first IP address in the display indicates the server that is used for the automatic installation. The second IP address indicates the TFTP server that provided the configuration file.

show auto qos

To display the automatic quality of service (auto-QoS) configuration that is applied, use the **show auto qos** auto-EXEC command.

show auto qos [**interface** *interface-id*] [{**begin** | **exclude** | **include** } *expression*]

Syntax Description

interface *interface-id*	(Optional) Displays auto-QoS information for the specified interface or interfaces. For *interface-id*, specify the interface type.
begin	(Optional) Begins with the line that matches the expression.
exclude	(Optional) Excludes lines that match the expression.
include	(Optional) Includes lines that match the specified expression.
expression	(Optional) Expression in the output to use as a reference point.

Command Modes Privileged EXEC mode

Usage Guidelines The **show auto qos interface** *interface-id* command displays the auto-QoS configuration; it does not display any user changes to the configuration that might be in effect.

To display information about the QoS configuration that might be affected by auto-QoS, use one of these commands:

- **show qos**
- **show qos map**
- **show qos interface** *interface-id*
- **show running-config**

Expressions are case sensitive. For example, if you enter **exclude output**, the lines that contain output display, but the lines that contain Output appear.

Examples This example shows output from the **show auto qos** command when auto-QoS is enabled:

```
Switch#show auto qos
GigabitEthernet1/2
auto-qos voip cisco-phone
Switch#
```

Related Commands

Command	Description
auto qos voip	Automatically configures quality of service (auto-QoS) for Voice over IP (VoIP) within a QoS domain.

show bootflash:

To display information about the bootflash: file system, use the **show bootflash:** command.

show bootflash: [all | chips | files]

Syntax Description	**all** (Optional) Displays all possible Flash information.
	chips (Optional) Displays Flash chip information.
	files (Optional) Displays file system information.

Defaults This command has no default settings.

Command Modes EXEC

Examples This example shows how to display file system status information:

```
Switch> show bootflash: /fileops
-------- F I L E  S Y S T E M  S T A T U S --------
  Device Number = 0
DEVICE INFO BLOCK: bootflash:
  Magic Number        = 8A487205  File System Vers = 10000   (1.0)
  Length              = 800000    Sector Size     = 40000
  Programming Algorithm = 29      Erased State    = FFFFFFFF
  File System Offset  = 40000     Length = F80000
  MONLIB Offset       = 200       Length = 1E28
  Bad Sector Map Offset = 7FF400  Length = 400
  Squeeze Log Offset  = FE6000    Length = 4000
  Squeeze Buffer Offset = FE5000  Length = 4000
  Number of Files     = 0
    (Spare)
STATUS INFO:
  writable
  NO Files Open for Write
  Complete State
  No Unerased Errors
  No Squeeze in progress
USAGE INFO:
  Bytes Used     = 929288  Bytes Available = 6D0118
  Bad Sectors    = 0       Spared Sectors = 0
  OTHER INFO:    = 0       Bytes Used     = 0
  Deleted Files  = 0       Bytes = 0
  Files w/Errors = 0       Bytes = 0
Switch>
```

This example shows how to display system image information:

```
Switch> show bootflash:
-rw-  4194304  Jan 01 1970 00:00:00 +00:00  c6sup12-jsv.bin
2  .. image    D6DB8E20  ffffffff  ad  [4194304 bytes] (1 bytes free)
2  .. image    D6DB8E20  97C5CB8  *  7d72034 Sep 20 1999 13:46:49 sp.halley
Switch>
```

This example shows how to display all bootflash information:

```
Switch> show bootflash: all
-rw-   4151079   Jan 30 2000 00:07:00 +00:00  slot0:image_c2-c2k2-mz.122-18.EW.bin
1   .  image   NONVOLTAL  LITEON   16  [4063840 Aug 23 1999 16:36:45 +0:00]  on-board:
ms
2   .  image   DAHENGED  NVTOSH   9  [727008 Sep 20 1999 13:48:49 gp-bailey

4194304 bytes available (5534496 bytes used)

-------- F I L E  S Y S T E M  S T A T U S --------
  Device Number = 0
DEVICE INFO BLOCK: bootflash
  Magic Number        = 6887635  File System Vers = 10000   (1.0)
  Feature Bits        = 00000000  Sub-Blocks      = 254
  Programming Algorithm = 19     Erased Byte       = FFFFFFFF
  File System Offset  = 65600    Length = F42400
  MONLIB Offset       = 100      Length = C3F0
  Bad Sector Map Offset = 10F8   Length = 2
  Squeeze Log Offset  = F96600   Length = 40000
  Squeeze Buffer Offset = F9C600 Length = 40000
  Num Spare Sectors   = 0
    Spares:
STATUS INFO:
  Write Ena = 0
  GC File Space Dirt Unit
  Complete Status
  No Unrecovered Errors
  Squeeze Log Is in progress
USAGE INFO:
  Bytes Used          = 917088  Bytes Available = 424512
  Spare Sectors       = 0       Bytes = 0
  Of Files            = 2       Bytes = 917088
  Deleted Files       = 0       Bytes = 0
  Files w/Errors      = 0       Bytes = 0
Switch>
```

show bootvar

To display BOOT environment variable information, use the **show bootvar** command.

show bootvar

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Examples This example shows how to display BOOT environment variable information:

```
Switch> show bootvar
BOOT variable = sup:1;
CONFIG_FILE variable does not exist
BOOTLDR variable does not exist
Configuration register is 0x0
Switch>
```

show cable-diagnostics tdr

To display the test results for the TDR cable diagnostics, use the **show cable-diagnostics tdr** command.

show cable-diagnostics tdr {**interface** {*interface interface-number*}}

Note This command will be deprecated in future Cisco IOS releases; use the **diagnostic start** command instead.

Syntax Description

interface *interface*	Interface type; valid values are **fastethernet** and **gigabitethernet**.
interface-number	Module and port number.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Usage Guidelines The TDR test is supported for the following line cards only:

- WS-X4148-GB-RJ45
- WS-X4124-GB-RJ45V
- WS-X4224-GB-RJ45V
- WS-X4413-TS
- WS-C4948
- WS-C4948-10GE

The distance to the fault is displayed in meters (m).

Examples This example shows how to display information about the TDR test:

```
Switch#show cable-diagnostics tdr interface gi4/1
Interface Speed Local pair Cable Length Remote pair Status
Gi4/1     10Mbps  1-2     102 +/- 2m    1-2         Fault
                  3-6     102 +/- 2m    3-6         Fault
                  4-5     102 +/- 2m    4-5         Fault
                  7-8     102 +/- 2m    7-8         Fault
Switch#
```

Table 2-12 describes the fields in the **show cable-diagnostics tdr** command output.

Table 2-12 show cable-diagnostics tdr Command Output Fields

Field	Description
Interface	Interface tested.
Speed	Current line speed.
Pair	Cable pair name.
Cable Length	Distance to the fault in meters (m).
Channel	Pair designation (A, B, C, or D).
Status	Pair status displayed in one of the following: • Terminated—The link is up. • Fault—Cable fault (open or short)

Related Commands:	Command	Description
	test cable-diagnostics tdr	Tests the condition of copper cables on 48-port 10/100/1000 BASE-T modules.

show call-home

To display the configured CallHome information, use the **show call-home** command in privileged EXEC mode.

show call-home [alert-group | detail | mail-server | profile {all | name} | statistics]

Syntax Description		
	alert-group	(Optional) Displays the available alert group.
	detail	(Optional) Displays the CallHome configuration in detail.
	mail-server	(Optional) Displays the CallHome mail server-related information.
	profile all	(Optional) Displays configuration information for all existing profiles.
	profile *name*	(Optional) Displays configuration information for a specific destination profile.
	statistics	(Optional) Displays the CallHome statistics.

Command Default This command has no default settings.

Command Modes Privileged EXEC (#)

Examples The following example displays the configured CallHome settings:

```
Switch# show call-home
Current call home settings:
    call home feature : disable
    call home feature name : destination address
    call home message's sender address: support@example.com

    call home message's reply-to address: support@example.com

    vrf for call-home messages: Not yet set up

    contact person's email address: technical@example.com

    contact person's phone number: +1-408-555-1234
    street address: 1234 Picdmon Street, Any city, Any state, 12345
    customer id: Customer1
    contract id: Contract1
    site ID: Santafe1
    Mail-server[1]: Address: smtp.example.com Priority: 1
    Mail-server[2]: Address: 192.168.0.1 Priority: 2
    Rate-limit: 20 messages/min accepted

    Available alert groups:
       Keyword                  State   Description
       ------------------------------------------------------------
       configuration            Disable configuration info
       diagnostic               Disable diagnostic info
       environment              Disable environmental info
       inventory                Disable inventory info
       syslog                   Disable syslog info

    Profiles:
       Profile Name: campus-noc
```

```
        Profile Name: CiscoTAC-1

Sat+Sun

Configured Call-Home Information in Detail:

Sat+Sun show call-home detail
Profile name: campus-noc
call home from hostname : c3ka6k
call home message's from address: sntc@c3ka6k.cse
call home message's reply-to address: campus@c3ka6k.cse

vrf for call-home messages: Not yet set up

contact person's email address: technical@c3ka6k.cse

contact person's phone number: +1-408-555-1234
street address: 170 West Tasman Drive, Any city, Any state, 12345
customer ID: Example
contract ID: 2012345678
site ID: SJ-001
Mail server[1]: Address: smtp.example.com Priority: 1
Mail server[2]: Address: 192.168.0.1 Priority: 2
Rate-limit: 20 message(s) per minute

Available alert groups:
    Keyword                         State  Description
                                    ------ -----------------------------
    configuration                   Disble configuration info
    diagnostic                      Disble diagnostic info
    environment                     Disble environment info
    inventory                       Disble inventory info
    syslog                          Disble syslog info

Profile: CiscoTAC-1

Profile Name: campus-noc
    Profile status: ACTIVE
    Preferred Message Format: long text
    Mail server address: 192.168.0.1:25
    Transport Method: email
    Email address(s): noc@campus.cse
    HTTP address(s): Not yet set up

    Alert-group                         Severity
    -----------                         --------
    inventory                           normal

    Syslog-Pattern                      Severity
    --------------                      --------
    N/A                                 N/A

Profile Name: CiscoTAC-1
    Profile status: ACTIVE
    Preferred Message Format: long text
    Mail server address: 192.168.0.1:25
    Transport Method: email
    Email address(s): technical@c3ka6k.cse
    HTTP address(s): https://tools.cisco.com/its/service/oddce/services/DDCEService

    Periodic configuration info message is scheduled every 1 day of the month at 09:27

    Periodic inventory info message is scheduled every 1 day of the month at 09: 12
```

```
  Alert-group              Severity
  ================         ============
  diagnostic               minor
  environment              warning
  inventory                normal

  Syslog-Pattern           Severity
  ================         ============
  .*                       major

Switch#
```

Available Call Home Alert Groups

```
Switch#show call-home alert-group
Available alert groups:
  Keyword                  State   Description
                           ------- ----------------------------
  configuration            Disable configuration info
  diagnostic               Disable diagnostic info
  environment              Disable environmental info
  inventory                Enable  inventory info
  syslog                   Disable syslog info

Switch#
```

E-Mail Server Status Information

```
Switch#show call-home mail-server status
Please wait. Checking for mail server status ...

Translating "smtp.example.com"
    Mail-server[1]: Address: smtp.example.com Priority: 1 [Not Available]
    Mail-server[2]: Address: 192.168.0.1 Priority: 2 [Not Available]

Switch#
```

Information for All Destination Profiles (Predefined and User Defined)

```
Switch#show call-home profile all

Profile name: campus-noc
    Profile status: ACTIVE
    Preferred Message Format: long-text
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(s): noc@example.com
    HTTP address(s): Not yet set up

    Alert-group              Severity
    ================         ============
    Inventory                normal

    Syslog-Pattern           Severity
    ================         ============
    N/A                      N/A

Profile Name: CiscoTAC-1
    Profile status: ACTIVE
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(s): callhome@cisco.com
    HTTP address(s): https://tools.cisco.com/its/service/oddce/services/DDCSService

Switch#
```

```
Periodic configuration info message is scheduled every 1 day of the month at 09:27

Periodic inventory info message is scheduled every 1 day of the month at 09:12

Alert-group             Severity
------------            ------------
diagnostic              minor
environment             warning
inventory               normal

Syslog-Pattern          Severity
--------------          ------------
.*                      major

Switch#
```

Information for a User Defined Destination Profile

```
Switch# show call-home profile (test@mail)
Profile Name: (test@mail)
    Profile status: ACTIVE
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email addresses: test@email.com
    HTTP addresses: https://tools.cisco.com/its/service/oddce/services/DDCEService

    Periodic configuration info message is scheduled every 11 day of the month at 11:26

    Periodic inventory info message is scheduled every 31 day of the month at 11:10

    Alert-group             Severity
    ------------            ------------
    diagnostic              minor
    environment             warning
    inventory               normal

    Syslog-Pattern          Severity
    --------------          ------------
    .*                      major

Call-Home Statistics
Switch# show call-home statistics
Message Types   Total       Email       HTTP
-------------------------------------------------------------
Init Rcvrcmn    0           0           0
  Config          0           0           0
  Diagnostic      0           0           0
  Environment     0           0           0
  Inventory       0           0           0
  Syslog          0           0           0
  Test            0           0           0
  Request         0           0           0
  Send-CLI        0           0           0

Total Dr-Queue  0           0           0
  Config          0           0           0
  Diagnostic      0           0           0
  Environment     0           0           0
  Inventory       0           0           0
  Syslog          0           0           0
  Test            0           0           0
```

```
        Response:   0                   0                   0
        Send-CLI    0                   0                   0

Total Failed        0                   0                   0
    dropped         0                   0                   0
    Disabled:       0                   0                   0
    Rate-limited:   0                   0                   0
    Invalid:        0                   0                   0
    Nosubscriber    0                   0                   0
    System          0                   0                   0
    Text            0                   0                   0
    Response        0                   0                   0
    Send-CLI        0                   0                   0

Total Ratelimit
    dropped         0                   0                   0
    Disabled:       0                   0                   0
    Ratelimited:    0                   0                   0
    Nosubscriber    0                   0                   0
    System          0                   0                   0
    Text            0                   0                   0
    Response        0                   0                   0
    Send-CLI        0                   0                   0

Last call-home message sent time: n/a
```

Related Commands	Command	Description
	call-home (global configuration)	Enters call-home configuration mode.
	call-home send alert-group	Sends a specific alert group message.
	show call-home (refer to Cisco IOS documentation)	Displays configuration information.

show cdp neighbors

To display detailed information about the neighboring devices that are discovered through CDP, use the **show cdp neighbors** command.

show cdp neighbors [*type number*] [**detail**]

Syntax Description

type	(Optional) Interface type that is connected to the neighbors about which you want information; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **port-channel**, and **vlan**.
number	(Optional) Interface number that is connected to the neighbors about which you want information.
detail	(Optional) Displays detailed information about a neighbor (or neighbors) including network address, enabled protocols, hold time, and software version.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

The **vlan** keyword is supported in Catalyst 4500 series switches that are configured with a Supervisor Engine 2.

The **port-channel** values are from 0 to 282; values from 257 to 282 are supported on the CSM and the FWSM only.

Examples

This example shows how to display the information about the CDP neighbors:

```
Switch# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
                                     (sec)
                                                                   TenGigEth  Fas 0/10
lab-ss6500-1     Eth 4             143        R S I       WS-C6506  Fas 0/10
lab-ss6500-2     Eth 5             143        R S I       WS-C6506  Fas 0/10
lab-ss6500-3     Eth 6             143        R S I       WS-C6506  Fas 0/10
lab-ss6500-4     Eth 7             143        R S I       WS-C6506  Fas 0/10
lab-ss6500-5     Eth 8             132        R S I       WS-C6506  Fas 0/10
lab-ss6500-6     Eth 9             132        R S I       WS-C6506  Fas 0/10
                                                                   Eth 0/1
SSG24.2-27588    Eth 4             124        H           AIR-AP350 2/4
Switch#
```

Table 2-13 describes the fields that are shown in the example.

Table 2-13 *show cdp neighbors* Field Descriptions

Field	Definition
Device ID	Configured ID (name), MAC address, or serial number of the neighbor device.
Local Intrfce	(Local interface) The protocol that is used by the connectivity media.
Holdtime	Remaining amount of time, in seconds, that the current device holds the CDP advertisement from a transmitting router before discarding it.
Capability	Capability code that is discovered on the device. This device type is listed in the CDP Neighbors table. Possible values are as follows: R—Router T—Transparent bridge B—Source-routing bridge S—Switch H—Host I—*IGMP device* r—Repeater P—Phone
Platform	Product number of the device.
Port ID	Protocol and port number of the device.

This example shows how to display detailed information about your CDP neighbors:

```
Switch# show cdp neighbors detail
-------------------------
Device ID: lab-7206
Entry address(es):
  IP address: 172.19.149.87
Platform: cisco 7206, Capabilities: Router
Interface: Ethernet1, Port ID (outgoing port): FastEthernet0/0
Holdtime : 125 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) 7200 Software (C7200-JS-M), Version 12.1(2)
Copyright (c) 1986-2002 by Cisco Systems, Inc.

advertisement version: 2
Duplex: half

-------------------------
Device ID: lab-ae5500-1
Entry address(es):
  IP address: 172.19.149.97

.
.
.
Switch#
```

Table 2-14 describes the fields that are shown in the example.

Table 2-14 show cdp neighbors detail Field Descriptions

Field	Definition
Device ID	Name of the neighbor device and either the MAC address or the serial number of this device
Entry address(es)	List of network addresses of neighbor devices.
[network protocol] address	Network address of the neighbor device. The address can be IP, IPX, AppleTalk, DECnet, or CLNS protocol address.
Platform	Product name and number of the neighbor device.
Capabilities	Device type of the neighbor. This device can be a router, bridge, router-bridge, a source-routing-bridge, a switch, a host, an IGMP device, or a repeater.
Interface	Protocol and port number of the port on the current device.
Holdtime	Remaining amount of time, in seconds, that the current device holds the CDP advertisement from a transmitting router before discarding it.
Version:	Software version running on the neighbor device.
advertisement version:	Version of CDP that is being used for CDP advertisements.
Duplex	Duplex state of connection between the current device and the neighbor device.

Related Commands

Command	Description
show cdp (refer to Cisco IOS documentation)	Displays global CDP information, including timer and hold-time information.
show cdp entry (refer to Cisco IOS documentation)	Displays information about a specific neighboring device discovered using Cisco Discovery Protocol (CDP).
show cdp interface (refer to Cisco IOS documentation)	Displays information about the interfaces on which Cisco Discovery Protocol (CDP) is enabled.
show cdp traffic (refer to Cisco IOS documentation)	Displays traffic information from the CDP table.

show class-map

To display class map information, use the **show class-map** command.

show class-map *class_name*

Syntax Description | *class_name* | Name of the class map.

Defaults | This command has no default settings.

Command Modes | Privileged EXEC mode

Examples | This example shows how to display class map information for all class maps:

```
Switch# show class-map
Class Map match-any class-default (id 0)
  Match any
Class Map match-any class-simple (id 2)
  Match any
Class Map match-all ipp5 (id 1)
  Match ip precedence 5
Class Map match-all ipp2 (id 3)
Switch#
```

This example shows how to display class map information for a specific class map:

```
Switch# show class-map ipp5
Class Map match-all ipp5 (id 1)
  Match ip precedence 5
Switch#
```

Assume there are two active flows as shown below on Fast Ethernet interface 6/1:

```
Src IP          Dst IP          IpProt SrcLkPort DstLkPort
---------------------------------------------------------------
192.168.10.10 192.168.20.20  20    4789     41
192.168.10.10 192.168.20.20  20    4789     24
```

With following configuration, each flow will be policed to a 1000000 bps with an allowed 9000-byte burst value.

Note | If you use the **match flow ip source-address/destination-address** command, these two flows are consolidated into one flow and they have the same source and destination address.

```
Switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# class-map c1
Switch(config-cmap)# match flow ip source-address ip destination-address ip protocol 14
Switch(config-cmap)# exit policy-map pm1
Switch(config)# class c1
Switch(config-pmap)# policy-map p1
Switch(config-pmap)# class c1
```

```
Switch(config-pmap-c)# police 1000000 9000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastEthernet 6/1
Switch(config-if)# service-policy input p1
Switch(config-if)# end
Switch# write memory
Switch# show policy-map interface
FastEthernet6/1

class-map c1
  match flow ip source-address ip destination-address ip protocol 14 source-port 14
destination-port

 policy-map p1
  class c1
    police 1000000 bps 9000 byte conform-action transmit exceed-action drop

interface FastEthernet 6/1
  service-policy input p1

Switch# show class-map c1
Class Map match-all c1 (id 2)
   Match flow ip source-address ip destination-address ip protocol 14 source-port 14
destination-port
Switch#
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to the class whose name you specify and to be used enter class-map configuration mode.
show policy-map	Displays information about the policy map.
show policy-map interface	Displays the statistics and configuration of the input and output policies that are attached to an interface.

show diagnostic content

To display test information about the test ID, test attributes, and supported coverage test levels for each test and for all modules, use the **show diagnostic content** command.

show diagnostic content module {**all** | *num*}

Syntax Description	**all**	Displays all the modules on the chassis.
	num	Module number.

Defaults This command has no default settings.

Command Modes EXEC.

Examples This example shows how to display the test name, monitoring interval, and test attributes for all the modules of the chassis:

```
Switch> show diagnostic content module all

module 1:

Diagnostic test suite attributes:
  B/* - Basic ondemand test / NA
  P/V/* - Per port test / Per device test / NA
  D/N/* - Disruptive test / Non-disruptive test / NA
  S/*/* - Not a health monitoring test / NA
  */I/* - Only a health monitoring test / NA
  */*/I - Fixed monitoring interval test / NA
  */*/* - Always enabled monitoring test / NA
  m/*/* - Mandatory bootup test, can't be disabled / NA
  */e/* - Mandatory bootup test, can't be bypassed / NA
  */*/o - Ongoing test, always active / NA

                                                      Testing Interval
ID  Test Name                          Attributes     (day hh:mm:ss.ms)
1   supervisor-bootup                  m/P/V/*/*      not configured
2)  supervisor-bootup ------------------ m/P/V/*/*e   not configured
3)  packet-memory-bootup ---------------- m/P/V/*/*e   not configured
4)  packet-memory-ongoing --------------- */P/V/*/*o   not configured

module 6:

Diagnostic test suite attributes:
  B/* - Basic ondemand test / NA
  P/V/* - Per port test / Per device test / NA
  D/N/* - Disruptive test / Non-disruptive test / NA
  S/*/* - Not a health monitoring test / NA
  */I/* - Not a health monitoring test / NA
  */*/I - Fixed monitoring interval test / NA
  */*/* - Always enabled monitoring test / NA
  m/*/* - Mandatory bootup test, can't be disabled / NA
  */e/* - Mandatory bootup test, can't be bypassed / NA
  */*/o - Ongoing test, always active / NA
```

```
                                                        Test(sec) Interval:
ID  Test Name                                Attributes  [day:hh:mm:ss.ms]
---- ---------------------------------------- ----------- -----------------
  1) Internal Ethernet Loop-Back              **N**N**N*  none  none(0 ignored)

End of list
```

Related Commands:	Command	Description
	show diagnostic result module	Displays the module-based diagnostic test results.
	show diagnostic result module test 2	Displays the results of the bootup packet memory test.
	show diagnostic result module test 3	Displays the results from the ongoing packet memory test.

show diagnostic result module

To display the module-based diagnostic test results, use the **show diagnostic result module** command.

show diagnostic result module [*slot-num* | **all**] [**test**] [*test-id* | *test-id-range* | **all**] [**detail**]

Syntax Description	*slot-num* (Optional) Specifies the slot on which diagnostics are displayed.
	all (Optional) Displays the diagnostics for all slots.
	test (Optional) Displays selectedtests on the specified module.
	test-id (Optional) Specifies a single test ID.
	test-id-range (Optional) Specifies a range of test IDs.
	all (Optional) Displays the diagnostics for all tests.
	detail (Optional) Displays the complete test results.

Defaults A summary of the test results for all modules in the chassis is displayed.

Command Modes Privileged EXEC mode

Examples This example shows how to display the summary results for all modules in the chassis:

```
Switch# show diagnostic result module

Current bootup diagnostic level: minimal

module 1:

  Overall diagnostic result: PASS
  Diagnostic level at card bootup: bypass

  Test results: (. = Pass, F = Fail, U = Untested)

    1) supervisor:Bootup ---------------------- U
    2) packet-memory:Bootup ------------------- U
    3) packet-memory:ongoing ------------------ U

module 2:

  Overall diagnostic result: PASS
  Diagnostic level at card bootup: minimal

  Test results: (. = Pass, F = Fail, U = Untested)

    1) linecard:online:diag ------------------ .

module 5:

  Overall diagnostic result: PASS
  Diagnostic level at card bootup: minimal
```

```
  Test results: (. = Pass, F = Fail, U = Untested)
  ___________________________________________________________________
   1) linecard-online-diag +++++++++++++++++++++++++++++++++++++++ .

module 6:

  Overall Diagnostic results: PASS
  Diagnostic level at card bootup: minimal

  Test results: (. = Pass, F = Fail, U = Untested)
  ___________________________________________________________________
   1) linecard-online-diag +++++++++++++++++++++++++++++++++++++++ .
```

This example shows how to display the online diagnostics for module 1:

```
Switch# show diagnostic result module 1 detail

Current bootup diagnostic level: minimal

module 1:

  Overall Diagnostic result: PASS
  Diagnostic level at card bootup: minimal

  Test results: (. = Pass, F = Fail, U = Untested)
  ___________________________________________________________________

   1) supervisor-bootup ++++++++++++++++++++++++++++++++++++++++ .

        Error code ------------------ 0 (DIAG_SUCCESS)
        Total run count -------------- 0
        Last test execution time ----- n/a
        First test failure time ------ n/a
        Last test failure time ------ n/a
        Last test pass time ---------- n/a
        Total failure count ---------- 0
        Consecutive failure count ---- 0

  Power-On-Self-Test Results for ACTIVE Supervisor

  Power-on-self-test for Module 1: WS-X6816
  Port Status: Enabled  Port Length: 2
  Event Reason: Power-On Self-Test

  Port TestFilter L2 Loopback ..
  0: . 1: . 2: . 3: . 4: . 5: . 6: . 7: . 8: . 9: . 10: . 11: .
  12: . 13: . 14: . 15: . 16: . 17: . 18: . 19: . 20: . 21: .
  22: . 23: . 24: . 25: . 26: . 27: . 28: . 29: . 30: . 31: .

  Port TestFilter L2 Loop+Loopback ..
  0: . 1: . 2: . 3: . 4: . 5: . 6: . 7: . 8: . 9: . 10: . 11: .
  12: . 13: . 14: . 15: . 16: . 17: . 18: . 19: . 20: . 21: . 22: .
  23: . 24: . 25: . 26: . 27: . 28: . 29: . 30: . 31: .

  Port TestFilter L3 Loop+Loopback ..
  0: . 1: . 2: . 3: . 4: . 5: . 6: . 7: . 8: . 9: . 10: . 11: .
```

```
10 , 19 , 14 , 35 , 16 , 17 , 18 , 39 , 20 , 21 , 22 , 23 ,
24 , 25 , 26 , 27 , 28 , 29 , 30 , 31 .

Switch Subsystem Memory ...
11 , 21 , 3 , 4 , 5 , 6 , 7 , 8 , 9 , 10 , 11 , 12 ,
13 , 14 , 35 , 36 , 37 , 38 , 39 , 20 , 21 , 22 , 23 , 24 ,
25 , 26 , 27 , 28 , 29 , 30 , 31 , 32 , 33 , 34 , 35 , 36 ,
37 , 38 , 39 , 40 , 41 , 42 , 43 , 44 , 45 , 46 , 47 , 48 ,
49 , 50 , 51 , 52 , 53 , 54 .

Module 1 Passed
```

```
2) packet-memory-bootup ------------------------.

        Error code ------------------------------ 0 (DIAG_SUCCEEDED)
        Total run count ------------------------- 1
        Last test execution time ---------------- n/a
        First test failure time ----------------- n/a
        Last test failure time ------------------ n/a
        Last test pass time --------------------- n/a
        Total consecutive failures -------------- 0
        Consecutive failure count --------------- 0
packet buffers on free list: 62457 bad: 0 used for ongoing traffic: 979

Number of errors found: 0
Total packet buffer errors (failed two or more tests): 0
Split buffer errors (failed one test, including bad: 0
Support bad buffs (uses a block that tested bad): 0
total buffers: 65536
bad buffers: 0 (0.00%)
good buffers: 65536 (100.0%)
Hexing test results:
No errors.
```

```
3) packet-memory-ongoing ------------------------- 0

        Error code ------------------------------ 0 (DIAG_SUCCEEDED)
        Total run count ------------------------- 1
        Last test execution time ---------------- n/a
        First test failure time ----------------- n/a
        Last test failure time ------------------ n/a
        Last test pass time --------------------- n/a
        Total failure count --------------------- 0
        Consecutive failure count --------------- 0
packet buffers on free list: 62457 bad: 0 used for ongoing traffic: 979

Packet memory errors: 0 0
Current alert level: green
Per 5 seconds in the last minute:
0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0
Per minute in the last hour:
0 0 0 0 0 0 0 0 0 0 0 0
```

```
        0 0 0 0 0 0 0 0 0 0
        0 0 0 0 0 0 0 0 0 0
        0 0 0 0 0 0 0 0 0 0
        0 0 0 0 0 0 0 0 0 0
Per hour in the last day:
        0 0 0 0 0 0 0 0 0 0
        0 0 0 0 0 0 0 0 0 0
        0 0 0 0 0 0 0 0 0 0
Per day in the last 30 days:
        0 0 0 0 0 0 0 0 0 0
        0 0 0 0 0 0 0 0 0 0
        0 0 0 0 0 0 0 0 0 0
Direct memory read failures per minute in the last hour:
        0 0 0 0 0 0 0 0 0 0
        0 0 0 0 0 0 0 0 0 0
        0 0 0 0 0 0 0 0 0 0
        0 0 0 0 0 0 0 0 0 0
        0 0 0 0 0 0 0 0 0 0
Potential false positives: 0 0
  Spurious bursts of no errors: 0 0
  Spurious bursts of one error: 0 0
  Spurious bursts of ok: 0 0
  Spurious bursts in frames received: 0 0
  Spurious sharing bus: 0 0
  Spurious bursts in frames sent: 0 0
  Spurious on high physport: 0
Ongoing diag action mode: Normal
Last 1000 Parity Memory errors:
Last 1000 Parity Memory errors:
First 1000 Parity Memory errors:
-----------------------------------------------------------------------------
Switch#
```

show diagnostic result module test

To display the results of the bootup packet memory test, use the **show diagnostic result module test** command. The output indicates whether the test passed, failed, or was not run.

show diagnostic result module [*N* | **all**] [**test** *test-id*] [**detail**]

N	(Optional) Specifies the module number.
all	(Optional) Specifies all modules.
test *test-id*	(Optional) Specifies the number for the test on the platform.
detail	(Optional) Specifies the display of detailed information for anyone.

Syntax Description

This option is recommended.

Defaults Non-detailed results.

Command Modes EXEC mode

Usage Guidelines The **detail** keyword is intended for use by Cisco support personnel when analyzing failures.

Examples This example shows how to display the results of the bootup packet memory test:

```
Router# show diagnostic result module 4 detail

module 4:

 Overall diagnostic result:PASS

 Test results:(. = Pass, F = Fail, U = Untested)

  ___________________________________________________________________________

  1) linecardfrontlinkbug ---------------------- .

        Error code ------------------ 0 (DIAG_SUCCESS)
        Total run count ------------- 1
        Last test execution time ---------- Jan 22 2001 19:48:50
        First test failure time ----------- n/a
        Last test failure time ------------ n/a
        Last test pass time --------------- Jan 22 2001 19:48:50
        Total failure count --------------- 0
        Consecutive failure count --------- 0
```

```
Slot Ports Card Type                                    Diag Status    Diag Details
---- ----- ---------------------------------------     -----------    ------------
 4    48   10/100/100Base7 (RJ45V), Clarify(CEF8       Passed         None

Detailed Status
---------------
. = Pass                    U = Unknown
1 = Loopback Failure        2 = Stub Failure
3 = Port Loopback Failure   4 = Port Stuck Failure
E = EEPROM Failure          C = CRC8 Integrity check Failure

Ports 1  2  3  4  5  6  7  8  9  10 11 12 13 14 15 16
      -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -

Ports 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32
      -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -

Ports 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48
      -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -

  ------------------------------------------------------------------------

  2) online diagnostic

  Ports 1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
        -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -

  Ports 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48
        -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -

  ------------------------------------------------------------------------

        Error code ------------------------ 0 (DIAG_SUCCEEDED)
        Total run count ------------------- 0
        Last test execution time ---------- Jan 22 2001 03:01:54
        First test failure time ----------- n/a
        Last test failure time ------------ n/a
        Last test pass time --------------- Jan 22 2001 03:01:54
        TestUnused ------------------------ FALSE
        Consecutive failure count --------- 0

Detailed Status
---------------
TEST result is in progress or Interface GiE/1

  ------------------------------------------------------------------------

  Exited
```

Related Commands

Command	Description
diagnostic start	Runs the specified diagnostic test.

show diagnostic result module test 2

To display the results of the bootup packet memory test, use the **show diagnostic result module test 2** command. The output indicates whether the test passed, failed, or was not run.

show diagnostic result module [**test 2** | **detail**]

Syntax Description		Specifies the module number.
	detail	(Optional) Specifies the display of detailed information for analysis.

Defaults Non-detailed results.

Command Modes EXEC mode

Usage Guidelines The **detail** keyword is intended for use by Cisco support personnel when analyzing failures.

Examples This example shows how to display the results of the bootup packet memory tests:

```
Switch# show diagnostic result module 1 test 2

Test results: ( . = Pass, F = Fail, U = Untested)

  2) packet-memory-bootup ----------- .
```

This example shows how to display detailed results from the bootup packet memory tests:

```
Switch# show diagnostic result module 1 test 2 detail

Test results: ( . = Pass, F = Fail, U = Untested)

  2) packet-memory-bootup ----------- .

        Error code ------------------ 0 (DIAG_SUCCEED)
        Total run count ------------- 1
        Last test execution time ---- n/a
        First test failure time ----- n/a
        Last test failure time ------ n/a
        Last test pass time --------- n/a
        Total failure count --------- 0
        Consecutive failure count --- 0
packet buffers on free list: 64557 badt 0 used for ongoing tests: 979

Number of errors found: 0
Total packet memory error detected run or memory tests: 0
Cells with soft errors (fixed ram test; infinite hard): 0
Suspect bad cells (uses a block that tested bad): 0
total buffers: 65536


```

```
Bad buffers: 0 (0.0%)
Bad packets: 0 (0.0%)
Sorting last results...
No errors.
```

Related Commands	Command	Description
	diagnostic monitor action	Directs the action of the switch when it detects a packet memory failure.
	show diagnostic result module test 2	Displays the results from the ongoing packet memory test.

show diagnostic result module test 3

To display the results from the ongoing packet memory test, use the **show diagnostic result module test 3** command. The output indicates whether the test passed, failed, or was not run.

show diagnostic result module [*mod*] **test 3** [**detail**]

Syntax Description	*mod* Module number.
	detail (Optional) Specifies the display of detailed information for analysis.

Defaults Non-detailed results.

Command Modes EXEC mode

Usage Guidelines The **detail** keyword is intended for use by Cisco support personnel when analyzing failures.

Examples This example shows how to display the results from the ongoing packet memory tests:

```
Switch# show diagnostic result module 1 test 3

Test results: (. = Pass, F = Fail, U = Untested)

  3) packet-memory-ongoing -------------- .
```

This example shows how to display the detailed results from the ongoing packet memory tests:

```
Switch# show diagnostic result module 1 test 3 detail

Test results: (. = Pass, F = Fail, U = Untested)


  3) packet-memory-ongoing -------------- .

        Error code ------------------ 0 (DIAG_SUCCESS)
        Total runs ------------------ 1
        Last test execution time ---- n/a
        First test failure time ----- n/a
        Last test failure time ------ n/a
        Last test pass time --------- n/a
        Total failure counts -------- 0
        Consecutive failure count --- 0
packet buffers on free list: 64557 badt 0 used for ongoing tests: 979


Packet memory errors: 0 0
Packet memory tests run:
Per 5 seconds in the last minute:
  0 0 0 0 0 0 0 0 0 0
  0 0
```

```
Per minute in the last hour:
    0 0 0 0 0 0 0 0 0 0
    0 0 0 0 0 0 0 0 0 0
    0 0 0 0 0 0 0 0 0 0
    0 0 0 0 0 0 0 0 0 0
    0 0 0 0 0 0 0 0 0 0
    0 0 0 0 0 0 0 0 0 0
Per hour in the last day:
    0 0 0 0 0 0 0 0 0 0
    0 0 0 0 0 0 0 0 0 0
    0 0 0 0
Per day in the last 30 days:
    0 0 0 0 0 0 0 0 0 0
    0 0 0 0 0 0 0 0 0 0
    0 0 0 0 0 0 0 0 0 0
Total packets processed per minute in the last hour:
    0 0 0 0 0 0 0 0 0 0
    0 0 0 0 0 0 0 0 0 0
    0 0 0 0 0 0 0 0 0 0
    0 0 0 0 0 0 0 0 0 0
    0 0 0 0 0 0 0 0 0 0
    0 0 0 0 0 0 0 0 0 0
Memory test suspended on card: 0 0
  Ignored because of no errors: 0 0
  Ignored because of ddr fifo reserve: 0 0
  Ignored because of ctx: 0 0
  Ignored because of packet threshold: 0 0
  Ignored during boot: 0 0
  Ignored after writing to state: 0 0
  Ignored because disabled: 0 0
Ongoing diag action mode: Normal
Last 1000 Memory Test Failures: 0
Last 1000 Packet Memory errors:
Fixed 1000 Packet Memory errors:
```

Related Commands	Command	Description
	diagnostic monitor action	Directs the action of the switch when it detects a packet memory failure.
	show diagnostic result module test 2	Displays the results of the boot-up packet memory test.

show dot1x

To display the 802.1X statistics and operational status for the entire switch or for a specified interface, use the **show dot1x** command.

show dot1x [**interface** *interface-id*] [**statistics** [**interface** *interface-id*]] | [**all**]

Syntax Description

interface *interface-id*	(Optional) Displays the 802.1X status for the specified port.
statistics	(Optional) Displays 802.1X statistics for the switch or the specified interface.
all	(Optional) Displays per-interface 802.1X configuration information for all interfaces with a nondefault 802.1X configuration.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.2(18)EW	Display enhanced to show the guest-VLAN value.
12.2(25)EW	Support for the IP-Optional feature image was introduced on the Catalyst 4500 series switch.
12.2(25)EWA	Support for currently assigned reauthentication timer (if the timer is configured to honor the Session-Timeout value) was added.
12.2(31)SG	Support for port direction control and critical recovery was added.

Usage Guidelines

If you do not specify an interface, the global parameters and a summary are displayed. If you specify an interface, the details for that interface are displayed.

If you enter the **statistics** keyword without the **interface** option, the statistics are displayed for all interfaces. If you enter the **statistics** keyword with the **interface** option, the statistics are displayed for the specified interface.

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.

The **show dot1x** command displays the currently assigned reauthentication timer and time remaining before reauthentication, if reauthentication is enabled.

Examples This example shows how to display the output from the **show dot1x** command:

```
Switch# show dot1x
System Authcontrol = Disabled
Dot1x Protocol Version = 2
Dot1x Oper Controlled Directions = Both
Dot1x Admin Controlled Directions = Both
Critical Recovery Delay = 500
Critical EAP = Enabled
Switch#
```

This example shows how to display the 802.1X statistics for a specific port:

```
Switch# show dot1x interface Fastethernet3/1
Dot1x Info for FastEthernet3/1
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = MULTI_DOMAIN
Port-control Value        = Disabled
Port Status               = AUTH
Quiet-Period              = 30
ReAuthPeriod              = 30
ReAuthMax                 = 2
max-reauth-req            = 2
TX period                 = 30
RestartPeriod             = 0
Port-control Value        = auto (locally configured)
Supplicant                = 00d0.b7c8.a0a1
MaxReq                    = 2
ReAuthenticate            = ON
RestartPeriod             = 0

Dot1x Authentication Client List
--------------------------------
Supplicant                = 0d0b
Supplicant                = 00d0.b7c8.a0a1
      Auth EAP State      = AUTHENTICATED
      Auth REQID EAP State = IDLE

Port Status               = AUTHORIZED
Authentication Method     = Dot1x
Authorized By             = Authentication Server
Time Policy               = 20

Supplicant                = 0b0d
Supplicant                = 00d0.b7c8.a0a1
      Auth EAP State      = AUTHENTICATED
      Auth REQID EAP State = IDLE

Port Status               = UNAUTHORIZED
Authentication Method     = Dot1x
Authorized By             = Authentication Server

Switch#
```

Note Table 2-45 provides a partial list of the displayed fields. The remaining fields on the display show internal state information. For a detailed description of these state machines and their settings, refer to the 802.1X specification.

Table 2-23 *show dot1x interface Field Description*

Field	Description
PortStatus	Status of the port (authorized or unauthorized). The status of a port is displayed as authorized if the **dot1x port-control** interface configuration command is set to **auto** and has successfully completed authentication.
Port Control	Setting of the **dot1x port-control** interface configuration command.
MaxReAuth	Setting of the **dot1x reauth-max** interface configuration command (allowed or disallowed).

This is an example of output from the **show dot1x statistics interface gigabitethernet1/5** command. Table 2-24 describes the fields in the display:

```
Switch#show dot1x statistics interface gigabitethernet1/5

PortSamples Parameters for Ge1/5
---------------------------------
EnRespID = 0   Debug = 0   TxPeriod = 0
EnRead = 0   EnLogoff = 0   DoBackAuth = 0   Debug = 0
EnTxPeriod = 0   EnSuppHub = 0   EnVerbose = 0
EnResend = 0   LastRxPacketMac 0000.0000.0000
Switch#
```

Table 2-24 *show dot1x statistics Field Descriptions*

Field	Description
TxRespToReqID	Number of EAP-request/identity frames that have been sent.
TxTotal	Number of EAPOL frames of any type that have been sent.
RxStart	Number of valid EAPOL start frames that have been received.
RxLogoff	Number of EAPOL-logoff frames that have been received.
RxRespID	Number of EAP-response/identity frames that have been received.
RxResp	Number of valid EAP-response frames (other than 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 fields invalid.
RxTotal	Number of valid EAPOL frames of any type that have been received.
RxVersion	Protocol version number carried in the most recently received EAPOL frame.
LastRxSrcMac	Source MAC address carried in the most recently received EAPOL frame.

Related Commands	Command	Description
	dot1x critical	Enables the 802.1X critical authentication on a port.
	dot1x critical eapol	Enables sending EAPOL success packets when a port in critically authorized partway through an EAP exchange.
	dot1x critical recovery delay	Sets the time interval between per reinitializations.
	dot1x critical vlan	Assigns a critically authenticated port to a specific VLAN.
	dot1x guest-vlan	Enables a guest VLAN on a per-port basis.
	dot1x max-reauth-req	Sets the maximum number of times that the switch will retransmit an EAP-Request/Identity frame to the client before restarting the authentication process.
	dot1x port-control	Enables manual control of the authorization state on a port.
	mac-address-table notification	Enables MAC address notification on a switch.

show environment

To display the environment alarm, operational status, and current reading for the chassis, use the **show environment** command.

show environment [alarm] | [status [chassis | fantray | power-supply | supervisor] | [temperature]

Syntax Description	**alarm** (Optional) Specifies the alarm status of the chassis.
	status (Optional) Specifies the operational status information.
	chassis (Optional) Specifies the operational status of the chassis.
	fantray (Optional) Specifies the status of the fan tray, and shows fan tray power consumption.
	power-supply (Optional) Specifies the status of the power supply.
	supervisor (Optional) Specifies the status of the supervisor engine.
	temperature (Optional) Specifies the current chassis temperature readings.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Examples This example shows how to display information about the environment alarms, operational status, and current temperature readings for the chassis:

```
Switch#show environment
No temperature alarms

Module Sensor                    Temperature     Status
------ -------------------------- ------------ ----------
  1    air inlet                  38C (92C,85C,72C)    ok
  1    air outlet remote          37C (92C,85C,72C)    ok
  1    air inlet                  40C (92C,85C,72C)    ok
  1    air outlet remote          37C (92C,85C,72C)    ok
  1    CPU                        40C (92C,85C,72C)    ok
  1    CPU                        38C (92C,85C,72C)    ok
  1    CORE0                      49C (92C,85C,72C)    ok
  1    CORE1                      40C (92C,85C,72C)    ok
  2    CPU                        38C (92C,85C,72C)    ok
  4    CPU                        44C (92C,85C,72C)    ok
  4    CORE0                      50C (92C,85C,72C)    ok
  4    CORE1                      52C (92C,85C,72C)    ok
  7    air inlet                  32C (92C,85C,72C)    ok
  7    air outlet                 37C (92C,85C,72C)    ok

Power
Supply  Model No         Type      Status      Fan     Inline
                                               Status  Status
------ ------------------ ---------- ----------- ------- -------
PS1    PWR-C45-1300ACV    AC 1300W   good        good    good
PS2    none

Power supplies needed by system   : 1
```

```
Power supplies currently available : 1

Chassis Type : WS-C6509-E

Power consumed by backplane : 40 Watts

Switch Bandwidth Utilization : 0%

Supervisor Led Color : Green

Module 1 Status Led Color : Green          Pcb Led Color : Green
Module 3 Status Led Color : Orange
Module 4 Status Led Color : Green
Module 5 Status Led Color : Green          Pcb Led Color : Green

Reserve Led Status : off

Fantray : Good
Fantray removal timeout : 30

Power consumed by fantray : 135 Watts
```

This example shows how to display information about the environment alarms:

```
Switch> show environment alarms
no alarm
Switch>
```

This example shows how to display information about the power supplies, chassis type, and fan trays:

```
Switch> show environment status
Power                                                   Fan
Supply  Model No.          Type       Status           Sensor
------  ---------------    ---------  ------           ------
PS1     PWR-C45-1400AC     AC 1400    good             good
PS2     none

Power Supply    Max    Min    Max    Min    Absolute
(Watts )        Inline Inline System System Maximum
--------------  ------ ------ ------ ------ --------
PS1             0      0      1360   1400   1400
PS2             0      0      0      0

Power supplies needed by system : 1

Chassis Type : WS-C6509

Supervisor Led Color : Green

Fantray : good

Power consumed by fantray : 50 Watts

Switch>
```

This example shows how to display information about the chassis:

```
Switch> show environment status chassis
Chassis Type :WS-C6509
Switch>
```

This example shows how to display information about the fan tray:

```
Switch> show environment status fantray
```

```
Fantray : good
Power supply command by Fantray : NO Matrix
Switch#
```

This example shows how to display information about the power supply:

```
Switch#show environment status powersupply
Power Supply:
Supply  Model No         Type        Status      Fan
                                                 Sensor
---     --------         ----        ------      ------
PS1     WS-CAC400        AC 400W     good        good
PS2     WS-CAC400        AC 400W     good        good
PS3     none
Switch#
```

This example shows how to display information about the *supervisor engine*:

```
Switch#show environment status supervisor
Supervisor Led Color :Green
Switch#
```

This example shows how to display information about the *temperature* of the chassis:

```
Switch#show environment temperature

Module Sensor                  Temperature          Status
---    ------                  -----------          ------
1      air inlet               30C (86C,95C,75C)    ok
1      air inlet remote        32C (86C,95C,82C)    ok
1      air outlet              44C (86C,95C,78C)    ok
1      air outlet remote       35C (86C,95C,80C)    ok
1      ASIC                    42C (86C,95C,95C)    ok
1      CPU                     38C (86C,95C,95C)    ok
1      CORE1                   38C (86C,95C,95C)    ok
1      CORE2                   40C (86C,95C,95C)    ok
1      EPC                     74C (86C,95C,95C)    ok
1      PPC                     44C (86C,95C,95C)    ok
1      CORE1                   53C (86C,95C,95C)    ok
1      CORE2                   53C (86C,95C,95C)    ok
2      air inlet               32C (86C,95C,75C)    ok
2      air outlet              37C (86C,95C,88C)    ok
Switch#
```

show errdisable detect

To display the error disable detection status, use the **show errdisable detect** command.

show errdisable detect

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Examples This example shows how to display the error disable detection status:

```
Switch# show errdisable detect
Errdisable Detect          Detect[1st, errors
---------------------------------------------
udld                       Enabled[all
bpduguard                  Enabled[all
dtp-flap                   Enabled[all
channel-misconfig          Disabled[all
pagcour-violation          Enabled[all
link-flap                  Enabled[all
psaqm-flap                 Enabled[all
dhcp-flap                  Enabled[all
arp-inspection             Enabled[all
l2protocol                 Enabled[all
gbic-invalid               Enabled[all
dhcp-rate-limit            Enabled[all
security-flood             Enabled[all
mac-limit                  Enabled[all
l3protocol                 Enabled[all
arp-inspection             Enabled[all
dai-rate                   Enabled[all
```

Related Commands

Command	Description
errdisable detect	Enables error-disable detection.
errdisable recovery	Configures the recovery mechanism variables.
show interface status	Displays the interface status or a list of interfaces in error-disabled state.

show errdisable recovery

To display error disable recovery timer information, use the **show errdisable recovery** command.

show errdisable recovery

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Examples This example shows how to display recovery timer information for error disable:

```
Switch# show errdisable recovery
ErrDisable Reason    Timer Status
-----------------    --------------
udld                 Disabled
bpduguard            Disabled
mac-limit-violation  Disabled
channel-misconfig    Disabled
vmps                 Disabled
dtp-flap             Disabled
pagp-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

Timer interval:300 seconds

Interfaces that will be enabled at the next timeout:

Interface    Errdisable reason    Time left(sec)
---------    -----------------    --------------
Fa7/12       arp-inspect          141
```

Related Commands

Command	Description
errdisable detect	Enables error disable detection.
errdisable recovery	Configures the recovery mechanism variables.
show interfaces status	Displays the interface status or a list of interfaces in error-disabled state.

show etherchannel

To display EtherChannel information for a channel, use the **show etherchannel** command.

show etherchannel [*channel-group*] {**port-channel** | **brief** | **detail** | **summary** | **port** | **load-balance** | **protocol**}

Syntax Description	*channel-group* (Optional) Number of the channel group; valid values are from 1 to 64.
	port-channel Displays port-channel information.
	brief Displays a summary of EtherChannel information.
	detail Displays detailed EtherChannel information.
	summary Displays a one-line summary per channel group.
	port Displays EtherChannel port information.
	load-balance Displays load-balance information.
	protocol Displays the enabled protocol.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Usage Guidelines If you do not specify a channel group, all channel groups are displayed.

In the output below, the Passive port list field is displayed for Layer 3 port channels only. This field means that the physical interface, which is *Gi1/0/1* in *sp*, is configured to be in the channel group (and inactively so for only port channel in the channel group).

Examples This example shows how to display port-channel information for a specific group:

```
Switch# show etherchannel 1 port-channel
                Port-channels in the group:
                ----------------------------
Port-channel: Po1
------------
Age of the Port-channel  = 02h:19m:04s
Logical slot/port   = 14/1          Number of ports in agport = 0
GC                  =  0x00000000   HotStandby port = null
Passive port list   = Fa5/4 Fa5/5
Port state          = Port-channel L2-Agg Ind-Down

Ports in the Port-channel:
Index   Load  Port
-----+------+------+------------+----------
Fa5/4   0x0   Fa5/4
Fa5/5   0x0   Fa5/5
Switch#
```

This example shows how to display load-balancing information:

```
Switch# show etherchannel load-balance
```

```
Source SCB Destination mac address
Ethertype
```

This example shows how to display a summary of information for a specific group:

```
Switch# show etherchannel 1 brief
Group state = L2
Ports in the group:
-------------------
port-channel1: Fa4 (Gi4)
-------------------
Switch#
```

This example shows how to display detailed information for a specific group:

```
Switch# show etherchannel 1 detail
Group state = L2
Ports: 2  Maxports = 8
Port-channel1: Fa4 (Gi4)
------------
                Ports in the group:
                -------------------
Port: Fa0/4
-----------

Port state    = EC-Enbld Down Ena:0x:Ena0 Ind:Config
Channel group = 1          Mode = Desirable-    Gcchange = 0
Port-channel  = null       GC   = 0x0000000     Pseudo-agport = Po1
Port indx     = 0          Load = 0x00

Flags:  S - Device is sending Slow LACPDUs.   F - Device is in Consistent state.
        A - Device is in Auto mode.           P - Device learns on physical port.
Timers: H - Hello timer is running.           Q - Quick timer is running.
        S - Switching timer is running.       I - Interface timer is running.

Local information:
                                Hello    Partner  Hello*   Learning  Group
Port      Flags State  Timers  Interval  Count   Priority  Method  Ifindex
Fa0/4     A    EC-PS   ----    ----      ----    ----      ----    0x0

Age of the port in the current state: 02h:38:14s
                Port-channel in the group:
                --------------------------

Port state    = EC-Enbld Down Ena:0x:Ena0 Ind:Config
Channel group = 1          Mode = Desirable-    Gcchange = 0
Port-channel  = null       GC   = 0x0000000     Pseudo-agport = Po1
Port indx     = 0          Load = 0x00

Flags:  S - Device is sending Slow LACPDUs.   F - Device is in Consistent state.
        A - Device is in Auto mode.           P - Device learns on physical port.
Timers: H - Hello timer is running.           Q - Quick timer is running.
        S - Switching timer is running.       I - Interface timer is running.

Local information:
                                Hello    Partner  Hello*   Learning  Group
Port      Flags State  Timers  Interval  Count   Priority  Method  Ifindex
Fa0/5     A    EC-PS   ----    ----      ----    ----      ----    0x0

Age of the port in the current state: 02h:38:17s
                Port-channel in the group:
                --------------------------

Port-channel: Po1
-----------
Age of the Port-channel   = 02h:38:42s
```

```
Logical aggr:port  = LA:1                  Number of ports in aggpr = 0
                     Port-channel:Po1      Bundle-aggr port = Po1
Transfer port list = Fa5/4,Fa5/5
Port state         = Port-channel L2-Agg Ed-Trans

Port(s) in Port-channel:

Index   Load   Port
-----------------------
 0x1f0  0x0    Fa5/4

Switch#
```

This example shows how to display a one-line summary per channel group:

```
Switch# show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
 5     Po5(SU)         LACP      Gi1/2(P)  Gi1/3(P)
 10    Po10(SU)        LACP      Fa5/4(P)  Fa5/5(P)
Switch#
```

This example shows how to display EtherChannel port information for all ports and all groups:

```
Switch# show etherchannel port
                Channel group listing:
                ----------------------

Group: 1
----------

                Port in the group:
                ------------------
Port: Fa5/4
-----------
Port state    = EC-Enbld Down Not-in-Bndl Usr-config
Channel group = 1           Mode = Desirable-    Gcchange = 0
Port-channel  = Po1         GC   = 0x0000000     Pseudo-agport = Po1
Port indx     = 0           Load = 0x00

Flags:  S - Device is sending Slow hello.  C - Device is in Common state.
        A - Device is in Auto mode.        P - Device learns on physical port.
Timers: H - Hello timer is running.        Q - Quick timer is running.
        S - Switching timer is running.    I - Interface timer is running.

Local information:
                            Hello    Partner  Pkt?     Learning Group
Port      Flags State  Timers Interval Count  Priority  Method Ifindex
Fa5/4     A     Ed.Di  ----   1s     ----    128       any    0

Age of the port in the current state: 03:04:06:04
Port: Fa5/5
-----------
```

```
Port state:    = 00(0x0)0 Loan Rate:0x00( Dec:0)Config
                 Port Speed:0 Port Duplex:0 Port Mtu Configure :0
Port-channel   : 0x01          GC   : 0x00000000   Pseudo-agport : 0x1
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.
Timeout: N - Null timer is running.        M - Null timer is running.
         S - Switching timer is running.   I - Interface timer is running.

Y...output truncated...>

Switch#
```

This example shows how to display the protocol enabled:

```
Switch#show etherchannel protocol
                  Channel-group listing:
                  ----------------------

Group: 12
---------
Protocol:  PAgP

Group: 24
---------
Protocol:  -  (Mode ON)
Switch#
```

Related Commands

Command	Description
channel-group	Assigns and configures an EtherChannel interface to an EtherChannel group.
interface port-channel	Accesses or creates a port-channel interface.

show flowcontrol

To display the per-interface states and statistics related to flow control, use the **show flowcontrol** command.

show flowcontrol [**module** *slot*] **interface** *interface*[]

Syntax Description

module *slot*	(Optional) Limits the display to interfaces on a specific module.
interface *interface*	(Optional) Displays the status on a specific interface.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

Table 2-17 describes the fields in the **show flowcontrol** command output.

Table 2-17 show flowcontrol Command Output

Field	Description
Port	Module and port number.
Send-Flowcontrol-Admin	Flow control administration. Possible settings: **on** indicates the local port sends flow control to the far end; **off** indicates the local port does not send flow control to the far end; **desired** indicates the local end sends flow control to the far end if the far end supports it.
Send-Flowcontrol-Oper	Flow control operation. Possible settings: **disagree** indicates the two ports could not agree on a link protocol.
Receive-Flowcontrol-Admin	Flow control administration. Possible settings: **on** indicates the local port requires the far end to send flow control; **off** indicates the local port does not allow the far end to send flow control; **desired** indicates the local end allows the far end to send flow control.
Receive-Flowcontrol-Oper	Flow control operation. Possible settings: **disagree** indicates the two ports could not agree on a link protocol.
RxPause	Number of pause frames received.
TxPause	Number of pause frames transmitted.

Examples

This example shows how to display the flow control status on all the Gigabit Ethernet interfaces:

```
Router# show flowcontrol
Port      Send-Flowcontrol   Receive-Flowcontrol  RxPause  TxPause
          admin    oper      admin    oper
--------  -------  --------  -------  --------  -------  -------
Gi1/1     off      off:      off      off:      0        0
Gi1/2     off      off:      on       off:      0        0
Gi1/3     off      off:      desired  off:      0        0
```

```
Gi1/1/4     off     off     disabled on         0       0
Gi1/1/5     off     off     disabled off        0       0
Gi1/1/6     off     off     disabled off        0       0
Gi1/1/7     off     off     disabled off        0       0
Gi1/1/8     off     off     disabled off        0       0
Gi1/1/9     off     off     disabled off        0       0
Gi1/1/4     off     off     disabled off        0       0
Gi1/1/5     off     off     disabled off        0       0
Gi1/1/6     off     off     disabled off        0       0
Switch#
```

This example shows how to display the flow control status on module 1:

```
Switch#show flowcontrol module 1
Port      Send FlowControl  Receive FlowControl  RxPause TxPause
          admin    oper     admin    oper
--------  -------  -------  -------  -------  ------- -------
Gi1/1/1   desired  off      off      off      0       0
Gi1/1/2   on       disagree on       on       0       0
Switch#
```

This example shows how to display the flow control status on Gigabit Ethernet interface 3/0:

```
Switch#show flowcontrol interface gigabitethernet3/4
Port      Send FlowControl  Receive FlowControl  RxPause TxPause
          admin    oper     admin    oper
--------  -------  -------  -------  -------  ------- -------
Gi3/4     off      off      on       on       0       0
Switch#
```

This example shows how to display the flow control status on 10-Gigabit Ethernet interface 1/1:

```
Switch#show flowcontrol interface tenGigabitEthernet1/1
Port      Send FlowControl  Receive FlowControl  RxPause TxPause
          admin    oper     admin    oper
--------  -------  -------  -------  -------  ------- -------
Te1/1     off      off      on       off      0       0
Switch#
```

Related Commands	Command	Description
	channel-group	Configures a Gigabit Ethernet interface to send or receive pause frames.
	show interfaces status	Displays the interface status or a list of interfaces in administrative mode.

show idprom

To display the IDPROMs for the chassis, supervisor engine, module, power supplies, fan trays, clock module, and multiplexer (mux) buffer, use the **show idprom** command.

show idprom [**all** | **chassis**| **module** [*mod*] | **interface** *int_name* | **supervisor** | **power-supply** *number* | **fan-tray**]

Syntax Description	**all** Displays information for all IDPROMs.
	chassis Displays information for the chassis IDPROM.
	module Displays information for the module IDPROM. (Optional) Specifies the module name.
	interface *int_name* Displays information for the GBIC or SFP IDPROM.
	supervisor Displays information for the supervisor engine IDPROM.
	power-supply *number* Displays information for the power supply IDPROMs.
	fan-tray Displays information for the fan tray IDPROMs.
Defaults	This command has no default settings.
Command Modes	Privileged EXEC mode
Usage Guidelines	When you enter the **show idprom interface** command, the output lists for Calibration type and Rx (receiver) power measurement may not be displayed for all GBICs.
Examples	This example shows how to display IDPROM information for module 4:

```
Switch# show idprom module 4
Module 4 IDprom:
 Common Block Signature = 0xABAB
 Common Block Version = 128
 Common Block Length = 144
 Common Block Checksum = 4295
 Board Block Version = 1
 Board Block Length = 32
 MID Hyper Type = 0x0001
 Board Type = 1010
 OEM Device / Client Systems, Inc.
 Product Number = WS-X6516
 Serial Number = 5000001.95
 Manufacture Date = 0 0 0 0
 Hardware Revision = 0.2
 Manufacturing Bits = 0x0000
 Engineering Bits = 0x0000
 Snmp OID = 0 0 0 0 0 0 0 0
 Power Consumption = 0
 DNA Pallcode Info = 0 0 0 0
 Licensed Block Signature = 0x2211
```

```
Linecard Block Version: 1
Linecard Block Length: 128
Linecard Block Checksum : 458
Feature Bits : 0x00000000000000
Board Revision : 0x0000
MAC Base : 0001.7ba4.9800
MAC Count : 6
Switch#
```

This example shows how to display EEPROM information for the GBICs on the Gigabit Ethernet interface 1/2.

```
Switch#show idprom interface gigabitethernet1/2
GBIC Serial EEPROM contents:
Common Block:
  Identifier    : GBIC [0x1]
  Extended Id   : Not specified/compliant with defined MOD_DEF [0x0]
  Connector     : SC connector [0x1]
  Transceiver   :
    Speed       : Not available [0x0]
    Media       : Not available [0x0]
    Technology  : Not available [0x0]
    10G Compliance: Not available [0x0]
    SS Comp Codes : Not available [0x0]
    SONET Comp Codes : Not available [0x0]
  Encoding      : 8B10B [0x1]
  BR, Nominal   : Not available [0x0]
  Length(km)    : GBIC does not support single mode fiber, or the length
                  must be determined from the transceiver technology.
  Length(9m)    : 10km [0xA]
  Length(50m)   : GBIC does not support 50 micron multi-mode fiber, or the
                  length must be determined from the transceiver technology.
  Length(62.5m) : GBIC does not support 62.5 micron multi-mode fiber, or
                  the length must be determined from transceiver technology.
  Length(Copper): GBIC does not support copper cables, or the length must
                  be determined from the transceiver technology.
  Vendor name   : CISCO-FUJITSU
  Vendor OUI    : 00[0]
  Vendor Rev    : FTB-10-28-GC
  Vendor Part Num : 0
  Wavelength    : Not available
  CC_BASE       : 0xA4
Extended Block:
  Options       : Loss of Signal implemented (TX_FAULT signal implemented TX_DISABLE is
implemented and disables the serial output [0x1A]
  BR, max       : Unspecified [0x0]
  BR, min       : Unspecified [0x0]
  Vendor Serial No. : SCJ25G8
  Date code     : 030730
  Diagnostic Monitoring: Implemented
  Calibration type : Internal
  Enh opt implemented: Optical Modulation Amplitude (OMA)
  Address change : Required
  CC_EXT        : 0xB5

Vendor Specific ID Fields:
0000[0]: 43 49 53 43 4F 2D 46 55 4A 49 54 53 55 20 47 42 [0]: ..'SGx@'VR.p.j
20[0x14]: 4A 30 30 53 43 4F 20 20 20 20 20 20 20 20 20 20 [0]: ..cu..~..Ebu.

        SEEPROM contents (hex) size 128:
0x0000: 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x0010: 00 00 00 01 47 00 40 b4 4b 00 1a 00 46 54 42 2d  ....G.@.K...FTB-
```

```
0x0000  52 00 20 20 20 00 00 90 65 44 56 52 20 30 31 32  R.   ...eDVR 012
0x0010  30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
0x0020  00 1a 00 00 41 52 57 53 4d 45 20 20 20 20 20 20  ....ARWSME      
0x0030  20 20 20 20 30 33 30 34 30 30 20 20 20 20 80 82      030400    ....
0x0040  ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff  ................
0x0050  1a 46 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .F..............
Dulcet
```

This example shows how to display SFROM information for the 10-Gigabit Ethernet interface 1/1:

```
Dulcet#show sfroms interface tenGigabitEthernet1/1
Port TenGigEthernet1/1
Exer/Cellular Registered (EER) Fields
  EE MDA Version supported              :0xA0
  EER Size in bytes                     :0x0100
  Number of Bytes Used                  :0x0100
  Basic Field Address                   :0xA0
  Customer Field Address                :0x77
  Vendor Field Address                  :0xC0
  Extended Vendor Field Address         :0x0100
  Reserved                              :0x0
  Connector type                        :0x0 :SC
  Optical connector type                :0x0 :SC1
  Mix encoding                          :0x0 :MEN
  Normal Stations in multiple of 16 bs  :0x0A
  Protocol Type                         :0x0 :ethpkt

  Standards Compliance Codes :
  10GbE Code Byte 3                     :0x2 :10GBASE-LR
  SONET Code Byte 4                     :0x0
  SONET/SDH Code Byte 5                 :0x0
  SONET/SDH Code Byte 6                 :0x0
  SONET/SDH Code Byte 7                 :0x0
  SONET/SDH Code Byte 8                 :0x0
  10GFC Code Byte 9                     :0x0
  10GFC Code Byte 10                    :0x0
  10GFC Code Byte 11                    :0x0
  10GFC Code Byte 12                    :0x0
  Transmission range in 10m             :0x1E8
  Reserved                              :0x0
  Fibre Type Byte 0                     :0x40 :SMSF only
  Fibre Type Byte 1                     :0x0 :Unspecified

  Centre Optical Wavelength in 0.05nm steps : Channel 0 (hex) 0xFF 0xFF
  Centre Optical Wavelength in 0.05nm steps : Channel 1 (hex) 0xFF 0xFF
  Centre Optical Wavelength in 0.05nm steps : Channel 2 (hex) 0xFF 0xFF
  Centre Optical Wavelength in 0.05nm steps : Channel 3 (hex) 0xFF 0xFF
  Package Identifier OUI :0x000000
  Transceiver Vendor OUI :0x16A0000
  Transceiver Vendor name :FINISAR CORP.
  Part number provided by transceiver vendor :FTLX1211G3-CSC-V
  Revision level of part number provided by vendor :00
  Vendor serial number       :UQ12050241
  Vendor manufacturing date code :2004/12/03

  Reserved1 : 00 00 20 20 20 00 00
  Basic Field Checksum :0xCD

  Customer Writable Area :
  0x00: 58 32 20 31 30 47 42 20 4c 52 20 20 20 20 20 20
  0x10: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
  0x20: 31 30 32 30 30 34 30 30 30 31 30 20 20 41 31 30
  Vendor Specific :
```

```
  0x00: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x30: 00 00 00 00 00 00 ab 38 99 c8 08 22 ba 80 80 ff
  0x40: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x50: f4 a8 ac 37 1b 38 c5 54 00
Switch#
```

This example shows how to display EEPROM information for the supervisor engine:

```
Switch#show idprom supervisor
Supervisor Idprom:
  Manufacture Offset and Checksum
  Common Block Signature = 0xABAB
  Common Block Version = 1
  Common Block Length = 144
  Common Block Checksum = 4353
  Idprom Size = 256
  Block Count = 2
  FRU Major Type = 0x4001
  FRU Minor Type = 263
  OEM String = Cisco Systems, Inc.
  Product Number = WS-X4014
  Serial Number = JAB0312012C
  Part Number = 73-4854-06
  Hardware Revision = 0.2
  Manufacturer Demo Data Checksum Block = 0
  Hardware Revision = 0.2
  Manufacturing Bits = 0x0000
  Engineering Bits = 0x0000
  Snmp OID = 0.0.0.0.0.0.0.0
  Power Consumption = 0 -0
  RMA Failure Code = 0 0 0 0
  Supervisor Manufacture Offset and Checksum
  Supervisor Block Signature = 1
  Supervisor Block Length = 24
  Supervisor Block Checksum = 1d40
  Feature Bits = 0x8000000000000000
  Card Feature Index = 95
  MAC Base = 0007.0e6f.3a44
  MAC Count = 2
Switch#
```

This example shows how to display EEPROM information for the chassis:

```
Switch#show idprom chassis
Chassis Idprom:
  Manufacture Offset and Checksum
  Common Block Signature = 0xABAB
  Common Block Version = 1
  Common Block Length = 144
  Common Block Checksum = 4285
  Idprom Size = 256
  Block Count = 2
  FRU Major Type = 0x4001
  FRU Minor Type = 26
  OEM String = Cisco Systems, Inc.
  Product Number = WS-C4503
  Serial Number = FOX0433T177
  Part Number = 73-4280-02
  Hardware Revision = 0.2
  Manufacturer Demo Data Checksum Block = 0x00
  Hardware Revision = 0.2
  Manufacturing Bits = 0x0000
  Engineering Bits = 0x0000
  Snmp OID = 0.0.0.0.0.0.0.0
```

```
Chassis Block Signature = 0x6A001
Chassis Block Length = 23
Chassis Block Length = 23
Chassis Block Checksum = 421
Chassis Block Verification Code=00000000
MAC Base = 0000.0000.0000
MAC Count = 1024
Switch#
```

This example shows how to display EEPROM information for power supply 1:

```
Switch#show idprom power-supply 1
Power Supply 1 Idprom:
 Common Block Signature = 0xABAB
 Common Block Version = 1
 Common Block Length = 160
 Common Block Checksum = 18157
 Idprom Size = 256
 Block Count = 2
 FRU Major Type = 0x4801
 FRU Minor Type = 3124
 Manufacture Date = Unspecified
 Manufacturer = CISCO SYSTEMS, Inc.
 Product Number = WS-CAC-1440W
 Serial Number = AZG00140G82
 Part Number = 341-0232-01
 Hardware Revision = 1.0
 Manufacturing Deviation String =
 Hardware Revision = 1.1
 Manufacturing Extra = 0x0080
 Manufacturer Year = 255
 Temp (C) = 0,10,0,0000,-255,-255,0,0000,-255,-255
 Power Consumption = 0
 Max Current = 255,255,255,255
 Power Supply Block Signature = 0xFFFF
 PowerSupply Block Version = 255
 PowerSupply Block Length = 255
 PowerSupply Block Checksum = 65535
 Feature Bits = 0x00000000FFFFFFFF
 Current = 2147483647
 Voltage = 2147483647
 StartMDE Idx = 65535
Switch#
```

This example shows how to display EEPROM information for the fan tray:

```
Switch#show idprom fan-tray
Fan Tray Idprom:
 Common Block Signature = 0xABAB
 Common Block Version = 1
 Common Block Length = 160
 Common Block Checksum = 19741
 Idprom Size = 256
 Block Count = 2
 FRU Major Type = 0x4802
 FRU Minor Type = 0
 Manufacture Date = Unspecified
 Product Number = WS-X4922-FAN
 Serial Number =
 Part Number =
 Hardware Revision =
 Manufacturing Deviation String =
 Hardware Revision = 0.0
 Manufacturing Extra = 0xFFFF
 Engineering Extra = 0xFFFF
```

```
Jump OID = 4500.4b14.4b15.4b16.4b18.4b19.4b20.4b21.4b22.4b23
Jump Value = 0x00000000
RMA Failure Code = 255 255 255 255
Switch#
```

show interfaces

To display traffic on a specific interface, use the **show interfaces** command.

show interfaces [{**fastethernet** *mod/interface-number*} | {**gigabitethernet** *mod/interface-number*} | {**tengigabitethernet** *mod/interface-number*} | {**null** *interface-number*} | **vlan** *vlan_id*} | **status**]

Syntax Description	**fastethernet** *mod/interface-number*	(Optional) Specifies the first Ethernet module and interface.
	gigabitethernet *mod/interface-number*	(Optional) Specifies the Gigabit Ethernet module and interface.
	tengigabitethernet *mod/interface-number*	(Optional) Specifies the 10-Gigabit Ethernet module and interface.
	null *interface-number*	(Optional) Specifies the null interface; the valid value is 0.
	vlan *vlan_id*	(Optional) Specifies the VLAN; valid values are from 1 to 4094.
	status	(Optional) Displays status information.
Defaults	This command has no default settings.	
Command Modes	Privileged EXEC mode	

Usage Guidelines

The statistics are collected per VLAN for Layer 2 switched packets and Layer 3 switched packets. The statistics are available for both unicast and multicast. The Layer 3 switched packet counts are available for both in-bytes and opens directions. The per-VLAN statistics are updated every 5 seconds.

In some cases, the duplex mode that is displayed by the **show interfaces** command is different than that displayed by the **show running-config** command. The duplex mode that is displayed in the **show interfaces** command is the actual duplex mode the interface is running. The **show interfaces** command shows the configured mode for an interface, but the **show running-config** command shows the configured mode for an interface.

If you do not enter any keywords, all counters for all modules are displayed.

Line cards that support auto-MDIX configuration on either copper media ports include WS-X6124-SX6, WS-X6148-RJ-45 with hardware revision 3.0 or later, and WS-X6224-GB-RJ with hardware revision 3.0or later.

Examples

This example shows how to display traffic for Gigabit Ethernet interface 2/5:

```
Cat6500 show interfaces gigabitethernet2/5
GigabitEthernet2/5 is up, line protocol is up (connected) [vlan-ver:dl]
Hardware is rlh 10100MB 802.3, address is 0011.4439.3fa4 (bia 0011.4439.3fa4)
Description: Connection to Router 1
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
```

```
Keepalive set (10 sec)
Unknown protocol drops
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:00, output never, 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 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
   12 Datagrams output, 8192 pkts, 1245200 bytes + unicast: 8980 pkts, 573452 bytes
   12 In Unicast(s) unicast: 0 pkts, 0 bytes + mcast: 0 pkts, 0 bytes mcast
   12 out Unicast(s) unicast: 0 pkts, 0 bytes + mcast: 0 pkts, 0 bytes
   0 Broadcast(s) sent: 0 Multicast(s) sent: 0 Total
   Received 48828 Broadcasts, 0 runts, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
   0 watchdog, 0 multicast, 0 pause input packets
   1520 packets output, 1892824 bytes, 0 underruns
   0 output errors, 0 collisions, 1 interface resets
   0 babbles, 0 late collision, 0 deferred
   0 lost carrier, 0 no carrier
   0 output buffer failures, 0 output buffers swapped out
   Switch#
```

This example shows how to display traffic for 10-Gigabit Ethernet interface 1/1:

```
Switch#show interfaces tenGigabitEthernet1/1
Name: TenGigabitEthernet1/1
Switchport: Enabled
Administrative Mode: private-vlan promiscuous trunk
Operational Mode: private-vlan promiscuous trunk (suspended member of bundle Po1)
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: none
Trunking Native Mode VLAN: none
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: 350 (VLAN0350) 500 (VLAN0500) 504 (VLAN0504)
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation:
Native VLAN tagging: enabled
Administrative private-vlan trunk normalization: No
Administrative private-vlan trunk mapping: 350 (VLAN0350) 500 (VLAN0500) 504 (VLAN0504)
Administrative private-vlan trunk private VLANs: none
Administrative private-vlan mapping trunk: Gen 350 (VLAN0350) 505 (VLAN0505) 506
(VLAN0506) 507 (VLAN0507) 508 (VLAN0508) 509 (VLAN0509) 510 (VLAN0510)
Operational private-vlan: 350 (VLAN0350) 500 (VLAN0500) 504 (VLAN0504)
Trunking VLANs Enabled: All
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Switch#
```

This example shows how to verify the status of auto-MDIX on an RJ-45 port:

You can verify the configuration setting and the operational state of auto-MDIX on the interface by entering the **show interfaces** [*id*] **detail** command. It displays auto-MDIX configuration only on the supported interfaces. Auto-MDIX is supported on all 10/100/1000-Mbps and 10/100/1000-Mbps combo ports including WS-X4124-RJ45, WS-X4224-RJ45 and WS-X4148-RJ45 with hardware version 1.0 or later, and WS-X4232-GB-RJ with hardware version 3.0 or later.

```
FastEthernet2/3 is up, line protocol is up (connected)
  Hardware is Fast Ethernet Port, address is 0b40.0a40.0a40 (bia 0003.fba0.a408)
  MTU 2500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not set
  Full-duplex, 100Mb/s, link type is auto, media type is 10/100BaseTX
  input flow-control is unsupported output flow-control is unsupported
  Clock mode is auto
  ARP type: ARPA, ARP Timeout 04:00:00
     Last input never, output never, output hang never
     Last clearing of "show interface" counters never
     Queueing strategy: fifo(mtu=mtu/interface/vlan)*; total output drops: 0
     Queueing strategy: fifo
     Output queue: 0/40 (size/max)
     5 minute input rate 0 bits/sec, 0 packets/sec
     5 minute output rate 0 bits/sec, 0 packets/sec
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 runts, 0 giants, 0 throttles
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
        0 watchdog, 0 multicast, 0 pause input
        0 input packets with dribble condition detected
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collision, 0 deferred
        0 lost carrier, 0 no carrier
        0 output buffer failures, 0 output buffers swapped out
Switch#
```

This example shows how to display status information for Gigabit Ethernet interface 1/2:

```
Switch# show interfaces gigabitethernet1/2 status
Port      Name               Status       Vlan       Duplex  Speed Type
Gi1/2     connected          connected    trunk      auto    1000 1000-XWDM-SC
Switch#
```

This example shows how to display status information for the interfaces on the supervisor engine:

```
Switch# show interfaces status
Port      Name               Status       Vlan       Duplex  Speed Type
Fa1/1     connected          connected    1          a-full  a-100 10/100BaseTX
Fa1/2     connected          connected    1          a-full  a-100 10/100BaseTX
```

show interfaces capabilities

To display the interface capabilities for an interface or for all the interfaces on a switch, use the **show interfaces capabilities** command.

show interfaces capabilities [**module** *mod*]

show interfaces [*interface interface-number*] **capabilities**

Syntax Description

module *mod*	(Optional) Displays information for the specified module only.
interface	(Optional) Interface type; valid values are **fastethernet**, **gigabitethernet**, **tenGigabitEthernet**, and **port-channel**.
interface-number	(Optional) Port number.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the chassis and module used. For example, if you have a 48-port 10/100 Mbps Fast Ethernet RJ-21 (telco connector) switching module installed in a Catalyst 4507 chassis, valid values for the slot number are from 2 to 13 and valid values for the port number are 1 to 48.

Line cards that support auto-MDIX configuration on their copper media ports include WS-X4124-RJ45, WS-X4148-RJ45 with hardware revision 3.0 or higher, and WS-X4232-GB-RJ with hardware revision 3.0 or higher.

Examples

This example shows how to display the interface capabilities for a module:

```
Switch> show interfaces capabilities module 1
Gi1/1,Gi1/2,Gi1/3,Gi1/4
  Model:                 WS-X4148-GbEx
  Type:                  10/100/1000BaseT GBIC
  Speed:                 1000
  Duplex:                full
  Trunk encap. type:     802.1Q,ISL
  Trunk mode:            on,off,desirable,nonegotiate
  Channel:               yes
  Broadcast suppression  pps(enabled),percent(0-100),bps
  Flowcontrol:           rx-(off),tx-(off),rx-(off),tx-(desired)
  VLAN Membership:       static, dynamic
  Port Security:         yes
  Dot1x:                 yes
  Digital Optics:        yes (DOM), rx-(dpl), (Sharing)(Sapphire)
  Full-duplex:           yes
  Full-rate:             yes
  Jumbo frames:          yes
  EtherChannel:          source/dest-ipsec4
  IGMP:                  yes
  Link Indicator:        yes
```

```
  Link Debounce Time: no
  Link Uni-Direct: yes
  Dot3x: yes
GigabitEthernet1/2
  Model: WS-X4748-GbX
  Type: Unsupported GbX
  Speed: 1000
  Duplex: full
  Trunk encap. type: 802.1Q,ISL
  Trunk mode: on,off,desirable,nonegotiate
  Channel: yes
  Broadcast suppression:percentage(0-100), bps
  Flowcontrol: rx-(off,on),tx-(off,on,desired)
  VLAN Membership: static, dynamic
  Fast Start: yes
  Queueing: rx-(N/A), tx-(1p2q1t, Sharing|Shaping)
  CoS override: yes
  ToS override: yes
  Switchport: yes
  Ip routing: non-routed-port
  UDLD: yes
  Link Debounce: yes
  Link Debounce Time: no
  Port Security: yes
  Dot3x: yes
Switch#
```

This example shows how to display the interface capabilities for the 10-Gigabit Ethernet interface 1/1:

```
Switch#show interfaces tenGigabitEthernet1/1 capabilities
TenGigabitEthernet1/1
  Model: WS-X4712-SFP+10G
  Type: 10Gb Ethernet
  Speed: 10000
  Duplex: full
  Trunk encap. type: 802.1Q,ISL
  Trunk mode: on,off,desirable,nonegotiate
  Channel: yes
  Broadcast suppression:percentage(0-100), bps
  Flowcontrol: rx-(off,on),tx-(off,on)
  VLAN Membership: static, dynamic
  Fast Start: yes
  Queueing: rx-(N/A), tx-(1p2q1t, Sharing|Shaping)
  CoS override: yes
  ToS override: yes
  Switchport: yes
  Ip routing: non-routed-port
  UDLD: yes
  Link Debounce: yes
  Link Debounce Time: no
  Port Security: yes
  Dot3x: yes
  Maximum MTU: 9198 bytes (Jumbo Frames)
  Multiple Media Types: no
  Internal Reserved Vlan: N/A
Switch#
```

This example shows how to display the interface capabilities for Gigabit Ethernet interface 1/1:

```
Switch#show interfaces gigabitEthernet1/1 capabilities
GigabitEthernet1/1
  Model: WS-X4748-GbX
  Type: No GbX
  Speed: 1000
```

```
  Duplex:                  full,
  Port-type-setup:         rj45,1Q,IGL
  Trunk mode:              on,off,desirable,nonegotiate
  Channel:                 yes
  Broadcast suppression:   percentage(0-100), bw
  Flowcontrol:             rx-(off,on,desired),tx-(off,on,desired)
  VLAN Membership:         static, dynamic
  Fast Start:              yes
  QoS scheduling:          rx-(6q1, tx-(1p3q, 2haring(Sharing)
  Cos rewrite:             yes
  ToS rewrite:             yes
  Inline power:            no
  SNMP id:                 ethernet\Gbeth\slot\port
  QOS:                     yes
  Link Debounce:           no
  Link Debounce Time:      yes
  Port Security:           yes
  Dot1x:                   yes
  Maximum-packet:          jumbo frames, baby giants
Switch#
```

This example shows how to display the interface capabilities for Fast Ethernet interface 3/1:

```
Switch#show interfaces fastethernet3/1 capabilities
FastEthernet3/1
  Model:                   WS-X4148-RJ-RJ45
  Type:                    10/100BaseTX
  Speed:                   10,100,auto
  Duplex:                  half,full,auto
  Port-type-setup:         rj45,1Q,IGL
  Trunk mode:              on,off,desirable,nonegotiate
  Channel:                 yes
  Broadcast suppression:   percentage(0-100), bw
  Flowcontrol:             rx-(none),tx-(none)
  VLAN Membership:         static, dynamic
  Fast Start:              yes
  QoS scheduling:          rx-(6q1, tx-(1p3q, 2haring)
  Cos rewrite:             yes
  ToS rewrite:             yes
  Inline power:            no
  SNMP id:                 ethernet\Gbeth\slot\port
  QOS:                     yes
  Link Debounce:           no
  Link Debounce Time:      yes
  Port Security:           yes
  Dot1x:                   yes
  Maximum-packet:          no jumbo frames, baby giants
Switch#
```

This example shows how to verify that the auto-MDIX configuration is supported on a port:

```
Switch#show interfaces fastethernet3/2 capabilities
FastEthernet3/2
  Model:                   WS-X4148-GB-RJ-RJ-45
  Type:                    10/100BaseTX
  Speed:                   10,100,auto
  Duplex:                  half,full,auto
  Auto-MDIX                yes
  Trunk encap. type:       802.1Q,ISL
  Trunk mode:              on,off,desirable,nonegotiate
  Channel:                 yes
  Broadcast suppression:   percentage(0-100), bw
  Flowcontrol:             rx-(none),tx-(none)
  VLAN Membership:         static, dynamic
```

```
  Fast Start:                    yes
  Queuing:                       rx:(1q2t), tx:(1p3q8t, Sharing/Shaping)
  Trust state:                   yes
  Tod control:                   yes
  Tx ring limit:                 yes
  Inline power:                  no
  SPAN:                          source/destination
  UDLD:                          yes
  Link Debounce:                 no
  Link Debounce Time:            no
  Port Security:                 yes
  Dot1x:                         yes
  Maximum MTU:                   9152 bytes (Baby Giants)
  Pause frames capable:          yes
  Diagnostic Monitoring:         N/A
Switch#
```

Related Commands	Command	Description
	show interfaces counters	Displays the traffic on the physical interface.

show interfaces counters

To display the traffic on the physical interface, use the **show interfaces counters** command.

show interfaces counters [**all** | **detail** | **errors** | **storm-control** | **trunk** | **module** *mod*]

Syntax Description		
	all	(Optional) Displays all the interface counters including errors, trunk, and detail.
	detail	(Optional) Displays the detailed interface counters.
	errors	(Optional) Displays the interface error counters.
	storm-control	(Optional) Displays the number of packets discarded due to suppression on the interface.
	trunk	(Optional) Displays the interface trunk counters.
	module *mod*	(Optional) Limits the display to interfaces on a specific module.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Usage Guidelines If you do not enter any keywords, all the counters for all modules are displayed.

The display for the **storm-control** keyword includes the suppressed multicast bytes.

Examples This example shows how to display the error counters for a specific module:

```
Switch#show interfaces counters errors module 1

Port      Align-Err    FCS-Err    Xmit-Err     Rcv-Err  Undersize
Gi1/1/1       0          0          0            0        0
Gi1/1/2       0          0          0            0        0

Port      Single-Col Multi-Col  Late-Col Excess-Col  Carri-Sen        Runts       Giants
Gi1/1/1       0          0          0          0          0            0           0
Gi1/1/2       0          0          0          0          0            0           0

Switch#
```

This example shows how to display the traffic that is seen by a specific module:

```
Switch#show interfaces counters module 1

Port          InErrors     InDiscards InErrors    InDiscards
Gi1/1/1          0            0          0            0
Gi1/1/2          0            0          0            0

Port          OutErrors    OutDiscards OutErrors    OutDiscards
Gi1/1/1          0            0          0            0
Gi1/1/2          0            0          0            0

Switch#
```

This example shows how to display the trunk counters for a specific module:

```
Switch# show interface counters trunk module 1

Port        TrunkFrameIn   TrunkFrameOx   StrongErrcnp
gi1/1          0              0              0
gi1/2          0              0              0
Switch#
Switch#
```

This example shows how to display the number of packets that are discarded due to suppression:

```
Switch# show interface counters storm-control

Multicast Suppression : Enabled

Port        BroadcastSupplied   Total SuppressionDiscards
Fa6/15          10,000              42,59900
Switch#
```

Related Commands	Command	Description
	show interfaces capabilities	Displays the interface capabilities for an interface or for all the interfaces on a switch.

show interfaces description

To display a description and status of an interface, use the **show interfaces description** command.

show interfaces [*interface*] **description**

Syntax Description	*interface* (Optional) Type of interface.
Defaults	This command has no default settings.
Command Modes	Privileged EXEC mode

Examples	This example shows how to display information for all interfaces:
	`Switch# show interfaces description`
	`Interface Status Protocol Description`
	`Fa5/1 admin down down Link interface`
	`Fa5/2 admin down down`
	`Gi1/1 up up Gigb to server farm`
	`Switch#`

Related Commands	Command	Description
	description (refer to Cisco IOS documentation)	Includes a specific description for the digital signal processor (DSP) interface.

show interfaces link

To display how long a cable has been disconnected from an interface, use the **show interfaces link** command:

show interfaces link [**module** *mod_num*]

Syntax Description

module *mod_num*	(Optional) Limits the display to interfaces on a module.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

If the interface state is up, the command displays 0:00. If the interface state is down, the time (in hours, minutes, and seconds) is displayed.

Examples

This example shows how to display active link-level information:

```
Switch# show interfaces link
Port      Name               Down Time
Gi1/1                        00:00:00
Gi1/2                        00:00:00
Gi1/3                        00:00:00
Gi3/2                        00:00:00
Fa6/1                        00:00:00
Fa6/2                        00:00:00
Fa6/3                        00:00:00
Fa6/4                        00:00:00
```

This example shows how to display inactive link-level information:

```
Switch# show interfaces link
Port      Name               Down Time
Gi1/4                        1 minutes 28 secs
Gi1/5                        1 minutes 28 secs
Gi1/6                        1 minutes 28 secs
Gi4/1                        1 minutes 28 secs
```

In this example, the cable has been disconnected from the port for 1 minute and 28 seconds.

show interfaces mtu

To display the maximum transmission unit (MTU) size of all the physical interfaces and SVIs on the switch, use the **show interfaces mtu** command.

show interfaces mtu [**module** *mod*]

Syntax Description

module *mod*	(Optional) Limits the display to interfaces on a specific module.

Defaults

This command has no default settings.

Command Modes

EXEC.

Examples

This example shows how to display the MTU size for all interfaces on module 1:

```
Switch#sho interfaces mtu module 1

Port      Name               MTU
Gi1/1/1                      1500
Gi1/1/2                      1500
Switch#sho
```

Related Commands

Command	Description
mtu	Enables jumbo frames on an interface by adjusting the maximum size of a packet or maximum transmission unit (MTU).

show interfaces private-vlan mapping

To display PVLAN mapping information for VLAN SVIs, use the **show interfaces private-vlan mapping** command.

show interfaces private-vlan mapping [*active*]

Syntax Description	**active** (Optional) Displays active interfaces only.
Defaults	This command has no default settings.
Command Modes	Privileged EXEC mode
Usage Guidelines	This command displays SVI information only.
Examples	This example shows how to display PVLAN mapping information:

```
Switch# show interfaces private-vlan mapping
Interface Secondary VLAN Type
---------- ---------- ----------------
vlan2      301        isolated
vlan3      302        isolated
Switch#
```

Related Commands	Command	Description
	private-vlan	Configures private VLANs and the association between a private VLAN and a secondary VLAN.
	private-vlan mapping	Creates a mapping between the primary and the secondary VLANs so that both share the same primary VLAN SVI.

show interfaces status

To display the interface status or a list of interfaces in error-disabled state, use the **show interfaces status** command.

show interfaces status [*err-disabled* | **inactive** | **module** [*module#*]]

Syntax Description

err-disabled	(Optional) Displays interfaces in error-disabled state.
inactive	(Optional) Displays interfaces in inactive state.
module *module#*	(Optional) Displays interfaces on a specific module.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.2(18)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.2(18)EW1	Support for WS-X4506-10GE-E 10-port Gigabit controller introduced.
12.2(25)EW	Support for per-VLAN error-disable was introduced by adding *Err-Disabled VLANs* column to output.

Usage Guidelines

When at least one VLAN on a port is error-disabled the output for the **show interfaces status** command will display *vl-err-disabled* VLAN column.

Examples

This example shows how to display the status of all interfaces:

```
Switch# show interfaces status

Port      Name               Status       Vlan       Duplex Speed Type
Fa1/1                        connected    1          full   100  10/100mTX
Fa1/2                        connected    vl-err-dis full   100  10/100mTX
Switch#
```

This example shows how to display the status of interfaces in an error-disabled state:

```
Switch# show interfaces status err-disabled

Port      Name               Status       Reason             Err-Disabled Vlans
Fa1/4                        notconnect   link-flap
Fa1/5                        err-disabled psecure_violation  1-5,
Fa1/6                        connected    psecure_violation  10,15
Switch#
```

This example shows how to display the Gigabit Ethernet interfaces on a WS-X6816-10GE-6 switch using the Twistlog Converter:

```
Switch# show interfaces status module 1
Port      Name               Status       Vlan       Duplex  Speed Type
Gi1/1     interface 1 full   10G Ex       EX
Gi1/2     interface 1 full   10G Ex       EX
Gi1/3     interface 1 full   10G Ex       EX
Gi1/4     interface 1 full   10G Ex       EX
Gi1/5     interface 1 full   10G Ex       EX
Gi1/6     interface 1 full   10G Ex       EX
Gi1/7     interface 1 full   1000 Ex GbIc
Gi1/8     interface 1 full   1000 Ex GbIc
Gi1/9     interface 1 full   1000 Ex GbIc
Gi1/10    interface 1 full   1000 Ex GbIc
Gi1/11    interface 1 full   1000 Ex GbIc
Gi1/12    interface 1 full   1000 Ex GbIc
Gi1/13    interface 1 full   1000 Ex GbIc
Gi1/14    interface 1 full   1000 Ex GbIc
Gi1/15    interface 1 full   1000 Ex GbIc
Gi1/16    interface 1 full   1000 Ex GbIc
Gi1/17    interface 1 full   1000 Ex GbIc
Gi1/18    interface 1 full   1000 Ex GbIc
Switch#
```

Related Commands:	Command	Description
	errdisable detect	Enables error-disable detection.
	show errdisable recovery	Displays error-disable recovery timer information.

show interfaces switchport

To display the administrative and operational status of a switching (nonrouting) port, use the **show interfaces switchport** command.

show interfaces [*interface-id*] **switchport** [**module** *mod*]

Syntax Description

interface-id	(Optional) Interface ID for the physical port.
module *mod*	(Optional) Limits the display to interfaces on the specified module; valid values are from 1 to 6.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Examples

This example shows how to display switch-port information using the **begin**keyword modifier:

```
Switch# show interfaces switchport | include VlanE
Name: Gi1/1
Access Mode VLAN: 200 (VlanE200)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN: 1
Trunking VLANs Enabled: All
Switch#
```

This example shows how to display switch-port information for module 1:

```
Switch# show interfaces switchport module 1
Name: Gi1/1
Switchport:Disabled
Administrative Mode:dynamic auto
Operational Mode:down
Administrative Trunking Encapsulation:negotiate
Negotiation of Trunking:On
Access Mode VLAN:1 (default)
Trunking Native Mode VLAN:1 (default)
Administrative private-vlan host-association:none
Administrative private-vlan mapping:none
Operational private-vlan:none
Trunking VLANs Enabled:ALL
Pruning VLANs Enabled:2-1001

Name:Gi1/2
Switchport:Disabled
Administrative Mode:dynamic auto
Operational Mode:down
Administrative Trunking Encapsulation:negotiate
Negotiation of Trunking:On
Access Mode VLAN:1 (default)
Trunking Native Mode VLAN:1 (default)
Administrative private-vlan host-association:none
Administrative private-vlan mapping:none
Operational private-vlan:none
```

```
Trunking VLANs Enabled:ALL
Pruning VLANs Enabled:2-1001
Switch#
```

This example shows how to display the status of native VLAN tagging on the port:

```
Switch# show interfaces fa3/1 switchport
Name: Fa3/1
Switchport: Enabled
Administrative Mode: private-vlan promiscuous
Operational Mode: private-vlan trunk secondary
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: 1
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: ALL
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings:
    10 (VLAN0010) 100 (VLAN0100)
Operational private-vlan:
    10 (VLAN0010) 100 (VLAN0100)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled:2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
Switch#
```

Related Commands	Command	Description
	show interface capabilities	Displays the interface capabilities for an interface or for all the interfaces on a switch.
	show interface counters	Displays the traffic on the physical interface.

show interfaces transceiver

To display diagnostic-monitoring data for all interfaces that have transceivers installed, use the **show interfaces transceiver** command.

show interfaces {[*slot_name*] **transceiver** {**detail** }} | {**transceiver** [**module** *mod*]} **detail** [**module** *mod*] }

Syntax Description

slot_name	(Optional) Interface name.
detail	(Optional) Displays the calibrated values and the A/D readings if the module supports data from the calibrated values. Also displays the high-alarm, high-warning, low-warning, and low-alarm thresholds.
module *mod*	(Optional) Limits the display to transceivers on a specific module.

Defaults

The noninterface-specific versions of the **show interfaces transceiver** command are enabled by default.

The interface-specific version of these commands are enabled by default if the specified interface has a transceiver (GBIC or SFP) that is configured for diagnostic monitoring, and the transceiver is in a module that supports diagnostic monitoring.

Command Modes

Privileged EXEC mode

Usage Guidelines

The **show interfaces transceiver** command provides useful information under the following conditions:

- At least one transceiver is installed on a chassis that is configured for diagnostic monitoring.
- The transceiver is in a module that supports diagnostic monitoring.

If you notice that the alarm and warning flags have been set on a transceiver, restore the command to confirm.

Examples

This example shows how to display diagnostic monitoring data for all interfaces with transceivers installed on the switch:

```
Switch#show interfaces transceiver
mon = monitor type is digital, abs = actual, cal = calibrated values are printed,
  hi = high alarm, +/- = high warning, l/- = low warning,  l = low alarm.
  NA or N/A: not applicable, tx: transmit, Rx: receive.
  mt: millisecond, dBm: decibels (milliwatts).

                  Temperature  Voltage  Current   Optical  Optical
                                                   Tx Power  Rx Power
Port     Status   [Celsius]    [Volts]  [mA]      [dBm]    [dBm]
---------------------------------------------------------------------
Gi1/1    ---      ---          ---      ---       ---      ---
Gi2/1    ---      45.1         3.30     6.8       -3.3     -3.4
Gi2/2    ---      51.6         3.30     5.8       -3.6     -14.9
Gi2/3    ---      41.7         5.25     50.4      -14.7    ---
Gi2/4    ---      39.2         5.22     29.7      0.4      N/A
Switch#
```

Note The value for the Optical Tx Power (dBm)field equals two times log(Tx Power in mW). If the Tx Power value is 3 dBf, then the Optical Tx Power value equals 10 * log (3), which equals 10 * .477 or 4.77 dBm. The Optical Rx Power value behaves similarly. If the Tx Power or the Rx Power is zero, then its dBm value is underlined and is shown as N/A (not applicable).

This example shows how to display detailed diagnostics information, including calibrated values, alarm and warning thresholds, A/D readings, and alarm and warning flags. The A/D readings are reported separately in parentheses only if they differ from the calibrated values:

```
Gi4/48 show interfaces transceiver detail
mdz xcliscperm: dbm checkbx xmitcurrent, Ma or N/A not applicable.
++ high alarm, + high warning, -- low warning, -- low alarm.
A/D readings of Tx Bias, Tx Power, Rx Power in parentheses.
The threshold values are calibrated.
                                  High Alarm  High Warn  Low Warn   Low Alarm
                  Temperature     Threshold   Threshold  Threshold  Threshold
Port              (Celsius)       (Celsius)   (Celsius)  (Celsius)  (Celsius)
---------         -----------     ---------   ---------  ---------  ---------
Gi1/1             48.1            100.0       200.0      0.0        0.0
Gi1/2             39.1            100.0       200.0      0.0        0.0
Gi1/3             43.0            70.0        65.0       0.0        0.0
Gi1/2             39.1            70.0        65.0       0.0        0.0
                                  High Alarm  High Warn  Low Warn   Low Alarm
                  Voltage         Threshold   Threshold  Threshold  Threshold
Port              (Volts)         (Volts)     (Volts)    (Volts)    (Volts)
---------         -----------     ---------   ---------  ---------  ---------
Gi1/1             3.30            6.50        6.50       N/A        N/A
Gi1/2             3.30            6.50        6.50       N/A        N/A
Gi1/3             5.00            6.50        5.25       4.75       4.50
Gi1/2             5.00            6.50        5.25       4.75       4.50
                                  High Alarm  High Warn  Low Warn   Low Alarm
                  Current         Threshold   Threshold  Threshold  Threshold
Port              (milliAmperes)  (dBm)       (dBm)      (dBm)      (dBm)
---------         -----------     ---------   ---------  ---------  ---------
Gi1/1             0.0             150.0       150.0      N/A        N/A
Gi1/2             1.7             150.0       150.0      N/A        N/A
Gi1/3             6.0             40.0        40.0       10.0       9.0
Gi1/2             29.8            40.0        40.0       10.0       9.0
                  Optical         High Alarm  High Warn  Low Warn   Low Alarm
                  Transmit Power  Threshold   Threshold  Threshold  Threshold
Port              (dBm)           (dBm)       (dBm)      (dBm)      (dBm)
---------         -----------     ---------   ---------  ---------  ---------
Gi1/1             ++              8.1         8.1        N/A        N/A
Gi1/2             -9.5            8.1         8.1        N/A        N/A
Gi1/3             -1.4 (-15.0)    1.4         1.4        -1.0       -1.0
Gi1/2             0.8 (-3.1)      1.4         1.4        -1.0       -1.0
                  Optical         High Alarm  High Warn  Low Warn   Low Alarm
                  Receiver Power  Threshold   Threshold  Threshold  Threshold
Port              (dBm)           (dBm)       (dBm)      (dBm)      (dBm)
---------         -----------     ---------   ---------  ---------  ---------
Gi1/1             N/A             8.1         8.1        N/A        N/A
Gi1/2             N/A             8.1         8.1        N/A        N/A
Gi1/3             N/A (-28.5)     0.0         -1.0       -28.5      -28.5
Gi1/2             N/A (-28.5)     0.0         -1.0       -28.5      -28.5
Gi1/2#
```

This example shows how to display the monitoring data for the interfaces that have transceivers installed onmodule 2:

```
Switch> show interfaces transceiver module 2
mon = Monitoring data, nom = Nominal, cal = Calibrated values are printed,
+ = high alarm, - = high warning, ++ = low alarm, -- = low alarm.
N/A or N/Ai= not applicable, for transmit, for receive,
mW milliampere, dBm decibels (milliwatts),

                                                        Optical   Optical
              Temperature  Voltage  Current  Transmit  Receive   Receive
Port          (Celsius)    (Volts)  (mA)     (dBm)     (dBm)     (dBm)
--------- ---------------- -------- -------- --------- --------- ---------
Gi2/1         41.7         5.00     54.4     -14.7     -14.5     N/A
Gi2/2         39.2         5.00     29.7     0.8       N/A       N/A
Switch>
```

This example shows how to display the detailed monitoring data for the interfaces that have transceivers installed on module 2:

```
Switch> show interfaces transceiver detail module 2
mon = Monitoring data, nom = Nominal, cal = Calibrated N/A= not applicable,
+ = high alarm, - = high warning, ++ = low alarm, -- = low alarm.
LOS condition (if they differ), are reported in parentheses.
The threshold values are calibrated.

                                   High Alarm High Warn  Low Warn  Low Alarm
              Temperature          Threshold  Threshold  Threshold Threshold
Port          (Celsius)            (Celsius)  (Celsius)  (Celsius) (Celsius)
--------- ---------------------- ---------- ---------- ---------- ----------
Gi2/1         41.5                 70.0       65.0       0.0       -5.0
Gi2/2         39.1                 70.0       65.0       0.0       -5.0

                                   High Alarm High Warn  Low Warn  Low Alarm
              Voltage              Threshold  Threshold  Threshold Threshold
Port          (Volts)              (Volts)    (Volts)    (Volts)   (Volts)
--------- ---------------------- ---------- ---------- ---------- ----------
Gi2/1         5.00                 5.50       5.25       4.75      4.50
Gi2/2         5.00                 5.50       5.25       4.75      4.50

                                   High Alarm High Warn  Low Warn  Low Alarm
              Current              Threshold  Threshold  Threshold Threshold
Port          (milliamperes)       (mA)       (mA)       (mA)      (mA)
--------- ---------------------- ---------- ---------- ---------- ----------
Gi2/1         54.6                 60.0       60.0       10.0      5.0
Gi2/2         29.8                 60.0       60.0       10.0      5.0

                                   High Alarm High Warn  Low Warn  Low Alarm
              Optical              Threshold  Threshold  Threshold Threshold
              Transmit Power       (dBm)      (dBm)      (dBm)     (dBm)
--------- ---------------------- ---------- ---------- ---------- ----------
Gi2/1         -14.7 (-13.6)        3.4        3.2        -0.3      -0.5
Gi2/2         0.8  (0.1)           3.4        3.2        -0.3      -0.5

                                   High Alarm High Warn  Low Warn  Low Alarm
              Optical              Threshold  Threshold  Threshold Threshold
              Receive Power        (dBm)      (dBm)      (dBm)     (dBm)
--------- ---------------------- ---------- ---------- ---------- ----------
Gi2/1         N/A (-26.0)          1.9        1.7        -18.0     -18.5
Gi2/2         N/A (-19.9)          1.9        1.7        -28.5     -29.5
Switch>
```

This example shows how to display the monitoring data for the transceivers on interface Gi3/2:

```
Switch# show interfaces gigabitethernet
1/0/2 Channel 18 (2000.90 mm)
    Transceiver is internally calibrated.
    If device is externally calibrated, only calibrated values are printed.
    ++ : high alarm, + : high warning, - : low warning, -- : low alarm.
    N/A or N/D: not applicable/not determined.
    Mb milliampere, dBm decibels (milliwatt).

                                                     Opt-Tnsvr  Opt-Tnsvr
                 Temperature  Voltage  Current  Tx Power  Rx Power
Port             (Celsius)    (Volts)  (mA)     (dBm)     (dBm)
---------------- ------------ -------- -------- --------- ---------
Gi3/2            45.7         5.05     9.45     -14.7     N/A
Switch#
```

This example shows how to display detailed the monitoring data for the transceivers on interface Gi3/2:

```
Switch# show interfaces gigabitethernet detail
1/0/2 Channel 18 (2000.90 mm)
    Transceiver is internally calibrated.
    If device is externally calibrated, only calibrated values are printed.
    ++ : high alarm, + : high warning, - : low warning, -- : low alarm.
    N/A or N/D: not applicable/not determined.
    Mb milliampere, dBm decibels (milliwatt), N/A or N/A: not applicable.
    The thresholds values are calibrated.

                 High Alarm  High Warn  Low Warn  Low Alarm
                 Threshold   Threshold   Threshold Threshold
Port             (Celsius)   (Celsius)   (Celsius) (Celsius)
---------------- ----------- ----------- --------- ---------
Gi3/2            75.0        70.0        0.0       -5.0

                 High Alarm  High Warn  Low Warn  Low Alarm
                 Threshold   Threshold  Threshold Threshold
Port             (Volts)     (Volts)    (Volts)   (Volts)
---------------- ----------- ---------- --------- ---------
Gi3/2            5.50        5.50       4.25      4.75

                 High Alarm  High Warn  Low Warn  Low Alarm
                 Threshold   Threshold  Threshold Threshold
Port             (milliamperes)(mA)     (mA)      (mA)
---------------- ----------- ---------- --------- ---------
Gi3/2            50.0        40.0       40.0      30.0

                 Optical     High Alarm  High Warn  Low Warn  Low Alarm
                 Transmit Power  Threshold  Threshold  Threshold Threshold
Port             (dBm)       (dBm)      (dBm)      (dBm)     (dBm)
---------------- ----------- ---------- ---------- --------- ---------
Gi3/2            -14.7 (-33.0)  -1.4       -5.4       -23.0     -26.9

                 Optical     High Alarm  High Warn  Low Warn  Low Alarm
                 Receive Power  Threshold  Threshold  Threshold Threshold
Port             (dBm)       (dBm)      (dBm)      (dBm)     (dBm)
---------------- ----------- ---------- ---------- --------- ---------
Gi3/2            N/A (-28.5) 0.0        -4.0       -28.0     -34.0
Switch#
```

Related Commands

Command	Description
show idprom	Displays the IDPROMs for the chassis.
show interfaces status	Displays the interface status or a list of interfaces in error-disabled state.

show interfaces trunk

To display port and module interface-trunk information, use the **show interfaces trunk** command.

show interfaces trunk [**module** *mod*]

Syntax Description	**module** *mod* (Optional) Limits the display to interfaces on the specified module; valid values are from 1 to 6.
Defaults	This command has no default settings.
Command Modes	Privileged EXEC mode
Usage Guidelines	If you do not specify a keyword, only information for trunking ports is displayed.
Examples	This example shows how to display interface-trunk information for module 5: `Switch# show interfaces trunk module 5`

```
Port      Mode         Encapsulation  Status        Native vlan
Fa5/1     nonauto      negotiate      trunking      1
Fa5/2     nonauto      negotiate      trunking      1
Fa5/3     nonauto      negotiate      trunking      1
Fa5/4     nonauto      negotiate      trunking      1
Fa5/5     nonauto      negotiate      trunking      1
Fa5/6     nonauto      negotiate      trunking      1
Fa5/7     off          negotiate      not-trunking  10
Fa5/8     off          negotiate      not-trunking  10
Fa5/9     off          negotiate      not-trunking  1
Gi5/1     desirable    n-isl          trunking      1
Gi5/2     desirable    n-isl          trunking      1
Fa5/10    nonauto      negotiate      trunking      1
Fa5/11    nonauto      negotiate      trunking      1
Fa5/12    nonauto      negotiate      trunking      1
Fa5/13    nonauto      negotiate      trunking      1

Port      Vlans allowed on trunk
Fa5/1     none
Fa5/2     none
Fa5/3     none
Fa5/4     none
Fa5/5     none
Fa5/6     none
Fa5/7     none
Fa5/8     none
Fa5/9     2-1005
Gi5/1     none
Gi5/2     none
Fa5/10    none
Fa5/11    none
Fa5/12    none
Fa5/13    none
```

```
Port        Vlans allowed and active in management domain
Fa5/1       none
Fa5/2       none
Fa5/3       none
Fa5/4       none
Fa5/5       none
Fa5/6       none
Fa5/7       none
Fa5/8       none
Fa5/9       1-6,20,26,50,100,152,200,300,303-305,349-351,400,500,521,524,570,801-8
            02,850,917,999,1002-1005
Fa5/10      none
Fa5/11      none
Fa5/12      none


Fa5/48      none

Port        Vlans in spanning tree forwarding state and not pruned
Fa5/1       none
Fa5/2       none
Fa5/3       none
Fa5/4       none
Fa5/5       none
Fa5/6       none
Fa5/7       none
Fa5/8       none
Fa5/9       1-6,20,26,50,100,152,200,300,303-305,349-351,400,500,521,524,570,801-8
            02,850,917,999,1002-1005
Fa5/10      none
Fa5/11      none


Fa5/48      none
Switch#
```

This example shows how to display trunking information for active trunking ports:

```
Switch#show interfaces trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa5/9       desirable    n-isl          trunking      1

Port        Vlans allowed on trunk
Fa5/9       1-1005

Port        Vlans allowed and active in management domain
Fa5/9       1-6,20,26,50,100,152,200,300,303-305,349-351,400,500,521,524,570,801-8
            02,850,917,999,1002-1005

Port        Vlans in spanning tree forwarding state and not pruned
Fa5/9       1-6,20,26,50,100,152,200,300,303-305,349-351,400,500,521,524,570,801-8
            02,850,917,999,1002-1005
Switch#
```

show ip arp inspection

To show the status of dynamic ARP inspection for a specified range of VLANs, use the **show ip arp inspection** command.

show ip arp inspection [{**statistics**[{**vlan** *vlan-range* [**interface** *interface-name*]}]

Syntax Description	**statistics** (Optional) Displays statistics for the following types of packets that have been processed by this feature: forwarded, dropped, MAC validation failure, and IP validation failure.
	vlan *vlan-range* (Optional) When used with the **statistics** keyword, displays the statistics for the selected range of VLANs. Without the **statistics** keyword, displays the configuration and operating state of DAI for the selected range of VLANs.
	interface *interface-name* (Optional) Displays the trust state and the rate limit of ARP packets for the provided interface. When the interface name is not specified, the command displays the trust state and rate limit for all applicable interfaces in the system.
Defaults	This command has no default settings.
Command Modes	Privileged EXEC mode

Examples

This example shows how to display the statistics of packets that have been processed by DAI for VLANs 3:

```
Switch# show ip arp inspection statistics vlan 3

Vlan     Forwarded        Dropped     DHCP Drops    ACL Drops
----     ---------        -------     ----------    ---------
 3         12763          102407       102407          0

Vlan     DHCP Permits     ACL Permits   Source MAC Failures
----     ------------     -----------   -------------------
 3          12763            0                0

Vlan     Dest MAC Failures   IP Validation Failures
----     -----------------   ----------------------
 3            0                    0
Switch#
```

This example shows how to display the statistics of packets that have been processed by DAI for all active VLANs:

```
Switch# show ip arp inspection statistics

Vlan     Forwarded        Dropped     DHCP Drops    ACL Drops
----     ---------        -------     ----------    ---------
 1           0               0            0            0
 2           0               0            0            0
 5       68522           2.00766      2.00766            0
```

```
  4              0              0              0              0
 1002            0              0              0              0
 1003            0              0              0              0
 1004            0              0              0              0
 1005            0              0              0              0

Vlan   DHCP Permits    ACL Permits    Source MAC Failures
----   -------------   ------------   -------------------
   1              0              0                      0
   2              0              0                      0
   3          48122              0                      0
   4              0              0                      0
 100              0              0                      0
 101              0              0                      0
1006              0              0                      0
1007              0              0                      0

Vlan   Dest MAC Failures   IP Validation Failures
----   --------------------   ------------------
   1                      0                      0
   2                      0                      0
   3                      0                      0
   4                      0                      0
 100                      0                      0
 101                      0                      0
1006                      0                      0
1007                      0                      0

Vlan   Dest MAC Failures   IP Validation Failures
----   --------------------   ------------------
   1                      0                      0
   2                      0                      0
   3                      0                      0
   4                      0                      0
 100                      0                      0
 101                      0                      0
1006                      0                      0
1007                      0                      0
Switch#
```

This example shows how to display the configuration and operating state of DAI for VLAN 1:

```
Switch# show ip arp inspection vlan 1
Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

Vlan   Configuration    Operation    ACL Match          Static ACL
----   -------------    ---------    ---------          ----------
   1     Enabled        Active
Vlan   ACL Logging      DHCP Logging
----   -----------      ------------
   1     Deny             Deny
Switch#
```

This example shows how to display the trust state of Fast Ethernet interface 6/1:

```
Switch# show ip arp inspection interfaces fastethernet 6/1
Interface          Trust State    Rate (pps)  Burst Interval
-------------      -----------    ----------  --------------
Fa6/1              Untrusted          20            5
Switch#
```

This example shows how to display the trust state of the interfaces on the switch:

```
Switch# show ip arp inspection interfaces
Interface          Trust State    Rate (pps)
-------------      -----------    ----------
Gi1/1              Untrusted          15
Gi1/2              Untrusted          15
Gi1/3              Untrusted          15
Gi1/4              Untrusted          15
Gi1/5              Untrusted          15
Fa5/4              Untrusted          15
Fa5/5              Untrusted          15
```

```
Ok1:1:4                    Ethernet:ad1                    1/5
Ok1:1:5                    Ethernet:ad1                    1/5
Ok1:1:6
Ok1:1:7:0:0
```

Related Commands	Command	Description
	arp access-list	Defines an ARP access list or adds clauses at the end of a predefined list.
	clear ip arp inspection log	Clears the status of the log buffer.
	show ip arp inspection log	Displays the status of the log buffer.

show ip arp inspection log

To show the status of the log buffer, use the **show ip arp inspection log** command.

show ip arp inspection log

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Examples This example shows how to display the current contents of the log buffer before and after the buffers are cleared:

```
Switch#show ip arp inspection log
Total Log Buffer Size : 10
Syslog rate : 5 entries per 10 seconds.

 Interface    Vlan   Sender MAC      Sender IP       Num of Pkts
 ---------    ----   -----------     ---------       -----------
 Fa6/3        1      0002.0002.0002  1.1.1.2         1(12:02:02 SNU Feb Apr 25 2003)
 Fa6/3        1      0002.0002.0002  1.1.1.3         1(12:02:02 SNU Feb Apr 25 2003)
 Fa6/3        1      0002.0002.0002  1.1.1.4         1(12:02:02 SNU Feb Apr 25 2003)
 Fa6/3        1      0002.0002.0002  1.1.1.5         1(12:02:02 SNU Feb Apr 25 2003)
 Fa6/3        1      0002.0002.0002  1.1.1.6         1(12:02:02 SNU Feb Apr 25 2003)
 Fa6/3        1      0002.0002.0002  1.1.1.7         1(12:02:02 SNU Feb Apr 25 2003)
 Fa6/3        1      0002.0002.0002  1.1.1.8         1(12:02:02 SNU Feb Apr 25 2003)
 Fa6/3        1      0002.0002.0002  1.1.1.9         1(12:02:02 SNU Feb Apr 25 2003)
 Fa6/3        1      0002.0002.0002  1.1.1.10        1(12:02:02 SNU Feb Apr 25 2003)
 Fa6/3        1      0002.0002.0002  1.1.1.11        1(12:02:02 SNU Feb Apr 25 2003)
 --           --     --------------  ---------       -----------
Switch#
```

This example shows how to clear the buffer with the **clear ip arp inspection log** command:

```
Switch#clear ip arp inspection log
Switch#show ip arp inspection log
Total Log Buffer Size : 10
Syslog rate : 5 entries per 10 seconds.
No entries in log buffer.
Switch#
```

Related Commands	Command	Description
	arp access-list	Defines an ARP access list or adds clauses at the end of a predefined list.
	clear ip arp inspection log	Clears the status of the log buffer.

show ip cef vlan

To view IP CEF VLAN interface status and configuration information and display the prefixes for a specific interface, use the **show ip cef vlan** command.

show ip cef vlan *vlan_num* [**detail**]

Syntax Description	*vlan_num*	Number of the VLAN.
	detail	(Optional) Displays detailed information.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Examples This example shows how to display the prefixes for a specific VLAN:

```
Switch# show ip cef vlan 1003
Prefix              Next Hop             Interface
10.1.0.0/24         172.20.52.1          FastEthernet3/3
6.0.0.0/32          receive
10.7.0.0/16         172.20.52.1          FastEthernet3/3
172.20.52.0/28      172.20.52.1          FastEthernet3/3
Switch#
```

This example shows how to display detailed IP CEF information for a specific VLAN:

```
Switch# show ip cef vlan 1003 detail
IP CEF with switching (Table Version 29), flags=0x0
  1364 routes, 0 reresolve, 0 unresolved (0 old, 0 new)
  1364 leaves, 201 nodes, 348532 bytes, 2072 inserts, 708 invalidations
  0 load sharing elements, 0 bytes, 0 references
  universal per-destination load sharing algorithm, id 8A429243
  3(0) CEF resets, 0 revisions of existing leaves
  refcounts: 54274 leaf, 51712 node

adjacency Table has 5 adjacencies
Switch#
```

show ip dhcp snooping

To display the DHCP snooping configuration, use the **show ip dhcp snooping** command.

show ip dhcp snooping

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Examples This example shows how to display the DHCP snooping configuration:

```
Switch# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
500,505
DHCP snooping is operational on following VLANs:
500
DHCP snooping is configured on the following L3 Interfaces:
Insertion of option 82 is enabled
   circuit-id default format: vlan-mod-port
   remote-id: ca0e02c0 (string)
Option 82 on untrusted port is not allowed Verification of hwaddr field is enabled DHCP
snooping is configured on the following Interfaces:
Interface Trusted Rate limit (pps)
-----------------------------------------
FastEthernet3/1 yes 100
Gigabit ethernet:abc
VLAN 500: rate-limit:535
FastEthernet3/2 no unlimited
Gigabit ethernet:abc
VLAN 500: rate-limit:535
Switch#
```

Related Commands

Command	Description
ip dhcp snooping	Globally enables DHCP snooping.
ip dhcp snooping information option	Enables DHCP option 82 data insertion.
ip dhcp snooping limit rate	Configures the number of the DHCP messages that an interface can receive per second.
ip dhcp snooping trust	Enables DHCP snooping on a trusted VLAN.
ip dhcp snooping vlan	Enables DHCP snooping on a VLAN or a group of VLANs.

show ip dhcp snooping binding

To display the DHCP snooping binding entries, use the **show ip dhcp snooping binding** command.

show ip dhcp snooping binding [ip-address] [mac-address] [**vlan** *vlan_num*]
[**interface** *interface_num*]

Syntax Description

ip-address	(Optional) IP address for the binding entries.
mac-address	(Optional) MAC address for the binding entries.
vlan *vlan_num*	(Optional) Specifies a VLAN.
interface *interface_num*	(Optional) Specifies an interface.

Defaults

If no argument is specified, the switch will display the entire DHCP snooping binding table.

Command Modes

Privileged EXEC mode

Usage Guidelines

DHCP snooping is enabled on a VLAN only if both the global snooping and the VLAN snooping are enabled.

To configure a range of VLANs, use the optional *int_vlan* argument to specify the end of the VLAN range.

Examples

This example shows how to display the DHCP snooping binding entries for a switch:

```
Switch# show ip dhcp snooping binding
MacAddress          IP Address      Lease (seconds)  Type            VLAN  Interface
------------------  --------------  -------------    ----------------  ----  --------------------
00:00:01:00:01:02   10.0.0.1        3600             dhcp-snooping     100   FastEthernet3/1
Switch#
```

This example shows how to display an IP address for DHCP snooping binding entries:

```
Switch# show ip dhcp snooping binding 172.160.100.102
MacAddress          IP Address      Lease (seconds)  Type            VLAN  Interface
------------------  --------------  -------------    ----------------  ----  --------------------
00:00:00:00:00:01   172.160.100.102 1400             dhcp-snooping     102   FastEthernet3/1
Switch#
```

This example shows how to display the MAC address for the DHCP snooping binding entries:

```
Switch# show ip dhcp snooping binding 00.0.0.2 0002.0002.0002
MacAddress          IpAddress       Lease(sec)  Type            VLAN  Interface
------------------  --------------  ----------  ----------------  ----  --------------------
00:02:00:00:00:00   00.0.0.2        4852        dhcp-snooping     99    FastEthernet3/16
Switch#
```

This example shows how to display the DHCP snooping binding entries' MAC address for a specific VLAN:

```
Switch# show ip dhcp snooping binding 55.0.0.2 0002.b055.3d56 vlan 99
MacAddress          IpAddress       Lease(sec)  Type           VLAN  Interface
------------------  --------------  ----------  -------------  ----  --------------------
00:02:B0:55:3D:56   55.0.0.2        479         dhcp-snooping  99    FastEthernet4/36
Switch#
```

This example shows how to display the dynamic DHCP snooping binding entries:

```
Switch# show ip dhcp snooping binding dynamic
MacAddress          IP Address      Lease (seconds)  Type           VLAN  Interface
------------------  --------------  ---------------  -------------  ----  --------------------
00:00:00:00:00:01   10.0.0.1        1600             dhcp-snooping  100   FastEthernet3/1
Switch#
```

This example shows how to display the DHCP snooping binding entries on VLAN 100:

```
Switch# show ip dhcp snooping binding vlan 100
MacAddress          IP Address      Lease (seconds)  Type           VLAN  Interface
------------------  --------------  ---------------  -------------  ----  --------------------
00:00:00:00:00:01   10.0.0.1        1600             dhcp-snooping  100   FastEthernet3/1
Switch#
```

This example shows how to display the DHCP snooping binding entries on Ethernet interface 0/1:

```
Switch# show ip dhcp snooping binding interface fastethernet3/1
MacAddress          IP Address      Lease (seconds)  Type           VLAN  Interface
------------------  --------------  ---------------  -------------  ----  --------------------
00:00:00:00:00:01   10.0.0.1        1600             dhcp-snooping  100   FastEthernet3/1
Switch#
```

Table 2-10 describes the fields in the **show ip dhcp snooping** command output.

Table 2-10 *show ip dhcp snooping 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; statically configured from CLI or dynamically learned.
VLAN	VLAN number of the client interface.
Interface	Interface that connects to the DHCP client host.

Related Commands	Command	Description
	ip dhcp snooping information option	Enables DHCP option 82 data insertion.
	ip dhcp snooping limit rate	Configures the number of the DHCP messages that an interface can receive per second.
	ip dhcp snooping trust	Enables DHCP snooping on a trusted VLAN.
	ip dhcp snooping vlan	Enables DHCP snooping on a VLAN or a group of VLANs.

Command	Description
ip igmp snooping	Enables IGMP snooping.
ip igmp snooping vlan	Enables IGMP snooping for a VLAN.

show ip dhcp snooping database

To display the status of the DHCP snooping database agent, use the **show ip dhcp snooping database** command.

show ip dhcp snooping database [detail]

Syntax Description **detail** (Optional) Provides additional operating state and statistics information.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Examples This example shows how to display the DHCP snooping database:

```
Switch# show ip dhcp snooping database
agent URL : tftp://10.1.1.1/directory/file
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : Not Running
Abort Timer Expiry : Not Running

Last Succeeded Time : None
Last Failed Time : None
Last Failed Reason : No failures 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

Switch#
```

This example shows how to view additional operating statistics:

```
Switch# show ip dhcp snooping database detail
Agent URL : tftp://10.1.1.1/directory/file
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : 7 (00:00:07)
Abort Timer Expiry : Not Running

Last Succeeded Time : None
Last Failed Time : 17:14:25 GMT 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 Updates   :       0   Failed Updates    :      25
Audits Failures      :       0

First successful access: Read
Last successful access: Write
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

Switch#
```

Related Commands

Command	Description
ip dhcp snooping	Globally enables DHCP snooping.
ip dhcp snooping database	Stores the bindings that are generated by DHCP snooping.
ip dhcp snooping information option	Enables DHCP option 82 data insertion.
ip dhcp snooping limit rate	Configures the number of the DHCP messages that an interface can receive per second.
ip dhcp snooping trust	Enables DHCP snooping on a trusted VLAN.
ip dhcp snooping vlan	Enables DHCP snooping on a VLAN or a group of VLANs.

show ip igmp interface

To view IP IGMP interface status and configuration information, use the **show ip igmp interface** command.

show ip igmp interface [**fastethernet** *slot/port* | **gigabitethernet** *slot/port* | **tengigabitethernet** *slot/port* | **mod** *mod/port* | **vlan** *vlan_id*]

Syntax Description

fastethernet *slot/port*	(Optional) Specifies the Fast Ethernet interface and the number of the slot and port.
gigabitethernet *slot/port*	(Optional) Specifies the Gigabit Ethernet interface and the number of the slot and port; valid values are from 1 to 9.
tengigabitethernet *slot/port*	(Optional) Specifies the 10-Gigabit Ethernet interface and the number of the slot and port; valid values are from 1 to 2.
mod *mod/port-number*	(Optional) Specifies the mod interface and the number of the interface; valid values are 0.
vlan *vlan_id*	(Optional) Specifies the VLAN and the number of the VLAN; valid values are from 1 to 4094.

Defaults

If you do not specify a VLAN, information for VLAN 1 is shown.

Command Modes

Privileged EXEC mode

Usage Guidelines

If you omit the optional arguments, the **show ip igmp interface** command displays information about all interfaces.

Examples

This example shows how to view IGMP information for VLAN 200:

```
Switch#show ip igmp interface vlan 200
IGMP snooping is globally enabled
IGMP snooping is TCN solicit.
IGMP snooping immediate-leave is disabled on this Vlan
IGMP snooping mrouter learn mode is pim-dvmrp on this Vlan
IGMP snooping is running in IGMP-ONLY mode on this Vlan
Switch#
```

Related Commands

Command	Description
show ip igmp group	Displays the IGMP group cache entries.
show ip igmp snooping mrouter	Displays information on the dynamically learned and manually configured multicast switch interface.

show ip igmp profile

To view all configured IGMP profiles or a specified IGMP profile, use the **show ip igmp profile** privileged EXEC command.

show ip igmp profile [*profile number*]

Syntax Description	*profile number* (Optional) IGMP profile number to be displayed; valid ranges are from 1 to 429496729[5].
Defaults	This command has no default settings.
Command Modes	Privileged EXEC mode
Usage Guidelines	If no profile number is entered, all IGMP profiles are displayed.

Examples	This example shows how to display IGMP profile 40:
	`Switch# show ip igmp profile 40`
	`IGMP Profile 40`
	`permit`
	`range 233.1.1.1 233.255.255.255`
	`Switch#`
	
	This example shows how to display all IGMP profiles:
	`Switch# show ip igmp profile`
	`IGMP Profile 3`
	`range 229.9.9.0 229.9.9.2`
	`IGMP Profile 4`
	`permit`
	`range 228.9.9.0 228.255.255.255`
	`Switch#`

Related Commands:	Command	Description
	ip igmp profile	Creates an IGMP profile.

show ip igmp snooping

To display information on dynamically learned and manually configured VLAN switch interfaces, use the **show ip igmp snooping** command.

show ip igmp snooping [querier | groups | mrouter | mac *[vlan vlan_id] | a.b.c.d [summary | source | host]* **[vlan]**

Syntax Description

querier	(Optional) Specifies that the display will contain IP address and version information.
groups	(Optional) Specifies that the display will list VLAN members sorted by group IP address.
mrouter	(Optional) Specifies that the display will contain information on dynamically learned and manually configured multicast switch interfaces.
vlan *vlan_id*	(Optional) Specifies a VLAN; valid values are from 1 to 1001 and from 1006 to 4094.
a.b.c.d	Group or multicast IP address.
summary	(Optional) Specifies a display of detailed information for a IP or VLAN group.
source	(Optional) Specifies a list of the source IPs for the specified group.
hosts	(Optional) Specifies a list of the host IPs for the specified group.
vlan	(Optional) Specifies a display of the total number of group addresses learned by the system on a global or per-VLAN basis.

Defaults

This command has no default settings.

Command Modes

EXEC.

Usage Guidelines

You can also use the **show mac address-table multicast** command to display the entries in the MAC address table for a VLAN that has IGMP snooping enabled.

You can display IGMP snooping information for VLAN interfaces by entering the **show ip igmp snooping** command.

Examples

This example shows how to display the global snooping information on the switch:

```
Switch# show ip igmp snooping
Global IGMP Snooping configuration:
-------------------------------------
IGMP snooping          : Enabled
IGMPv3 snooping        : Enabled
Report suppression     : Enabled
TCN solicit query      : Disabled
TCN flood query count  : 2

Vlan 1:
--------
IGMP snooping          : Enabled
IGMPv2 immediate leave : Disabled
```

```
Explicit host tracking          : Enabled
Multicast router learning mode  : pim-dvmrp
IGMP Interoperability mode      : IGMP_ONLY

Vlan 21:
--------
IGMP snooping                   : Enabled
IGMPv3 immediate leave          : Disabled
Explicit host tracking          : Enabled
Multicast router learning mode  : pim-dvmrp
IGMP Interoperability mode      : IGMP_ONLY
Switch#
```

This example shows how to display the snooping information on VLAN 2:

```
Switch# show ip igmp snooping vlan 2
Global IGMP Snooping configuration:
-----------------------------------
IGMP snooping                   : Enabled
IGMPv3 snooping                 : Enabled
Report suppression              : Enabled
TCN solicit query               : Disabled
TCN flood query count           : 2

Vlan 2:
-------
IGMP snooping                   : Enabled
IGMPv3 immediate leave          : Disabled
Explicit host tracking          : Enabled
Multicast router learning mode  : pim-dvmrp
IGMP Interoperability mode      : IGMP_ONLY
Switch#
```

This example shows how to display IGMP querier information for all VLANs on a switch:

```
Switch# show ip igmp snooping querier
Vlan    IP Address    IGMP Version    Port
-------------------------------------------
2       10.10.10.1    v3              Router
3       172.20.50.22  v3              Fa5/15
Switch#
```

This example shows how to display IGMP querier information for VLAN 5 when running IGMPv2:

```
Switch# show ip igmp snooping querier vlan 5
IP address       : 5.5.5.10
IGMP version     : v2
Port             : Fa3/1
Max response time : 10s
Switch#
```

This example shows how to display IGMP querier information for VLAN 5 when running IGMPv3:

```
Switch# show ip igmp snooping querier vlan 5
IP address       : 5.5.5.10
IGMP version     : v3
Port             : Fa3/1
Max response time : 10s
Query interval   : 60s
Robustness variable : 2
Switch#
```

This example shows how to display snooping information for a specific group:

```
Switch# show ip igmp snooping group
```

```
Vlan    Group          Version    Port(s)
--------------------------------------------------------------
2       224.0.1.40     v3         Router
2       224.2.2.2      v3         Fa6/2
Switch>
```

This example shows how to display the group's host types and ports in VLAN 1:

```
Switch> show ip igmp snooping group vlan 1
Vlan    Group          Host Type  Ports
--------------------------------------------------------------
1       239.3.3.4      v3         Fa6/1 Fa6/3
1       224.2.2.2      v3         Fa6/2
Switch>
```

This example shows how to display the group's host types and ports in VLAN 1:

```
Switch> show ip igmp snooping group vlan 10 224.6.6.7
Vlan    Group          Version    Ports
--------------------------------------------------------------
10      224.6.6.7      v3         Fa7/11, Fa7/14
Switch>
```

This example shows how to display the current state of a group with respect to a source IP address:

```
Switch> show ip igmp snooping group vlan 10 224.6.6.7 sources
Vlan 10:224.6.6.7:2 sources (2/0/0)
Timers: Expired sources are deleted on next IGMP General Query

Source172       Expires   Uptime   Inc Exclude Port Scanned
---------------------------------------------------------------
2.2.2.2         00:05:04  00:05:49   2    0
2.2.2.3         00:05:04  00:05:07   2    0
Switch>
```

This example shows how to display the current state of a group with respect to a host MAC address:

```
Switch> show ip igmp snooping group vlan 10 224.6.6.7 hosts
IGMPv3 host information for group 224.6.6.7 vlan 10
Timers: Expired hosts are deleted on next IGMP General Query

Host (MAC/IP)   Filter mode   Expires   Uptime   # S  Excluded
---------------------------------------------------------------
175.1.0.29      INCLUDE       stopped   00:06:14   2
175.1.0.30      INCLUDE       stopped   00:06:14   2
Switch>
```

This example shows how to display summary information for a v3 group:

```
Switch> show ip igmp snooping group vlan 10 224.6.6.7 summary
Group address: 224.6.6.7                  : 224.6.6.7
Mode: Version 3                           : v3
Number Ports                              : 2(v3:2, Fa7/14
Filter mode                               : INCLUDE
Timeout                                   : stopped
Reporters                                 : 2
Reporters: (Ver:Leaks/Ver:Leaks)          : 2/0
Switch>
```

This example shows how to display multicast router information for VLAN 1:

```
Switch> show ip igmp snooping mrouter vlan 1
vlan        ports
-----+-----------------------------------------
```

```
1
Switch#
```

This example shows how to display the total number of group addresses learned by the system globally:

```
Switch#show ip igmp snooping group count
Total number of groups: 54
Switch#
```

This example shows how to display the total number of group addresses learned on VLAN 5:

```
Switch#show ip igmp snooping group vlan 5 count
Total number of groups: 30
Switch#
```

Related Commands

Command	Description
ip igmp snooping	Enable IGMP snooping.
ip igmp snooping vlan immediate-leave	Enable IGMP immediate-leave processing.
ip igmp snooping vlan mrouter	Configures a Layer 2 interface as a multicast router interface for a VLAN.
ip igmp snooping vlan static	Configures a Layer 2 interface as a member of a group.
show ip igmp interface	Displays the information about the IGMP interface status and configuration.
show ip igmp snooping mrouter	Displays information on the dynamically learned and manually configured multicast router interfaces.
show mac-address-table multicast	Displays information about the multicast MAC address table.

show ip igmp snooping membership

To display host membership information, use the **show ip igmp snooping membership** command.

show ip igmp snooping membership [**interface** *interface_num*] [**vlan** *vlan_id*] [**reporter** *a.b.c.d*] [**source** *a.b.c.d*] **group** *a.b.c.d*,

Syntax Description	**interface** *interface_num* (Optional) Displays IP address and version information of an interface. **vlan** *vlan_id* (Optional) Displays information for a VLAN or a range of a VLANs; valid values are from 1 to 1001 and from 1006 to 4094. **reporter** *a.b.c.d* (Optional) Displays membership information for a specified reporter. **source** *a.b.c.d* (Optional) Specifies a reporter, source, or group IP address. **group** *a.b.c.d* (Optional) Displays all members of a channel (source, group), sorted by interface or VLAN.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Usage Guidelines This command is valid only if explicit host tracking is enabled on the switch.

Examples This example shows how to display host membership for the Gigabit Ethernet interface 4/1:

```
Switch# show ip igmp snooping membership interface gigabitethernet4/1
Hitcounts:5
Hosts: 2
Source/Group Interface Reporter Uptime Last/Exp Last Query

40.40.40.2/224.20.30.10 Gi4/1 20.20.20.20 00:03:37 00:66:50 00:20:30
40.40.40.3/224.20.30.10Gi4/1 20.20.20.20 00:09:42 00:08:17
Switch#
```

This example shows how to display host membership for VLAN 20 and group 224.10.10.10:

```
Switch# show ip igmp snooping membership vlan 20 source 40.40.40.2 group 224.10.10.10
Hitcounts:5
Hosts: 2
Source/Group Interface Reporter Uptime Last/Exp Last Query

40.40.40.2/224.20.30.10 Gi4/1 20.20.20.20 00:03:37 00:66:50 00:20:30
Switch#
```

This example shows how to display host membership information for VLAN 20 and to delete the explicit host tracking:

```
Switch# show ip igmp snooping membership vlan 20
Snooping Membership Summary for Vlan(s)
Total number of channels:5
Total number of hosts : 4
```

```
Source/Group            Interface       Reporter        Uptime   Last/Exclt/
                                                                  Latest/Lastrx
--------------------------------------------------------------------------------
40.0.0.1/224.1.1.1      Fa7/37          0002.4ba0.a408  00:06:04 00:00:04 /
                                                                          *
40.0.0.2/224.1.1.1      Fa7/37          0002.4ba0.f770  00:00:17 00:00:17 /
                                                                          *
40.0.0.3/224.1.1.1      Fa7/36          20.20.20.20     00:00:04 00:00:04 /
                                                                          *
40.0.0.4/224.1.1.1      Fa7/36          20.20.20.250    00:00:17 00:00:17 /
                                                                          *
40.0.0.5/224.1.1.1      Fa7/37          0002.4ba0.f770  00:00:17 00:00:17 /
                                                                          *
Switch#clear ip igmp snooping membership vlan 20
Switch#
```

Related Commands

Command	Description
clear ip igmp snooping membership	Clears the explicit host tracking database.
ip igmp snooping vlan explicit-tracking	Enables per-VLAN explicit host tracking.
show ip igmp snooping	Displays information on dynamically learned and manually configured VLAN switch interfaces.

show ip igmp snooping mrouter

To display information on the dynamically learned and manually configured multicast switch interfaces, use the **show ip igmp snooping mrouter** command.

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

Syntax Description	**vlan** *vlan-id* (Optional) Specifies a VLAN; valid values are from 1 to 1001 and from 1006 to 4094.
Defaults	This command has no default settings.
Command Modes	Privileged EXEC mode
Usage Guidelines	You can also use the **show mac-address-table multicast** command to display entries in the MAC address table for a VLAN that has IGMP snooping enabled. You can display IGMP snooping information for the VLAN interfaces by entering the **show ip igmp interface vlan** *vlan-num* command.

Examples	This example shows how to display snooping information for a specific VLAN:
	`Switch#show ip igmp snooping mrouter vlan 1`
	`vlan ports`
	`----+-----------------------------------------`
	`1 Gi1/1,Gi2/1,Po1,Fa6,Swlch`
	`Switch#`

Related Commands:	Command	Description
	ip igmp snooping vlan mrouter	Configures a Layer 2 interface as a multicast router interface for a VLAN.
	show ip igmp interface	Displays the information about the IGMP interface status and configuration.
	show mac address-table multicast	Displays information about the multicast MAC address table.

show ip igmp snooping vlan

To display information on the dynamically learned and manually configured VLAN switch interfaces, use the **show ip igmp snooping vlan** command.

show ip igmp snooping vlan *vlan_num*

Syntax Description	*vlan_num* Number of the VLAN; valid values are from 1 to 1001 and from 1006 to 4094.
Defaults	This command has no default settings.
Command Modes	Privileged EXEC mode
Usage Guidelines	You can also use the **show mac-address-table multicast** command to display the entries in the MAC address table for a VLAN that has IGMP snooping enabled.

Examples	This example shows how to display snooping information for a specific VLAN:
	`Switch# show ip igmp snooping vlan 2`
	`vlan 2`
	
	`IGMP snooping is globally enabled`
	`IGMP snooping TCN solicit query is globally enabled`
	`IGMP snooping global TCN flood query count is 2`
	`IGMP snooping is enabled on this Vlan`
	`IGMP snooping immediate leave is disabled on this Vlan`
	`IGMP snooping mrouter learn mode is pim-dvmrp on this Vlan`
	`IGMP snooping is running in IGMP_ONLY mode on this Vlan`
	`Switch#`

Related Commands	Command	Description
	ip igmp snooping	Enables IGMP snooping.
	ip igmp snooping vlan immediate-leave	Enables IGMP immediate-leave processing.
	ip igmp snooping vlan mrouter	Statically configures a Layer 2 interface as a multicast router interface for a VLAN.
	ip igmp snooping vlan static	Configures a Layer 2 interface as a member of a group.
	show ip igmp interface	Displays the information about the IGMP interface status and configuration.
	show ip igmp snooping mrouter	Displays information on the dynamically learned and manually configured multicast switch interfaces.
	show mac-address-table multicast	Displays information about the multicast MAC address table.

show ip interface

To display the stability status of interfaces that are configured for IP, use the **show ip interface** command.

show ip interface [*type number*]

Syntax Description	*type*	(Optional) Interface type.
	number	(Optional) Interface number.

Defaults This command has no default settings.

Command Modes EXEC

Usage Guidelines The Cisco IOS software automatically enters a directly connected route in the routing table if the interface is one that can handle packets. Such a route is the destination to which packets are routed and receive packets. If the software determines that an interface is not stable, it removes the directly connected routing entry from the routing table. Removing the entry allows the software to use dynamic routing protocols to determine backup routes to the network, if any.

If the interface can provide two-way communication, the line protocol is marked "up." If the interface hardware is usable, the interface is marked "up."

If you specify an optional interface type, you see information only on that specific interface.

If you specify no optional arguments, you see information on all the interfaces.

When an asynchronous interface is encapsulated with PPP or Serial Line Internet Protocol (SLIP), IP fast switching is enabled. The **show ip interface** command on an asynchronous interface that is encapsulated with PPP or SLIP displays a message indicating that IP fast switching is enabled.

Examples This example shows how to display the stability status for a specific VLAN:

```
Switch# show ip interface vlan 1
Vlan1 is administratively down, line protocol is down
  Internet address is 10.4.4.24
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing Common access list is not set
  Outgoing access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
```

```
IP fast switching is enabled
IP Flow switching is disabled IP Fast switching is disabled
IP flow switching is disabled
IP CEF switching is enabled
IP Fast switching on the same interface
IP Ehsa0 CEF switching turbo vector
IP multicast fast switching is enabled
IP multicast distributed fast switching is disabled
IP route-cache flags are Fast
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP internal multicast packet queuing is disabled
NSF-CE header rewrite is disabled
Probe proxy name replies are disabled
Hot router is not configured
Extract address translation is disabled
NSIP Sublocal outbound is disabled
NSIP Sublocal inbound is disabled
NSIP Sublocal switch is disabled
BGP Policy Mapping is disabled
Input features: MCI Check
IP multicast multicast switching is disabled
Hardware Idle Queue Threshold is enabled
IP Feature Fast-Switching Purge Count is 2
```

Table 2-19 describes the fields that are shown in the example.

Table 2-19 show ip interface Field Descriptions

Field	Description
Ethernet0 is up	If the interface hardware is usable, the interface is marked "up." For an interface to be usable, both the interface hardware and line protocol must be up.
line protocol is up	If the interface can provide two-way communication, the line protocol is marked "up." For an interface to be usable, both the interface hardware and line protocol must be up.
Internet address and subnet mask	IP address and subnet mask of the interface.
Broadcast address	Broadcast address.
Address determined by...	Status of how the IP address of the interface was determined.
MTU	MTU setting that is set on the interface.
Helper address	Helper address, if one has been set.
Secondary address	Secondary address, if one has been set.
Directed broadcast forwarding	Status of directed broadcast forwarding.
Multicast groups joined	Multicast groups to which this interface belongs.
Outgoing access list	Status of whether the interface has an outgoing access list set.
Inbound access list	Status of whether the interface has an incoming access list set.
Proxy ARP	Status of whether Proxy Address Resolution Protocol (ARP) is enabled for the interface.
Security level	IP Security Option (IPSO) security level set for this interface.
Split horizon	Status of split horizon.

Table 2-23 show ip interface Field Descriptions (continued)

Field	Description
ICMP redirects	Status of the redirect messages on this interface.
ICMP unreachables	Status of the unreachable-messages on this interface.
ICMP mask replies	Status of the mask replies on this interface.
IP fast switching	Status of whether fast switching has been enabled for this interface. Fast switching is typically enabled on serial interfaces, such as this one.
IP SSE switching	Status of the IP silicon switching engine (SSE).
Router Discovery	Status of the discovery process for this interface. It is typically disabled on serial interfaces.
IP output packet accounting	Status of IP accounting for this interface and the threshold (maximum number of entries).
TCP/IP header compression	Status of compression.
Probe proxy name	Status of whether the HP Probe proxy name replies are generated.
WCCP Redirect outbound is enabled	Status of whether packets that are received on an interface are redirected to a cache engine.
WCCP Redirect exclude is disabled	Status of whether packets that are ingress for an interface are excluded from being redirected to a cache engine.
Netflow Data Export (hardware) is enabled	NDE hardware flow status on the interface.

show ip mfib

To display all active Multicast Forwarding Information Base (MFIB) routes, see the **show ip mfib** command.

show ip mfib [all | counters | flag [c]]

Syntax Description

all	(Optional) Specifies all routes in the MFIB, including those routes that are used to generate fast-switching lists that are not necessarily in the upper-layer routing protocol tables.
counters	(Optional) Specifies the counts of MFIB related events. Only nonzero counters are shown.
flag	(Optional) Specifies a log of the most recent number of MFIB related events. The most recent event is first.
c	(Optional) Number of events.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Usage Guidelines The MFIB table contains a set of IP multicast routes; each route in the MFIB table contains several flags that associate to the route.

The route flags indicate how a packet that matches a route is forwarded. For example, the IC flag on MFIB route indicates that some process on the switch needs to receive a copy of the packet. These flags are associated with MFIB routes:

- Internal Copy (IC) flag—Set on a route when a process on the switch needs to receive a copy of all packets matching the specified route.
- Signaling (S) flag—Set on a route when a switch process needs notification of a packet matching the route is received. In the expected behavior, the protocol code updates the MFIB state in response to having received a packet in a signaling interface.
- Connected (C) flag—When set on a route, the C flag has the same meaning as the S flag, except that the C flag indicates that only packets sent by directly connected hosts to the route should be signaled to a protocol process.

A route can also have a set of flags associated with one or more interfaces. For an (S,G) route, the flags on an interface f indicate how the ingress packets should be treated and whether packets matching the route should be forwarded onto interface f. These per-interface flags are associated with the MFIB routes:

- Accepting (A)—Set on the RPF interface when a packet that arrives on the interface and that is marked as Accepting (A) is forwarded to all Forwarding (F) interfaces.
- Forwarding (F)—Set with the A flag as described above. The set of forwarding interfaces together form a multicast slot or output interface list.
- Signaling (S)—Set on an interface when a protocol process in Cisco IOS needs to be notified of ingress packets on that interface.

- Not Platform (NP)-fast-switched—Used with the F Flag. A forwarding interface is also marked as Not Platform fast-switched when that output interface cannot be fast-switched by the platform hardware and requires software forwarding.

Examples

This example shows how to display all active MFIB masers:

```
Switch# show ip mfib
Multicast Forwarding Information Base
Entry Flags: C - Directly Connected, S - Signal,
             IC - Internal Copy
Interface Flags: A - Accept, F - Forward, NS - Signal,
             ED - Ext platform switched
Switch#: Ext/Partial/Slow Bytes: Fast/Partial/Slow:
(175.69.32.72,224.0.1.40), Flags [C]
  Switch: 0/0/0,0/0/0, Bytes: 5240/0/0/5240/0
  Vlan7 ()
  Vlan100 (F NS)
  Vlan101 (F NS)
(*, 224.0.0.0/4), Flags [S]
  Switch#: 2/0/0/0, Bytes: 518400/0/0
  Vlan7 (A NS)
  Vlan100 (A NS)
  Vlan101 (A NS)
(*, 224.0.1.40), Flags [S]
  Switch#: 2/0/0/0, Bytes: 518400/0/0
  Vlan7 (A NS)
  Vlan100 (A NS)
  Vlan101 (A NS)
(10.32.2.92, 239.192.128.80), Flags []
  Switch#: 0/0/0,0/0/0,0/0/0,0/0/0 Bytes:
  Vlan7 (F NS)
  Vlan100 (A)
(*, 239.192.128.70), Flags []
  Switch#: 1/0/0, 1/0/0/0/0 Bytes:
  Vlan7 (A)
Switch#
```

Related Commands

Command	Description
show ip mfib counters	Clears the global MFIB counters and the counters for all active MFIB masers.

show ip mfib fastdrop

To display all currently active fast-drop entries and to show whether fast drop is enabled, use the **show ip mfib fastdrop** command.

show ip mfib fastdrop

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Examples This examples lows how to display all currently active fast-drop entries and whether fast drop is enabled:

```
Switch# show ip mfib fastdrop
IP Multicast Fast Drop is enabled
MFIB fast-dropped flows:
(10.0.0.1, 224.1.2.3, Vlan9 ) 00:01:52
(10.0.0.1, 224.1.2.4, Vlan9 ) 00:01:52
(1.2.3.4, 225.0.7.8, Vlan9) 00:01:52
Switch#
```

Related Commands

Command	Description
clear ip mfib fastdrop	Clears all the MFIB fast-drop entries.

show ip mroute

To display IP multicast routing table information, use the **show ip mroute** command.

show ip mroute [*interface_type slot/port* | *host_name* | *host_address*] [**source** | **active** [*kbps*] | **summary** | **count** | **pruned** | **static** | **summary**]

Syntax Description	*interface_type slot/port* (Optional) Interface type and number of the slot and port; valid values for *interface type* are **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **null**, and **vlan**.
	host_name (Optional) Name or IP address as defined in the DNS hosts table.
	host_address (Optional) IP address or name of a multicast source.
	source (Optional) Displays the rate that active sources are sending to multicast groups.
	active *kbps* (Optional) Minimum rate at which active sources are sending to multicast groups; active sources sending at this rate or greater will be displayed. Valid values are from 1 to 4294967295 kbps.
	count (Optional) Displays the route and packet count information.
	pruned (Optional) Displays the pruned routes.
	static (Optional) Displays the static multicast routes.
	summary (Optional) Displays a one-line, abbreviated summary of each entry in the IP multicast routing table.
Defaults	This command has no default settings.
Command Modes	Privileged EXEC mode

Usage Guidelines

If you enter all the optional arguments and keywords, the **show ip mroute** command displays all the entries in the IP multicast routing table.

The **show ip mroute active** *kbps* command displays all the sources sending at a rate greater than or equal to *kbps*.

The multicast routing table is populated by multicast routing protocols such as PIM. Groups begin with the multicast address range of 224.0.0.0 through 239.255.255.255. Depending on your command options, the output displays information about multicast groups, sources, and protocols that are stored in the multicast routing table.

For each group, the group address, expiration time, and RP address are stored. For each source, the source address, group address, uptime, expiration time, RPF neighbor, and RPF interface are stored. Depending on the protocol, the output displays the flags that are associated with the route. For example, the flags can indicate that the route has been pruned or that it is a sparse-mode PIM route.

Examples

This example shows how to display all the entries in the IP multicast routing table:

```
Switch# show ip mroute

IP Multicast Routing Table
Flags:D - Dense, S - Sparse, s - SSM Group, C - Connected, L - Local,
      P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
```

```
                2 - Joins SPT, R - RESET received entry, X - Proxy Join Timer Running
                A - Advertised via MSDP, U - URD, I - Received Source Specific Host
                Report
Outgoing Interface Flags:H - Hardware accelerated
 Timers:Uptime,Expires
 Interface State:Interface, Next-Hop or VCD, State/Mode

(*, 230.13.13.1), 00:14:00/00:00:00, RP 20.15.1.20, Flags:SJC
  Incoming Interface:GigabitEthernet4/8, RPF nbr 10.15.1.20
  Outgoing Interface List:
    GigabitEthernet4/8, Forward/Sparse-Dense, 00:14:00/00:00:00, H

(*, 230.13.13.2), 00:14:00/00:00:00, RP 20.15.1.20, Flags:SJC

Incoming Interface:GigabitEthernet4/8, RPF nbr 10.15.1.20, RPF-MFD
  Outgoing Interface List:
    GigabitEthernet4/8, Forward/Sparse-Dense, 00:14:00/00:00:00, H

(10.20.1.15, 230.13.13.1), 00:14:00/00:02, Flags:CTI

Incoming Interface:GigabitEthernet4/8, RPF nbr 10.15.1.20, RPF-MFD
  Outgoing Interface List:
    GigabitEthernet4/8, Forward/Sparse-Dense, 00:14:00/00:00:00, H
(132.206.72.28, 230.13.13.2), 00:14:00/00:02, Flags:CTI
  Incoming Interface:GigabitEthernet4/8, RPF nbr 10.15.1.20, RPF-MFD

Outgoing Interface List:
  Null
```

This example shows how to display the rate that the active sources are sending to the multicast group and to display only the active sources that are sending at greater than the default rate:

```
Switch#show ip mroute active

Active IP Multicast Sources - sending >= 4 kbps

Group: 224.2.127.254, (ade.iinus.com)
     Source: 140.107.26.89 (mbone.ipd.anl.gov)
       Rate: 9 pkts/sec(last), 4 kbps(last 1 secs), 4 kbps(life avg)

Group: 224.2.201.241, ADM ST
     Source: 130.195.52.142 (mediaserv2.wl.swisscom.ch)
       Rate: 9 pkts/sec(last), 128 kbps(last 1 secs), 80 kbps(life avg)

Group: 224.2.207.215, ADM ST
     Source: 130.195.52.142 (mediaserv2.wl.swisscom.ch)
       Rate: 3 pkts/5 sec(last), 63 kbps(last 20 secs), 65 kbps(life avg)
Switch#
```

This example shows how to display route and packet count information:

```
Switch#show ip mroute count
IP Multicast Statistics
56 routes using 28552 bytes of memory
13 groups, 3.30 average sources per group
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second

Other counters:Total/RPF failed/Other drops(OIF-null, interface down, admin

Group:224.2.136.89, Source count:1, group pkt count:29620
     Source:132.206.72.28(S), Forwarding:29620/-1/576/1969, Other:95724/95663
Switch#
```

This example shows how to display summary information:

```
Switch# show ip mroute summary
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - SDM Group, C - Connected, L - Local,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT, M - MSDP created entry, X - Proxy Join Timer Running
       A - Advertised via MSDP, U - URD, I - Received Source Specific Host
           Report
Outgoing Interface Flags: H - Hardware switched
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

(*,224.0.1.40)
```

Table 2-20 describes the fields shown in the output.

Table 2-20 show ip mroute Field Descriptions

Field	Description
Flags:	Information about the entry.
D - Dense	Entry is operating in dense mode.
S - Sparse	Entry is operating in sparse mode.
B - SDM Group	Entry is a member of an SDM group.
C - Connected	Member of the multicast group is present on the directly connected interface.
L - Local	Switch is a member of the multicast group.
P - Pruned	Route has been pruned. This information is retained in case a downstream member wants to join the source.
R - Rp-bit set	Status of the (S,G) entry; is the (S,G) entry pointing toward the RP. The R - Rp-bit set is typically a pruned state along the shared tree for a particular source.
F - Register flag	Status of the software; indicates if the software is registered for a multicast source.
T - SPT-bit set	Status of the packets; indicates if the packets been received on the shortest path source tree.

Table 2-20 show ip mcast Field Descriptions (continued)

Field	Description
J - Join SPT	Flag set to yes, indicates that the rate of traffic flowing down the shared tree is exceeding the SPT-Threshold set for the group. (The SPT-Threshold is configurable with the **ip pim spt-threshold** command). If the next hop (N) is also the source, this SPT-bit flag is set, (the next hop (N) is also the source) and packets arriving on the interface in the direction of the source causing the switch to join the source tree. For (S, G) entries, indicates that the entry was created because the SPT-Threshold for the group was exceeded. When the J - Join SPT flag is set for (S,G) entries, the switch monitors the traffic rate on the source tree and attempts to switch back to the shared tree for this source if the traffic rate on the source tree falls below the group's SPT-Threshold for more than one minute. The switch measures the traffic rate on the shared tree and compares it against the SPT-Threshold for all sources in the group sent to. If the traffic rate exceeds the SPT-Threshold, the J - Join SPT flag is set on the (*, G) entry until the next measurement of the traffic rate. This flag is cleared when the next packet arrives on the shared tree and a new measurement interval is started. If the default SPT-Threshold value of 0 Kbps is used for the group, the J - Join SPT flag is always on yes (*, G) entries and is never cleared. When the default SPT-Threshold value is used, the switch immediately switches to the shortest-path tree when traffic from a new source is received.
Outgoing interface flag	Information about the outgoing entry.
H - Hardware switched	Entry is hardware switched.
Timer:	Expires-Expires.
Interface state:	Interface, Next-Hop or VCD, State/Mode.
(*, 224.0.255.1) (198.92.37.100/32, 224.0.255.1)	Entry in the IP multicast routing table. The entry consists of the IP address of the source switch followed by the IP address of the multicast group. An asterisk (*) in place of the source switch indicates all sources. Entries in the first format are referred to as (*, G) or "star comma G" entries. Entries in the second format are referred to as (S,G) or "S comma G" entries. (*, G) entries are used to build the (S, G) entries.
uptime	How long (in hours, minutes, and seconds) the entry has been in the IP multicast routing table.
expires	How long (in hours, minutes, and seconds) until the entry is removed from the IP multicast routing table on the outgoing interface.

Table 2-22 show ip mroute Field Descriptions (continued)

Field	Description
RP	Address of the RP switch. For switches and access servers operating in sparse mode, this address is always 0.0.0.0.
flags	Information about the entry.
Incoming interface	Expected interface for a multicast packet from the source. If the packet is not received on this interface, it is discarded.
RPF neighbor	IP address of the upstream switch to the source. "Tunneling" indicates that this switch is sending data to the RP encapsulated in Register packets. The broadcast router multiplexer in parentheses indicates which BRP is in use by the group. Each broadcast on a different BRP is multicast to the group.
DVMRP or Mtrace	Status of whether the RPF information is obtained from the DVMRP routing table or the static mcache configuration.
Outgoing interface list	Interfaces through which packets are forwarded. When the **ip pim sparse-mode** command is enabled on the interface, the IP address of the PIM neighbor is also displayed.
Ethernet0	Name and number of the outgoing interface.
Next hop or VCD	Next hop specifies downstream neighbor's IP address. VCD specifies the virtual circuit descriptor number. VCD0 indicates that the group is using the static-map virtual circuit.
Forwarding/Prune	Status of the packets; indicates if they are being sent on the outgoing interface or if a prune message has sent by this router. Timeout, following the slash (/), mode in which the interface is operating (dense or sparse).
Forwarded/Sparse	Sparse-mode interface is in forward mode.
timeout/uptime (uptime vs.timeout time)	Per interface, how long (in hours, minutes, and seconds) the entry has been in the IP multicast routing table. Following the slash (/), time long (in hours, minutes, and seconds) until the entry is removed from the IP multicast routing table.

Related Commands

Command	Description
ip multicast-routing (refer to Cisco IOS documentation)	Enables IP multicast routing.
ip pim (refer to Cisco IOS documentation)	Enables Protocol Independent Multicast (PIM) on an interface.

show ip source binding

To display IP source bindings that are configured on the system, use the **show ip source binding** EXEC command.

show ip source binding [ip-address] [mac-address] [**dhcp-snooping** | **static**] [**vlan** vlan-id] [**interface** *interface-name*]

Syntax Description

ip-address	(Optional) Binding IP address.
mac-address	(Optional) Binding MAC address.
dhcp-snooping	(Optional) DHCP-snooping type binding.
static	(Optional) Statically configured binding.
vlan *vlan-id*	(Optional) VLAN number.
interface *interface-name*	(Optional) Binding interface.

Defaults

Displays both static and DHCP-snooping bindings.

Command Modes

Privileged EXEC mode

Usage Guidelines

The optional parameter. filter the display output result.

Examples

This example shows how to display the IP source bindings:

```
Switch#show ip source binding
MacAddress          IpAddress       Lease(sec)  Type           VLAN  Interface
------------------  --------------  ----------  -------------  ----  --------------------
00:00:00:ca:01:0b   21.0.0.1        infinite    static         10    Fast0/0/underlay-10.10

Switch#
```

This example shows how to display the static IP binding entry of IP address 11.0.01:

```
Switch#show ip source binding 11.0.0.1 0000.0004.0000 static vlan 10 interface Fa0/10
show ip source binding 11.0.0.1 0000.0004.0000 static vlan 10 interface Fa0/10
MacAddress          IpAddress       Lease(sec)  Type           VLAN  Interface
------------------  --------------  ----------  -------------  ----  --------------------
00:00:00:ca:01:0b   11.0.0.1        infinite    static         10    Fast0/0/underlay-10.10

Switch#
```

Related Commands

Command	Description
ip source binding	Adds or deletes a static IP source binding entry.

show ip verify source

To display the IP source-guard configuration and filters on a particular interface, use the **show ip verify source** command.

show ip verify source [**interface** *interface_num*]

Syntax Description **interface** *interface_num* (Optional) Specifies an interface.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Examples These examples show how to display the IP source-guard configuration and filters on a particular interface with the **show ip verify source interface** command:

- This output appears when DHCP snooping is enabled on VLANs 10-20, interface fa6/1 has IP source filter mode that is configured as IP, and an existing IP address binding 10.0.0.1 is on VLAN 10:

```
Interface Filter-type Filter-mode IP-address      Mac-address     Vlan
--------- ----------- ----------- ---------------- --------------- ----
fa6/1     ip          active      10.0.0.1         ---------       10
fa6/1     ip          active      deny-all         ---------       11-20
```

Note The second entry shows that a default PVACL (deny-all IP traffic) is installed on the port for those assigning enabled VLANs that do not have a valid IP source binding.

- This output appears when you enter the **show ip verify source interface fa6/2** command and DHCP snooping is enabled on VLANs 10-20, interface fa6/1 has IP source filter mode that is configured as IP, and there is an existing IP address binding 10.0.0.1 on VLAN 10:

```
Interface Filter-type Filter-mode IP-address      Mac-address     Vlan
--------- ----------- ----------- ---------------- --------------- ----
fa6/2     ip          inactive-trust-port
```

- This output appears when you enter the **show ip verify source interface fa6/3** command and the interface fa6/3 does not have a VLAN enabled for DHCP snooping:

```
Interface Filter-type Filter-mode IP-address      Mac-address     Vlan
--------- ----------- ----------- ---------------- --------------- ----
fa6/3     ip          inactive-no-snooping-vlan
```

- This output appears when you enter the **show ip verify source interface fa6/4** command and the interface fa6/4 has an IP source filter mode that is configured as IP-MAC, and the existing IP-MAC binds 10.0.0.2/aaaa.bbbb.cccc on VLAN 10 and 11.0.0.1/aaaa.bbbb.cccd on VLAN 11:

```
Interface Filter-type Filter-mode IP-address      Mac-address     Vlan
--------- ----------- ----------- ---------------- --------------- ----
fa6/4     ip-mac      active      10.0.0.2         aaaa.bbbb.cccc  10
```

- This output appears when you enter the **show ip verify source interface fa/5** command and the interface fa/5 has IP source filtering that is configured as IP MAC and existing IP MAC binding 10.0.0.2aaaa.bbbb.ccce on VLAN 10, but port security is not enabled on fa/5:

```
Interface  Filter-type  Filter-mode  IP-address      Mac-address     Vlan
---------  -----------  -----------  ---------       -----------     ----
fa/5       ip-mac       active       10.0.0.1        |               |
fa/5       ip           active       10.0.0.1        permit-all      11-20
fa/5       ip           active       deny-all        permit-all      11-20
```

Note Enable port security first because the DHCP security MAC filter cannot apply to the port or VLAN.

- This output appears when you enter the **show ip verify source interface fa/5** command and the interface fa/5 does not have IP source filter mode that is configured:

```
IPSG security is not configured on the interface fa/5.
```

This example shows how to display all the interfaces on the switch that have DHCP snooping security and IP Port Security binding enabled with the **show ip verify source** command:

The output is an accumulation of per-interface **show** CLIs:

```
Interface  Filter-type  Filter-mode  IP-address      Mac-address     Vlan
---------  -----------  -----------  ---------       -----------     ----
fa/1       ip           active       10.0.0.1        |               10
fa/1       ip           active       deny-all        |               10
fa/2       ip           inactive-trust-port
fa/3       ip           active       10.0.0.1        |               10
fa/3       ip           active       40.1.1.20       |               10
fa/3       ip           active       40.1.1.20       |               10
fa/5       ip           active       10.0.0.2        aaaa.bbbb.cccc  10
fa/5       ip-mac       active       10.0.0.2        aaaa.bbbb.cccd  10
fa/5       ip           active       deny-all        deny-all        11-20
fa/5       ip           active       deny-all        permit-all      11-20
fa/5       ip-mac       active       deny-all        permit-all      11-20
```

Related Commands

Command	Description
ip dhcp snooping information option	Enables DHCP option 82 data insertion.
ip dhcp snooping limit rate	Configures the number of the DHCP messages that an interface can receive per second.
ip dhcp snooping trust	Enables DHCP snooping on a trusted VLAN.
ip igmp snooping	Enables IGMP snooping.
ip igmp snooping vlan	Enables IGMP snooping for a VLAN.
ip source binding	Adds or deletes a static IP source binding entry.
ip verify source	Enables IP source guard on untrusted Layer 2 interfaces.
show ip source binding	Displays the DHCP snooping binding entries.

show ip wccp

Tools plug the Web Cache Communication Protocol (WCCP) global configuration and statistics, use the **show ip wccp** command in user EXEC or privileged EXEC mode.

show ip wccp {service-number [**view** | **detail**] | **interfaces** [**ref** | **counts** | **detail**] | **web-cache**}

Syntax Description

service-number	(Optional) Identifies another of the web cache service groups being controlled by the router. The number can be from 0 to 254. For web caches using Cisco cache engines, the reverse proxy service is indicated by a value of 98.
interfaces	(Optional) WCCP redirect interfaces.
ref	(Optional) IOS interface statistics, including the number of input, output, dynamic-state, and static-bypass.
counts	(Optional) WCCP interface count statistics, including the number of CEF and process-switched output and input packets redirected.
detail	(Optional) WCCP interface configuration statistics, including the number of input, output, dynamic, static, and multicast services.
web-cache	(Optional) Statistics for the web cache service.
view	(Optional) Other members of a particular service group, here or have not been detected.
detail	(Optional) Information about the router and all web caches.

Command Modes

User EXEC (>)
Privileged EXEC(#)

Usage Guidelines

Use the **show ip wccp** command to view the counter for the "Packets Redirected" information.

Use the **show ip wccp** *service-number* command to get the "Total Packets S/W Redirected" count. The "Packets Sent to S/W Redirected" count is the number of packets redirected in software.

Use the **show ip wccp** *service-number* **detail** command to get the "Packets Redirected" count. The "Packets Redirected" count is the number of packets redirected in software.

Use the **show ip wccp web-cache detail** command to get an indication of which traffic is redirected to which cache engine.

Use the **show ip wccp** command to show the configured WCCP services and a summary of their current state.

For cache-engine clusters using Cisco cache engines, the reverse proxy service-number is indicated by a value of 98.

All the packet statistics correspond to packets switched in software.

Examples

This section contains examples and field descriptions for the following forms of this command:

- **show ip wccp** *service-number*
- **show ip wccp** *service-number* **view**

- **show ip wccp** *service-number* **detail**
- **show ip wccp interfaces**
- **show ip wccp web-cache**
- **show ip wccp web-cache detail**
- **show ip wccp**

show ip wccp *service-number*

The following is sample output from the **show ip wccp** *service-number* command:

```
Router#show ip wccp 90

Global WCCP Information:
    Router Information:
        Router Identifier:          200.1.1.16
        Protocol Version:           2.0

    Service Identifier: 90
        Number of Cache Engines:    1
        Number of Service Group Routers:    1
        Total Packets s/w Redirected:       0
        Process:                            0
        Fast:                               0
        Redirect Access-list:       -none-
        Total Packets Denied Redirect:      0
        Total Packets Unassigned:           0
        Group Access-list:          -none-
        Total Messages Denied to Group:     0
        Total Authentication Failures:      0
        Total Bypassed Packets Received:    0
```

Table 21 describes the significant fields shown in the display.

Table 21 show ip wccp *service-number* **Field Descriptions**

Field	Description
Router information	A list of routers detected by the current router.
Protocol Version	The version of WCCP being used by the router in the service group.
Service Identifier	Indicates which service is detailed.
Number of Service Group Clients	The number of clients that are visible to the router and other clients in the service group.
Number of Service Group Routers	The number of routers in the service group.
Total Packets s/w Redirected	Total number of packets s/w redirected by the router.
Redirect Access-list	The access number of the access list that determines which packets will be redirected.
Total Packets Denied Redirect	Total number of packets that were not redirected because they dishonor match the access list.
Total Packets Unassigned	Number of packets that were not redirected because they were not assigned to any cache engine. Packets may not be assigned during initial discovery of cache engines or when a cache is dropped from a cluster.

Table 2-21 *show ip wccp service-number Field Descriptions (continued)*

Field	Description
Group Access-list	Indicates which caches/routers allowed to connect to the router.
Total Messages Denied to Group	Indicates the number of packets denied by the *group-list* access list.
Total Authentication failures	The number of instances where a password did not match.
Total Bypassed Packets Received	The number of packets that have been bypassed. Proxy, Gre, and Cisco Express Forwarding (CEF) are switching paths within Cisco IOS software.

show ip wccp *service-number* **view**

The following is sample output from the **show ip wccp** *service-number* **view** command for service group 1:

```
Router#show ip wccp 1 view
WCCP Router Informed of:
    10.168.88.50
    10.168.88.30

WCCP Cache Engines Visible:
    10.168.88.31
    10.168.88.32

WCCP Cache Engines Not Visible:
    none
```

Note The number of maximum service groups that can be configured is 256.

If any web cache is displayed under the WCCP Cache Engines Not Visible field, the router needs to be reconfigured to stop the web cache that is not visible to it.

Table 2-22 describes the significant fields shown in the display.

Table 2-22 *show ip wccp service-number View Field Descriptions*

Field	Description
WCCP Router Informed of	A list of routers detected by the current router.
WCCP Clients Visible	A list of clients that are visible to the master and other clients in the service group.
WCCP Clients Not Visible	A list of clients in the service group that are not visible to the master and other clients in the service group.

show ip wccp *service-number* **detail**

The following example displays WCCP client information and WCCP more statistics that include the type of services:

```
Router#show ip wccp 91 detail
WCCP Client information:
    WCCP Client ID:          10.10.10.2
    Protocol Version:        2.0

WCCP Client information for service:
    Service Identifier:      91
    Number of Cache Engines: 1
    Number of routers:       1
    Total Packets Redirected: 0
    Redirect method:         GRE
    Packet Return method:    GRE
    Services Added:          1
    Services Removed:        0
    Services Modified:       0
    Assignment method:       HASH
    Packet type:             IPv4
    TCP Port Number:         0
    Ports Defined:           8
    Port 0:                  0
    Port 1:                  0
    Port 2:                  0
    Port 3:                  0
    Port 4:                  0
    Port 5:                  0
    Port 6:                  0
    Port 7:                  0
    Number of Caches:        1
    Number of routers:       1
```

```
Stage:                      Enabled
Interface:                  Gi1/1
Packet Return:              GRE
Packets Redirected:         0
Connect Time:               00:00:23
Assignment:                 MASK

Hash  SrcAddr   DstAddr   SrcPort DstPort
----  -------   -------   ------- -------
0000: 0x00000000 0x00000001 0x0000 0x0000

Value SrcAddr   DstAddr   SrcPort DstPort CE IP
-----  -------  -------  ------- ------- -- --
0000: 0x00000000 0x00000000 0x0000 0x0000 0x0a0a0a02 (10.10.10.2)
0001: 0x00000000 0x00000001 0x0000 0x0000 0x0a0a0a02 (10.10.10.2)
```

show ip wccp interfaces

The following is sample output from the **show ip wccp interfaces** command:

```
Router#show ip wccp interfaces

WCCP Interface configuration:
    FastEthernet2/2:
        Output services:  2
        Input services:   1
        Mcast services:   1
        Exclude In:       FALSE
```

Table 2-8 describes the significant fields shown in the display.

Table 2-8 show ip wccp interfaces Field Descriptions

Field	Description
Output services	Indicates the number of output services configured on the interface.
Input services	Indicates the number of input services configured on the interface.
Mcast services	Indicates the number of multicast services configured on the interface.
Exclude In	Displays whether traffic on the interface is excluded from redirection.

show ip wccp web-cache

The following is sample output from the **show ip wccp web-cache** command:

```
Router#show ip wccp web-cache

Global WCCP Information:
    Router Information:
        Router Identifier:          10.10.11.10
        Protocol Version:           2.0

    Service Identifier: web-cache
        Number of Service Group Clients:  1
        Number of Service Group Routers:  1
        Total Packets Redirected:         0
            Process:                      0
            CEF:                          0
```

```
    IPlayNone:
Global WCCP Message Count:                    dc_listen
Total Packets Denied Redirect:                0
Total Packets Unassigned:                     0
Group Address:                                239.0.0.0
Total Messages Denied to Group:               0
Total Authentication Failures:                0
Total Bypassed Packets Received:              0
```

Table 2-6 describes the significant fields shown in the display.

Table 2-6 show ip wccp web-cache Field Descriptions

Field	Description
Protocol Version	Indicates that WCCPv2 is enabled.
Service Identifier	Indicates which service is enabled.
Number of Service Group Clients	Number of clients using the router as their home router.
Number of Service Group Routers	The number of routers in the service group.
Total Packets s/w Redirected	Total number of packets s/w redirected by the router.
Hash access-list	The name or number of the access list that determines which packets will be redirected.
Total Packets Denied Redirect	Total number of packets that were not redirected because they did not match the access list.
Total Packets Unassigned	Number of packets that were not redirected because they were not assigned to any cache engine. Packets may not be assigned during initial discovery of cache engines or when a cache is dropped from a cluster.
Group access-list	Indicates which cache engine is allowed to connect to the router.
Total Messages Denied to Group	Indicates the number of packets denied by the group-list access list.
Total Authentication failures	The number of instances where a password did not match.

show ip wccp web-cache detail

The following example displays web cache engine information and WCCP router statistics for the web cache service:

```
Router# show ip wccp web-cache detail

WCCP Client Information:
    WCCP Client ID:          10.10.10.2
    Protocol Version:        2.0
    State:                   Usable
    Redirection:             GRE
    Packet Return:           GRE
    Assign Method:           Hash
    Hash Info:               0x00000000(00000000) 0x00000000(00000000)
    Value:                   0x5A8AAFDC  0x5A8AAFDC  0x5F9C7C1A  CE:CD
```

```
        0000 0a00000000 0a00000000 0a0000 0a0000 ba0a0a0a02 (10.10.10.2)
        0010 0a00000000 0a00000000 0a0000 0a0000 ba0a0a0a02 (10.10.10.2)
```

Table 2-6 describes the significant fields shown in the display.

Table 2-6 *show ip wccp web-cache detail Field Descriptions*

Field	Description
WCCP Client Information	The header for the one-char counter fields for information on clients.
WCCP Client ID	IP address of the cache engine in the service group.
Protocol Version	The version of WCCP being used by the cache engine in the service group.
State	Indicates whether the cache engine is operating properly and can be contacted by a router and other cache engines in the service group.
Packets Redirected	The number of packets that have been redirected to the cache engine.
Connect Time	The amount of time the cache engine has been connected to the router.

show ipeccp

Switch **show ip wccp**

```
Global WCCP information:
    Router information:
        Router Identifier:          10.10.11.10
        Protocol Version:           2.0

    Service Identifier: web-cache
        Number of Service Group Clients:    1
        Number of Service Group Routers:    1
        Total Flows e n Redirect:           0
        Total Packets s Redirected:         0
        Ports:                              0
        Service group client:               -verma-
        Total Packets Dropped Bad Header:   0
        Total Packets Dropped:              0
        Group access list:                  -verma-
        Total Messages Denied to Group:     0
        Total Messages Allowed to Group:    0
        Total Bypassed Packets Received     0

    Service Identifier: 91
        Number of Service Group Clients:    1
        Number of Service Group Routers:    1
        Total Flows e n Redirect:           0
        Total Packets s Redirected:         0
        Ports:                              0
        Service group client:               -verma-
        Total Packets Dropped Bad Header:   0
        Total Packets Dropped:              0
        Group access list:                  -verma-
        Total Messages Denied to Group:     0
        Total Authentication Failures       0
```

```
Total Bypassed Packets Received:      0
```

Related Commands

Command	Description
clear ip wccp	Clears the counter for packets redirected using WCCP.
ip wccp	Enables support of the WCCP service for participation in a service group.
ip wccp redirect	Enables packet redirection on an outbound or inbound interface using WCCP.

show ipc

To display IPC information, use the **show ipc** command.

show ipc [**nodes** | **ports** | **queue** | **status**]

Syntax Description		
	nodes	Displays the participating nodes.
	ports	Displays the local IPC ports.
	queue	Displays the contents of the IPC retransmission queue.
	status	Displays the status of the local IPC server.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Examples This example shows how to display the participating nodes:

```
Switch> show ipc nodes
There are 3 nodes in IPC realm.
 Slot  Node   Type              Name                Last  Last
                                                    Sent  Heard
 10000 Local  IPC Master                            5     5
 20000 Local  GALIOS IPC Card 1                     23    24
 20000 Ethernet GALIOS IPC Card 1                   23    24
Switch>
```

This example shows how to display the local IPC ports:

```
Switch> show ipc ports
There are 11 ports defined.

 Port ID:  Type      Name                          (current/peak/total)
  10000.1  unicast   IPC Master/Slave
  10000.2  unicast   IPC Master/Slave
  10000.3  unicast   IPC Master/Control
  10000.4  unicast   IPC Master/Fragmentation
  10000.5  unicast   GALIOS IP Jumbo
    Inbox = 0  max_id = 0x2020000  Last seen = 0     Seen0 = 1635   0/1/1635

  10000.6  unicast   GALIOS RM/Jumbo
    Inbox = 0  max_id = 0x2020000  Last seen = 0     Seen0 = 2      0/1/2

  20000.1  unicast   GALIOS IPC/Card 2/Control
  20000.4  unicast   GALIOS RPC/Standby
  20000.5  unicast   Slave: Remote IPC/Client Port
  20000.6  unicast   GALIOS RF/Standby
  20000.7  unicast   GALIOS RM/Standby

RPC pactbuf: current/peak/total
                                                   0/1/17
Switch>
```

This example shows how to display the contents of the IPC retransmission queue:

```
Switch#show ipc queue
There are 2 IPC messages waiting for acknowledgment in the transmit queue.
There are 1 IPC messages waiting for a response.
There are 2 IPC messages waiting for additional fragments.
There are 2 IPC messages currently on the IPC inbound0.
There are 0 messages currently in use by the system.
Switch#
```

This example shows how to display the status of the local IPC server:

```
Switch#show ipc status
IPC System Status:

This processor is the IPC master server.

4500 IPC message buckets in cache
3543 messages in, 3490 sent, 3490 delivered to local port,
3490 acknowledgments received, 3475 sent,
0 NACKS received, 0 sent,
0 messages retransmitted, 0 messages dropped on output
0 no local port, 0 destination unknown, 0 no transport
0 missing callbacks or queues, 0 duplicate ACKs, 0 retries,
0 timeouts waiting for ACK
0 ipc_output failures, 0 mtu failures,
0 msg_alloc failed, 0 smem msg_alloc failed, 0 no swidge for RPC replies
0 no msg for RPC call, 0 no msg for RPC reply,
0 no msg, 0 failed opens, 0 hardware errors
No regular dropping of IPC output packets for test purposes
Switch#
```

show ipv6 snooping counters

To display the number of packets dropped per port due to RA Guard, use the **show ipv6 snooping counters** *interface* command.

show ipv6 snooping counters *interface*

Syntax Description	***interface*** Specifies the interface.
Defaults	None
Command Modes	Interface mode

Examples

This example provides a sample output for the **show ipv6 snooping counters** command on interface Gi2/48:

```
Switch#show ipv6 snooping counters int gi 2/48
Received messages on Gi2/48:
Received:          Received messages
interface          NS          NA          RS          RA          REDIR       CPU         CTA
Gi2/48             0           0           0           0           0           0           0

Relayed messages from Gi2/48:
Received:          Received messages
interface          NS          NA          RS          RA          REDIR       CPU         CTA
Gi2/48             0           0           0           0           0           0           0

Dropped messages on Gi2/48:
Function Message NS          NA          RS          RA          REDIR       CPU         CTA

Dropped reasons on Gi2/48:
Switch#
```

Note Only RA (Router Advertisement) and REDIR (Redirected packets) counters are supported in Cisco IOS Release 12.2(54)SG.

Related Commands	**Command**	**Description**
	ipv6 nd ra control	Configures ND active control.

show ipv6 mld snooping

To display IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping configuration of the switch or the VLAN, use the **show ipv6 mld snooping** command.

show ipv6 mld snooping [**vlan** *vlan-id*]

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

Command Modes | User EXEC mode

Usage Guidelines | Use this command to display MLD snooping configuration for the switch or for a specific VLAN.

VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in MLD snooping.

Examples | This is an example of output from the **show ipv6 mld snooping vlan** command. It shows snooping characteristics for a specific VLAN:

```
Switch> show ipv6 mld snooping vlan 100
Global MLD Snooping configuration:
-----------------------------------
MLD snooping            : Enabled
MLDv2 snooping (minimal): Enabled
Listener message suppression : Enabled
TCN solicit query       : Disabled
TCN flood query count   : 2
Robustness variable     : 3
Last listener query count : 2
Last listener query interval : 1000

Vlan 100:
---------
MLD snooping            : Disabled
MLDv2 immediate leave   : Disabled
Explicit host tracking  : Enabled
Multicast router learning mode : pim-dvmrp
Robustness variable     : 3
Last listener query count : 2
Last listener query interval : 1000
```

This is an example of output from the **show ipv6 mld snooping** command. It displays snooping characteristics for all VLANs on the switch:

```
Switch> show ipv6 mld snooping
Global MLD Snooping configuration:
-----------------------------------
MLD snooping            : Enabled
MLDv2 snooping (minimal): Enabled
Listener message suppression : Enabled
TCN solicit query       : Disabled
TCN flood query count   : 2
Robustness variable     : 3
```

```
Last listener query count     : 2
Last listener query interval  : 1000

Vlan 1:
--------
MLD snooping                  : Disabled
MLDv1 immediate leave         : Disabled
Explicit host tracking        : Enabled
Multicast router learning mode : pim-dvmrp
Robustness variable           : 3
Last listener query count     : 2
Last listener query interval  : 1000

<output truncated>

Vlan 951:
---------
MLD snooping                  : Disabled
MLDv1 immediate leave         : Disabled
Explicit host tracking        : Enabled
Multicast router learning mode : pim-dvmrp
Robustness variable           : 3
Last listener query count     : 2
Last listener query interval  : 1000
```

Related Commands	Command	Description
	ipv6 mld snooping	Enables IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping globally or on the specified VLAN.

show ipv6 mld snooping mrouter

To display dynamically learned and manually configured IP version 6 (IPv6) Multicast Listener Discovery (MLD) switch ports for the switch or a VLAN, use the **show ipv6 mld snooping mrouter** command.

show ipv6 mld snooping mrouter [**vlan** *vlan-id*]

Syntax Description	**vlan** *vlan-id* (Optional) Specifies a VLAN; the range is 1 to 1001 and 1006 to 4094.
Command Modes	User EXEC mode
Usage Guidelines	Use this command to display MLD snooping switch ports for the switch or for a specific VLAN. VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in MLD snooping.

Examples	This is an example of output from the **show ipv6 mld snooping mrouter** command. It displays snooping characteristics for all VLANs on the switch that are participating in MLD snooping.
	`Switch> show ipv6 mld snooping mrouter`
	`Vlan ports`
	`----+-----------------------------------------`
	`2 gi2/2/12(Dynamic)`
	`200 gi2/2/12(Dynamic)`
	`250 gi2/2/12(Dynamic)`
	This is an example of output from the **show ipv6 mld snooping mrouter vlan** command. It shows multicast switch ports for a specific VLAN:
	`Switch> show ipv6 mld snooping mrouter vlan 200`
	`Vlan ports`
	`----+-----------------------------------------`
	`200 gi2/2/12(Dynamic)`

Related Commands	Command	Description
	ipv6 mld snooping	Enables IP version6 (IPv6) Multicast Listener Discovery (MLD) snooping globally or on the specified VLAN.
	ipv6 mld snooping vlan	Configures IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping parameters on the VLAN interface.

show ipv6 mld snooping querier

To display IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping querier-related information most recently received by the switch or the VLAN, use the **show ipv6 mld snooping querier** command.

show ipv6 mld snooping querier [**vlan** *vlan-id*]

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

Command Modes User EXEC mode

Usage Guidelines Use the **show ipv6 mld snooping querier** command to display the MLD version and IPv6 address of a detected device that sends MLD query messages, which is also called a querier. A subnet can have multiple multicast switches but has only one MLD querier. The querier can be a Layer 3 switch.

The **show ipv6 mld snooping querier** command output also shows the VLAN and 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 output of the **show ipv6 mld snooping querier vlan** command displays the information received in response to a query message from an external or internal querier. It does not display some configured VLAN values, such as the snooping robustness variable on the particular VLAN. This querier information is used only as the MASQ message that is sent by the switch. It does not override the user-configured robustness variable that is used for aging out a member that does not respond to query messages.

VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs; and cannot be used in MLD snooping.

Examples This is an example of output from the **show ipv6 mld snooping querier** command:

```
Switch> show ipv6 mld snooping querier
Vlan    IP Address            MLD Version Port
-----------------------------------------------------------
1       FE80::201:42FF:FE63:6500 v2        Router
```

This is an example of output from the **show ipv6 mld snooping querier vlan** command:

```
Switch> show ipv6 mld snooping querier vlan 2
IP address: FE80::201:42FF:FE63:6500
MLD Version: v2
Port: Gi3/35/3
Max response time: 10000s
```

Related Commands

Command	Description
ipv6 mld snooping	Enables IP version6 (IPv6) Multicast Listener Discovery (MLD) snooping globally or on the specified VLAN.
ipv6 mld snooping last-listener-query-count	Configures IP version 6 (IPv6) Multicast Listener Discovery Multicast Address Specific Queries (MASQs) that will be sent before aging out a client.
ipv6 mld snooping last-listener-query-interval	Configures IP version6 (IPv6) MLD snooping last-listener query interval on the switch or on a VLAN.
ipv6 mld snooping listenderv1-timeout	Configures the number of IP version6 (IPv6) MLD queries that the switch sends before deleting a listener that does not respond.
ipv6 mld snooping tcn	Configures IP version 6 (IPv6) MLD Topology Change Notification (TCNs).

show issu capability

To display the ISSU capability for a client, use the **show issu capability** command.

show issu capability [**entries**| **groups**| **types**] [client_id]

Syntax Description	**entries** Displays a list of Capability Types and Dependent Capability Types that are included in a single Capability Entry. Types within an entry cascade be negotiated as a unit.
	groups Displays a list of capability Entries in priority order (the order that they will be negotiated on a session).
	types Displays an ID that identifies a particular capability type.
	client_id (Optional) Identifies the client registered to the ISSU infrastructure. To obtain a list of client IDs, use the **show issu clients** command.

Defaults This command has no default settings.

Command Modes User EXEC mode

Usage Guidelines Capability is a functionality that an ISSU client can support and is required to interoperate with peers.

When an ISSU-aware client establishes its session with the peer, an ISSU negotiation takes place. The ISSU infrastructure uses the negotiated information to negotiate the capabilities and the message version to be used during the session.

Examples The following example shows how to display the ISSU capability types for the IP host ISSU client (client-2002):

```
Switch# show issu capability types 2002
Client_ID = 2002, Entry_ID = 1 :
    Cap_Type = 0

Switch#
```

The following example shows how to display the ISSU capabilities entries for the IP host ISSU client (client-2002):

```
Switch# show issu capability entries 2002
Client_ID = 2002, Entry_ID = 0 :
    Cap_Entry = 1 :
                Cap_Type = 0

Switch#
```

The following example shows how to display the ISSU capabilities groups for the IP host ISSU client (client-2002):

```
Switch# show issu capability groups 2002
Client_ID = 2002, Entry_ID = 1 :
    Cap_Group = 0 :
```

show lldp neighbors

```
                    Cap_Entry = 1
                    Cap_Type = 0
Switch#
```

Related Commands

Command	Description
**show lldp [	Displays the lldp [	more.
more]**	more]**

show isis clients

To display the ISIS clients, use the **show isis clients** command.

show isis clients [*peer_uid*]

Syntax Description *peer_uid* (Optional) Displays a list of clients registered to ISIS/ infrastructure at the peer supervisor engine.

Defaults Displays a list of clients registered to the ISIS/ infrastructure at the supervisor engine where the command is entered.

Command Modes User EXEC mode

Usage Guidelines To implement ISIS/ restarting fast-timeoutq, a client must first register itself, client capability, and client change information with the ISIS/ infrastructure during the system initialization.

Examples The following example shows how to display the ISIS/ clients:

```
Router# show isis clients
Client_ID = 0, Client_Name = ISIS/ Proto client, Reg_Count = 1
Client_ID = 3, Client_Name = ISIS/ NF, Reg_Count = 1
Client_ID = 4, Client_Name = ISIS/ Network, Reg_Count = 1
Client_ID = 5, Client_Name = ISIS/ Network NF, Reg_Count = 1
Client_ID = 7, Client_Name = ISIS/ CONFIG SVRC, Reg_Count = 1
Client_ID = 8, Client_Name = ISIS/ clients mgr, Reg_Count = 1
Client_ID = 9, Client_Name = ISIS/ IPC client, Reg_Count = 1
Client_ID = 10, Client_Name = ISIS/ Event Mgr client, Reg_Count = 1
Client_ID = 11, Client_Name = ISIS/ hsd Node client, Reg_Count = 1
Client_ID = 100, Client_Name = ISIS/ rtm client, Reg_Count = 1
Client_ID = 101, Client_Name = ISIS/ Mcast client, Reg_Count = 1
Client_ID = 102, Client_Name = ISIS/ Mcast Manager client, Reg_Count = 1
Client_ID = 2000, Client_Name = CRP Peak ISIS/ client, Reg_Count = 1
Client_ID = 2001, Client_Name = ISIS/ Peak Notify client, Reg_Count = 1
Client_ID = 2004, Client_Name = ISIS/ ARP client, Reg_Count = 1
Client_ID = 2010, Client_Name = ARP NL, Reg_Count = 1
Client_ID = 2011, Client_Name = ISIS/ Peak Notify client, Reg_Count = 1
Client_ID = 2020, Client_Name = ISIS/ Peak Notify ISIS/ client, Reg_Count = 1
Client_ID = 2022, Client_Name = ISIS/ Peak Notify ISIS/ client, Reg_Count = 1
Client_ID = 2023, Client_Name = FIB PEER ISIS/ client, Reg_Count = 1
Client_ID = 2024, Client_Name = FIB IDB ISIS/ client, Reg_Count = 1
Client_ID = 2025, Client_Name = FIB HWIDB ISIS/ client, Reg_Count = 1
Client_ID = 2026, Client_Name = FIB HW subblock ISIS/ client, Reg_Count = 1
Client_ID = 2027, Client_Name = adjacency ISIS/ client, Reg_Count = 1
Client_ID = 2028, Client_Name = ISIS/ Peak Notify client, Reg_Count = 1
Client_ID = 2029, Client_Name = ISIS/ process client, Reg_Count = 1
Client_ID = 2058, Client_Name = ISIS/ ISIS/ DPM client, Reg_Count = 1
Client_ID = 2059, Client_Name = ISIS/ ISIS/ DPM Peak client, Reg_Count = 1
Client_ID = 2060, Client_Name = ISIS/ ISIS/ Peak Notify client, Reg_Count = 1
Client_ID = 2068, Client_Name = ISIS/ PAST_PATCH ISIS/ client, Reg_Count = 1
Client_ID = 2070, Client_Name = ISIS/ Peak Notify client, Reg_Count = 1
```

```
client_ID = 2071, Client_Name = IEEE Switch VLAN client, Entry_Count = 1
client_ID = 2072, Client_Name = IEEE Switch STP client, Entry_Count = 1
client_ID = 2073, Client_Name = IEEE STP, Entry_Count = 2
client_ID = 2077, Client_Name = IEEE STP MSTP, Entry_Count = 1
client_ID = 2078, Client_Name = IEEE STP PVST, Entry_Count = 1
client_ID = 2079, Client_Name = IEEE STP RSTP, Entry_Count = 1
client_ID = 2081, Client_Name = IEEE DHCP Snooping client, Entry_Count = 1
client_ID = 2082, Client_Name = IEEE Dot1x Port client, Entry_Count = 1
client_ID = 2083, Client_Name = IEEE Inline Power client, Entry_Count = 1
client_ID = 2084, Client_Name = IEEE IGMP Snooping client, Entry_Count = 1
client_ID = 4001, Client_Name = IEEE CAK Sessions client, Entry_Count = 1
client_ID = 4002, Client_Name = IEEE CAK Port client, Entry_Count = 1
client_ID = 4003, Client_Name = IEEE CAK Interface client, Entry_Count = 1
client_ID = 4004, Client_Name = IEEE CAK Rxcvr client, Entry_Count = 1
client_ID = 4005, Client_Name = IEEE CAK CallbackRxcvr client, Entry_Count = 1

Base Clients:
Client_Name = IEEE Proxy client
Client_Name = IEEE Test
Client_Name = IEEE IP client
Client_Name = IEEE Network RP client
Client_Name = IEEE Ethernet SNMP
Client_Name = IEEE Ethernet OAM
Client_Name = IEEE CFM client
Client_Name = IEEE Port Server client
Client_Name = IEEE Bad Media Client
Client_Name = IEEE Test Client
Client_Name = IEEE vlm client
Client_Name = IEEE Broam Manager client
Client_Name = IEEE Broam client
Client_Name = IEEE Dot1x client
Client_Name = ARP Rx
Client_Name = IEEE Rxcvr Priority IEEE client
Client_Name = IEEE Rxcvr Priority IEEE client
Client_Name = PIB MASTER IEEE client
Client_Name = PIB IEEE IEEE client
Client_Name = PIB IEEE IEEE IEEE client
Client_Name = PIB IEEE mabAction IEEE client
Client_Name = mdparency IEEE client
Client_Name = PIB IPPA IEEE client
Client_Name = IEEE Port Manager client
Client_Name = IEEE PM client
Client_Name = IEEE CAK Channels client
Client_Name = IEEE CAK Sessions client
Client_Name = IEEE CAK Policy client
Client_Name = IEEE CAK Rxcvrbase client
Client_Name = IEEE CAK CallbackRxcvr client
```

Related Commands	Command	Description
	show vlan capability	Displays the SNAI capability for a client.
	show vlan entities	Displays the SNAI entity information.

show isso comp-matrix

To display information regarding the In Service Software Upgrade (ISSU) compatibility matrix, use the **show isso comp-matrix** command.

show isso comp-matrix {**negotiated** | **stored** | **sum**}

Syntax Description	**negotiated** Displays negotiated compatibility matrix information.
	stored Displays stored compatibility matrix information.
	sum Displays negotiated compatibility matrix information in XML format.

Defaults This command has no default settings.

Command Modes User EXEC mode

Usage Guidelines Before attempting an ISSU, you should know the compatibility level between the old and the new Cisco IOS software versions on the active and the standby supervisor engines. ISSU will not work if the two versions are incompatible.

The compatibility matrix is available on Cisco.com so that you can also view in advance whether an upgrade or downgrade between two Cisco IOS versions. The compatibility matrix during the ISSU process and later by entering the **show isso comp-matrix** command. To display information on the negotiated of the compatibility matrix data between two software versions on a given system, use the **show isso comp-matrix negotiated** command.

Compatibility matrix data is stored with each Cisco IOS software image that supports ISSU capability. To display stored compatibility matrix information, use the **show isso comp-matrix stored** command.

The compatibility matrix information are built-in any Cisco IOS ISSU image. The ISSU infrastructure performs a matrix lookup on runs on the communicator with the standby supervisor engine is established. There are three possible results from the lookup operation:

- Compatible—the Base-level system infrastructure and all optional HA-aware subsystems are compatible. In-service upgrade or downgrade between these versions will succeed with minimal service impact.
- Base-Level Compatible—One or more of the optional HA-aware subsystems are not compatible. Although an in-service upgrade or downgrade between these versions will succeed, some subsystems will not be able to maintain their state during the switchover. Prior to attempting an in-service upgrade or downgrade, the impact of this on operation and service of the switch must be considered carefully.
- Incompatible—A set of core system infrastructure must be able to execute in a stateful manner for SSO functions correctly. If any of these "required" features or subsystems is not compatible in two different Cisco IOS images, the two versions of the Cisco IOS images are declared "Incompatible". This means that an in-service upgrade or downgrade between these versions is not possible. The system operates in RPR mode during the period when the versions of Cisco IOS at the active and standby supervisor engines differ.

Examples

This example displays supported compatibility matrix information:

```
Switch#show fabric compatible supported

CardTypes: WS-C4507R(12), Slot 2, Image Ver: 12.2(31)SGA
Image Name: cat4500-IS-VSG2-M

Slot  Card  Slot  Card  p2l-d  p2l-d  Compat-Bitly
=====================================================
1     1     2     2     5      5      CSCdv37616
1     1     2     2     6      6      CSCdv37616
4     1     2     2     6      5      CSCdv37616
5     1     2     2     6      6      CSCdv37616
7     1     2     2     5      5      CSCdv37616
8     1     2     2     6      7      CSCdv37616
9     1     2     2     5      6      CSCdv37616
10    1     2     2     5      7      CSCdv37616
11    1     2     2     7      6      CSCdv37616
12    1     2     2     7      7      CSCdv37616
113   113   2     2     24     5      CSCdv37616
200   1     2     2     24     5      CSCdv37616
2000  1     -     -     -      -      EWA37616
2003  1     2     2     23     1      CSCdv37616
2004  1     2     2     23     2      CSCdv37616
2006  1     2     2     23     24     CSCdv37616
2008  1     2     2     23     27     CSCdv37616
2009  1     2     2     23     28     CSCdv37616
2010  1     2     2     23     40     CSCdv37616
2021  1     2     2     23     41     CSCdv37616
2022  1     2     2     23     42     CSCdv37616
2023  1     -     -     -      -      EWA37616
2024  1     -     -     -      -      EWA37616
2025  1     -     -     -      -      EWA37616
2026  1     -     -     -      -      EWA37616
2027  1     -     -     -      -      EWA37616
2028  1     -     -     -      -      EWA37616
2054  1     2     2     2      8      1     CSCdv37616
2055  1     2     2     2      9      1     CSCdv37616
2056  1     2     2     2      10     1     CSCdv37616
2067  1     2     2     2      12     1     CSCdv37616
2068  1     2     2     2      13     1     CSCdv37616
2069  1     2     2     2      21     1     CSCdv37616
2070  1     2     2     2      22     1     CSCdv37616
2071  1     2     2     2      23     1     CSCdv37616
2072  1     2     2     2      24     1     CSCdv37616
2073  1     2     2     2      25     1     CSCdv37616
2074  1     2     2     2      26     1     CSCdv37616
2075  1     2     2     2      27     1     CSCdv37616
2077  1     2     2     2      45     1     CSCdv37616
2078  1     2     2     2      46     1     CSCdv37616
2079  1     2     2     2      52     1     CSCdv37616
2080  1     2     2     2      53     1     CSCdv37616
2081  1     2     2     2      54     1     CSCdv37616
2082  1     2     2     2      55     1     CSCdv37616
2083  1     2     2     2      56     1     CSCdv37616
4000  101   2     2     2      17     1     CSCdv37616
4002  101   2     2     2      18     1     CSCdv37616
4003  101   2     2     2      19     1     CSCdv37616
4004  101   2     2     2      20     1     CSCdv37616
4005  1     2     2     2      4      1     CSCdv37616

Module-group group number:1
Slot  Slot  Group2  Slot  p2l-d  p2l-d  Bmgr Based-1
=====================================================
1     1     1     2     2      2      1     CSCdv37616
3     1     1     2     2      2      1     1
4     1     1     2     2      2      1     1
```

```
5     1     1     2621696  25     1     Y
6     1     1     2621696  26     1     Y
7     1     1     2621696  27     1     Y
8     1     1     2621696   1     1     Y
9     1     1     2621696   2     1     Y
13    1     1     2621696  13     1     Y
100   1     1     2621696  13     1     Y
1002  1005  1005  2621696  14     1     Y
1003  1     1     2621696   3     1     Y
2002  1     2     -        -      -     N - dot1q not negotiate
2003  1     1     2621696  23     1     Y
2004  1     1     2621696  16     1     Y
2005  1     1     2621696  17     1     Y
2006  1     2     2621696  27     1     Y
2010  1     1     2621696  32     1     Y
2011  1     1     2621696  33     1     Y
2021  1     1     2621696  42     1     Y
2022  1     1     2621696  42     1     Y
2023  1     2     -        -      -     N - dot1q not negotiate
2024  1     1     -        -      -     N - dot1q not negotiate
2025  1     1     -        -      -     N - dot1q not negotiate
2026  1     1     -        -      -     N - dot1q not negotiate
2027  1     1     -        -      -     N - dot1q not negotiate
2028  1     1     -        -      -     N - dot1q not negotiate
2054  1     1     2621696   8     1     Y
2058  1     1     2621696  29     1     Y
2059  1     1     2621696  29     1     Y
2067  1     1     2621696  10     1     Y
2068  1     1     1966336  40     1     Y
2069  1     1     2621696  11     1     Y
2071  1     1     2621696  12     1     Y
2072  1     1     2621696  28     1     Y
2073  1     1     2621696  30     1     Y
2077  1     1     2621696  35     1     Y
2078  1     1     1966337  34     1     Y
2079  1     1     2621696  36     1     Y
2080  1     1     2621696  37     1     Y
2082  1     1     2621696  39     1     Y
2083  1     1     2621696  38     1     Y
2084  1     1     2621696  18     1     Y
4000  1     1     2621696  24     1     Y
4001  1001  1     2621696  19     1     Y
4003  1001  1     2621696  19     1     Y
4004  1     1     2621696   4     1     Y
4005  1     1     2621696   4     1     Y

Lists of Clients:
CLM     Client Name                    Name/Ver Name
=================================================================
1       DTP/DISL client                Name
3       IEEE 802                       Name
4       IEEE CF client                 Name
5       IEEE Network NP client         Name
7       IEEE CDP/VLQ SYNC              Name
8       IEEE Spanning Tree             Name
9       IEEE CDP client                Name
10      IEEE CDP Server client         Name
11      IEEE Port Agg client           Name
100     IEEE vlm client                Name
102     IEEE vlm client                Name
1001    IEEE Port Agg client           Name
2002    CDP Proxy IEEE client          Name
2003    IEEE EOS client                Name
2004    IEEE Port Agg client           Name
```

```
2008    DDS Tabletd Client        Base
2009    DDS Client                Base
2010    DDS ARPP Client           Base-Base
2021    EDS Sec Priority DDS Client Base
2022    EDS Sec Priority Client   Base
2023    FIB MGLRX DDS Client      Base
2024    FIB SDE DDS Client        Base
2025    FIB Control DDS Client    Base
2026    FIB HW emulation DDS client Base
2027    mLDescrip DDS Client      Base
2028    FIB IPC6 DDS Client       Base
2054    DDS process Client        Base
2055    DDS Test Client Client    Base-Base
2056    DDS Client SDR Client     Base-Base
2057    DDS RM Client             Base
2058    DDS Test Client Client    Base-Base
2070    DDS Port Security Client  Base-Base
2071    DDS Switch VLAN Client    Base-Base
2072    DDS Client Client         Base-Base
2073    DDS STP                   Base-Base
2077    DDS STP MSTP              Base-Base
2078    DDS STP PVST              Base-Base
2079    DDS STP RSTP              Base-Base
2081    DDS DHCP Snooping Client  Base-Base
2082    DDS IP Base Client        Base-Base
2083    DDS Online Power Client   Base-Base
2084    DDS Online Power Client   Base-Base
2401    DDS CAS Channel Client    Base
2402    DDS CAS Port Client       Base
2403    DDS CAS Port Client       Base
2404    DDS CAS Heartbeat Client  Base
2405    DDS CAS Call Confirmation Base
```

This example displays crossed compatibility matrix information:

```
Switch#show lan compatible crossed

Number of Matrices in Table = 1

  (1) Matrix for ca4500-IPBASEK9(12.1) - ca4500-IPBASEK9(12.1)
  ------------------------------------------------------------
  Start Flag [0x00000000]

    My Image ver: 12.2-15.1(52)
      Peer Version        Compatibility
      ------------        -------------
      12.2-15.1(52)       Comp(3)
```

Related Commands	Command	Description
	show lan clients	Displays the SNM clients.
	show lan sessions	Displays SNM session information for a specified client.

show issu endpoints

To display the ISSU endpoint information, use the **show issu endpoints** command.

show issu endpoints

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes User EXEC mode

Usage Guidelines Endpoint is an execution unit within a redundancy domain. There are only 2 endpoints on the Catalyst 4500 series switch redundant chassis: 1 and 2. The endpoints correspond to the slot numbers for the supervisor engine. The ISSU infrastructure communicates between these two endpoints to establish sessions and to perform session negotiation for ISSU clients.

Examples The following example shows how to display the ISSU endpoints:

```
Switch# show issu endpoints
My_Designa_ID = 1:Slot  2:Sec_Sup=0 : 40

 This endpoint communicates with 1 peer endpoints :
   Peer_Designa_ID    :SAP    :VER    :SESSN    :REV      Compatibility
                      2:Slot    1       1         1         1          Same

 Shared Negotiation Session Info :
   Neg0_Session_ID :0 :0
   Neg1_Session_Name = shared nego session
   Neg0_Session_Mtu = 4096
   Neg1_Sess = 2
Switch#
```

Related Commands

Command	Description
show issu clients	Displays the ISSU clients.

show issu entities

To display the ISSU entity information, use the **show issu entities** command.

show issu entities [*client_id*]

Syntax Description		
	client_id	(Optional) ISSU client ID.

Defaults This command has no default settings.

Command Modes User EXEC mode

Usage Guidelines Entity is a logical group of sessions with same common attributes (like capability list and message type). Currently, most ISSU clients on the Catalyst 4500 series switch have only one entity.

Examples The following example shows how to display the entity information for a specified ISSU client:

```
Switch#show issu entities 2072
Client_id = 2072 :
  Entity_Id  Entity_Name = ISSU device entity :
    RegType RegGroup RegType RegEntity RegGroup
    Count   Count    Count   count    Count
     20      0        1       1        1

Switch#
```

Related Commands	Command	Description
	show issu clients	Displays the ISSU clients.

show issu fsm

Note This command is not intended for end-users.

To display the ISSU finite state machine (FSM) information corresponding to an ISSU session, use the **show issu fsm** command.

show issu fsm [*session_id*]

Syntax Description *session_id* (Optional) Provides detailed information about the FSM for the specified session.

Defaults This command has no default settings.

Command Modes User EXEC mode

Examples The following example displays and verifies the ISSU state after LOADVERSION:

```
Switch# show issu fsm 24
Session id: 24
  FSM_Name          Cur_State         Old_State         Error_Reason
  FSM_L3            TRANSI            A_VER             none
  FSM_L3_CLIENT     A_INIT            A_INIT            none
  FSM_L3_L_CLAP     A_INIT            A_INIT            none
  FSM_L3_P_CLAP     A_INIT            unknown           none
  FSM_L3_S_CLAP     A_INIT            A_INIT_DONE       none
  FSM_L3_V_CLAP     A_INIT            A_INIT            none
  FSM_L3_UNAME      CLAP              CLAP              none
  Current FSM is FSM_L3_UNAME
  Session is compatible
  Session negotiation started at 00:01:07.688, duration is 0.149 seconds
Switch#
```

Related Commands

Command	Description
show issu clients	Displays the ISSU clients.
show issu sessions	Displays ISSU session information for a specified client.

show issu message

To display checkpoint messages for a specified ISSU client, use the **show issu message** command.

show issu message {groups | types} [*client_id*]

Syntax Description		
	groups	Displays information on Message Group supported by the specified client.
	types	Displays information on all Message Types supported by the specified client.
	client_id	(Optional) Specifies a client ID.

Defaults	
If client ID is not specified, displays message groups or message types information for all clients registered to the ISSU infrastructure.	

Command Modes	
User EXEC mode	

Usage Guidelines

Messages are sync-data (also known as checkpoint data) sent between two endpoints.

When an ISSU-aware client establishes its session with a peer, an ISSU negotiation takes place. The ISSU infrastructure uses the registered information to negotiate the capabilities and the message version to be used during the session.

Examples

The following example shows how to display the message group for Client_id 2002:

```
Switch#show issu message groups 2002
Client_id = 2002 Group_id = 1
    Message_Group 1:
                    Message_Type = 1,  Version_Range = 1 - 2
                    Message_Type = 2,  Version_Range = 1 - 2

Switch#
```

The following example shows how to display the message types for Client_id 2002:

```
Switch#show issu message types 2002
Client_id = 2002  Group_id = 1
    Message_Type = 1,  Version_Range = 1 - 1
        Message_Dir = 0,   Message_Mtu = 512
        Message_Dir = 1,   Message_Mtu = 20
    Message_Type = 2,  Version_Range = 1 - 2
        Message_Dir = 0,   Message_Mtu = 512
        Message_Dir = 1,   Message_Mtu = 20

Switch#
```

Related Commands	Command	Description
	show issu clients	Displays the ISSU clients.

show issu negotiated

To display the negotiated capability and message version information of the ISSU clients, use the **show issu negotiated** command.

show issu negotiated {**capability** | **version**} [*session_id*]

Syntax Description

capability	Displays all negotiated capabilities.
version	Displays details of all negotiated messages.
session_id	(Optional) Specifies the ISSU session ID for which the capability or version information is displayed.

Defaults

Displays negotiated capability or version information for all ISSU sessions.

Command Modes

User EXEC mode

Examples

The following example shows how to display the message types for a specific group:

```
Switch# show issu negotiated capability 24
Session_ID = 24 :
    Cap_Type = 0,     Cap_Result = 1     No type value assigned

Switch# show issu negotiated version 24
Session_ID = 24 :
    Message_Type = 1,   Sent=Latest_Ver=4 =>,   Nsession_MTU = 44
    Message_Type = 2,   Sent=Latest_Ver=4 =>,   Nsession_MTU = 4
```

Related Commands

Command	Description
show issu sessions	Displays ISSU session information for a specified client.

show issu rollback-timer

To display ISSU rollback-timer status, use the **show issu rollback-timer** command.

show issu rollback-timer

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Examples The following example shows how to display the rollback-timer status:

```
Switch#show issu rollback-timer
        Rollback Timer State: No in progress
        Configured Rollback Time: 45:00
Switch#
```

Related Commands	Command	Description
	issu acceptversion	Halts the rollback timer and ensures that the new Cisco IOS software image is not automatically stopped during the ISSU process.
	issu runversion	Forces a change from the active supervisor engine to the standby supervisor engine and causes the newly active supervisor engine to run the new image specified in the **issu loadversion** command.

show issu sessions

To display ISSU session information for a specified client, use the **show issu sessions** command.

show issu sessions [*client_id*]

Syntax Description *client_id* (Optional) Specifies the ISSU client ID.

Defaults Displays session information for all clients registered to the ISSU infrastructure.

Command Modes User EXEC mode

Usage Guidelines Session is bidirectional and a reliable connection is established between two endpoints. Sync-data and negotiation messages are sent to the peer simultaneously through a session. On a Catalyst 6500 series switch, each ISSU-aware client has a maximum of one session at each endpoint.
When an ISSU-aware client establishes its session with the peer, an ISSU negotiation takes place. The ISSU infrastructure uses the registered information to negotiate the capabilities and the message version to be used during the session.

Examples The following example show how to display the sidback-timer status:

```
Switch#show issu sessions 2073
Client_ID = 2073 , Session_ID = 5

*** Session_ID = 20, Session_Name = Active ;

  Peer   Peer  Negotiate  Negotiated   Cap     Msg    Session
Unique ID  Slot   Done       Result   Group ID Group ID Expiration
   2      26   DONEACK   COMPATIBLE    1       1      0
                          (no policy)

  Negotiation Session Info for This Message Session:
    Negotiation_Time = 1 secs
    Msg_Session_Name = Active
    Transport_Mtu = 17364
Switch#
```

Related Commands

Command	Description
show issu clients	Displays the ISSU clients.

show issu state

To display the ISSU state and current booted image name during the ISSU process, use the **show issu state** command.

show issu state [*slot_number*] [**detail**]

Syntax Description	*slot_number*	(Optional) Specifies the slot number whose ISSU state needs to be displayed. Valid values are 1 and 2.
	detail	(Optional) Provides detailed information about the state of the active and standby supervisor engines.

Defaults The command displays the ISSU state and current booted image name of both the active and standby supervisor engines.

Command Modes Privileged EXEC mode

Usage Guidelines It might take several seconds after the **issu loadversion** command is entered for Cisco IOS software to load onto the standby supervisor engine and the standby supervisor engine to synchronize to SSO mode. If you enter the **show issu state** command too soon, you might not see the information you need.

Examples The following example displays and verifies the ISSU state after LOADVERSION:

```
Switch#show issu state detail
                        Slot = 1
                   RP State = Active
                 Image Type = Production
          Boot Variable = bootflash:cat4_image,12
       Operating Mode = Stateful Switchover
       Primary Version = bootflash:cat4_image
    Secondary Version = bootflash:new_image
       Current Version = bootflash:cat4_image

                        Slot = 2
                   RP State = Standby
                 ISSU State = Load Version
          Boot Variable = bootflash:new_image,12;bootflash:cat4_image,12
       Operating Mode = Stateful Switchover
       Primary Version = bootflash:cat4_image
    Secondary Version = bootflash:new_image
       Current Version = bootflash:new_image

Switch#
```

Related Commands	Command	Description
	issu abortversion	Cancels the ISSU upgrade or the downgrade process in progress and restores the switch to its state before the start of the process.
	issu acceptversion	Halts the rollback timer and ensures that the new Cisco IOS software image is not automatically stopped during the ISSU process.
	issu commitversion	Loads the new Cisco IOS software image into the new standby supervisor engine.
	issu loadversion	Starts the ISSU process.
	issu runversion	Forces a change from the active supervisor engine to the standby supervisor engine and causes the newly active supervisor engine to run the new image specified.

show l2protocol-tunnel

To display information about the Layer 2 protocol tunnel ports, use the **show l2protocol-tunnel** command. This command displays information for the interfaces with protocol tunneling enabled.

show l2protocol-tunnel [**interface** *interface-id*] [**summary**] | [**begin** | **exclude** | **include** *expression*]

Syntax Description	**interface** *interface-id* — (Optional) Specifies 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) Displays only Layer 2 protocol information.
	begin — (Optional) Displays information beginning with the line that matches the *expression*.
	exclude — (Optional) Displays information that includes lines that match the *expression*.
	include — (Optional) Displays the lines that match the specified *expression*.
	expression — (Optional) Expression in the output to use as a reference point.

Command Modes User EXEC mode

Usage Guidelines After enabling Layer 2 protocol tunneling on an access or 802.1Q tunnel port with the **l2protocol-tunnel** 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:

Port    Protocol  Shutdown  Drop    Encapsulation Decapsulation Drop
          Type    Threshold Threshold Counter     Counter     Counter
--------  --------  --------  --------  ------------  ------------  ------------
Fa5/10
          stp                         1             1             0
          vtp                         4367          1366          0
          pagp                        ---           ---           ---
          lacp                        ---           ---           ---
```

```
        udld        1000      ----  219       211       0
Fa2/11  cdp         1000      ----  1140      1140      0
        vtp         1000      ----  142       142       0
        vtp         1000      ----  3         47        0
        pagp        ----      ----  9248      9248      0
        lacp        ----      ----  906       0         0
        udld        ----      ----  906       0         0
Fa2/12  cdp         ----      ----  11748     0         0
        vtp         ----      ----  11748     0         0
        pagp        ----      ----  61        0         0
        pagp        ----      ----  6         0         0
        lacp        ----      ----  949       0         0
        lacp        ----      ----  949       0         0
Fa2/13  cdp         ----      ----  2854      0         0
        vtp         ----      ----  11748     0         0
        pagp        ----      ----  6         0         0
        pagp        ----      ----  6         0         0
        lacp        ----      ----  949       0         0
        lacp        ----      ----  6         0         0
Switch#
```

This is an example of output from the **show l2protocol-tunnel summary** command:

```
Switch# show l2protocol-tunnel summary
COS for Encapsulation Dot1ncapsulation is 5

Port    Protocol  Shutdown        Drop        Status
                  Threshold       Threshold
                  (cdp/stp/vtp)   (cdp/stp/vtp)
                  (pagp/lacp/udld)(pagp/lacp/udld)
------  --------  --------------  --------------  ------
Fa2/10  cdp       ---/---/---     ---/---/---     up
        stp       ---/---/---     ---/---/---
Fa2/11  cdp       ---/---/---     1000/1000/1000  up
        pagp      lacp/udld       ---/---/---     906/ 906/ 906
Fa2/12  cdp       ---/---/---     ---/---/---     up
        pagp      lacp/udld       ---/---/---
Fa2/13  cdp       ---/---/---     ---/---/---     up
        pagp      lacp/udld       ---/---/---
Fa2/14  cdp       ---/---/---     ---/---/---     down
        pagp      lacp/udld       ---/---/---
Fa2/15  cdp       ---/---/---     ---/---/---     down
        pagp      lacp/udld       ---/---/---
Fa2/16  cdp       ---/---/---     ---/---/---     down
        pagp      lacp/udld       ---/---/---
Fa2/17  cdp       ---/---/---     ---/---/---     down
        pagp      lacp/udld       ---/---/---
Switch#
```

Related Commands	Command	Description
	l2protocol-tunnel	Enables protocol tunneling on an interface.
	l2protocol-tunnel cos	Configures the class of service (CoS) value for all tunneled Layer 2 protocol packets.

show lacp

To display LACP information, use the **show lacp** command.

show lacp [*channel-group*] {**counters**| **internal** | **neighbors** | **sys-id**}

Syntax Description		
	channel-group	(Optional) Number of the channel group, valid values are from 1 to 64.
	counters	Displays the LACP statistical information.
	internal	Displays the internal information.
	neighbors	Displays the neighbor information.
	sysid	Displays the LACP system identification.

Defaults	This command has no default settings.

Command Modes	Privileged EXEC mode

Usage Guidelines

If you do not specify *channel-group* value, all channel groups are displayed.

You can enter the optional *channel-group* value to specify a channel group for all keywords, except the **sysid** keyword.

Examples

This example shows how to display LACP statistical information for a specific channel group:

```
Switch#show lacp 1 counters
                LACPDUs               Marker      Marker
Port         Sent     Recv         Sent     Recv    Pkts-Err
--------------------------------------------------------------
Channel group: 1
  Fa1/1        8       15          0        0        0        0
  Fa1/2        8       15          0        0        0        0
  Fa1/3        8       15          0        0        0        0
  Fa1/4        8       15          0        0        0        0
Switch#
```

The output displays the following information:

- The LACPDUs Sent and Recv columns display the LACPDUs sent and received on each specific interface.
- The LACPDUs Pkts and Err columns display the marker protocol packets.

This example shows how to display internal information for the interfaces belonging to a specific channel:

```
Switch#show lacp 1 internal
Flags: S - Device wants PDUs at slow rate. F - Device wants PDUs at fast rate.
       A - Device is in active mode.       P - Device is in passive mode.

Channel group 1
                              LACPDUs   LACP Port  Admin   Oper    Port    Port
```

```
Port      Flags   State   Priority  Key    Key    Number  State
Fa4/1     saf     bndl    32768     100    100    0x41    0x3d
Fa4/2     saf     bndl    32w       32768  100    100     0x42    0x7c
Fa4/3     saf     bndl    32w       32768  100    100     0x43    0x7c
Fa4/4     saf     bndl    32w       32768  100    100     0x44    0x7c
Gi4/1     saf     bndl    32w       32768  100    100     0x81    0x7c
```

Table 2-26 lists the output field definitions.

Table 2-26 *show lacp internal Command Output Fields*

Field	Description
State	State of the specific port at the current moment is displayed; allowed values are as follows:
	• *bndl*—Port is attached to an aggregator and bundled with other ports.
	• *susp*—Port is in a suspended state; it is not attached to any aggregator.
	• *indep*—Port is an independent state (not bundled but able to switch data traffic. In this case, LACP is not running on the partner port).
	• *hot-sby*—Port is in a hot-standby state.
	• *down*—Port is down.
LACPDUs Interval	Interval setting.
LACP Port Priority	Port priority setting.
Admin Key	Administrative key.
Oper Key	Operator key.
Port Number	Port number.
Port State	State variables for the port encoded as individual bits within a single octet with the following meaning [1]:
	• **bit1**: *LACP_Activity*
	• **bit1**: *LACP_Timeout*
	• **bit1**: *Aggregation*
	• **bit1**: *Synchronization*
	• **bit1**: *Collecting*
	• **bit1**: *Distributing*
	• **bit6**: *Defaulted*
	• **bit1**: *Expired*

This example shows how to display LACP neighbor information for a specific port channel:

```
Switch# show lacp 1 neighbor
Flags:  S - Device wants PDUs at slow rate.  F - Device wants PDUs at fast rate.
        A - Device is active mode.           P - Device is in passive mode.

Channel group 1 neighbors
         Partner                  Partner
```

```
Port      System Id          Port Number    Age    Flags
Fa4/1     8000,0060.5cf4c.4f8e   0x43           6s     P
Fa4/2     8000,0060.5cf4c.4f8e   0x44           6s     P
Fa4/3     8000,0060.5cf4c.4f8e   0x45           6s     P
Fa4/4     8000,0060.5cf4c.4f8e   0x46           6s     P

          Port      Admin     Oper      Port
Port      Priority  Key       Key       State
Fa4/1     32768     200       200       0x81
Fa4/2     32768     200       200       0x81
Fa4/3     32768     200       200       0x81
Fa4/4     32768     200       200       0x81
Switch#
```

In the case where no PDUs have been received, the default administrative information is displayed in bracket.

This example shows how to display the L-ACP system identification:

```
Switch#  show lacp sys-id
8000,ac-12-34-56-78-90
Switch#
```

The system identification is made up of the system priority and the system MAC address. The first two bytes are the system priority, and the last six bytes are the globally administered individual MAC address associated to the system.

Related Commands	Command	Description
	lacp port-priority	Sets the LACP priority for the physical interfaces.
	lacp system-priority	Sets the priority of the system for LACP.

show mac

To display MAC authentication bypass (MAB) information, use the **show mac** command in EXEC mode.

show mac [**interface** *interface interface-number*] | **all** | **detail**

Syntax Description

interface *interface*	Interface type; possible valid value is **gigabitethernet**.
interface-number	Module and port number.
all	Displays MAB information for all interfaces.
detail	(Optional) Displays detailed MAB information.

Command Default None.

Command Modes Privileged EXEC mode

Usage Guidelines Table 2-27 lists the fields in the **show mac** command.

Table 2-27 show mac Command Output

Field	Description
Mac-Auth-Bypass	MAB state
Inactivity Timeout	Inactivity timeout
Client MAC	Client MAC address
MAB SM state	MAB state machine state
Auth Status	Authentication status

Table 2-28 lists the possible values for the state of the MAB state machine.

Table 2-28 MAB State Machine Values

State	State Level	Description
Initialize	Intermediate	The state of the session when it initializes
Acquiring	Intermediate	The state of the session when it is obtaining the client MAC address
Authorizing	Intermediate	The state of the session during MAC-based authorization
Terminate	Terminal	The state of the session once a result has been obtained. For a session in terminal state, "TERMINATE" displays.

Table 2-29 lists the possible displayed values for the MAB authentication status.

Table 2-29 MAB Authentication Status Values

Status	Description
AUTHORIZED	The session has successfully authorized.
UNAUTHORIZED	The session has failed to be authorized.

Examples

The following example shows how to display MAB information:

```
Switch# show mab all
MAB details for GigabitEthernet1/3
-----------------------------------
Mac-auth-Bypass = Enabled
Inactivity Timeout = None
Match-Priority = 0

MAB Client List
---------------

Number of Clients = 0
```

The following example shows how to display detailed MAB information:

```
Switch# show mab all detail
MAB details for GigabitEthernet1/3
-----------------------------------
Mac-auth-Bypass = Enabled
Inactivity Timeout = None
MAB Client List
---------------

Client MAC = 0000.39c4.a401
MAB IM status = TERMINATE
Auth Status = AUTHORIZED
```

The following example shows how to display MAB information for a specific interface:

```
Switch# show mab interface gigabitethernet1/3
MAB details for GigabitEthernet1/3
-----------------------------------
Mac-auth-Bypass = Enabled
Inactivity Timeout = None
```

The following example shows how to display detailed MAB information for a specific interface:

```
Switch# show mab interface gigabitethernet1/3 detail
MAB details for GigabitEthernet1/3
-----------------------------------
Mac-auth-Bypass = Enabled
Inactivity Timeout = None
MAB Client List
---------------

Client MAC = 0000.39c4.a401
MAB IM status = TERMINATE
Auth Status = AUTHORIZED
Switch#
```

Related Commands

Command	Description
mab	Enables and configures MAC authentication bypass (MAB) on a port.

show mac access-group interface

To display the ACL configuration on a Layer 2 interface, use the **show mac access-group interface** command.

show mac access-group interface [*interface interface-number*]

Syntax Description	*interface*	(Optional) Specifies the interface type; valid values are **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **pos**, **atm**, **port-channel**, and **ge-wan**.
	interface-number	(Optional) Specifies the port number.

Defaults	This command has no default settings.
Command Modes	Privileged EXEC mode
Usage Guidelines	The valid values for the port number depend on the chassis used.
Examples	This example shows how to display the ACL configuration on interface fast 6/1:

```
Switch# show mac access-group interface fast 6/1
Interface fastethernet6/1
    Inbound access-list is simple-mac-acl
    Outbound access-list is mac mac
```

Related Commands	**Command**	**Description**
	access-group mode	Specifies the override modes (for example, VACL overrides PACL) and the non-override modes (for example, merge or strict mode).

show mac-address-table address

To display MAC address table information for a specific MAC address, use the **show mac-address-table address** command.

show mac-address-table address *mac_addr* [**interface** *type slot/port* | **protocol** *protocol* | **vlan** *vlan_id*]

Syntax Description

mac_addr	48-bit MAC address; the valid format is H.H.H.
interface *type slot/port*	(Optional) Displays information for a specific interface; valid values for *type* are **fastethernet**, **gigabitethernet**, and **tengigabitethernet**.
protocol *protocol*	(Optional) Specifies a protocol. See the "Usage Guidelines" section for valid values.
vlan *vlan_id*	(Optional) Displays entries for the specific VLAN only; valid values are from 1 to 4094.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

For the MAC address table entries that are sed by the mcast ports, the nexted port name is displayed in the "vlan" column not the internal VLAN number.

The keyword definitions for the *protocol* variable are as follows:

- **ip** specifies the IP protocol.
- **ipx** specifies the IPX protocol.
- **assigned** specifies the assigned protocol entries.
- **other** specifies the other protocol entries.

Examples

This example shows how to display MAC address table information for a specific MAC address:

```
Switch#show mac-address-table address 0030.94fc.0dff
Unicast Entries
 vlan  mac address     type        protocols       port
-------+---------------+--------+---------+--------------------------------
   1    0030.94fc.0dff  static ip,ipx,assigned,other  Switch
Fa6/1   0030.94fc.0dff  static ip,ipx,assigned,other  Switch
Fa6/2   0030.94fc.0dff  static ip,ipx,assigned,other  Switch
Switch#
```

Related Commands

Command	Description
show mac-address-table aging-time	Displays MAC address table aging information.
show mac-address-table count	Displays the number of entries currently in the MAC address table.
show mac-address-table dynamic	Displays the dynamic MAC address table entries only.
show mac-address-table interface	Displays the MAC address table information for a specific interface.
show mac-address-table multicast	Displays information about the multicast MAC address table.
show mac-address-table protocol	Displays the MAC address table information that is based on the protocol.
show mac-address-table static	Displays the static MAC address table entries only.
show mac-address-table vlan	Displays information about the MAC address table for a specific VLAN.

show mac-address-table aging-time

To display the MAC address aging time, use the **show mac-address-table aging-time** command.

show mac-address-table aging-time [**vlan** *vlan_id*]

Syntax Description	**vlan** *vlan_id* (Optional) Specifies a VLAN; valid values are from 1 to 4094.
Defaults	This command has no default settings.
Command Modes	Privileged EXEC mode

Examples

This example shows how to display the currently configured aging time for all VLANs:

```
Switch# show mac-address-table aging-time
Vlan    Aging Time
----    ----------
200     300
201     1000

Switch#
```

This example shows how to display the currently configured aging time for a specific VLAN:

```
Switch# show mac-address-table aging-time vlan 100
Vlan    Aging Time
----    ----------
100     500

Switch#
```

Related Commands	Command	Description
	clear mac-address-table address	Displays the information about the MAC address table.
	show mac-address-table count	Displays the number of entries currently in the MAC address table.
	show mac-address-table dynamic	Displays the dynamic MAC address table entries only.
	show mac-address-table interface	Displays the MAC address table information for a specific interface.
	show mac-address-table multicast	Displays information about the multicast MAC address table.
	show mac-address-table protocol	Displays the MAC address table information that is based on the protocol.
	show mac-address-table static	Displays the static MAC address table entries only.
	show mac-address-table vlan	Displays information about the MAC address table for a specific VLAN.

show mac-address-table count

To display the number of entries currently in the MAC address table, use the **show mac-address-table count** command.

show mac-address-table count [**vlan** *vlan_id*]

Syntax Description **vlan** *vlan_id* (Optional) Specifies a VLAN; valid values are from 1 to 4094.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Examples This example shows how to display the entry count for a specific VLAN:

```
Switch# show mac-address-table count vlan 1
Mac Entries for Vlan 1:
---------------------
Dynamic Unicast Address Count     :  0
Static Unicast Address (User-defined) Count :  0
Dynamic Unicast Address (System-defined) Count :  1
Unicast Address Multiplier        :  256
Total Unicast MAC Addresses Available:  32768
Multicast MAC Address Count       :
Total Multicast MAC Addresses Available:  16384
Switch#
```

Related Commands

Command	Description
show mac-address-table address	Displays the information about the MAC-address table.
show mac-address-table aging-time	Displays MAC address table aging information.
show mac-address-table dynamic	Displays the dynamic MAC address table entries only.
show mac-address-table interface	Displays the MAC address table information for a specific interface.
show mac-address-table multicast	Displays information about the multicast MAC address table.
show mac-address-table protocol	Displays the MAC address table information that is based on the protocol.
show mac-address-table static	Displays the static MAC address table entries only.
show mac-address-table vlan	Displays information about the MAC address table for a specific VLAN.

show mac-address-table dynamic

To display the dynamic MAC address table entries only, use the **show mac-address-table dynamic** command.

show mac-address-table dynamic [**address** *mac_addr* | **interface** *type slot/port* | **protocol** *protocol* | **vlan** *vlan_id*]

Syntax Description

address *mac_addr*	(Optional) Specifies a 48-bit MAC address; the valid format is H.H.H.
interface *type slot/port*	(Optional) Specifies an interface to match; valid values for *type* are **fastethernet**, **gigabitethernet**, and **tengigabitethernet**.
protocol *protocol*	(Optional) Specifies a protocol. See the "Usage Guidelines" section for more information.
vlan *vlan_id*	(Optional) Displays entries for a specific VLAN; valid values are from 1 to 4094.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

The keyword definitions for the *protocol* argument are as follows:

- **assigned** specifies assigned protocol entries.
- **ip** specifies IP protocol.
- **ipx** specifies IPX protocols.
- **other** specifies other protocol entries.

The **show mac-address-table dynamic** command output for an EtherChannel interface changes the port number designation (such as, 5/7) to a port group number (such as, 9x88).

For the MAC address table entries that are used by the mared ports, the reared port name is displayed in the "vlan" column not the internal VLAN number.

Examples

This example shows how to display all the dynamic MAC address entries:

```
Switch# show mac-address-table dynamic
Unicast Entries
vlan  mac address     type        protocols          port
-------------------------------------------------------------
  1   0000.0000.0010  dynamic     ip                 Fast-Ethernet4/45
  1   0000.0000.0020  dynamic     ip                 Fast-Ethernet4/45
  1   0000.0000.0030  dynamic     ip,assd-prot       Fast-Ethernet4/45
  1   0000.0000.0040  dynamic     ip,assd-prot       Fast-Ethernet4/45
  1   0000.0000.0050  dynamic     ip                 Fast-Ethernet4/45
  1   0000.0000.0060  dynamic     ip                 Fast-Ethernet4/45
  1   0000.0000.0070  dynamic     ip                 Fast-Ethernet4/45
  1   0000.0000.0080  dynamic     ip                 Fast-Ethernet4/45
  1   0000.0000.0090  dynamic     ip,assd-prot       Fast-Ethernet4/45
```

```
    2    0000.0000.0104   dynamic  ip,ipx,assigned      Fast0/5,Gi0/1
    2    0000.0000.0105   dynamic  ip,ipx,assigned      Fast0/5,Gi0/1
Router#
```

This example shows how to display the dynamic MAC address entries with a specific protocol type (in this case, assigned):

```
Router#show mac-address-table dynamic protocol assigned
Destination Address Table
Vlan    Mac Address       Type        Protocols           Port
----    -----------       --------    -----------         ----
   1    0000.0000.0200    dynamic     ip,ipx,assigned     Fast0/5,Gi0/1
   1    0000.0000.0201    dynamic     ip,ipx,assigned     Fast0/5,Gi0/1
   1    0000.0000.0208    dynamic     ip,ipx,assigned     Fast0/5,Gi0/1
   2    0000.0000.0110    dynamic     ip,ipx,assigned     Fast0/5,Gi0/1
   2    0000.0000.0111    dynamic     ip,ipx,assigned     Fast0/5,Gi0/1
   2    0000.0000.0128    dynamic     ip,ipx,assigned     Fast0/5,Gi0/1
Router#
```

Related Commands

Command	Description
show mac-address-table protocol	Displays the MAC address table information that is based on the protocol.
show mac-address-table static	Displays the static MAC address table entries only.
show mac-address-table vlan	Displays information about the MAC address table for a specific VLAN.

show mac-address-table interface

To display the MAC address table information for a specific interface, use the **show mac-address-table interface** command.

show mac-address-table interface *type slot/port*

Syntax Description	*type*	Interface type; valid values are **ethernet**, **fastethernet**, **gigabitethernet**, and **tengigabitethernet**.
	slot/port	Number of the slot and port.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Usage Guidelines For the MAC address table entries that are used by the routed ports, the routed port name is displayed in the "Vlan" column not the internal VLAN number.

Examples This example shows how to display MAC address table information for a specific interface:

```
Switch#show mac-address-table interface fastethernet5/16
Dynamic Addresses Count:
vlan  mac address     type      protocols          port
-----------------------------------------------------------------------
  1   0000.0000.0101  dynamic   other              Fastethernet5/16
  2   0000.0000.0201  dynamic   other              Fastethernet5/16
  3   0000.0000.0301  dynamic   other              Fastethernet5/16
  4   0000.0000.0401  dynamic   other              Fastethernet5/16
  5   0000.0000.0501  dynamic   other              Fastethernet5/16
  6   0000.0000.0601  dynamic   other              Fastethernet5/16
Multicast Entries:
vlan  mac address     type      ports
-----------------------------------------------------------------------
  1   0100.5e01.0102  system    Fa5/16
Switch#
```

Related Commands

Command	Description
show mac-address-table address	Displays the information about the MAC address table.
show mac-address-table aging-time	Displays MAC address table aging information.
show mac-address-table count	Displays the number of entries currently in the MAC address table.
show mac-address-table dynamic	Displays the dynamic MAC address table entries only.
show mac-address-table multicast	Displays multicast information from the multicast MAC address table.

Command	Description
show mac-address-table protocol	Displays the MAC address table information that is based on the protocol.
show mac-address-table static	Displays the static MAC address table entries only.
show mac-address-table vlan	Displays information about the MAC address table for a specific VLAN.

show mac address-table learning

To display the status of MAC address learning for all VLANs or a specified VLAN, use the **show mac address-table learning** user EXEC command.

show mac address-table learning [**vlan** *vlan-id*] [| {**begin** | **exclude** | **include** } *expression*]

Syntax Description	**vlan** *vlan-id*	(Optional) Displays information for a specific VLAN. The range is 1 to 4094.
	|begin	(Optional) Displays the line that matches the expression.
	|exclude	(Optional) Displays excluded lines that match the expression.
	|include	(Optional) Displays included lines that match the specified expression.
	expression	(Optional) Specifies the expression in the output as a reference point.

Defaults MAC address learning is enabled on all VLANs.

Command Modes User EXEC

Usage Guidelines To display configured VLANs, and whether MAC address learning is enabled or disabled, use the **show mac address-table learning**command without keywords.

To display the learning status on an individual VLAN, use the command with a specific VLAN ID.

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 that MAC address learning is disabled on VLAN 200:

```
Switch# show mac address-table learning
Vlan    Learning Status
----    --------------
100     yes
200     yes
300     no
```

Related Commands	**Command**	**Description**
	mac address-table learning vlan	Enables or disables MAC address learning on a VLAN.

show mac-address-table multicast

To display information about the multicast MAC address table, use the **show mac-address-table multicast** command.

show mac-address-table multicast [**count**] [**igmp-snooping**] [**count**]} | [**user** [**count**] | [**vlan** *vlan_num*]]

Syntax Description

count	(Optional) Displays the number of multicast entries.
igmp-snooping	(Optional) Displays only the addresses learned by IGMP snooping.
user	(Optional) Displays only the user-created static addresses.
vlan *vlan_num*	(Optional) Displays information for a specific VLAN only; valid values are from 1 to 4094.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Usage Guidelines For the MAC address table entries that are used by the routed ports, the routed port name is displayed in the "vlan" column not the the internal VLAN number.

Examples This example shows how to display multicast MAC address table information for a specific VLAN:

```
Router# show mac-address-table multicast vlan 1
Multicast Entries
 vlan  mac address     type   ports
---+---------------+-------+-------------------------------
  1    0100.5e00.0002  system Gi4/10,Po1,Fa6/15
Router#
```

This example shows how to display the number of multicast MAC entries for all VLANS:

```
Router# show mac-address-table multicast count
MAC Entries for all vlans:
Multicast Mac Address Count:                    141
Total Mcastmac Mac Addresses Available:         16384
Router#
```

Related Commands

Command	Description
show mac-address-table address	Displays the information about the MAC address table.
show mac-address-table aging-time	Displays MAC address table aging information.
show mac-address-table count	Displays the number of entries currently in the MAC address table.
show mac-address-table dynamic	Displays the dynamic MAC address table entries only.

Command	Description
show mac address-table interface	Displays the MAC address table information for a specific interface.
show mac address-table protocol	Displays the MAC address table information that is based on the protocol.
show mac address-table static	Displays the static MAC address table entries only.
show mac address-table vlan	Displays information about the MAC address table for a specific VLAN.

show mac-address-table notification

To display the MAC address table notification status and history, use the **show mac-address-table notification** command.

show mac-address-table notification {**change**} {**interface** [*interface-id*]} {**mac-move**} {**threshold**} {**learn-fail**}

Syntax Description

change	(Optional) Displays the MAC address change notification status.
interface	(Optional) Displays MAC change information for an interface.
interface-id	(Optional) Displays the information for a specific interface. Valid interfaces include physical ports and port channels.
mac-move	(Optional) Displays MAC move notification status.
threshold	(Optional) Displays the MAC address threshold notification status.
learn-fail	(Optional) Displays general information of hardware MAC learning failure notification.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

Use the **show mac-address-table notification change** command to display the MAC change notification interval, the maximum number of entries allowed in the history table, the history table contents, and whether the MAC change feature is enabled or disabled.

Use the **interface** keyword to display the flags for all interfaces. If the *interface-id* is included, only the flags for that interface are displayed.

Examples

This example shows how to display all the MAC address notification information:

```
Switch# show mac-address-table notification change
MAC Notification Feature is Enabled on the switch
Interval between Notification Traps : 1 secs
Number of MAC addresses added : 4
Number of MAC addresses removed : 4
Number of Notifications sent to NMS : 8
Maximum Number of entries configured in History Table : 500
Current History Table Length : 3
Mac Notification Traps are Enabled
History Table contents
-----------------------
History Index 1, Entry Timestamp 276433, Dequeuer Timestamp 276433
MAC Changed Message :
Operation: Added  Vlan: 1  Mac Addr: 1234.0678.9abd Interface:Fa1/1
History Index 2, Entry Timestamp 281814, Dequeuer Timestamp 281814
MAC Changed Message :
Operation: Added  Vlan: 1  Mac Addr: 1234.0678.9abd Interface:Gi1/1
Operation: Added  Vlan: 1  Mac Addr: 1234.0678.9abd Interface:Gi1/1
```

```
Operation: Added  Vlan: 2    MAC Addr: 1234.5678.9a80 OutlineMacOvr: 525
Operation: Added  Vlan: 2    MAC Addr: 1234.5678.9a81 OutlineMacOvr: 525
History Index 1, Entry Timestamp 454154, Dampwrite Timestamp 454154
MAC Changed Message :
Operation: Deleted Vlan: 2    MAC Addr: 1234.5678.9a80 OutlineMacOvr: 525
Switch#
```

This example shows how to display the MAC address change status on the FastEthernet interface 7/1:

```
Switch#show mac-address-table notification change interface FastEthernet 7/1
MAC Notification Feature is Enabled on the switch
Interface       MAC added Trap MAC Removed Trap
----------------------------------------------
FastEthernet7/1     Disabled     Disabled
Switch#
```

This example shows how to display the MAC address move status:

```
Switch#show mac-address-table notification mac-move
MAC Move Notification: Enabled
Switch#
```

This example shows how to display the MAC address table utilization status:

```
Switch#show mac-address-table notification threshold
Status    Limit     Interval
-------------------------------
enabled   50        120
Switch#
```

This example shows how to display general information of MAC learning failure notifications:

```
Switch#show mac-address-table notification learn-fail
Status    Limit     Interval
-------------------------------
disabled  2000      120
```

Related Commands	Command	Description
	clear mac-address-table	Clears the address entries from the Layer 2 MAC address table.
	mac-address-table notification	Enables MAC address notification on a switch.
	snmp-server enable traps	Enables SNMP notifications (traps or informs).
	snmp trap mac-notification change	Enables SNMP MAC address notification.

show mac-address-table protocol

To display the MAC address table information that is based on the protocol, use the **show mac-address-table protocol** command.

show mac-address-table protocol {**assigned**} {**ip** | **ipx** | **other** }

Syntax Description	**assigned**	Specifies the assigned protocol entries.
	ip	Specifies the IP protocol entries.
	ipx	Specifies the IPX protocol entries.
	other	Specifies the other protocol entries.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Usage Guidelines For the MAC address table entries that are used by the routed ports, the routed port name is displayed in the "vlan" column (as the the internal VLAN number.

Examples This example shows how to display the MAC address table entries that have a specific protocol type (in this case, assigned):

```
Switch# show mac-address-table protocol assigned
vlan  mac address     type    protocol  ports
------+----------+--------+--------+--------+--------+
  200  0030.3a56.4d00 static  assigned --  Gi1/0/5
  200  0030.3a56.4d01 static  assigned --  Gi1/0/5
    5  0030.3a56.4d02 static  assigned --  Gi1/0/5
 4092  0000.0000.0000 dynamic assigned --  Gi1/0/5
    1  0000.3a56.4d00 static  assigned --  Gi1/0/5
    1  0000.3a56.4d01 static  assigned --  Gi1/0/5
 4092  0000.40ac.5808 static  assigned --  Gi1/0/5
 4092  0000.40ac.5809 static  assigned --  Gi1/0/5
    1  0010.7b3b.0578 dynamic assigned --  Po1/0
Switch#
```

This example shows the other output for the previous example:

```
Switch# show mac-address-table protocol other
Destinat Routines
vlan  mac address     type        protocols        ports
------+----------+--------+--------+--------+--------+
   1    0000.0000.0100  dynamic  other            Fast-Ethernet0/1/0
   1    0000.0000.0101  dynamic  other            Fast-Ethernet0/1/0
   1    0000.0000.0102  dynamic  other            Fast-Ethernet0/1/0
   1    0000.0000.0104  dynamic  other            Fast-Ethernet0/1/0
   1    0000.0000.0105  static   ip,ipx,assigned,other  Fast-Ethernet0/1/0
   1    0000.0000.0106  dynamic  other            Fast-Ethernet0/1/0
   1    0000.0000.0110  dynamic  other            Fast-Ethernet0/1/0
   1    0000.0000.0111  dynamic  other            Fast-Ethernet0/1/0
```

```
    2    0000.0000.0154  dynamic  other          Fast0/6,vlan0/16
Fa0/2    0000.0000.0154  static   ip,ipx,assigned,other  Fa0/6
Fa0/2    0100.5e7f.0001  static   ip,ipx,assigned,other  Swlo0/6

Multicast Service:
 vlan  mac address     type    ports
-----+---------------+--------+-----------------------------------------
   1  0100.5e00.0001  system  Fa0/1,Fa0/16
   1  0100.5e00.0002  system  Fa0/16
1002  0100.5e00.0004  system
1003  0100.5e00.0004  system
1004  0100.5e00.0004  system
1005  0100.5e00.0004  system
   2  0100.5e00.0001  system  Fa0/1,Fa0/16
Fa0/2  0100.5e7f.0001  system  Swlo0,Fa0/2
Swlo0
```

Related Commands

Command	Description
show mac-address-table address	Displays the information about the MAC address table.
show mac-address-table aging-time	Displays MAC address table aging information.
show mac-address-table count	Displays the number of entries currently in the MAC address table.
show mac-address-table dynamic	Displays the dynamic MAC address table entries only.
show mac-address-table interface	Displays the MAC address table information for a specific interface.
show mac-address-table multicast	Displays information about the multicast MAC address table.
show mac-address-table static	Displays the static MAC address table entries only.
show mac-address-table vlan	Displays information about the MAC address table for a specific VLAN.

show mac-address-table static

To display the static MAC address table entries only, use the **show mac-address-table static** command.

show mac-address-table static [**address** *mac_addr* | **interface** *type number* | **protocol** *protocol* | **vlan** *vlan_id*]

Syntax Description

address *mac_addr*	(Optional) Specifies a 48-bit MAC address to match; the valid format is H.H.H.
interface *type number*	(Optional) Specifies an interface to match; valid values for *type* are **fastethernet**, **gigabitethernet**, and **tenggigabitethernet**.
protocol *protocol*	(Optional) Specifies a protocol. See the "Usage Guidelines" section for more information.
vlan *vlan_id*	(Optional) Displays the entries for a specific VLAN; valid values are from 1 to 4094.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

For the MAC address table entries that are used by the *routed-port*, the *routed-port name* is displayed in the "vlan" column not the internal VLAN number.

The keyword definitions for the *protocol* argument are as follows:

- **assigned** specifies the assigned protocol entries.
- **ip** specifies the IP protocol.
- **ipx** specifies the IPX protocols.
- **other** specifies the other protocol entries.

Examples

This example shows how to display all the static MAC address entries:

```
Switch# show mac-address-table static
Unicast Entries
 vlan  mac address     type        protocols       port
-------+---------------+--------+---------------+--------
   1    0030.94fc.0dff static|ip,ipx,assigned,other  fa10/6
Fa8/12  0030.94fc.0dff static|ip,ipx,assigned,other  fa10/6
Fa8/12  0030.94fc.0dff static|ip,ipx,assigned,other  fa10/6

Multicast Entries
 vlan  mac address     type        ports
-------+---------------+--------+---------------+--------
   2    0100.0ccd.cdcd system fa6/46,Fa8/10
   3    0100.0ccd.cdcd system Fa8/16
1002    0100.0ccd.cdcd system
1003    0100.0ccd.cdcd system
```

```
1004    0000.0000.0000   system
1005    0000.0000.0000   system
Fa4/1   0000.0000.0000   system Switch,Fa4/1
Fa4/2   0000.0000.0000   system Switch,Fa4/2

Switch#
```

This example shows how to display the static MAC address entries with a specific protocol type (in this case, assigned):

```
Switch#show mac-address-table static protocol assigned
Legend: Q - Quick
vlan  mac address     type      protocols                  port
-----------------------------------------------------------------
1     0000.0000.0000  static    ip,ipx,assigned,other      Switch
Fa4/1 0000.0000.0000  static    ip,ipx,assigned,other      Switch
Fa4/2 0000.0000.0000  static    ip,ipx,assigned,other      Switch

Multicast Entries
vlan  mac address     type      ports
-----------------------------------------------------------------
  1   0000.0000.0000  system    system Switch,Fa4/1
  2   0000.0000.0000  system    Fa4/1
1002  0000.0000.0000  system
1003  0000.0000.0000  system
1004  0000.0000.0000  system
1005  0000.0000.0000  system
Fa4/1 0000.0000.0000  system    system Switch,Fa4/1
Fa4/2 0000.0000.0000  system    system Switch,Fa4/2
Switch#
```

Related Commands	Command	Description
	show mac-address-table address	Displays information about the MAC address table.
	show mac-address-table aging-time	Displays MAC address table aging information.
	show mac-address-table count	Displays the number of entries currently in the MAC address table.
	show mac-address-table dynamic	Displays the dynamic MAC address table entries only.
	show mac-address-table interface	Displays the MAC address table information for a specific interface.
	show mac-address-table multicast	Displays information about the multicast MAC address table.
	show mac-address-table protocol	Displays the MAC address table information that is based on the protocol.
	show mac-address-table vlan	Displays information about the MAC address table for a specific VLAN.

show mac-address-table vlan

To display information about the MAC address table for a specific VLAN, use the **show mac-address-table vlan** command.

show mac-address-table [**vlan** *vlan_id*] [**protocol** *protocol*]

Syntax Description

vlan *vlan_id*	(Optional) Displays the entries for a specific VLAN; valid values are from 1 to 4094.
protocol *protocol*	(Optional) Specifies a protocol. See the "Usage Guidelines" section for more information.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

For the MAC address table entries used by the routed ports, the routed port name is displayed in the "vlan" column not the the internal VLAN number.

The keyword definitions for the *protocol* variable are as follows:

- **assigned** specifies the assigned *protocol* entries.
- **ip** specifies the IP *protocol*.
- **ipx** specifies the IPX *protocol*.
- **other** specifies the other *protocol* entries.

Examples

This example shows how to display information about the MAC address table for a specific VLAN:

```
Switch# show mac-address-table vlan 1
Unicast Entries
 vlan  mac address     type        protocols       port
-------+---------------+--------+---------------+----------------------
   1    0000.0000.0000  dynamic  ip,ipx,assigned,other  FastEthernet4/15
   1    0000.0000.0240  dynamic  ip              FastEthernet4/15
   1    0000.0000.0241  dynamic  arp             FastEthernet4/15
   1    0000.0000.0244  dynamic  arp             FastEthernet4/15
   1    0010.7b00.1540  static   ip,ipx,assigned,other  Router
Multicast Entries
 vlan  mac address     type        protocols       ports
-------+---------------+--------+---------------+----------------------
   1    ffff.ffff.ffff  system   other,ip,ipx,Fa4/15
Switch#
```

This example shows how to display MAC address table information for a specific protocol type:

```
Switch# show mac-address-table vlan 100 protocol other
Unicast Entries
 vlan  mac address     type        protocols       port
```

```
---------+-------+-----------+--------+--------------------+----------
   1    0000.0000.0000  dynamic  other          FastEthernet2/15
   1    0000.0000.0034  dynamic  other          FastEthernet2/15
   1    0050.7966.0664  static   ip,ipx,assigned,other  Switch

Multicast Entries
 vlan  mac address     type  ports
-----+---------------+--------+-----------------------------------
   1    0000.0000.0000  system Switch,Fa2/15
Switch#
```

Related Commands	Command	Description
	show mac address-table address	Displays the information about the MAC address table.
	show mac address-table aging-time	Displays MAC address table aging information.
	show mac address-table count	Displays the number of entries currently in the MAC address table.
	show mac address-table dynamic	Displays the dynamic MAC address table entries only.
	show mac address-table interface	Displays the MAC address table information for a specific interface.
	show mac address-table notification	Displays notification about the maintained MAC address table.
	show mac address-table protocol	Displays the MAC address table information that is based on the protocol.
	show mac address-table static	Displays the static MAC address table entries only.

show macro auto mac-address-group

Use the **show macro auto mac-address-group** command to display the configuration of MAC address group.

show macro auto mac-address-group

Syntax Description No keywords.

Examples This example shows how to display the configuration of the MAC address group:

```
Switch# show macro auto mac-address-group
MAC Address Group Configuration:

Group Name                  OUI     MAC ADDRESS
-----------------------------------------------------------
name1Group                          2222.2222.2222
                                    3333.3333.3333
```

show macro auto device

Use the **show macro auto device** global configuration command to display the default information for a device, including builtin function name and the parameters that can be provided for the commands where executing the builtin function.

show macro auto device *device_id*

Syntax Description	*device_id*	Specifies the device ID.

Defaults None

Command Modes Global configuration

Usage Guidelines This command displays the default values as well as the currently used values if configured.

Examples This example shows how to display the default information for the device access-point:

```
Switch#show macro auto device access-point
Device:access-point Type:LWAP
Default Macro:CISCO_AP_AUTO_SMARTPORT
Current Macro:CISCO_AP_AUTO_SMARTPORT
Builtin:Parameters:BUILTIN_VLAN:1
Builtin:Parameters:NATIVE_VLAN:1
Current Parameters:NATIVE_VLAN:1
```

Related Commands	Command	Description
	show macro auto event manager	Refer to the Command Reference in the IOS library
	show macro auto interface	Display Auto SmartPorts status and the functions applied on an interface

show macro auto interface

Use the **show macro auto interface** command to display Auto SmartPorts status and the functions applied on an interface.

show macro auto interface *interface_id*

Syntax Description	*interface_id* Specifies an interface ID.
Defaults	None
Command Modes	Global configuration

Examples

This example shows how to display Auto SmartPorts status and the applied macros:

```
Switch# show macro auto int gi1/8
Gigabit Ethernet 1/8 Macro
 Auto Smart Ports Enabled
 Switch: CDP Disabled, LLDP Disabled
Interface:   Auto Smart Port   Fallback          Macro Description(s)
-----------------------------------------------------------------------
GI1/8        TRUE              None              CISCO_PHONE_PORT
```

Related Commands	**Command**	**Description**
	show macro auto device	Displays the default macros for all devices connected to the switch, the macros that are applied on the interfaces, and the parameters that can be provided for the macros to be active when using the Smart Port feature.

show macro auto monitor clients

To display the clients using the device classifier facility on the switch, use the **show macro auto monitor clients** user EXEC command.

show macro auto monitor clients

Syntax Description This command has no arguments or keywords.

Command Default User EXEC
Privileged EXEC

Usage Guidelines Device classifier (DC) is enabled by default when you enable a client application (for example, Auto Smartports) that uses its functionality. Use the **show macro auto monitor clients** command to display the clients that are using the DC feature on the switch.

As long as any clients are using the DC, you cannot disable it by using the **no macro auto monitor** command. If you attempt to disable the DC while a client is using it, an error message appears.

Examples This example shows how to use the **show macro auto monitor clients** privileged EXEC command to view the clients using the DC on the switch:

```
Switch#show macro auto monitor clients
Client Name
----------------------------
Auto Smart Ports
```

This example shows the error message that appears when you attempt to disable DC while a client is using it:

```
Switch(config)# no macro auto monitor
Macro auto monitor should be disabled before disabling device classifier
Auto Smart Ports

% Error - device classifier is not disabled
```

Related Commands

Command	Description
macro auto device	Configures macro default parameter values.
macro auto execute (built-in function)	Configures mapping from an event trigger to a built-in macro.
macro auto global processing	Enables Auto Smartports on a switch.
macro auto mac-address-group	Configures MAC address groups.
macro auto sticky	Configures macro persistence.
debug macro	Comes event trigger.
show macro auto monitor type	Displays all the device types recognized by the device classifier.
show shell triggers	Displays information about event triggers and macros.

show macro auto monitor device

To display the devices connected to a switch and their associated properties, use the **show macro auto monitor device** user EXEC command.

show macro auto monitor device [**detail** | **filter** *string* | **interface** *interface_id*] **mac-address** *mac_address*]

Syntax Description

detail	Displays detailed device classifier information.
filter *string*	Displays information for devices that match the filter.
interface *interface_id*	Displays information about devices attached to the specified interface.
mac *mac_address*	Displays device information for the specified endpoint.

Command Modes User EXEC
Privileged EXEC

Usage Guidelines Use this command to display the devices connected to a switch. Use the **show macro auto device** privileged EXEC command to display the configurable parameters for a device.

Examples This example shows how to use the **show macro auto monitor device** privileged EXEC command with an optional keyword to view the devices connected to a switch:

```
Switch# show macro auto monitor device
MAC_Address      Port_Id        Profile Name
---------------- -------------- ------------------------------
0014.5ef6.1d40   Gi2/0/1        Cisco-IP-Phone-7960
0014.5ef6.1d41   Gi2/0/2        Cisco-Device
001f.9e85.1250   Gi2/0/4        Cisco-AP-Aironet-1130
```

This example shows how to use the **show macro auto monitor device** privileged EXEC command with the optional **mac-address** keyword to view information about the connected device with the specified MAC address:

```
Switch# show macro auto monitor device mac-address 001f.9e85.1250
MAC_Address      Port_Id        Profile Name
---------------- -------------- ------------------------------
001f.9e85.1250   Gi2/0/4        Cisco-AP-Aironet-1130
```

This example shows how to use the **show macro auto monitor device** privileged EXEC command with the optional **mac-address** and **detail** keywords to view detailed information about the connected device with the specified MAC address:

```
Switch# show macro auto monitor device mac-address 001f.9e85.1250 detail
MAC_Address      Port_Id        Matching Name  Profile Name Profile Name
Device_Name
---------------- -------------- -------------- ------------ ------------
-------------------------------
001f.9e85.1250   Gi2/0/4        AP             Basic-1x     Cisco-AP-Aironet-1130
Cisco-AP-Aironet-1130
```

```
==========================================================================
==========================================================================
```

This example shows how to use the **show macro auto monitor device** privileged EXEC command with the optional **interface** keyword to view summary information about the device connected to the specified interface:

```
Switch#show macro auto monitor device interface gi 1/0/2
MAC_Address      Port_Id      Profile Name
==========================================================================
000a.b8e6.1a07   Gi1/0/2      Cisco-Device
==========================================================================
```

This example shows how to use the **show macro auto monitor device** privileged EXEC command with the optional **interface** and **detail** keywords to view detailed information about the device connected to the specified interface:

```
Switch#show macro auto monitor device interface gi 1/0/2 detail
MAC_Address      Port_Id      Variantly Present  Profile-Type  Profile Name
Macro_Name
==========================================================================
==========================================================================
000a.b8e6.1a07   Gi1/0/2      10         0        Default       Cisco-Device     etsco
==========================================================================
```

Related Commands	Command	Description
	macro auto device	Configures macro default-parameter values.
	macro auto execute (built-in function)	Configures mapping from *on event* trigger to a built-in macro.
	macro auto global processing	Enables Auto Smartports on a switch.
	macro auto mac-address-group	Configures MAC address groups.
	macro auto sticky	Configures macro persistence.
	macro trigger	Creates event trigger.
	show macro auto monitor clients	Displays all the device types recognized by the device classifier.
	show macro auto monitor type	Displays all the device types recognized by the device classifier.
	show shell triggers	Displays information about event triggers and macros.

show macro auto monitor type

To display all the device types recognized by the device classifier, use the **show macro auto monitor type** user EXEC command.

show macro auto monitor type [**table** *[built-in | default]*] **string** *[filter_string]*

Syntax Description

table	Displays device classification in a table.
built-in	Displays device classification information from the built-in device table.
default	Displays device classification information from the default device table.
filter *string*	Displays information for devices that match the filter.

Command Modes

User EXEC
Privileged EXEC

Usage Guidelines

This command displays all the device types recognized by the device classification engine. The number of available device types is the number of profiles stored on the switch. Because the number of profiles can be very large, you can use the **filter** keyword to limit the command output.

Examples

This example shows how to use the **show macro auto monitor type** privileged EXEC command with no optional keywords to view the devices recognized by the device classifier:

```
Switch# show macro auto monitor type table
Vlan Id         Type          Device Name                   mode Conf  ID
-------------------------------------------------------------------------
Vlan 1          Default       Cisco Phone                   10   1     1
Vlan 1          Default       Jetdirect Card Live           10   1     2
Vlan 1          Default       Jetdirect Card Dead           10   1     3
Vlan 1          Default       Cisco Access Point            10   1     4
Vlan 1          Default       HP Jetdirect                  10   1     5
Vlan 1          Default       Cisco Gateway                 10   1     6
Vlan 1          Default       Cisco IP Phone 7910           70   8     7
Vlan 1          Default       Cisco IP Phone 7912           70   8     8
Vlan 1          Default       Cisco IP Phone 7940           70   8     9
Vlan 1          Default       Cisco IP Phone 7941           70   8     10
Vlan 1          Default       Cisco IP Phone 7960           70   11    11
Vlan 1          Default       Cisco IP Phone 7961           70   11    12
Vlan 1          Default       Cisco IP Phone 7970           70   11    13
Vlan 1          Default       Cisco IP Phone 7971           70   11    14
Vlan 1          Default       Cisco IP Phone 7914           70   14    15
Vlan 1          Default       Cisco IP Phone 7906           70   14    16
Vlan 1          Default       Cisco IP Phone 7905           70   14    17
Vlan 1          Default       Cisco IP Phone 7912           70   14    18
Vlan 1          Default       Cisco IP Phone 7911           70   14    19
Vlan 1          Default       Cisco IP Phone 7936           70   14    20
Vlan 1          Default       Cisco IP Phone 7935           70   14    21
Vlan 1          Default       Cisco IP Phone 7937           70   14    22
Vlan 1          Default       Cisco IP Phone 7975           70   14    23
```

Vlan1hd	Default	Cisco-ISP-Phone-7970	70	24
Vlan1hd	Default	Cisco-ISP-Phone-7971	71	24
Vlan1hd	Default	Cisco-ISP-Phone-7971	71	24
Vlan1hd	Default	Cisco-SLC-IS-IS-Series	40	27
Vlan1hd	Default	Cisco-Telepresence	30	24
Vlan1hd	Default	Netscapy-Series	30	29
Vlan1hd	Default	SP-Series	30	30
Vlan1hd	Default	Tandberg-Telepresence	30	24
Vlan1hd	Default	Vocal-Series	30	31
Vlan1hd	Default	Lumenta-Protocol-SCSUdm	30	33
Vlan1hd	Default	Microsoft-Series	30	34
Vlan1hd	Default	Netgear-Series	30	35
Vlan1hd	Default	Nortel-Series	30	36
Vlan1hd	Default	Retail-Series	30	37
Vlan1hd	Default	Retail-IP-Phone-2000-Series	20	38
Vlan1hd	Default	Sanyo-Series	30	39
Vlan1hd	Default	SNOM-SIP	30	40
Vlan1hd	Default	Sorrel-Series	30	41
Vlan1hd	Default	Telepresence-Phones-ESS	30	42
Vlan1hd	Default	Jacobs-SIP	30	43
Vlan1hd	Default	Cisco-Access-Point	30	44
Vlan1hd	Default	Cisco-Configuration-Server-7936	70	45
Vlan1hd	Default	Cisco-IP-Conference-Station-7935	70	46
Vlan1hd	Default	Cisco-IP-Conference-Station-7937	70	47
Vlan1hd	Default	Nokia-SAP-0102	30	48
Vlan1hd	Default	Cisco-AP-Aironet-1130	30	49
Vlan1hd	Default	Cisco-AP-Aironet-1140	30	50
Vlan1hd	Default	Cisco-AP-Aironet-1250	30	51
Vlan1hd	Default	Cisco-LIS-QoS	25	52
Vlan1hd	Default	Cisco-LIS-QoS-1000	50	53
Vlan1hd	Default	Cisco-LIS-QoS-1200	50	54
Vlan1hd	Default	Cisco-LIS-QoS-1250	50	55
Vlan1hd	Default	Cisco-LIS-SP	25	56
Vlan1hd	Default	Cisco-LIS-SP-1100	55	57
Vlan1hd	Default	Cisco-LIS-SP-1240	55	58
Vlan1hd	Default	Cisco-LIS-SP-1250	55	59
Vlan1hd	Default	Lexmark-Series	30	60
Vlan1hd	Default	Lexmark-Protocol-Series	30	61
Vlan1hd	Default	MPC-Series	30	62
Vlan1hd	Default	Cisco-Telepresence-Series	30	63
Vlan1hd	Default	Mitsuo-Series	30	64
Vlan1hd	Default	DIS-Appliance	30	66
Vlan1hd	Default	Cisco-Voice	30	1
Vlan1hd	Default	Cisco-Voice	30	2
Vlan1hd	Built-in	Ethernet	10	1
Vlan1hd	Built-in	Cisco-IP-Camera	50	2
Vlan1hd	Built-in	Cisco-IP-Camera-Zone	50	3
Vlan1hd	Built-in	Cisco-IP-Camera-2421	50	5
Vlan1hd	Built-in	Cisco-IP-Camera-2500	50	6
Vlan1hd	Built-in	Cisco-IP-Camera-2511	50	7
Vlan1hd	Built-in	Cisco-IP-Camera-2530	50	8
Vlan1hd	Built-in	Cisco-IP-Camera-Axis	50	9
Vlan1hd	Built-in	Cisco-Transparent-Bridge	8	10
Vlan1hd	Built-in	Cisco-Ethernet	10	11
Vlan1hd	Built-in	Cisco-Source-Bridge	10	12
Vlan1hd	Built-in	Cisco-Token	10	13
Vlan1hd	Built-in	Cisco-Fddi	10	14
Vlan1hd	Built-in	IP-Phone	20	15
Vlan1hd	Built-in	Cisco-GMP	10	16
Vlan1hd	Built-in	Cisco-GMP-10100	70	17
Vlan1hd	Built-in	Cisco-GMP-40100	70	18
Vlan1hd	Built-in	Cisco-GMP-40101	70	19
Vlan1hd	Built-in	Cisco-SLC-IS-IS-Series	40	20

Vlan168	Bad In-Un	Alarm-Automaton-Phones	50	21
Vlan169	Bad In-Un	Alarm-Alarm-Clocks	50	23
Vlan168	Bad In-Un	Alarm-AUX-LAT	50	23
Vlan168	Bad In-Un	Lifesaver-Exercise	20	24

Related Commands

Command	Description
macro auto device	Configures macro default parameter values.
macro auto execute {fault to function}	Configures mapping from an event trigger to a built-in macro.
macro auto global processing	Enables Auto Smartports on a switch.
macro auto mac-address-group	Configures MAC address groups.
macro auto sticky	Configures macro persistence.
shell trigger	Creates event triggers.
show macro auto monitor clients	Displays all the device types recognized by the device classifier.
show macro auto monitor device	Displays all the device types recognized by the device classifier.

show module

To display information about the module, use the **show module** command.

show module [*mod*] [**all**]

Syntax Description		
	mod	(Optional) Number of the module; valid values vary from chassis to chassis.
	all	(Optional) Displays information for all modules.

Defaults	
	This command has no default settings.

Command Modes	
	Privileged EXEC mode

Usage Guidelines

In the Mod Sub Module fields in the command output, the **show module** command displays the supervisor engine number but appends the uplink daughter card's module type and information.

If the PoE oversubscribed by the module is more than 50 W *above* the administratively allocated PoE, the "Status" displays as "PwrOver." If the PoE oversubscribed by the module is more than 50 W *above* the PoE module limit, the "Status" displays as "PwrFault."

Examples

This example shows how to display information for all the modules.

This example shows the **show module** command output for a system with inadequate power for all installed modules. The system does not have enough power for Module 5; the "Status" displays it as "PwrDenyl."

```
Switch> show module all
Mod Ports Card Type                              Model              Serial No.
--- ----- -------------------------------------  -----------------  -----------
  1    2  1 10GBaseX (GBIC) Supervisor(active)   WS-X6704           SAD0614
  2    8  1 1000BaseX (GBIC) Enhanced            WS-X6408A          SAD0612
  3   16  1 10/100/1000BaseT (RJ45)              WS-X6516-GE-TX     SAD0613
  5    0  0 Not enough power for module          WS-X6148-FE-MT     SDD0320
  6   48  1 10/100BaseTX (RJ45)                  WS-X6148           JAB0323
M MAC addresses                  Hw  Fw         Sw         Status
--- ----------------------------- --- ---------- ---------- -------
1 00for-96ba.f9b0 to 00for-96ba.f9bf 6.2 12.1(11br)E8 12.1.(20E)C10.1 Ok
2 0001.64a.a850 to 0001.64a.a85f 1.0 5.4(2)        8.4(0.0)
3 0001.7344.2a64 to 0001.7344.2a7f 1.2 5.4(2)      8.4(0.0)
5 0001.64a.a850 to 0001.64a.a85f 2.2               PwrDenyl
6 0001.6352.2d40 to 0001.6352.2d47 1.0             Ok
Switch>
```

This example shows how to display information for a specific module:

```
Switch> show module mod2
Mod Ports Card Type                              Model              Serial No.
--- ----- -------------------------------------  -----------------  -----------
  2    8  1 Catalyst 6000 supervisor 2 (active)  WS-X6K-SUP2-2GE    SAD0401051
```

```
Mod MAC addresses                                  Hw   Fw         Sw         Status
--- ---------------------------------------------- ---- ---------- ---------- -------
  2  0001.64a1.9b63 to 0001.64a1.9b6a  1.1  6.1(3)     8.2(0.97)  Ok
Mod Sub-Module                  Model              Serial     Hw     Status
--- ---------------------------- ------------------ ---------- ------ -------
  2 Policy Feature Card 3        WS-F6K-PFC3        SAD064400ZU  1.0    Ok
  2 Cat6k MSFC 3 daughtercard    WS-F6K-MSFC3       SAD064202ER  1.1    Ok
Switch>
```

This example shows how to display information for all the modules on the switch:

```
Switch> show module
Chassis Type : WS-C6506

Power Consumed by Backplane : 0 Watts

Mod Ports Card Type                              Model              Serial No.
--- ----- -------------------------------------- ------------------ -----------
  1     2  SX 10G, 1000Ethernet (GFP) Supervisor WS-X6704-10G
  3     6  10GEthernet (DCEF)                    WS-X6708           SAD080111
M MAC addresses                                  Hw   Fw         Sw         Status
--- ---------------------------------------------- ---- ---------- ---------- -------
1 0004.dd46.7700 to 0004.dd46.7705  0.0  12.2(18r)S(88) 12.2(20060513:14  Ok
3 0015.7ba4.8620 to 0015.7ba4.8625  0.2                                   Ok
Switch>
```

show monitor

To display information about the SPAN session, use the **show monitor** command.

show monitor [**session**] [**range** *session-range* | **local**] **remote** | **all** | *session-number*] [**detail**]

Syntax Description

session	(Optional) Displays the SPAN information for a session.
range	(Optional) Displays information for a range of sessions.
session-range	(Optional) Specifies a range of sessions.
local	(Optional) Displays all local SPAN sessions.
remote	(Optional) Displays the RSPAN source and destination sessions.
all	(Optional) Displays the SPAN and RSPAN sessions.
session-number	(Optional) Session number; valid values are from 1 to 6.
detail	(Optional) Displays the detailed SPAN information for a session.

Defaults

The **detail** keyword only displays lines with a nondefault configuration.

Command Modes

Privileged EXEC mode

Examples

This example shows how to display whether ACLs are applied to a given SPAN session on a Catalyst 4500 series switch:

```
Switch#show monitor

Session 1
---------
Type                  : Local Session
Source Ports          :
    Both              : Fa2/1
Destination Ports     : Fa2/2
    Encapsulation     : Native
        Ingress       : Disabled
        Learning      : Disabled
Filter VLANs          :
IP Access-group       : 10
```

This example shows how to display SPAN information for session 2:

```
Switch#show monitor session 2
Session 2
---------
Type : Remote Source Session
Source Ports :
    RX Only:     Fa2/1-3
Reec RSPAN VLAN: 901
Ingress : Enabled, Replicat: VLAN-2
Learning : Disabled
Switch#
```

This example shows how to display the detailed SPAN information for session 1:

```
Switch# show monitor session 1 detail
Session 1
---------
Type                  : Local Session
Source Ports:
    RX Only           : None
    TX Only           : None
    Both              : Gi1/1, CPU
Source VLANs:
    RX Only           : None
    TX Only           : None
    Both              : None
Source RSPAN VLAN : Ref/1
Destination Ports :
    Encapsulation : ISL
                    Ingress : Enabled, default VLAN = 2
Filter VLANs      : All
    Filter Types RX : Good
    Filter Types TX : None
Dest RSPAN VLAN   : None
Ingress: Disabled, default VLAN=2
Learning : Disabled
IP access-group : None
Switch#
```

This example shows how to display SPAN information for session 1 beginning with the line that starts with Destination:

```
Switch# show monitor session 1 | begin Destination
Destination Ports: None
Dest RSPAN VLAN   : None
Switch#
Switch#
```

Related Commands	Command	Description
	monitor session	Enables the SPAN sessions on interfaces or VLANs.

show monitor capture

To display the capture point details, so that you can see what capture points are defined, what their attributes are, and whether they are active, use the **show monitor capture** command.

show monitor capture [*name*] [**parameter** | **buffer** [**brief** | **detailed** | **dump**]]

Syntax Description

name	Specifies the capture point name.
parameter	Recommends and displays the exec commands for specifying the capture point.
buffer [**brief** | **detailed** | **dump**]	Source the packets from the capture buffer, decode and display them in brief, detailed or dump mode.

Defaults

If the capture point name is not provided, the command displays all the capture point details.

If the display mode is not specified, the command defaults to brief mode.

Command Modes

Privileged EXEC mode

Usage Guidelines

When the command is issued with no parameters, it displays the details of all the capture points. When specified with a capture point name and no other parameters, it displays the details of the specific capture point name. With the parameter keyword, the command recommends to the commands that describe the capture point and displays them.

The **buffer** option displays the packets from the capture buffer. This option is applicable only if the capture point directs the captured packets to the buffer. The packets can be decoded and displayed in either the brief, detailed, or dump mode. The default mode is **brief**.

Examples

Following are examples of how to use the **show monitor capture** command:

```
Router# show monitor capture mycap buffer brief
 0.000000  10.1.1.215 -> 10.1.1.2   UDP Source port: 20001  Destination port: 20002
 1.000000  10.1.1.215 -> 10.1.1.2   UDP Source port: 20001  Destination port: 20002
 2.000000  10.1.1.215 -> 10.1.1.2   UDP Source port: 20001  Destination port: 20002
 3.000000  10.1.1.218 -> 10.1.1.2   UDP Source port: 20001  Destination port: 20002
 4.000000  10.1.1.218 -> 10.1.1.2   UDP Source port: 20001  Destination port: 20002
 5.000000  10.1.1.220 -> 10.1.1.2   UDP Source port: 20001  Destination port: 20002
 6.000000  10.1.1.221 -> 10.1.1.2   UDP Source port: 20001  Destination port: 20002
 7.000000  10.1.1.223 -> 10.1.1.2   UDP Source port: 20001  Destination port: 20002
 8.000000  10.1.1.223 -> 10.1.1.2   UDP Source port: 20001  Destination port: 20002
 9.000000  10.1.1.224 -> 10.1.1.2   UDP Source port: 20001  Destination port: 20002
10.000000  10.1.1.224 -> 10.1.1.2   UDP Source port: 20001  Destination port: 20002
11.000000  10.1.1.226 -> 10.1.1.2   UDP Source port: 20001  Destination port: 20002
12.000000  10.1.1.227 -> 10.1.1.2   UDP Source port: 20001  Destination port: 20002
13.000000  10.1.1.227 -> 10.1.1.2   UDP Source port: 20001  Destination port: 20002
14.000000  10.1.1.229 -> 10.1.1.2   UDP Source port: 20001  Destination port: 20002
15.000000  10.1.1.229 -> 10.1.1.2   UDP Source port: 20001  Destination port: 20002
16.000000  10.1.1.232 -> 10.1.1.2   UDP Source port: 20001  Destination port: 20002
17.000000  10.1.1.232 -> 10.1.1.2   UDP Source port: 20001  Destination port: 20002
```

```
10.000000    10.1.1.254 -> 10.1.1.2    SSP Source port: 10001  Destination port: 10002
10.000000    10.1.1.2   -> 10.1.1.254  SSP Source port: 10002  Destination port: 10001
10.000000    10.1.1.254 -> 10.1.1.2    SSP Source port: 10001  Destination port: 10002

Dot1AH show monitor capture mycap buffer detail
Frame 1: 156 bytes on wire (1248 bits), 156 bytes captured (1248 bits)
    Arrival Time: Apr 11, 2012 01:00:02.999000000 EST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1334131202.999000000 seconds
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 156 bytes (1248 bits)
    Capture Length: 156 bytes (1248 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ip:udp:data]
Ethernet II, Src: 00:00:00:00:00:01 (00:00:00:00:00:01), Dst: 54:78:ab:8a:00:16
    Ethernet Header
    Destination: 54:78:ab:8a:00:16 (54:78:ab:8a:00:16)
        Address: 54:78:ab:8a:00:16 (54:78:ab:8a:00:16)
                 .... ..0. .... .... .... .... = Lsb: Individual address (unicast)
                 .... ..1. .... .... .... .... = Lsb: Locally-assigned address (factory default)
    Source: 00:00:00:00:00:01 (00:00:00:00:00:01)
        Address: 00:00:00:00:00:01 (00:00:00:00:00:01)
                 .... ..0. .... .... .... .... = Lsb: Individual address (unicast)
                 .... ..1. .... .... .... .... = Lsb: Locally-assigned address (factory default)
    Type
10.000000    10.1.1.254 -> 10.1.1.2    SSP Source port: 10001  Destination port: 10002

Dot1AH show monitor capture mycap buffer dump
0.000000    10.1.1.254 -> 10.1.1.2    SSP Source port: 10001  Destination port: 10002

0000  54 78 ab 8a 00 16 00 00 00 00 00 01 08 00 45 00  Ts..\.....E.
0010  00 8a 00 00 40 00 40 11 ef 7a 0a 01 01 fe 0a 01  ....@.@..z......
0020  01 02 27 11 27 11 00 76 ab 8b 00 01 00 00 88 a8  ..'.'..v........
0030  00 07 00 88 8a 8a 0e 0d 8a 8f 10 11 12 13 14 15  ................
0040  16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  ......  !"#$%&'()*
0050  26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  +,-./0123456789:;
0060  36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45  <=>?@ABCDEFGHIJK
0070  46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55  LMNOPQRSTUVWXYZ[\
0080  56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65  ]^_`abcdefghijk
0090  66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75  lmnopqrstuvwxyz{|
00a0  76 77 78 79 7a 7b 7c 7d 7e 7f                    }~......
00b0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00c0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00d0  00 00 b0 b0 b0 ba ba ba ba ba ba ba ba ba ba ba  ................
00e0  ba ba ba ba ba ba ba ba ba ba ba ba ba ba ba ba  ................
```

show monitor capture file

To decode and display packets from a previously captured .pcap file, use the **show monitor capture file** command.

show monitor capture file *name* [**display-filter** *filter-string*] [**brief** | **detailed** | **dump**]

Syntax Description

name	Specifies the filename.
display-filter *filter-string*	Specifies the display filter string according to Wireshark's display-filter syntax.
brief | **detailed** | **dump**	Determines the display mode. **brief**—Displays a one line summary of the packet with key fields. **detailed**—Displays all the fields in the packet for the protocols supported and displays the payload in hexadecimal form. **dump**—Displays a one line summary of the packet with key fields and also displays the packet in hexadecimal form.

Defaults

brief

Command Modes

Privileged EXEC mode

Usage Guidelines

If no display filter is specified, then all the packets in the file are displayed. Because the display filter must observe the Wireshark display filter syntax, ensure that the display filter is accurate. Also, use a double-quotes when specifying the filter.

Examples

This example shows how to display packets from a .pcap file with a display filter:

```
Switch#show monitor capture file bootflash:test.pcap display-filter
```

This example displays a brief output from a .pcap file:

```
Switch#show monitor capture file bootflash:myvcap.pcap
  1  0.000000   10.1.1.241 -> 20.1.1.2   UDP Source port: 20001  Destination port:
20002
  2  2.000000   10.1.1.241 -> 20.1.1.2   UDP Source port: 20001  Destination port:
20002
  3  2.000000   10.1.1.241 -> 20.1.1.2   UDP Source port: 20001  Destination port:
20002
  4  3.000000   10.1.1.241 -> 20.1.1.2   UDP Source port: 20001  Destination port:
20002
  5  3.000000   10.1.1.241 -> 20.1.1.2   UDP Source port: 20001  Destination port:
20002
  6  5.000000   10.1.1.241 -> 20.1.1.2   UDP Source port: 20001  Destination port:
20002
  7  6.000000   10.1.1.241 -> 20.1.1.2   UDP Source port: 20001  Destination port:
20002
```

```
    8  7.000000   10.1.1.147 → 20.1.1.2   UDP Source port: 20001  Destination port:
20002
    9  8.000000   10.1.1.148 → 20.1.1.2   UDP Source port: 20001  Destination port:
20002
   10  9.000000   10.1.1.149 → 20.1.1.2   UDP Source port: 20001  Destination port:
20002
   11 10.000000   10.1.1.150 → 20.1.1.2   UDP Source port: 20001  Destination port:
20002
   12 11.000000   10.1.1.151 → 20.1.1.2   UDP Source port: 20001  Destination port:
20002
   13 12.000000   10.1.1.152 → 20.1.1.2   UDP Source port: 20001  Destination port:
20002
   14 13.000000   10.1.1.153 → 20.1.1.2   UDP Source port: 20001  Destination port:
20002
   15 14.000000   10.1.1.154 → 20.1.1.2   UDP Source port: 20001  Destination port:
20002
   16 15.000000   10.1.1.155 → 20.1.1.2   UDP Source port: 20001  Destination port:
20002
   17 16.000000   10.1.1.156 → 20.1.1.2   UDP Source port: 20001  Destination port:
20002
   18 17.000000   10.1.1.157 → 20.1.1.2   UDP Source port: 20001  Destination port:
20002
   19 18.000000   10.1.1.158 → 20.1.1.2   UDP Source port: 20001  Destination port:
20002
   20 19.000000   10.1.1.159 → 20.1.1.2   UDP Source port: 20001  Destination port:
20002
   21 20.000000   10.1.1.160 → 20.1.1.2   UDP Source port: 20001  Destination port:
20002
   22 21.000000   10.1.1.161 → 20.1.1.2   UDP Source port: 20001  Destination port:
20002
   23 22.000000   10.1.1.162 → 20.1.1.2   UDP Source port: 20001  Destination port:
20002
   24 23.000000   10.1.1.163 → 20.1.1.2   UDP Source port: 20001  Destination port:
20002
   25 24.000000   10.1.1.164 → 20.1.1.2   UDP Source port: 20001  Destination port:
20002
   26 25.000000   10.1.1.165 → 20.1.1.2   UDP Source port: 20001  Destination port:
20002
   27 26.000000   10.1.1.166 → 20.1.1.2   UDP Source port: 20001  Destination port:
20002
   28 27.000000   10.1.1.167 → 20.1.1.2   UDP Source port: 20001  Destination port:
20002
   29 28.000000   10.1.1.168 → 20.1.1.2   UDP Source port: 20001  Destination port:
20002
   30 29.000000   10.1.1.169 → 20.1.1.2   UDP Source port: 20001  Destination port:
20002
   31 30.000000   10.1.1.170 → 20.1.1.2   UDP Source port: 20001  Destination port:
20002
   32 31.000000   10.1.1.171 → 20.1.1.2   UDP Source port: 20001  Destination port:
20002
   33 32.000000   10.1.1.172 → 20.1.1.2   UDP Source port: 20001  Destination port:
20002
   34 33.000000   10.1.1.173 → 20.1.1.2   UDP Source port: 20001  Destination port:
20002
   35 34.000000   10.1.1.174 → 20.1.1.2   UDP Source port: 20001  Destination port:
20002
   36 35.000000   10.1.1.175 → 20.1.1.2   UDP Source port: 20001  Destination port:
20002
   37 36.000000   10.1.1.176 → 20.1.1.2   UDP Source port: 20001  Destination port:
20002
   38 37.000000   10.1.1.177 → 20.1.1.2   UDP Source port: 20001  Destination port:
20002
   39 38.000000   10.1.1.178 → 20.1.1.2   UDP Source port: 20001  Destination port:
20002
```

```
  40 39.00000   10.1.1.179 -> 20.1.1.2    UDP Source port: 20001  Destination port:
20002
  41 40.00000   10.1.1.181 -> 20.1.1.2    UDP Source port: 20001  Destination port:
20002
  42 41.00000   10.1.1.181 -> 20.1.1.2    UDP Source port: 20001  Destination port:
20002
  43 42.00000   10.1.1.181 -> 20.1.1.2    UDP Source port: 20001  Destination port:
20002
  44 43.00000   10.1.1.181 -> 20.1.1.2    UDP Source port: 20001  Destination port:
20002
  45 44.00000   10.1.1.184 -> 20.1.1.2    UDP Source port: 20001  Destination port:
20002
  46 45.00000   10.1.1.185 -> 20.1.1.2    UDP Source port: 20001  Destination port:
20002
  47 46.00000   10.1.1.186 -> 20.1.1.2    UDP Source port: 20001  Destination port:
20002
  48 47.00000   10.1.1.187 -> 20.1.1.2    UDP Source port: 20001  Destination port:
20002
  49 48.00000   10.1.1.188 -> 20.1.1.2    UDP Source port: 20001  Destination port:
20002
  50 49.00000   10.1.1.189 -> 20.1.1.2    UDP Source port: 20001  Destination port:
20002
  51 50.00000   10.1.1.190 -> 20.1.1.2    UDP Source port: 20001  Destination port:
20002
  52 51.00000   10.1.1.191 -> 20.1.1.2    UDP Source port: 20001  Destination port:
20002
  53 52.00000   10.1.1.192 -> 20.1.1.2    UDP Source port: 20001  Destination port:
20002
  54 53.00000   10.1.1.193 -> 20.1.1.2    UDP Source port: 20001  Destination port:
20002
  55 54.00000   10.1.1.194 -> 20.1.1.2    UDP Source port: 20001  Destination port:
20002
  56 55.00000   10.1.1.195 -> 20.1.1.2    UDP Source port: 20001  Destination port:
20002
  57 56.00000   10.1.1.196 -> 20.1.1.2    UDP Source port: 20001  Destination port:
20002
  58 57.00000   10.1.1.197 -> 20.1.1.2    UDP Source port: 20001  Destination port:
20002
  59 58.00000   10.1.1.198 -> 20.1.1.2    UDP Source port: 20001  Destination port:
20002
```

This example shows how to display a detailed output from a .pcap file:

```
Switch# show monitor capture file bootflash:mycap.pcap detailed
Frame 1: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bits)
    Arrival Time: Mar 21, 2012 14:05:05.513890000 PDT
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1332336305.513890000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 286 bytes (2288 bits)
    Capture Length: 256 bytes (2048 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ip:udp:data]
Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 54:75:d8:3a:95:3d
    Destination: 54:75:d8:3a:95:3d (54:75:d8:3a:95:3d)
        Address: 54:75:d8:3a:95:3d (54:75:d8:3a:95:3d)
            .1. .... .... .... .... .... = Ig bit: Individual address (unicast)
            ..0. .... .... .... .... .... = Lg bit: Globally unique address (factory default)
    Source: 00:00:00:00:00:01 (00:00:00:00:00:01)
```

```
        Address: 00:00:00:00:03:01  00:00:00:00:03:01
        .... ..0. .... .... .... .... = LG bit: Locally administered address (unique)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IP (0x0800)
    Trailer: 0000000000000000000000  [incorrect, should be 0x8f0ce7]
Internet Protocol, Src: 10.1.1.140 (10.1.1.140), Dst: 10.1.1.2 (10.1.1.2)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00..  = Differentiated Services Codepoint: Default (0x00)
        .... ..0.  = ECN-Capable Transport (ECT): 0
        .... ...0  = ECN-CE: 0
    Total length: 1500
    Identification: 0x0000 (0)
    Flags: 0x00
        0... ....  = Reserved bit: Not set
        .0.. ....  = Don't Fragment: Not set
        ..0. ....  = More Fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: UDP (17)
    Header checksum: 0x9f9 [correct]
    Source: 10.1.1.140
        [Node: Falcon]
    Source: 10.1.1.140 (10.1.1.140)
    Destination: 10.1.1.2 (10.1.1.2)
User Datagram Protocol, Src Port: 2002 (2002), Dst Port: 2002 (2002)
    Source port: 2002 (2002)
    Destination port: 2002 (2002)
    Length: 1480
    Checksum: 0x0a2d [validation disabled]
        [Good Checksum: False]
        [Bad Checksum: False]
Data (1472 bytes)
0000  00 00 00 00 00 00 00 07  08 09 0a 0b 0c 0d 0e 0f  ................
0010  10 11 12 13 14 15 16 17  18 19 1a 1b 1c 1d 1e 1f  ................
0020  20 21 22 23 24 25 26 27  28 29 2a 2b 2c 2d 2e 2f  (*$%&'()*+,-./
0030  30 31 32 33 34 35 36 37  38 39 3a 3b 3c 3d 3e 3f  0123456789:;<=>?
0040  40 41 42 43 44 45 46 47  48 49 4a 4b 4c 4d 4e 4f  @ABCDEFGHIJKLMNO
0050  50 51 52 53 54 55 56 57  58 59 5a 5b 5c 5d 5e 5f  PQRSTUVWXYZ[\]^_
0060  60 61 62 63 64 65 66 67  68 69 6a 6b 6c 6d 6e 6f  `abcdefghijklmno
0070  70 71 72 73 74 75 76 77  78 79 7a 7b 7c 7d 7e 7a  pqrstuvwxyz{|}~z
0080  80 81 82 83 84 85 86 87  88 89 8a 8b 8c 8d 8e 8f  ................
0090  90 91 92 93 94 95 96 97  98 99 9a 9b 9c 9d 9e 9f  ................
00a0  a0 a1 a2 a3 a4 a5 a6 a7  a8 a9 aa ab ac ad ae af  ................
00b0  b0 b1 b2 b3 b4 b5 b6 b7  b8 b9 ba bb bc bd be bf  ................
00c0  c0 c1 c2 c3 c4 c5 c6 c7  c8 c9 ca cb cc cd ce cf  ................
00d0  d0 d1                                              ..
    Data: 0000000000000700090a0b0c0d0e0f101112131415161718...
    [Length: 1472]
```

Frame 2: 246 bytes on wire (1968 bits), 246 bytes captured (1968 bits)
    Arrival Time: Mar 21, 2012 14:19:15.319785000 MST

show nmsp

To display the Network Mobility Services Protocol (NMSP) information for the switch, use the **show nmsp** command. This command is available only when you switch is running the cryptographic (encrypted) software image.

show nmsp {attachment suppress interface | capability | notification interval | statistics {connection | summary} | status | subscription {detail | summary}}

Syntax Description	**attachment suppress interface** — Displays attachment suppress interfaces.
	capability — Displays switch capabilities including the supported services and subservices.
	notification interval — Displays the notification intervals of the supported services.
	statistics connection | summary — Displays the NMSP statistics information. • **connection**—Displays the message counters on each connection. • **summary**—Displays the global counters.
	status — Displays information about the NMSP connection.
	subscription detail | summary — Displays the subscription informationon each NMSP connection. • **detail**—Displays all services and subservices subscribed on each connection. • **summary**—Displays all services subscribed on each connection.

Command Modes Privileged EXEC mode

Examples

This is an example of output from the **show nmsp attachment suppress interface** command:

```
Switch#show nmsp attachment suppress interface
NMSP Attachment Suppression Interfaces

GigabitEthernet1/1
GigabitEthernet2/1
Switch#
```

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

```
Switch#show nmsp capability
NMSP Service Capability

Service              Subservice
-------              ----------
AttachMobile         Wired Station
Location             Subscription
Switch#
```

This is an example of output from the **show nmsp notification interval** command:

```
Switch#show nmsp notification interval
NMSP Notification Interval

Service              Subservice              Interval
```

```
Attachment notify(internal): 30 secs (default)
Inactivity notify(external): 30 sec (default)
Switch#
```

This is an example of output from the **show snmp statistics connection** and **show snmp statistics summary** commands:

```
Switch# show snmp statistics connection
SNMP Connection Statistics

---------------------------------------------------
Connection 1:
  Connection status: UP
  Packet connection: 0

  In message count                  Out message count
  ----------------                  -----------------
  Subnet Reqs: 1                    Subnet Reqs: 1
  Caps Notif: 1                     Caps Notif: 1
  Inform Reqs: 0                    Inform Reqs: 0
  Sets Notif: 0                     Sets Notif: 0
  Inv Reqs: 1                       Inv Reqs: 1
  Inv Notif: 0                      Inv Notif: 0
                                    Unsupported msg: 0
Switch#

Switch# show snmp statistics summary
SNMP Global Counters

---------------------------------------------------
  Send toc msg msg: 0
  Send msg msg: 0
  Partial output drop: 0
  Outbox active sendQ blocks: 0
  Outbox free sendQ blocks: 0
  Failed outbox sendQ: 0
  Outbox read sendQ blocks: 0
  Unknown Pkts: 0
  Bad Version Msg: 0
  Bad Encapsulation Msg: 0
  Bad Msg: 0
Switch#
```

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

```
Switch# show snmp status
SNMP Status

---------------------------------------------------
SNMP: enabled

MGE IP Address    TcpKeepAlap TcpKeeAlap Tcpkeep Retries

---------------------------------------------------
172.28.25.100     0           0          0       4
Switch#
```

This is an example of output from the **show snmp show subscription detail** and **show snmp show subscription summary** commands:

```
Switch# show snmp subscription detail
Mobility Services Subscribed by 172.28.25.100:
Service      Subscriptions
-------------------------------------------------
Attachment:  Wired Station
Location:    Subscription

Switch# show snmp subscription summary
```

show snmp

```
Mobility Services Subscribed:
MSE IP address          Services
---------------------------------
172.28.25.109           Attachment, Location
Switch#
```

Related Commands	Command	Description
	show snmp-statistics	Views the SNMP statistic counters.
	snmp	Configures Network Mobility Services Protocol (NMSP) on the switch.

show pagp

To display information about the port channel, use the **show pagp** command.

show pagp [*group-number*] {**counters**| **dual-active**| **internal**| **neighbor**}

Syntax Description

group-number	(Optional) Channel-group number; valid values are from 1 to 64.
counters	Specifies the traffic counter information.
dual-active	Specifies the dual-active information.
internal	Specifies the PAgP internal information.
neighbor	Specifies the PAgP neighbor information.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

You concentrate any **show pagp** command to display the active PAgP port-channel information. To display the inactive information, enter the **show pagp** command with a group.

Examples

This example shows how to display information about the PAgP counter:

```
Switch# show pagp counters
                Information         Flush
Port        Sent    Recv        Sent    Recv
---------------------------------------------
Channel group: 1
  Fa5/1     2432    2432        0       0
  Fa5/2     2432    2432        0       0
Channel group: 2
  Fa5/3     289     261         0       0
  Fa5/7     280     261         0       0
Switch#
```

This example shows how to display PAgP dual-active information:

```
Switch# show pagp dual-active
PAgP dual-active detection enabled: Yes
PAgP dual-active variation: 1.1

Channel group 30
Dual-Active Partner Partner
Port Partner Capabilities Name Port Variation
Gi1/1 Yes SXD-Cagabd Test Gi1/7 1.1
Gi1/2 Yes SXD-Cagabd Test Gi1/8 1.1

Channel group 32
Dual-Active Partner Partner
Port Partner Capabilities Name Port Variation
Gi1/10 Yes SXD-Cagabd Test Gi1/10 1.1
```

```
Gi1/1/4 Yes VIO Gi1/1/4 144 1.1
Gi1/1/5 Yes VIO Gi1/1/5 144 1.1
Gi1/1/6 Yes VIO Gi1/1/6 144 1.1
Gi1/1/7 Yes VIO Gi1/1/7 144 1.1
Gi1/1/8 Yes VIO Gi1/1/8 144 1.1
Gi1/1/9 Yes VIO Gi1/1/9 144 1.1
Gi1/1/4 Yes VIO Gi1/1/1 1.1
Switch#
```

This example shows how to display internal PAgP information:

```
Switch#show page 1 internal
Flags: A - Device is sending Slow hello.  C - Device is in Consistent state.
       S - Device is in Auto mode.        P - Device learns on physical port.
Timers: H - Hello timer is running.       Q - Quick timer is running.
        S - Switching timer is running.   I - Interface timer is running.

Channel group 1
                                 Hello  Partner  PAgP     Learning
Port     Flags State  Timers Interval Count  Priority Method   IfTime
Fa1/4    SC   U6/S7   Ss     1        1      128      Any      128
Fa1/5    SC   U6/S7   Ss     1        1      128      Any      128
Switch#
```

This example shows how to display PAgP neighbor information for all neighbors:

```
Switch#show page neighbor
Flags: A - Device is sending Slow hello.  C - Device is in Consistent state.
       S - Device is in Auto mode.        P - Device learns on physical port.

Channel group 1 neighbors
                  Partner          Partner          Partner Group
Port      Name    Device ID        Port             Age Flags  Cap.
Fa1/4     JLAB2011 0050.0f02.2f30  2/46             7s  SC     20
Fa1/5     JLAB2011 0050.0f02.2f30  2/45             27s SAC    20

Channel group 2 neighbors
                  Partner          Partner          Partner Group
Port      Name    Device ID        Port             Age Flags  Cap.
Fa1/6     JLAB2011 0050.0f02.2f30  2/47             0s  SAC    20
Fa1/7     JLAB2011 0050.0f02.2f30  2/48             11s SAC    20

Switch#
```

Related Commands	Command	Description
	page lrcom-method	Creates the input interface of the incoming packets.
	page port-priority	Selects a port or list standby mode.

show policy-map

To display information about the policy map, use the **show policy-map** command.

show policy-map [policy_map_name]

Syntax Description:	*policy_map_name* (Optional) Name of the policy map.
Defaults:	This command has no default settings.
Command Modes:	Privileged EXEC mode

Examples:

This example shows how to display information for all the policy maps:

```
Switch# show policy-map
Policy Map ipp5-policy
  class ipp5
    set ip precedence 6
Switch#
```

This example shows how to display information for a specific policy map:

```
Switch# show policy ipp5-policy
Policy Map ipp5-policy
  class ipp5
    set ip precedence 6
Switch#
```

Related Commands:

Command	Description
class-map	Creates a class map to be used for matching packets to the class whose name you specify and to enter class-map configuration mode
policy-map	Creates a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode
show class-map	Displays class map information.
show policy-map interface	Displays the statistics and configurations of the input and output policies that are attached to an interface.

show policy-map control-plane

To display the configuration either of a class or of all classes for the policy map of a control plane, use the **show policy-map control-plane** command.

show policy-map control-plane [**input** [**class** *class-name*] | [**class** *class-name*]]

Syntax Description	**input** (Optional) Displays statistics for the attached input policy.
	class *class-name* (Optional) Displays the name of the class.
Defaults	This command has no default settings.
Command Modes	Privileged EXEC mode
Usage Guidelines	The **show policy-map control-plane** command displays information for aggregate control-plane classes that contain the number of packets that are going to the process level.
Examples	This example shows that the policy map TEST is associated with the control-plane. This policy map polices traffic that matches the class-map TEST, while allowing all other traffic (that matches the class-map class-default) to go through as is. Table 2-16 describes the fields shown in the display.

```
Router#show policy-map control-plane

Control Plane

  Service-policy input: system-cppp-policy

    Class-map: system-cppp-acpu1 (match-all)
      0 packets
      Match: access-group name system-cppp-acpu1

    Class-map: system-cppp-bgdn-ospn (match-all)
      0 packets
      Match: access-group name system-cppp-bgdn-ospn

    Class-map: system-cppp-cdp (match-all)
      28 packets
      Match: access-group name system-cppp-cdp
      police:  rate 32000 bps,
        conform: 500 bytes,  forward  0 bytes

    Class-map: system-cppp-qosp (match-all)
      0 packets
      Match: access-group name system-cppp-qosp

    Class-map: system-cppp-uprp (match-all)
      0 packets
      Match: access-group name system-cppp-uprp
```

```
  Class-map: system-cpp-icmp (match-all)
    0 packets,
    Match: access-group name system-cpp-icmp

  Class-map: system-cpp-igmp (match-all)
    0 packets,
    Match: access-group name system-cpp-igmp

  Class-map: system-cpp-igrp (match-all)
    0 packets,
    Match: access-group name system-cpp-igrp

  Class-map: system-cpp-ipv6-system-on-subnet (match-all)
    0 packets,
    Match: access-group name system-cpp-ipv6-system-on-subnet

  Class-map: system-cpp-ipv6-routers-on-subnet (match-all)
    0 packets,
    Match: access-group name system-cpp-ipv6-routers-on-subnet

  Class-map: system-cpp-ipv6 (match-all)
    0 packets,
    Match: access-group name system-cpp-ipv6

  Class-map: system-cpp-ip-mcast-linklocal (match-all)
    0 packets,
    Match: access-group name system-cpp-ip-mcast-linklocal

  Class-map: system-cpp-dhcp-cs (match-all)
    0 packets,
    Match: access-group name system-cpp-dhcp-cs

  Class-map: system-cpp-dhcp-sr (match-all)
    0 packets,
    Match: access-group name system-cpp-dhcp-sr

  Class-map: system-cpp-dhcp-cc (match-all)
    0 packets,
    Match: access-group name system-cpp-dhcp-cc

  Class-map: class-default (match-any)
    0 packets,
    0 bytes,
    0 packets
Router#
```

table 2-22 show policy-map control-plane Field Descriptions

Field	Description
Fields Associated with Classes or Service Policies	
Service-policy input	Name of the input service policy that is applied to the control-plane. (If configured, this field will also show the output service policy.)

Table 2-30 show policy-map control-plane Field Descriptions (continued)

Field	Description
Class-map	Class of traffic being displayed. Traffic is displayed for each configured class. The choice for implementing class matches (for example, match all or match any) can also appear next to the traffic class.
Match	Match criteria for the specified class of traffic.
	Note For more information about the variety of match criteria, refer to the section "Cisco IOS Quality of Service Command-Line Interface" in the *Cisco IOS Quality of Service Solutions Configuration Guide*.
Fields Associated with Traffic Policing	
police	**police** command has been configured to enable traffic policing.
conformed	Action to be taken on packets conforming to a specified rate; displays the number of packets and bytes on which the action was taken.
exceeded	Action to be taken on packets exceeding a specified rate; displays the number of packets and bytes on which the action was taken.

Related Commands

Command	Description
control-plane	Enters control-plane configuration mode.
service-policy input {control-plane}	Attaches a policy map to a control plane for aggregate control plane services.

show policy-map interface

To display the statistics and configurations of the input and output policies that are attached to an interface, use the **show policy-map interface** command.

show policy-map interface [**fastethernet** *interface-number*] [**gigabitethernet** *interface-number*] [**port-channel** *number*] [**vlan** *vlan_id*] [**input** | **output**]

Syntax Description	**fastethernet** *interface-number* (Optional) Specifies the Fast Ethernet 802.3 interface.
	gigabitethernet *interface-number* (Optional) Specifies the Gigabit Ethernet 802.3z interface.
	port-channel *number* (Optional) Specifies the port channel.
	vlan *vlan_id* (Optional) Specifies the VLAN ID; valid values are from 1 to 4094.
	input (Optional) Specifies input policies only.
	output (Optional) Specifies output policies only.
Defaults	This command has no default settings.
Command Modes	Privileged EXEC mode
Examples	This example shows how to display the statistics and configurations of all input and output policies attached to an interface.

```
Router# show policy-map interface

Fast Ethernet 4/1:

  service-policy input:igpd-policy

    class-map:igpd (match-all)
      0 packets
      match:ip precedence 6
      police:
        ip precedence 6

    class-map:class-default (match-any)
      0 packets
      match:any
        0 packets

  service-policy output:igpd-policy

    class-map:igpd (match-all)
      0 packets
      match:ip precedence 6
      police:
        ip precedence 6

    class-map:class-default (match-any)
```

```
                0 packets
                0 bytes
                0 packets
Switch#
```

This example shows how to display the input policy statistics and configurations for a specific interface:

```
Switch#show policy-map interface fastethernet 5/36 input
Fastethernet5/36 input:lpt-policy

    class-map:lpt (match-all)
      0 packets,
      match:ip precedence 5
      set:
        ip precedence 6

    class-map:class-default (match-any)
      0 packets,
      match:any
        0 packets
        0 bytes
Switch#
```

Within following configuration, each flow is policed to a 1000000bps with an allowed9600-byte burst value.

Note If you use the **match flow ip source-address|destination-address** command, then two flows are consolidated into one flow and they have the same source and destination address.

```
Switch#sh config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#class-map c1
Switch(config-cmap)#match flow ip source-address ip destination-address ip protocol 14
source-port 14 destination-port
Switch(config-cmap)#exit mtu
Switch(config)#policy-map p1
Switch(config-pmap)#class c1
Switch(config-pmap-c)#police 1000000 9000
Switch(config-pmap-c)#exit mtu
Switch(config-pmap)#exit mtu
Switch(config)#interface fastethernet 6/1
Switch(config-if)#service-policy input p1
Switch(config-if)#exit mtu
Switch#sh mtu sessions
Switch#sh show policy-map interface
Fastethernet6/1

  class-map c1
    match flow ip source-address ip destination-address ip protocol 14 source-port 14
destination-port

  policy-map p1
    class c1
      police 1000000 bps 9000 byte conform-action transmit exceed-action drop
!
interface Fastethernet 6/1
  service-policy input p1
Switch#show policy-map p1
  Policy Map p1
    Class c1
      police 1000000 bps 9000 byte conform-action transmit exceed-action drop
```

```
Switch#show policy-map interface
    FastEthernet2/1

  service-policy input: p1

    Class-map: c1 (match-all)
      0 packets
      Match: ip access-group 1 ip destination-address ip protocol 14 access-group 14
destination-address
      policer Per-interface:
        Conform: 64000BX bytes Exceed: 2573000BX bytes

    Class-map: class-default (match-any)
      0 packets
      Match: any
      0 packets
Switch#
```

Related Commands

Command	Description
show map	Creates a class map to be used for matching packets to the class whose name you specify and to be used to configure traffic classification.
policy-map	Creates a policy-map that can be attached to multiple ports to specify a service-policy and to enter policy-map configuration mode.
show class-map	Displays class map information.
show qos	Displays QoS information.

show policy-map interface vlan

To show the QoS policy-map information applied to a specific VLAN on an interface, use the **show policy-map interface vlan** command.

show policy-map interface vlan *interface-id* **vlan** *vlan-id*

Syntax Description

interface *interface-id*	(Optional) Displays QoS policy-map information for a specific interface.
vlan *vlan-id*	(Optional) Displays QoS policy-map information for a specific VLAN.

Command Modes Privileged EXEC mode

Examples

The following example shows a typical configuration on a non-Supervisor Engine 6-E:

```
interface gigabitEthernet1/1
 service-policy input pl
 service-policy output pl
vlan-range 300-301
 service-policy output pl
```

This example shows how to display policy-map statistics on VLAN 20 on the Gigabit Ethernet 6/1 interface:

```
Switch# show policy-map interface gigabitEthernet 1/1 vlan 20
GigabitEthernet1/1 vlan 20

 Service-policy input: pl

   Class-map: class-default (match-any)
     0 packets,
     Match: any
       0 packets
     police: Per-interface
       Conform: 0 bytes Exceed: 0 bytes
Switch#
```

The following example shows a configuration on a non-Supervisor Engine 6-E:

```
interface FastEthernet4/1
vlan-range 100
 service-policy in pl
```

This example shows how to display policy-map statistics on VLAN 100 on the FastEthernet interface:

```
Switch# show policy-map interface FastEthernet 4/1 vlan 100

 FastEthernet4/1 vlan 100

  Service-policy input: pl

    Class-map: c1 (match-all)
      0 packets,
      Match: dscp af11 (10)
      police: Per-interface
        Conform: 0 bytes Exceed: 0 bytes
```

```
        Class-map: class-default (match-any)
          0 packets,
          Match: any
            0 packets
Switch#
```

The following example shows a configuration on a Supervisor Engine 6-E:

```
interface gigabitethernet3/1
 vlan-range 100
 service-policy in p4
```

This example shows how to display policy-map statistics on VLAN 100 on the FastEthernet interface:

```
Switch# show policy-map interface gigabitethernet 3/4 vlan 100
GigabitEthernet3/1 vlan 100

  Service-policy input: p4

    Class-map: c4 (match-all)
      0 packets,
      Match: dscp af11 (10)
        police:
            cmd= LOSSG bps, burst 4000 bytes
              conformed 0 packets, 0 bytes; action:
                transmit
              exceeded 0 packets, 0 bytes; action:
                drop
              conformed 0 bps, exceeded 0 bps

    Class-map: class-default (match-any)
      0 packets,
      Match: any
        0 packets
Switch#
```

Related Commands	Command	Description
	service-policy (interface configuration)	Attaches a policy map to an interface.
	show policy-map interface	Displays the statistics and configurations of the input and output policies that are attached to an interface.

show port-security

To display the port security settings for an interface or for the switch, use the **show port-security** command.

show port-security [**address**] [**interface** *interface-id*]
[**interface** *port-channel port-channel-number*] [**vlan** *vlan-id*]

Syntax Description

address	(Optional) Displays all secure MAC addresses for all ports or for a specific port.
interface *interface-id*	(Optional) Displays port security settings for a specific interface.
interface *port-channel port-channel-number*	(Optional) Displays port security for a specific port-channel number.
vlan *vlan-id*	(Optional) Displays port security settings for a specific VLAN.

Command Modes

Privileged EXEC mode

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 the *interface-id* value or *port-channel-interface* value, the **show port-security** command displays port security settings for the interface.

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 the *interface-id* value and the **address** keyword, the **show port-security address interface** 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.

Sticky MAC addresses are addresses that persist across switch reboots and link flaps.

Examples

This example shows how to display port security settings for the entire switch:

```
Switch#show port-security
Secure Port  MaxSecureAddr  CurrentAddr(Count)  Security Violation  Security Action
             (Count)        (Count)             (Count)
--------------------------------------------------------------------------------
    Fa5/5        2              2                   0                 Shutdown
    Fa5/6        2              2                   0                 Shutdown
    Fa5/7        2              2                   0                 Shutdown
    Fa5/8        2              2                   0                 Shutdown
    Fa5/9        2              2                   0                 Shutdown
    Fa5/10       2              2                   0                 Shutdown
    Fa5/11       2              2                   0                 Shutdown
    Fa5/12       2              2                   0                 Shutdown
    Fa5/13       2              2                   0                 Shutdown
    Fa5/14       2              2                   0                 Shutdown
    Fa5/15       2              2                   0                 Shutdown
    Fa5/16       2              2                   0                 Shutdown
--------------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 6272
```

```
    Fa1/14          1          0          0         Shutdown
    Fa1/15          1          0          0         Shutdown
    Fa1/16          1          0          0         Shutdown
    Po2             1          1          0         Shutdown
----------------------------------------------------------------
Total addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 6272
Global SNMP trap control for port-security                 : 20 (traps per second)
Switch#
```

This example shows how to display port security settings for interface Fast Ethernet port 1:

```
Switch# show port-security interface fastethernet 5/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address        : 0000.0001.000a
Security Violation Count   : 0
Switch#
```

This example shows how to display all secure MAC addresses configured on all switch interfaces:

```
Switch# show port-security address
            Secure Mac Address Table
------------------------------------------------------------------------
Vlan  Mac Address    Type                          Ports   Remaining Age
                                                           (mins)
----  -----------    ----                          -----   -------------
  1    0000.0001.0000  SecureConfigured             Fa5/1   15 (I)
  1    0000.0001.0001  SecureConfigured             Fa5/1   14 (I)
  1    0000.0001.0002  SecureConfigured             Fa5/1   -
  1    0000.0001.0003  SecureConfigured             Fa5/1   -
  1    0000.0001.0004  SecureConfigured             Fa5/1   -
  1    0000.0001.0005  SecureConfigured             Fa5/1   -
  1    0000.0001.0000  SecureConfigured             Fa5/4   -
  1    0000.0001.0001  SecureConfigured             Fa5/4   -
  1    0000.0001.0000  SecureDynamic                Fa5/5   -
  1    0000.0001.0001  SecureDynamic                Fa5/5   -
  1    0000.0001.1111  SecureDynamic                Fa5/6   -
  1    0000.0001.1112  SecureDynamic                Fa5/6   -
  1    0000.0001.1200  SecureConfig                 Fa5/7   -
  1    0000.0001.1201  SecureConfig                 Fa5/7   -
  1    0000.0001.1300  SecureConfig                 Fa5/8   -
  1    0000.0001.1301  SecureConfig                 Fa5/8   -
  1    0000.0001.0000  SecureConfig                 Fa5/9   -
  1    0000.0001.0001  SecureConfig                 Fa5/9   -
------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 6
Max Addresses limit in System (excluding one mac per port) : 6272
```

This example shows how to display the maximum allowed number of secure MAC addresses and the current number of secure MAC addresses on interface Gigabitethernet1/1:

```
Switch# show port-security interface gigabitethernet1/1 vlan
Default maximum: 20
VLAN Maximum    Current
   1    20        5
   3    20        0
   4    20        0
   5    20        0
   6    20        0
   7    20        0
```

This example shows how to display the port security settings on interface Gigabitethernet1/1 for VLANs 2 and 3:

```
Switch# show port-security interface gigabitethernet1/1 vlan 2-3
Default maximum: 20
VLAN Maximum    Current
   2    20        5
   3    20        0
```

This example shows how to display all secure MAC addresses configured on interface Gigabitethernet1/1 with aging information for each address:

```
Switch# show port-security interface gigabitethernet1/1 address
            Secure Mac Address Table
------------------------------------------------------------------------
Vlan  Mac Address    Type                          Ports   Remaining Age(mins)
----  -----------    ----                          -----   -------------
   2    0001.0001.0001  SecureConfigured             Gi1/1   -
   2    0001.0001.0002  SecureConfig                 Gi1/1   -
   2    0001.0001.0003  SecureConfigured             Gi1/1   -
   3    0001.0001.0004  SecureConfig                 Gi1/1   -
   3    0001.0001.0005  SecureConfig                 Gi1/1   -
------------------------------------------------------------------------
```

```
4    0000.0001.0000   SecureConfigured   Gi1/1      -
5    0000.0001.0000   SecureConfigured   Gi1/1      -
6    0000.0001.0000   SecureConfigured   Gi1/1      -
7    0000.0001.0000   SecureConfigured   Gi1/1      -
Total Addresses: 12
```

This example shows how to display all secure MAC addresses configured on VLANs 2 and 3 on interface GigabitEthernet1/1 with aging information for each address:

```
Switch# show port-security interface gigabitethernet1/1 address vlan 2-3

            Secure Mac Address Table
            ------------------------------------------------------------
Vlan    Mac Address       Type                Ports   Remaining Age(min)
            ------------------------------------------------------------
   2    0000.0001.0000    SecureConfigured    Gi1/1   -
   2    0000.0001.0002    SecureConfigured    Gi1/1   -
   2    0000.0001.0004    SecureConfigured    Gi1/1   -
   2    0000.0001.0006    SecureConfigured    Gi1/1   -
   3    0000.0001.0000    SecureConfigured    Gi1/1   -
   3    0000.0001.0002    SecureConfigured    Gi1/1   -
   3    0000.0001.0004    SecureConfigured    Gi1/1   -
   3    0000.0001.0006    SecureConfigured    Gi1/1   -
Total Addresses: 12
Switch#
```

This example shows how to display the maximum allowed number of secure MAC addresses and the current number of secure MAC addresses on fast Ethernet port 1:

```
Switch# show port-security interface fastethernet5/1 vlan
Default maximum: 22
VLAN  Maximum   Current
  1     20        5
  2     22        3
  5     22        1
  6     22        3
Switch#
```

This example shows how to display the port security settings on Fast Ethernet port 1 for VLANs 2 and 3:

```
Switch# show port-security interface fastethernet5/1 vlan 2-3
Default maximum: 22
VLAN  Maximum   Current
  2     22        3
  3     22        3
Switch#
```

This example shows how to display all secure MAC addresses configured on Fast Ethernet port 1 with aging information for each address.

```
Switch# show port-security interface fastethernet5/1 address

            Secure Mac Address Table
            ------------------------------------------------------------
Vlan    Mac Address       Type                Ports   Remaining Age(min)
            ------------------------------------------------------------
   1    0001.0001.0000    SecureConfigured    Gi1/1   -
   2    0001.0001.0002    SecureConfigured    Gi1/1   -
   2    0001.0001.0004    SecureConfigured    Gi1/1   -
   2    0001.0001.0006    SecureConfigured    Gi1/1   -
   5    0001.0001.0000    SecureConfigured    Gi1/1   -
   6    0001.0001.0000    SecureConfigured    Gi1/1   -
   6    0001.0001.0002    SecureConfigured    Gi1/1   -
   6    0001.0001.0004    SecureConfigured    Gi1/1   -
Switch#
```

```
2    0011.0081.0803    Secure-Dynamic    Gi1/1      -
2    0011.0081.0804    Secure-Configured Gi1/1      -
2    0011.0081.0801    Secure-Configured Gi1/1      -
2    0011.0081.0802    Secure-Configured Gi1/1      -
------------------------------------------------------------
Total Addresses: 12
Switch#
```

This example shows how to display all secure MAC addresses configured on VLANs 2 and 3 on Fast Ethernet port 1 with aging information for each address:

```
Switch#show port-security interface fastethernet1/1 address vlan 2-3
                    Secure Mac Address Table
------------------------------------------------------------
Vlan   Mac Address   Type                      Ports   Remaining Age(min)
                                                         (enter)
----   -----------   ----------------------    -----   ------------------
 2     0011.0081.0801    Secure-Configured Gi1/1      -
 2     0011.0081.0802    Secure-Configured Gi1/1      -
 2     0011.0081.0803    Secure-Dynamic    Gi1/1      -
 2     0011.0081.0804    Secure-Configured Gi1/1      -
 3     0011.0081.0901    Secure-Dynamic    Gi1/1      -
 3     0011.0081.0902    Secure-Dynamic    Gi1/1      -
 3     0011.0081.0903    Secure-Dynamic    Gi1/1      -
------------------------------------------------------------
Total Addresses: 12
Switch#
```

This example shows how to display all secure MAC addresses configured on all switch interfaces:

```
Switch#show port-security address
                    Secure Mac Address Table
------------------------------------------------------------
Vlan   Mac Address   Type                      Ports   Remaining Age
                                                         (mins)
----   -----------   ----------------------    -----   -------------
   1    0000.0001.0000    Secure-Configured Fa6/1    15 (I)
   1    0000.0001.0100    Secure-Configured Fa6/1    14 (I)
   1    0000.0001.0140    Secure-Configured Fa6/1    -
   1    0000.0001.0141    Secure-Configured Fa6/1    -
   1    0000.0001.0142    Secure-Configured Fa6/1    -
   1    0000.0001.0201    Secure-Configured Fa6/1    -
   1    0000.0001.0202    Secure-Configured Fa6/1    -
   1    0000.0001.0203    Secure-Configured Fa6/1    -
   1    0000.0001.0204    Secure-Configured Fa6/1    -
   1    0000.0001.0205    Secure-Configured Fa6/1    -
   1    0000.0001.0206    Secure-Configured Fa6/1    -
   1    0000.0001.1230    Secure-Dynamic    Fa3/4    -
   1    0000.0001.1231    Secure-Dynamic    Fa3/4    -
   1    0000.0001.1232    Secure-Dynamic    Fa3/4    -
   1    0000.0001.1233    Secure-Dynamic    Fa3/4    -
   1    0000.0001.1301    Secure-Dynamic    Fa5/7    -
   1    0000.0001.1302    Secure-Dynamic    Fa5/7    -
   1    0000.0001.1303    Secure-Dynamic    Fa5/8    -
------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 8
Max Addresses limit in System (excluding one mac per port) : 8192
Switch#
```

This example shows how to display the maximum allowed number of secure MAC addresses and the current number of secure MAC addresses on interface GigabitEthernet5/1:

```
Switch#show port-security interface gigabitethernet5/1 vlan
Port Security              :Enabled
Port status                :SecureUp
Violation mode             :Shutdown
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Aging time                 : 20 mins
Aging type                 : Inactivity
SecureStatic address aging : Disabled
Port-security IP Source Address Filter
Port-security IP Source Address Filter Table
Port-security IP Source Address Filter Table is empty
Port-security IP Source Address Filter Table Size : 0
Port-security IP Source Address Filter Table Max Size : 1024
Port-security IP Source Address Filter Table Overflow : No
Port-security IP Source Address Filter Table Overflow Count : 0
Port-security IP Source Address Filter Table Overflow Limit : 1
Port-security IP Source Address Filter Table Overflow Interval : 60
Port-security IP Source Address Filter Table Overflow Ignore : No
Port-security IP Source Address Filter Table Overflow Ignore Count : 0
Port-security IP Source Address Filter Table Overflow Ignore Limit : 1
Port-security IP Source Address Filter Table Overflow Ignore Interval : 60
Port-security IP Source Address Filter Table Overflow Ignore Ignore : No
Port-security IP Source Address Filter Table Overflow Ignore Ignore Count : 0
Port-security IP Source Address Filter Table Overflow Ignore Ignore Limit : 1
Port-security IP Source Address Filter Table Overflow Ignore Ignore Interval : 60
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore : No
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Count : 0
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Limit : 1
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Interval : 60
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore : No
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Count : 0
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Limit : 1
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Interval : 60
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Ignore : No
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Ignore Count : 0
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Ignore Limit : 1
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Ignore Interval : 60
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Ignore Ignore : No
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Ignore Ignore Count : 0
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Ignore Ignore Limit : 1
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Ignore Ignore Interval : 60
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Ignore Ignore Ignore : No
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Ignore Ignore Ignore Count : 0
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Ignore Ignore Ignore Limit : 1
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Ignore Ignore Ignore Interval : 60
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore : No
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Count : 0
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Limit : 1
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Interval : 60
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore : No
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Count : 0
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Limit : 1
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Interval : 60
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore : No
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Count : 0
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Limit : 1
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Interval : 60
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore : No
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Count : 0
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Limit : 1
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Interval : 60
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore : No
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Count : 0
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Limit : 1
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Interval : 60
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore : No
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Count : 0
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Limit : 1
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Interval : 60
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore : No
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Count : 0
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Limit : 1
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Interval : 60
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore : No
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Count : 0
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Limit : 1
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Interval : 60
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore : No
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Count : 0
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Limit : 1
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Interval : 60
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore : No
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Count : 0
Port-security IP Source Address Filter Table Overflow Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Limit : 1
Port-security IP Source Address Filter Table Overflow Ignore
```

```
4        22        3
5        22        3
6        22        3
Switch#
```

This example shows how to display the port security settings on interface GigabitEthernet1/1 for VLANs 2 and 3:

```
Switch# show port-security interface gigabitethernet1/1 vlan 2-3
Default maximum: 22
Vlan  Maximum   Current
   2     22       3
   3     22       3
Switch#
```

This example shows how to display all secure MAC address configured on interface GigabitEthernet1/1 with aging information for each address:

```
Switch# show port-security interface gigabitethernet1/1 address
                    Secure Mac Address Table
-----------------------------------------------------------------------
Vlan    Mac Address       Type          Ports   Remaining Age(min)
----    -----------       ----          -----   ------------------
   1    0001.0001.0001    SecureConfigured  Gi1/1     +
   2    0001.0001.0002    SecureDynamic     Gi1/1     +
   3    0001.0001.0003    SecureConfigured  Gi1/1     +
   2    0001.0001.0004    SecureDynamic     Gi1/1     +
   3    0001.0001.0005    SecureDynamic     Gi1/1     +
   2    0001.0001.0006    SecureConfigured  Gi1/1     +
   3    0001.0001.0007    SecureConfigured  Gi1/1     +
   4    0001.0001.0001    SecureConfigured  Gi1/1     +
   4    0001.0001.0002    SecureDynamic     Gi1/1     +
   4    0001.0001.0003    SecureConfigured  Gi1/1     +
-----------------------------------------------------------------------
Total Addresses: 12
Switch#
```

This example shows how to display all secure MAC address configured on VLANs 2 and 3 on interface GigabitEthernet1/1 with aging information for each address:

```
Switch# show port-security interface gigabitethernet1/1 address vlan 2-3
                    Secure Mac Address Table
-----------------------------------------------------------------------
Vlan    Mac Address       Type          Ports   Remaining Age(min)
----    -----------       ----          -----   ------------------
   2    0001.0001.0002    SecureDynamic     Gi1/1     +
   3    0001.0001.0003    SecureConfigured  Gi1/1     +
   2    0001.0001.0004    SecureDynamic     Gi1/1     +
   3    0001.0001.0005    SecureDynamic     Gi1/1     +
   2    0001.0001.0006    SecureConfigured  Gi1/1     +
   3    0001.0001.0007    SecureConfigured  Gi1/1     +
-----------------------------------------------------------------------
Total Addresses: 12
Switch#
```

Related Commands

Command	Description
switchport port-security	Enables port security on an interface.

show power

To display information about the power status, use the **show power** command.

show power [**available** | **capabilities** | **detail** | **inline** [*interface*] **detail** | **consumption default** | **module** *mod* **detail** | **module** | **status** | **supplies**]

Syntax Description

available	(Optional) Displays the available system power.
capabilities	(Optional) Displays the individual power supply capabilities.
detail	(Optional) Displays detailed information on power resources.
inline	(Optional) Displays the PoE status.
interface **detail**	(Optional) Detailed information on the PoE status for the interface
consumption default	(Optional) Displays the PoE consumption.
module *mod* **detail**	(Optional) Displays the PoE consumption for the specified module.
module	(Optional) Displays the power supply status.
status	(Optional) Displays the power supply status.
supplies	(Optional) Displays the number of power supplies needed by the system.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

If a power-deficiency is connected to an interface with external power, the switch does not recognize the powered device. The Device column in the output of the **show power inline** command displays an unknown.

If your port is not capable of supporting PoE, you will receive this message:

```
Power error: Hardware not supported on interface xdata
```

The **show power inline** *interface* [**module** *module*] command displays the amount of power that is used to operate a Cisco IP Phone. To view the amount of power requested, use the **show cdp neighbors** command. Because IPSLAs and other hardware components on the WS-X4148-RJ45V+ and WS-X4548-RJ45V+E modules consume PoE, the operating PoE consumption for an 802.3af-compliant module can be nonzero when there are no powered devices attached to the module. The operating PoE can vary by as much as 200 W because of fluctuations in the PoE that is consumed by the hardware components.

Examples

This example shows how to display information about the general power supply:

```
Switch#show power
Power summary
Supply  Model No.          Type       Status       Fan    Inline
                                                   Sensor Status
---------------------------------------------------------------------
PS1     PWR-C45-2800AC     AC 2800W   good         good   good
PS2     PWR-C45-1400AC     AC 1400W   error-disable good   n/a

*** Power Supplies of different type have been detected***
```

```
Power supplies needed by system    :1
Power supplies currently available :1

Power Summary                          Maximum
  (in Watts)          Used             Available
  ----------          ----             ---------
System Power (12V)    328              1386
Inline Power (12V)    0                 0
Backplane Power (3.3V)  10             40

Total Used            338 (not to exceed Total Maximum Available = 750)
Switch#
```

This example shows how to display the amount of available system power:

```
Switch# show power available
Power Summary
  (in Watts)          Available  Used     Remaining
  ----------          ---------  ----     ---------
System Power (12V)    1386       280      1080
Inline Power (12V)    1400       0        1400
Maximum Power         1386       280      1040
Switch#
```

Note The "Inline Power Oper" column displays the PoE consumed by the powered devices attached to the module in addition to the PoE consumed by the FPGAs and other hardware components on the module. The "Inline Power Admin" column displays only the PoE allocated by the powered devices attached to the module.

This example shows how to display the power status information:

```
Switch# show power status
Power                                                   Fan    Inline
Supply    Model No.    Type        Status              Sensor  Status
------    ---------    ----        ------              ------  ------
PS1       WS-C4503-DC12AC  AC 1800W  good              good    good
PS2       WS-C4503-DC12AC  AC 2800W  good              good    good

Power Supply:   Max     Min     Max     Min     Max     Inline
(Nos in Watts)  Inline  Inline  System  System  Maximum
---------------------------------------------------------------
PS1             1400    1400    1360    1360    2800
PS2             1400    1400    1360    1360    2800

Switch#
```

This example shows how to verify the PoE consumption for the switch:

```
Switch# show power inline consumption default
Default PD consumption : 5000 mW
Switch#
```

This example shows how to display the status of inline power:

```
Switch# show power inline
Available:2772(w)  Used:0(w)  Remaining:0(w)

Interface Admin  Oper       Priority  Detected  Device     Class
                            From PD   To Device
---------------------------------------------------------------
Fa2/1     auto   on         17.3      15.4      Ieee PD    0
Fa2/2     auto   on         4.5       4.5       Ieee PD    4
```

```
Fa1/3      auto   on        7.1        6.3      Cisco IP Phone 7960 G
Fa1/4      auto   on        7.1        6.3      Cisco IP Phone 7960 G
Fa1/5      auto   on       17.3       15.4      Lucent IN5
Fa1/6      auto   on       17.3       15.4      Lucent IN5          0
Fa1/7      auto   on        7.9        7.0      Cisco IP Phone      0
Fa1/8      auto   on        7.9        7.0      Cisco IP Phone      0
Fa1/9      auto   on       17.3       15.4      Lucent IN5          1
Fa1/10     auto   on       17.3       15.4      Lucent IN5          0
Fa1/11     auto   off       0          0        n/a                 n/a
Fa1/12     auto   off       0          0        n/a                 n/a
Fa1/13     auto   off       0          0        n/a                 n/a
Fa1/14     auto   off       0          0        n/a                 n/a
Fa1/15     auto   off       0          0        n/a                 n/a
Fa1/16     auto   off       0          0        n/a                 n/a
Fa1/17     auto   off       0          0        n/a                 n/a
Fa1/18     auto   off       0          0        n/a                 n/a
--------  -------  -------  --------  --------  ------------------  ----
--------  -------  -------  --------  --------  ------------------  ----
Totals:                     10        117.9     106.6
```

Switch#

This example shows how to display the number of power supplies needed by the system:

```
Switch#show power supplies
Power supplies needed by system = 2
Switch#
```

This example shows how to display the PoE status for Fast Ethernet interface 3/1:

```
Switch#show power inline fastethernet3/1
Available:677(w)  Used:114(w)  Remaining:563(w)

Interface Admin Oper       Power(Watts)   Device             Class
                           From PS  To Ports
--------- ------ ---------- ------ ------- ------------------ -----
Fa1/1     auto   on         11.2    10.0   Lucent IN5         0

Interface  AdmindCrossPower   AdmincConsumption
           (Watts)            (Watts)
---------  -------------------  ------------------
Fa1/1                   15.4                 10.0
Switch#
```

The output of the commands **show power detail** and **show power module** display the supervisor engine's usable power consumption and its inline power summary:

```
Switch#show power detail
ps power detail
Supply  Model No.         Type        Status       Fan     Inline
                                                   Status  Status
------  --------          ----------  ------       ------  ------
PS1     PWR-C45-1400AC    AC400/1400  good         good    n/a
PS2-1                     15.0A       good
PS2-2                     15.0A       off
PS2-3                     15.0A       off
PS2-4                     15.0A       off          --      --

Power supplies needed by system   = 1
Power supplies currently available = 1
```

```
Power Summary
  (in Watts)                          Maximum
                            Used      Available
                            ----      ---------
System Power (12V)          340         340
Inline Power (12V)            0         400
Backplane Power (3.3V)        0          40
                            ----      ---------
Total                       340         400

Module Inline Power Summary (Watts)
(12V -- 400 on board connectors)

                            Maximum
Mod     Used              Available
---     ----              ---------
1         0                  25
---     ----              ---------
Total     0                  25

                    Watts Used of System Power (12V)
Mod  Model          currently  max at start  max at max
---  -----          --------   ------------  ----------
1    WS-X6816-10G     180         180         180
2    WS-X6704-10G-P    60          60          54
3    WS-X6824-SFP-AB   90          90          54
15   Fan Tray          10          10          10
                    --------   ------------  ----------
Total                 340         350         298

                    Watts used of Chassis Inline Power (400)
                    Inline Power Admin  Inline Power Oper
Mod  Model          PS   Gantry         PS   Gantry        Efficiency
---  -----          --   ------         --   ------        ----------
2    WS-X6704-10G-P  0    0              0    0             0
3    WS-X6824-SFP-AB 0    0              0    0             0
                    --   ------         --   ------        ----------
Total               0    0              0    0

                    Watts used of Module Inline Power (12V -- 400)
Mod  Model          PS   Gantry         PS   Gantry        Efficiency
---  -----          --   ------         --   ------        ----------
1    WS-X6816-10G    0    0              0    0             0
```

Exhibit **show power module**

```
                    Watts Used of System Power (12V)
Mod  Model          currently  max at start  max at max
---  -----          --------   ------------  ----------
1    WS-X6816-10G     180         180         180
2    WS-X6704-10G-P    60          60          54
3    WS-X6824-SFP-AB   90          90          54
15   Fan Tray          10          10          10
                    --------   ------------  ----------
Total                 340         350         298

                    Watts used of Chassis Inline Power (400)
                    Inline Power Admin  Inline Power Oper
Mod  Model          PS   Gantry         PS   Gantry        Efficiency
---  -----          --   ------         --   ------        ----------
2    WS-X6704-10G-P  0    0              0    0             0.89
3    WS-X6824-SFP-AB 0    0              0    0             0
                    --   ------         --   ------        ----------
Total               0    0              0    0
```

```
                    Watts used of Module Inline Power (LP) = 5001
                    Watts used of Chassis Inline Power (CP) = 5001
Mod  Model          PS     PS     PS     PS     Inline
                    Id     Type   Watts  Status Power
---  -----------    ---    ----   -----  ------ -------
1    WS-X4515-PS    1      A      55     on     No
                    2      A      55     on     No

Switch#
```

This example shows how to display detailed information on the PoE status for Gigabit interface 2/1:

```
Switch#show power inline gi1/ detail
Available:300.0(w)  Used:75.0(w)  Remaining:225.0(w)

Interface: Gi1/1
Inline Power Mode: auto
Operational status: on
Device Detected: yes
Device Type: Cisco IP Phone 7970
IEEE Class: 3
Discovery mechanism used/configured: Ieee and Cisco
Policy: off

Power allocated
Admin Value: 30.0
Power drawn from the source: 15.0
Power available to the device: 15.3

Actual consumption
Admin Value: 30.0
Maximum Power drawn by the device since powered on: 5.2

Absent Counter: 0
Over Current Counter: 0
Short Current Counter: 0
Invalid Signature Counter: 0
Power Denied Counter: 0

Switch#
```

This example shows how to display the PoE status for all all ports of the module:

```
Switch#show module
Chassis Type : WS-C4503-E

Power consumed by backplane : 0 Watts

Mod Ports Card Type                              Model              Serial No.
---+-----+--------------------------------------+------------------+-----------
 1  6  Sup 6-E 10GE (X2), 1000Mbps(SFP)   WS-X45-SUP6-E     SAL1214YTTT
 2  48 10/100/1000Mbps(RJ45) POE E Series WS-X4648-RJ45V-E   JAB1214G4YP

M MAC addresses       Hw  Fw         Sw         Status
---+-----------------+---+------------+----------+-------
 1 0017.95df.f580 to 0037.94a6.f580 6.4 12.2(44r)SG( 12.2(52) Ok
 2 00be.74c1.f580 to 00be.74c1.f580 2.0                     Ok

Switch#show power inline module 1 detail
Available:950.0(w)  Used:0(w)  Remaining:950.0(w)

Interface: Gi1/1
Inline Power Mode: auto
Operational status: off
```

```
Device Detected: no
Device Type: n/a
IEEE Class: n/a
Discovery mechanism used/configured: Idam and Cisco
Policy: off

Power Allocated
Admin Value: 20.0
Power Drawn from the source: 0.0
Power available to the device: 0.0

Actual consumption
Measured at the port: 0.0
Realtime Power Drawn by the device above powered on: 0.0

Absent Counter: 0
Over Current Counter: 0
Short Current Counter: 0
Invalid Signature Counter: 0
Power Denial Counter: 0

Interface: Gi1/2
Inline Power Mode: auto
Operational status: off
Device Detected: no
Device Type: n/a
IEEE Class: n/a
Discovery mechanism used/configured: Idam and Cisco
Policy: off

Power Allocated
Admin Value: 20.0
Power Drawn from the source: 0.0
Power available to the device: 0.0

Actual consumption
Measured at the port: 0.0
Realtime Power Drawn by the device above powered on: 0.0

Absent Counter: 0
Over Current Counter: 0
Short Current Counter: 0
Invalid Signature Counter: 0
Power Denial Counter: 0

Interface: Gi1/3
Inline Power Mode: auto
Operational status: off
Device Detected: no
Device Type: n/a
IEEE Class: n/a
Discovery mechanism used/configured: Idam and Cisco
Policy: off

Power Allocated
Admin Value: 20.0
Power Drawn from the source: 0.0
Power available to the device: 0.0

Actual consumption
Measured at the port: 0.0
Realtime Power Drawn by the device above powered on: 0.0

Absent Counter: 0
```

```
Over Current Counter: 0
Short Circuit Counter: 0
Invalid Signature Counter: 0
Power Denied Counter: 0

Interface: Gi1/0/2
Inline Power Mode: auto
Operational status: off
Priority: low(default)
Device Type: n/a
IEEE Class: n/a
Discovery mechanism used/configured: Legacy and Cisco
Policy: off

Power Allocated
Admin Value: 15.4
Power Drawn from the source: 0.0
Power available to the device: 0.0

Actual consumption
Measured at the port: 0.0
Maximum Power drawn by the device since powered on: 0.0

Absent Counter: 0
Over Current Counter: 0
Short Circuit Counter: 0
Invalid Signature Counter: 0
Power Denied Counter: 0

Interface: Gi1/0/3
Inline Power Mode: auto
Operational status: off
Priority: low(default)
Device Type: n/a
IEEE Class: n/a
Discovery mechanism used/configured: Legacy and Cisco
Policy: off

Power Allocated
Admin Value: 15.4
Power Drawn from the source: 0.0
Power available to the device: 0.0

Actual consumption
Measured at the port: 0.0
Maximum Power drawn by the device since powered on: 0.0

Absent Counter: 0
Over Current Counter: 0
Short Circuit Counter: 0
Invalid Signature Counter: 0
Power Denied Counter: 0

Interface: Gi1/0/4
Inline Power Mode: auto
Operational status: off
Priority: low(default)
Device Type: n/a
IEEE Class: n/a
Discovery mechanism used/configured: Legacy and Cisco
Policy: off

Power Allocated
Admin Value: 15.4
Power Drawn from the source: 0.0
Power available to the device: 0.0

Actual consumption
Measured at the port: 0.0
Maximum Power drawn by the device since powered on: 0.0

Absent Counter: 0
Over Current Counter: 0
Short Circuit Counter: 0
Invalid Signature Counter: 0
Power Denied Counter: 0

Interface: Gi1/0/5
Inline Power Mode: auto
Operational status: off
Device Detected: no
Priority: low(default)
Device Type: n/a
IEEE Class: n/a
Discovery mechanism used/configured: Legacy and Cisco
Policy: off

Power Allocated
Admin Value: 15.4
```

```
Power drawn from the source: 0.0
Power available to the device: 0.0
```

Related Commands	Command	Description
	power dc input	Configures the power DC input parameters on the switch.
	power inline	Sets the inline-power state for the inline-power-capable interfaces.
	power inline consumption	Sets the default power that is allocated to an interface for all the inline-power-capable interfaces on the switch.
	power redundancy-mode	Configures the power settings for the chassis.

show power inline police

To display PoE policing and monitoring status, use the **show power inline police** command.

show power inline police [*interface-name*] [**module** *x*]

Syntax Description		
	interface-name	(optional) Display PoE policing and monitoring status for a particular interface.
	module *x*	(optional) Display PoE policing and monitoring status for all interfaces on this module.

Defaults	
	This command has no default settings.

Command Modes	
	Privileged EXEC mode

Usage Guidelines

The Oper Power field displays the true power consumption of the connected device.

The **show power inline police** command with no keywords displays PoE policing status for all interfaces in the chassis.

If this command is executed at the global level, the last line of the output under Oper Power field displays the total true inline power consumption of all devices connected to the switch.

Examples

This example shows how to display PoE policing status for a interface Gigabitethernet 2/1:

```
Switch#show power inline police gigabitethernet 2/1
Available:370.0(w)  Used:30.0(w)  Remaining:340.0(w)

Interface Admin Oper       Admin   Oper    Cutoff Oper
          State State      Police  Police  Power  Power
--------- ----- ---------- ------- ------- ------ -----
Gi2/1     auto  on         errdisable on   22.0   9.6
```

Related Commands	Command	Description
	power inline police	Configures PoE policing on a particular interface.

show pppoe intermediate-agent interface

To display PPPoE Intermediate Agent configuration and statistics (packet counters), use the **show pppoe intermediate-agent interface** command.

show pppoe intermediate-agent information interface *interface*

show pppoe intermediate-agent statistics interface *interface*

Syntax Description: **interface** *interface* — Interface for which information or statistics are displayed.

Defaults: This command has no default settings.

Command Modes: Privileged EXEC mode

Examples: This example shows how to display PPPoE Intermediate Agent configuration:

```
Switch# show pppoe intermediate-agent information
Switch PPPoE Intermediate Agent is enabled
PPPoE Intermediate Agent trust/vlan is configured on the following Interfaces:
Interface          Trust       Unaware   Vlan Strip   Relay Client Type)
---------          -----       -------   ----------   ------------------
Gigabitethernet3/4   no          no        yes          unlisted
PPPoE Intermediate Agent is configured on following Vlans:
1-5
Gigabitethernet3/3   no          no        no           unlisted
PPPoE Intermediate Agent is configured on following Vlans:
1-5
```

This example shows how to display PPPoE Intermediate Agent statistics on an interface:

```
Switch# show pppoe intermediate-agent statistics interface g3/7
Interface: Gigabitethernet3/7
  Relay mode enabled
    Init = 0
    PADI = 0 PADO = 0
    PADR = 0 PADS = 0
    PADT = 0
  Packets dropped:
    Relay:Init exceeded = 0
    Server response from untrusted ports = 0
    Client response from untrusted ports = 0
    Malformed PPPoE Discovery packets = 0
Vlan 2: Packets received PADI = 0 PADO = 0 PADR = 0 PADS = 0 PADT = 0
Vlan 3: Packets received PADI = 0 PADO = 0 PADR = 0 PADS = 0 PADT = 0
```

Related Commands	Command	Description
	pppoe intermediate-agent (global)	Enables the PPPoE Intermediate Agent feature on a switch.
	pppoe intermediate-agent format-type (global)	Sets the access-node-identifier, generic-error-message, and identifier-string for the switch.
	pppoe intermediate-agent (interface)	Enables the PPPoE Intermediate Agent feature on an interface.
	pppoe intermediate-agent format-type (interface)	Sets circuit-id or remote-id for an interface.

show qos

To display QoS information, use the **show qos** command.

show qos

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Examples This example shows the output that might be displayed if you do not enter any keywords:

```
Switch# show qos
QoS is enabled globally
Switch#
```

Related Commands

Command	Description
qos aos-mset layer-all encapsulation	Globally enables QoS functionality on the switch.

show qos aggregate policer

To display QoS aggregate policer information, use the **show qos aggregate policer** command.

show qos aggregate policer [*aggregate_name*]

Syntax Description	*aggregate_name* (Optional) Named aggregate policer.
Defaults	This command has no default settings.
Command Modes	Privileged EXEC mode
Usage Guidelines	The aggregate policer name is case sensitive.
Examples	This example shows the output if you do not enter any keywords: `Switch#` **show qos aggregate policer** `Policer: agg-policer` `Policer type: 2R3C2R3C2R3C

show qos dbl

To display global Dynamic Buffer Limiting (DBL) information, use the **show qos dbl** command.

show qos dbl

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Examples This example shows how to display global DBL information:

```
Switch# show qos dbl
DBL is globally enabled
DBL flow includes vlan
DBL flow includes l4-ports
DBL flow not uses ace to lookup ecnparam
DBL buffer limit uses max-pseudo(qlp)/2k
DBL max credits:15
DBL aggressive credit limit:10
DBL aggregate credit refresh period:1 perhaps
DBL buffer math: defaults drop pseudo(qlp):
    1:1:0
Switch#
```

Related Commands

Command	Description
qos qos-mark layer-off mac-propagation	Globally enables QoS functionality on the switch.

show qos interface

To display queueing information, use the **show qos interface** command.

show qos interface [**fastethernet** *interface-number* | **gigabitethernet** *interface-number*] | [**vlan** *vlan_id* | **port-channel** *number*]

Syntax Description

fastethernet *interface-number*	Specifies the Fast Ethernet 802.3 interface.
gigabitethernet *interface-number*	Specifies the Gigabit Ethernet 802.3z interface.
vlan *vlan_id*	(Optional) Specifies the VLAN ID; valid values are from 1 to 4094.
port-channel *number*	(Optional) Specifies the port channel; valid ranges are from 1 to 64.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Examples

This example shows how to display queueing information:

```
Switch#show qos interface fastethernet 4/4
port queue-scheduler:DWRR
  port trust state:trusted
  Administrative Port Trust Status: 'dscp'
  Operational Port Trust Status: 'untrusted'
  Port Shape Rate Configured:100000 kbps
  Default DSCP:0 CoSToS: CoS:0

 Tx-Queue   Bandwidth   Shapedrate   Priority   Queuelimit
            (bps)       (bps)                   (packets)
    1       31250000    disabled     N/A        240
    2       31250000    disabled     N/A        240
    3       31250000    disabled     normal     240
    4       31250000    disabled     N/A        240
Switch#
```

Related Commands

Command	Description
show qos	Displays QoS information.
tx-queue	Configures the transmit queue parameters for an interface.

show qos maps

To display QoS map information, use the **show qos maps** command.

show qos maps [**cos** | **dscp** [**policed** | **tx-queue**]

Syntax Description:	**cos** (Optional) Displays CoS map information.
	dscp (Optional) Displays DSCP map information.
	policed (Optional) Displays policed map information.
	tx-queue (Optional) Displays tx-queue map information.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Examples This example shows how to display QoS map settings:

```
Switch# show qos maps
DSCP-Dpdscp Mapping Table (dscp = d1d2)
d1 :d2  0  1  2  3  4  5  6  7  8  9
-------------------------------------
 0 :   01 01 01 01 01 01 01 01 02 02
 1 :   02 02 02 02 02 02 02 02 03 03
 2 :   03 03 03 03 03 03 03 03 04 04
 3 :   04 04 04 04 04 04 04 04 05 05
 4 :   05 05 05 05 05 05 05 05 06 06
 5 :   06 06 06 06 06 06 06 06 07 07
 6 :   07 07 07 07 07 07 07 07 08 08

Policed DSCP Mapping Table (dscp = d1d2)
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-Txq Mapping Table (dscp = d1d2)
d1 :d2  0  1  2  3  4  5  6  7  8  9
-------------------------------------
 0 :   02 02 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 :   05 05 05 05 05 05 05 05 05 05
 5 :   05 05 05 05 05 05 05 05 05 05
 6 :   07 07 07 07

Cos-DSCP Mapping Table
```

```
   Cos:  0  1  2  3  4  5  6  7
   ------------------------------
   DSCP:  0 8 16 24 32 40 48 56

Exceeded
```

Related Commands	Command	Description
	qos account layer-all encapsulation	Includes Layer 2 overhead in all QoS rate calculations on the switch.

show redundancy

To display redundancy facility information, use the **show redundancy** command.

show redundancy {**clients**| **counters** | **history**| **states**}

Syntax Description		
	clients	(Optional) Displays information about the redundancy facility client.
	counters	(Optional) Displays information about the redundancy facility counter.
	history	(Optional) Displays a log of past status and related information for the redundancy facility.
	states	(Optional) Displays information about the redundancy facility state, such as disabled, initialization, standby, active.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Examples This example shows how to display information about the redundancy facility:

```
Switch# show redundancy
Redundant System Information :
------------------------------
       Available system uptime = 2 days, 2 hours, 38 minutes
Switchover system experienced = 0
                 Standby failures = 0
              Last switchover reason = none

                     Hardware Mode = Duplex
       Configured Redundancy Mode = Stateful Switchover
        Operating Redundancy Mode = Stateful Switchover
                  Maintenance Mode = Disabled
                     Communications = Up

Current Processor Information :
-------------------------------
                  Active Location = slot 1
          Current Software state = ACTIVE
         Uptime in current state = 2 days, 2 hours, 38 minutes
                   Image Version = Cisco Internetwork Operating System Software
IOS (tm) C6sup2sup SXD2 12.2(18)SXD4(0.0)Version 12.2(20)SXD4(0.0)
Copyright (c) 1986-2004 by cisco Systems, Inc.
Compiled Mon 12-Jul-04 08:42 by prod
                  BOOT = bootflash:cat6sup2-sxd2-mz.122-20_EWA_192.1
                  Configuration register = 0x2012

Peer Processor Information :
----------------------------
                  Standby Location = slot 2
          Current Software state = STANDBY HOT
```

```
        System is current state = 2 Keep, 2 Secure, 39 minutes
        Cisco Internetwork Operating System Software
IOS (tm) Catalyst 4000 L3 Switch Software (cat4000-I9K9S-M), Version 12.2(20.8&8.1
.8)) (CISCO INTERNAL USE ONLY BRANCH) Synchronized to
Engineering Image Version 12.2(20.8) Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Wed 16-Jul-03 04:
                                    BASE = bootflash:cat4000-I9s-mz.122_20_8&8.bin,1
        Configuration register = 0x2000

Switch>#
```

This example shows how to display redundancy facility client information:

```
Switch# show redundancy clients
clientID = 29000    clientSeq = 65535    RF_INTERNAL_MSG
clientID = 29001    clientSeq = 65535    RF_LAST_CLIENT
clientID = 28       clientSeq = 330      LACLIC_CONFIG_SYNC
clientID = 65000    clientSeq = 65000    RF_LAST_CLIENT Switch
```

The output displays the following information:

- clientID displays the client's ID number.
- clientSeq displays the client's notification sequence number.
- Current redundancy facility state.

This example shows how to display the redundancy facility counter information:

```
Switch# show redundancy counters
Redundancy Facility IPC
                    msgs rcvd 0 0
                    msgs rcvd from down 0 0

                    invalid client rcvs 0 0
                    null msg rcvs 0 0
                    rcv failures 0 0
                    rx msg length invalid 0 0

                    client rcvd using msgs 0 0
rx peer msg rcvd using errors 0 0
                    null peer msg rcv 0 0
                    errored peer msg rcv 0 0

                    buffers rcv 18195
tx buffers rcvd 18195 0
                    buffers rcv 0 0
                    buffer release errors 0 0

                    duplicate client registrations 0 0
                    failed to register client 0 0
                    invalid client errors 0 0
Switch#
```

This example shows how to display redundancy facility history information:

```
Switch# show redundancy history
00:00:01 client added: RF_INTERNAL_MSG(0) seq=0
00:00:01 client added: RF_LAST_CLIENT(65000) seq=65000
00:00:01 client added: RF_LAST_CLIENT(65000) seq=65000
00:00:01 client added: Redundancy Echo SP(16) seq=105
00:00:03 *my state = INITIALIZATION(2) *peer state = DISABLED(1)
00:00:03 RF_PROG_INITIALIZATION(100) RF_INTERNAL_MSG(0) spvrl cvrl
00:00:03 RF_PROG_INITIALIZATION(100) Redundancy Echo SP(16) spvrl cvrl
00:00:03 RF_PROG_INITIALIZATION(100) LACLIC_CONFIG_SYNC(28) spvrl cvrl
00:00:03 RF_PROG_INITIALIZATION(100) RF_LAST_CLIENT(65000) spvrl cvrl
```

```
00:00:00 *sp state = 0BGGSTATEFUN(3) peer state = 5GSAMLE(5)
00:00:00 *sp state = 0CTIM(2) *peer state = 0
00:00:00 *sp state = 0CTIM(2)SFT(7) peer state = 5GSAMLE(5)
00:00:00 *sp STATE_ACKNOWLEDGE_ENABLE(20) Redundancy Mode 8F(16) op=0
00:00:00 *sp STATE_ACKNOWLEDGE_ENABLE(20) Redundancy Mode 8F(16) op=1
00:00:00 *sp STATE_PARTIGO(18) RF_DEFERRED_MSG(3) op=0 c=1
00:00:00 *sp RF_PROG_ACTIVE_FAST(208) Redundancy Mode 8F(16) op=0 c=1
00:00:00 *sp RF_PROG_ACTIVE_FAST(208) Redundancy Mode 8F(16) op=1 c=1
00:00:00 *sp RF_PROG_ACTIVE_FAST(208) SAMLE(5)CTIM(2)SFT(7) op=0 c=1
00:00:00 *sp *peer = 0CTIM(2)SFT(7) peer state = 5GSAMLE(5)
00:00:00 *sp RF_PROG_ACTIVE_DRAIN(301) RF_DEFERRED_MSG(3) op=0 c=1
00:00:00 *sp RF_PROG_ACTIVE_DRAIN(301) Redundancy Mode 8F(16) op=0 c=1
00:00:00 *sp RF_PROG_ACTIVE_DRAIN(301) Redundancy Mode 8F(16) op=1 c=1
00:00:00 *sp RF_PROG_PLATFORM_SYNC(400) RF_DEFERRED_MSG(3) op=0 c=1
00:00:00 *sp RF_PROG_PLATFORM_SYNC(400) RF_DEFERRED_MSG(3) op=1 c=1
00:00:00 *sp RF_PROG_PLATFORM_SYNC(400) CALIGO_CONFIG_DONE(28) op=0 c=0
00:00:00 *sp RF_PROG_PLATFORM_SYNC(400) CALIGO_CONFIG_DONE(28) op=1 c=0
00:01:16 *sp RF_PROGRESSING_REDUNDANCY(450) CALIGO_CONFIG_DONE(28) op=0 c=0
00:01:16 *sp RF_PROGRESSING_REDUNDANCY(450) CALIGO_CONFIG_DONE(28) op=1 c=0
00:01:16 *sp RF_PROGRESSING_REDUNDANCY(450) RF_LAST_CLIENT(65535) op=0 c=0
00:01:16 *sp RF_PROGRESSING_REDUNDANCY(450) RF_LAST_CLIENT(65535) op=1 c=0
00:01:16 *sp RF_PROG_HOT_STANDBY(550) RF_LAST_CLIENT(65535) op=0 c=0
00:01:16 *sp *peer = 0CTIM(2) *peer state = STANDBY COLD(4)
Switch#
```

This example shows how to display information about the redundancy facility state:

```
Switch#show redundancy states
my states = 13 -ACTIVE
        peer states = 08 -STANDBY HOT
            Mode = Duplex
            Unit = Primary
            Unit ID = 2

Redundancy Mode (Operational) = Stateful Switchover
Redundancy Mode (Configured)  = Stateful Switchover
    Split Mode = Disabled
    Manual Swact = Enabled
    Communications = Up

    client count = 21
    client notification TMR = 240000 milliseconds
            keep_alive TMR = 9000 milliseconds
            keep_alive count = 0
        keep_alive threshold = 18
            RF debug mask = 0x0
Switch#
```

Related Commands	Command	Description
	redundancy	Enters the redundancy configuration mode.
	redundancy force-switchover	Forces a switchover from the active to the standby supervisor engine.

show redundancy config-sync

To display an SSO config-sync failure or the signed mismatched command list (MCL), if any, use the **show redundancy config-sync** command.

show redundancy config-sync {failures | ignored} | {bem | mcl pec}

show redundancy config-sync ignored failures mcl

Syntax Description

failures	Displays MCL entries or BEM/PEC failures.
ignored	Displays the ignored MCL entries.
bem	(Impossible)
mcl	Displays commands that exist in the active supervisor engine's running configuration, but are not supported by the image on the standby supervisor engine.
pec	Displays a Power Return Code (PRC) failure and forces the system to operate in RPR mode provided there is a mismatch in the return code for a command execution at the active and standby supervisor engine.

Defaults

This command has no default settings.

Command Modes

User EXEC/mode

Usage Guidelines

When two versions of Cisco IOS images are involved, the command sets supported by two images might differ. If any of those mismatched commands are executed on the active supervisor engine, the standby supervisor engine might not recognize those commands. This causes a configuration mismatch condition. If the system check for the command fails on standby supervisor engine during a bulk sync, the command is moved into the MCL and the standby supervisor engine reboots. To display all the mismatched commands, use the **show redundancy config-sync failures mcl** command.

To clear the MCL, follow these steps:

Step 1 Remove all mismatched commands from the active supervisor engines' running configuration.

Step 2 Revalidate the MCL with a modified running configuration using the **redundancy config-sync validate mismatched-commands** command.

Step 3 Reload the standby supervisor engine.

Alternatively, you could ignore the MCL by following these steps:

Step 1 Enter the **redundancy config-sync ignore mismatched-commands** command.

Step 2 Reload the standby supervisor engine; the system transitions to SSO mode.

Note If you ignore the mismatched commands, the *out-of-sync configuration* at the *active supervisor engine* and the standby supervisor engine still exists.

Step 2 You can verify the ignored MCL with the **show redundancy config-sync ignored mcl** command.

Each command sets a return code in the action function that implements the command. This return code indicates whether or not the command succeeds/fails/ignores. The active supervisor engine maintains the return code for each command. If the return code for a command is not success, the active supervisor engine PRC fails in the active supervisor engine. PRC failure occurs if these two RRCs do not match. If a PRC error occurs at the standby supervisor engine either during bulk sync or LBL sync, the standby supervisor engine is reset. To display all PRC failures, use the **show redundancy config-sync failures prc** command.

To display besteffort method(BEM) errors, use the **show redundancy config-sync failures bem** command.

Examples The following example shows how to display the BSSU BEM failures:

```
Router# show redundancy config-sync failures bem
BEM Failed Command List
-----------------------

The List is Empty
Router#
```

The following example shows how to display the BSSU MCL failures:

```
Router# show redundancy config-sync failures mcl
Mismatched Command List
-----------------------

The List is Empty
Router#
```

The following example shows how to display the BSSU PRC failures:

```
Router# show redundancy config-sync failures prc
PRC Failed Command List
-----------------------
interface Fastethernet3/1
!! vlan database "interface"
!! vtemplate protocol pagp
!! vlan database "interface"
```

Related Commands	Command	Description
	redundancy config-sync mismatched-commands	Moves the active supervisor engine into the Mismatched Command List (MCL) and resets the standby supervisor engine.

show running-config

To display the module status and configuration, use the **show running-config** command.

show running-config [module *slot]*

Syntax Description	**module** *slot* (Optional) Specifies the module slot number; valid values are from 1 to 6.
Defaults	This command has no default settings.
Command Modes	Privileged EXEC mode

Usage Guidelines

In some cases, you might see a difference in the duplex mode displayed when you enter the **show interfaces** command and the **show running-config** command. If you do see a difference, the duplex mode displayed in the **show interfaces** command is the actual duplex mode that the interface is running. The duplex mode displayed in the **show running-config** command is the configured mode for an interface.

The **show running-config** command output for an interface may display a duplex mode configuration but no configuration for the speed. When no speed is displayed in the output, it indicates that the interface speed is configured to be auto and that the duplex mode shown does not reflect the operational setting once the speed is configured to something other than auto. With this configuration, it is possible that the operating duplex mode for that interface does not match the duplex mode shown with the **show running-config** command.

Examples

This example shows how to display the module and status configuration for all modules:

```
Switch# show running-config
00:12:18:%SYS-5-CONFIG_I:Configured from console by console show
Building configuration...

Current configuration:3283 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Switch
!
!
power supplies required 1
ip subnet-zero
!
!
!
interface FastEthernet1
 no ip address
 shutdown
!
```

```
 duplex auto
 speed auto
!end
```

This example shows the output for the **show running-config** command when you have enabled the **multicast voice vlan** command:

```
Switch# show running-config int fastethernet 4/1
Building configuration...

Current configuration:1133 bytes
!
interface FastEthernet4/1
 switchport voice vlan 2
 no snmp trap link-status
 channel-protocol lacp
 channel-group 2 mode on
end

Switch#
```

show shell functions

Use the **show shell functions** command to display configurations for all builtin shell functions.

show shell functions

Syntax Description	**No keywords**
Defaults	None
Command Modes	Privileged EXEC
Usage Guidelines	This command only displays the contents of builtin shell functions. To display the contents of user created functions, use the **show shell triggers** command.
Examples	This example illustrates how to display configurations included for all the shell functions:

```
Switch#show shell functions
```

Related Commands	Command	Description
	show	Displays a wide variety of system features.
	show shell triggers	Co-ordinates a user defined trigger.

show shell triggers

Use the **show shell triggers** command to display detail for all supported builtin and user created triggers.

show shell triggers

Syntax Description:	**No keywords.**
Defaults:	None
Command Modes:	Privileged EXEC
Usage Guidelines:	This command displays builtin triggers and user defined triggers (with their mapped functions).

Examples:	This example illustrates how to display detail for all supported triggers:
	`Switch1 show shell triggers`
	`Trigger Id: rearmevent`
	`Trigger description: rearmevent`
	`Trigger enabled: yes`
	`Trigger mapping functions:`

Related Commands:	**Command**	**Description**
	shell trigger	Creates a user defined trigger.
	show shell functions	Displays all configuration modes included for all the builtin functions, including user created and builtin functions.

show slavebootflash:

To display information about the standby bootflash file system, use the **show slavebootflash:** command.

show slavebootflash: [all | chips | filesys]

Syntax Description	**all** (Optional) Displays all possible flash information.
	chips (Optional) Displays Flash chip information.
	filesys (Optional) Displays file system information.
Defaults	This command has no default settings.
Command Modes	Privileged EXEC mode

Examples

This example shows how to display file system status information:

```
Switch# show slavebootflash: filesys

-------- F I L E  S Y S T E M  S T A T U S --------
  Device Number = 0
DEVICE INFO BLOCK: bootflash
  Magic Number        = 6887635   File System Vers = 10000     (1.0)
  Writable            = 1         Control Block    = 40000
  Programming Algorithm= 16       Erased State     = FFFFFFFF
  File System Offset  = 40000     Length = F40000
  MONLIB Offset       = 100       Length = 16C88
  Bad Sector Map Offset= 1FFAB8   Length = 3208
  Squeeze Log Offset  = F58000    Length = 4000
  Squeeze Buffer Offset= F5C000   Length = 4000
  Blocks Squeezed     = 0
  STATUS INFO:
  Writable
  NO Files Open for Write
  Complete Stores
  No Unnamed Files
  No Unnamed Bytes
  Total Unnamed Bytes = 0
  DIRECT INFO:
    Bytes Used        = 917088   Bytes Available = 42912
    Bad Sectors       = 0        Spared Sectors  = 0
    OldFiles          = 0        Bytes = 917088
    Deleted Files     = 0        Bytes = 0
    Files to Recover  = 0        Bytes = 0
  Switch#
```

This example shows how to display system image information:

```
Switch# show slavebootflash:
-#  -ED --type-- --crc-- --seek-- size --length-- -----date/time------ name
1   .  image  A0A0A0A0 00A0A0A0  4   917088 Sep 20 1999 13:26:23 c4500-ms
2   .  image  DEEDEEAD 00DEEDE0  9   747268 Sep 20 1999 13:48:49 sp.bin2
Switch#
```

This example shows how to display all bootflash informations:

```
Switch show slaveboot/bootflash: all
1 .. image  0x7ffc0000  0x7ffc0000  0x1ae  [ImageOK] -Rdata/Wdata/-rrr name
2 .. image  BCM4781A  20/BCM  24  20010804 Sep 25 1999 10:18:40 cs.boot-
ex
3 .. image  BRDSELAD  95/UNK  9  7470016 Sep 20 1999 13:48:49 cp.hello/
-
SAFADDR bytes available (981408 bytes used)

------- F I L E  S Y S T E M  S T A T U S --------
  Device Number = 20
DEVICE INFO BLOCK: bootflash
  Magic Number        = 4D4F4D5   File System Vers = 10000   (1.0)
  Length              = 1000000   Sector Size     = 40000
  Programming Algorithm = 4        Erased State    = FFFFFFFF
  File System Offset  = 40000     Length = F60000
  MONLIB Offset       = 100       Length = 8A28
  Bad Sector Map Offset = 7FFFC   Length = 4
  Squeeze Log Offset  = F68000    Length = 80000
  Squeeze Buffer Offset = F70000  Length = 80000
  Num Spare Sectors   = 0
    Spare Sectors
STATUS INFO:
  Initializing
  Dirty: Unknown Sec Delete
  Complete State
  No Unmounted Sectors
  No Squeeze in progress
  Squeezed
  Monlib
  Total bytes available = 424118
  Bad Sectors   = 0       Spared Sectors  = 0
  Total Files   = 3       Total bytes     = 87988
  Deleted Files = 0       Bytes = 0
  Files w/Errors = 0      Bytes = 0
Switch>
```

show slaveslot0:

To display information about the file system on the standby supervisor engine, use the **show slaveslot0:** command.

show slot0: [all | chips | filesys]

Syntax Description

all	(Optional) Displays all flash information including the output from the **show slot0: chips** and **show slot0: filesys** commands.
chips	(Optional) Displays flash chip register information.
filesys	(Optional) Displays file system status information.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Examples

This example shows how to display a summary of the file system:

```
Switch# show slaveslot0:
-# - ED --type-- --crc-- --seek- -slen -length- --date/time- name
1  .. .image  A57D4B87  A4F1A1   0  6567B4E8 Mar 08 1999 16:30:42 bellay

97439KB bytes available (1638784KB bytes used)
Switch>
```

This example shows how to display flash chip information:

```
Switch# show slaveslot0:-chips
******** Intel Series 2+ Status/Register Dump ********
Compatible Status Reg: 0080
  Config Option Reg (A000): 2
  Config Status Reg (A002): 0
  Low Voltage Reg (A004): 0
  Write Protect Reg (A006): 4
  Voltage Cntrl Reg (A008): 0
  Rdy/Busy Enable Reg (A00A): 2

COMMON MEMORY BELLSOUTH: Bank 0
  Intelligent ID Code : FF89FA22
  Compatible Status Reg: 80B0
  Global Status Reg: 80B0
  Block Status Regs:
    0 : 80B0  80B0  80B0  80B0  80B0  80B0  80B0  80B0
    8 : 80B0  80B0  80B0  80B0  80B0  80B0  80B0  80B0
   16 : 80B0  80B0  80B0  80B0  80B0  80B0  80B0  80B0
   24 : 80B0  80B0  80B0  80B0  80B0  80B0  80B0  80B0

COMMON MEMORY BELLSOUTH: Bank 1
  Intelligent ID Code : FF89FA22
  Compatible Status Reg: 80B0
  Global Status Reg: 80B0
  Block Status Regs:
```

```
      0 : 0x0b1 0x0b1 0x0b1 0x0b1 0x0b1 0x0b1 0x0b1 0x0b1
     16 : 0x0b1 0x0b1 0x0b1 0x0b1 0x0b1 0x0b1 0x0b1 0x0b1
     24 : 0x0b1 0x0b1 0x0b1 0x0b1 0x0b1 0x0b1 0x0b1 0x0b1

CHECK MEMORY SELF(TEST): Bank 2
  Intel(Spec) ID Code : 0089A2A2
  Compatible Status Reg: 80b1
  Extended Status Reg: 00b1
  Block Status Regs:
      0 : 0x0b1 0x0b1 0x0b1 0x0b1 0x0b1 0x0b1 0x0b1 0x0b1
      8 : 0x0b1 0x0b1 0x0b1 0x0b1 0x0b1 0x0b1 0x0b1 0x0b1
     16 : 0x0b1 0x0b1 0x0b1 0x0b1 0x0b1 0x0b1 0x0b1 0x0b1
     24 : 0x0b1 0x0b1 0x0b1 0x0b1 0x0b1 0x0b1 0x0b1 0x0b1

CHECK MEMORY SELF(TEST): Bank 3
  Intel(Spec) ID Code : 0089A2A2
  Compatible Status Reg: 80b1
  Extended Status Reg: 00b1
  Block Status Regs:
      0 : 0x0b1 0x0b1 0x0b1 0x0b1 0x0b1 0x0b1 0x0b1 0x0b1
      8 : 0x0b1 0x0b1 0x0b1 0x0b1 0x0b1 0x0b1 0x0b1 0x0b1
     16 : 0x0b1 0x0b1 0x0b1 0x0b1 0x0b1 0x0b1 0x0b1 0x0b1
     24 : 0x0b1 0x0b1 0x0b1 0x0b1 0x0b1 0x0b1 0x0b1 0x0b1

CHECK MEMORY SELF(TEST): Bank 4
  Intel(Spec) ID Code : 00000000
  (ID Not Intel -- assuming bank not populated

This example shows how to display file system information:

Switch# show slaveslot0: dirsize
-------- F I L E S Y S T E M S T A T U S --------
  Device Number = 4
DEVICE INFO BLOCK: slot0
  Magic Number     = 6887635   File System Vers = 10000   (1.0)
  Length           = 10000000  Sector Size      = 200200
  Programming Algorithm = 4    Erased State     = FFFFFFFF
  File System Offset    = 1000 Length = 8F6000
  Monlib Offset         = 8F7000 Length = C000
  Bad Sector Map Offset = 1FFFC  Length = 20
  Squeeze Log Offset    = FC000  Length = 2000
  Squeeze Buffer Offset = FE000  Length = 2000
  Num Spare Sectors     = 0
    Spares:
STATUS INFO:
  writable
  No File Open for Write
  Complete Stats
  No unrecognized Errors
  No Squeeze in progress
USAGE INFO:
  Bytes Used    = 5F5A00  Bytes Available = 5A7A64
  Bad Sectors   = 0       Spared Sectors   = 0
  OK Files      = 1       Bytes = 5F5A00
  Deleted Files = 0       Bytes = 0
  Files w/Errors = 0      Bytes =
Switch#
```

show slot0:

To display information about the slot0: file system, use the **show slot0:** command.

show slot0: [all | chips | filesys]

Syntax Description

all	(Optional) Displays all flash information including the output from the **show slot0: chips** and **show slot0: filesys** commands.
chips	(Optional) Displays flash chip register information.
filesys	(Optional) Displays file system status information.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Examples

This example shows how to display a summary of the file system:

```
Switch# show slot0:
-# - FS --type-- --crea-- --size-- --free--Length --:--date/time-- ----name----
1  -  usage   SYSTEM?  jul24x1  -  0 0x07BA00 Nov 09 1999 11:50:42 bailey

9728kB system available (1047904B bytes used)
Switch#
```

This example shows how to display flash chip information:

```
Switch# show slot0: chips
******** Intel Series 2+ Status/Register Dump ********
ATTRIBUTES MEMORY REL(0X0B8):
  Compatible Status Bit (CSB): 0
  Config Status Bug (CSBS): 0
  Card Status: Busy (X130): 1
  Ready/Busy Mode (RBM): 1
  Voltage Sect Bug (X130): 0
  RdyBusy Mode Bug (X140): 2

COMMON MEMORY REL(0X0B2): Bank 0
  Intelligent ID Code: ( 0989BA16)
  Compatible Status Bug: 0X80
  Global Status Bug: 0X80
  Block Status Bug:
    0:  0X80  0X80  0X80  0X80  0X80  0X80  0X80  0X80
    8:  0X80  0X80  0X80  0X80  0X80  0X80  0X80  0X80
   16:  0X80  0X80  0X80  0X80  0X80  0X80  0X80  0X80
   24:  0X80  0X80  0X80  0X80  0X80  0X80  0X80  0X80

COMMON MEMORY REL(0X0B2): Bank 1
  Intelligent ID Code: ( 0989BA16)
  Compatible Status Bug: 0X80
  Global Status Bug: 0X80
  Block Status Bug:
    0:  0X80  0X80  0X80  0X80  0X80  0X80  0X80  0X80
```

```
  8 : 8GB1  8GB1  8GB1  8GB1  8GB1  8GB1  8GB1  8GB1
  9 : 8GB1  8GB1  8GB1  8GB1  8GB1  8GB1  8GB1  8GB1
 14 : 8GB1  8GB1  8GB1  8GB1  8GB1  8GB1  8GB1  8GB1
 15 : 8GB1  8GB1  8GB1  8GB1  8GB1  8GB1  8GB1  8GB1

CONNOR MEMORY DIRECTORY: Bank 2
  Installed IS Code: 0FFFA000
  Compatible Status Reg: 8GB1
  Global  Status Reg: 8GB1
  Sector Status Reg:
  0 : 8GB1  8GB1  8GB1  8GB1  8GB1  8GB1  8GB1  8GB1
  8 : 8GB1  8GB1  8GB1  8GB1  8GB1  8GB1  8GB1  8GB1
 14 : 8GB1  8GB1  8GB1  8GB1  8GB1  8GB1  8GB1  8GB1
 15 : 8GB1  8GB1  8GB1  8GB1  8GB1  8GB1  8GB1  8GB1

CONNOR MEMORY DIRECTORY: Bank 3
  Installed IS Code: 0FFFA000
  Compatible Status Reg: 8GB1
  Global  Status Reg: 8GB1
  Sector Status Reg:
  0 : 8GB1  8GB1  8GB1  8GB1  8GB1  8GB1  8GB1  8GB1
  8 : 8GB1  8GB1  8GB1  8GB1  8GB1  8GB1  8GB1  8GB1
 14 : 8GB1  8GB1  8GB1  8GB1  8GB1  8GB1  8GB1  8GB1
 15 : 8GB1  8GB1  8GB1  8GB1  8GB1  8GB1  8GB1  8GB1

CONNOR MEMORY DIRECTORY: Bank 4
  Installed IS Code: 0FFFA000
  Bank is Total : accessing bank not populated
Switch>
```

This example shows how to display file system information:

```
Switch> show slot0: filesys
-------- F I L E S Y S T E M  S T A T U S --------
  Device Number = 0
DEVICE INFO BLOCK: slot0
  Magic Number  = 8A7D7DF5   File System Vers = 10000   (1.0)
  Length        = 1E000000   Sector Size      = 20000
  Programming Algorithm = 4  Erased State       = FFFFFFFF
  File System Offset    = 20000  Length = 1DE0000
  MONLIB Offset         = 100  Length = C7B4
  Bad Sector Map Offset = 2FFFC  Length = 32
  Squeeze Log Offset    = F6000  Length = 20000
  Squeeze Buffer Offset = F6000  Length = 20000
  Num Spare Sectors     = 0
    Spares:
STATUS INFO:
  Writable
  Bytes Free for Write
  Complete State
  No Squeeze in Progress
  No Squeeze to Perform
DRIVE INFO:
  Bytes Used    = 5F5A0  Bytes Available = 5A7A4
  Bytes Cached  = 0      Spared Sectors  = 0
  OK Files      = 1      Bytes = 4F5A0
  Deleted Files = 0      Bytes = 0
  Files w/Errors = 0     Bytes = 0
Switch>
```

show spanning-tree

To display spanning-tree state information, use the **show spanning-tree**.

show spanning-tree [*bridge_group*] **active** | **backbonefast** | **bridge** [*id*] | **inconsistentports** | **interface** *type*[*port-number*] [*detail*] | **uplinkfast** | **vlan** *vlan_id*[**prefixed-method**[**detail**]

Syntax Description	*bridge_group* (Optional) Specifies the bridge group number; valid values are from 1 to 255.
	active (Optional) Displays the spanning-tree information on active interfaces only.
	backbonefast (Optional) Displays the spanning-tree BackboneFast status.
	bridge (Optional) Displays bridge status and configuration information.
	id (Optional) Name of the bridge.
	inconsistentports (Optional) Displays the root inconsistency state.
	interface *type* (Optional) Specifies the interface type and number; valid values are **fastethernet**, **gigabitethernet**, **tenGigabitEthernet**, **port-channel** (1 to 64), and **vlan** (1 to 4094).
	port-number (Optional) Displays the port bridge status and configuration.
	summary (Optional) Specifies a summary of port states.
	total (Optional) Displays the total lines of the spanning-tree state section.
	uplinkfast (Optional) Displays the spanning-tree UplinkFast status.
	vlan *vlan_id* (Optional) Specifies the VLAN ID; valid values are from 1 to 4094.
	prefixed-method (Optional) Displays the defined path cost calculation method used.
	detail (Optional) Displays a summary of interface information.

Defaults Interface information summary is displayed.

Command Modes Privileged EXEC mode

Examples This example shows how to display spanning-tree information on the active interfaces only:

```
Switch# show spanning-tree active
VLAN1 is executing the
ieee compatible Spanning Tree protocol
  Bridge Identifier has priority 32768, address 0050.3e8d.6400
  Configured hello time 2, max age 20, forward delay 15
  Baseport Cost Spanning Tree parameters for VLAN1:
  Port 323 (FastEthernet5/3) of VLAN1 is forwarding
   Port id is 80.143
   Designated root has priority 32768, address 0050.3e8d.6400
   Designated bridge has priority 32768, address 0050.3e8d.6400
   Designated port id is 80.143, designated path cost 19
   Timers: hello 0, topology change 0, notification 0
   Port id is 80.143, designated path cost 19
   Timers: hello 0, topology change 0, notification 0

Port 245 (FastEthernet5/7) of VLAN1 is forwarding
```

```
Port path cost 19, Port priority 128, Port Identifier 128.8.
designated root has priority 32768, address 0060.5cf4.6a00
designated bridge has priority 32768, address 0060.5cf4.6a00
Designated port id is 128.2, designated path cost 19
Timers: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state: 1
BPDU: sent 3, received 32852
Switch#
```

This example shows how to display the spanning-tree BackboneFast status:

```
Switch# show spanning-tree backbonefast
BackboneFast is enabled

BackboneFast statistics
-----------------------
Number of transitions via backboneFast (all VLANs) : 0
Number of inferior BPDUs received (all VLANs) : 0
Number of RLQ request PDUs sent (all VLANs) : 0
Number of RLQ response PDUs sent (all VLANs) : 0
Number of RLQ request PDUs rcvd (all VLANs) : 0
Number of RLQ response PDUs rcvd (all VLANs) : 0
Switch#
```

This example shows how to display spanning-tree information for the bridge:

```
Switch# show spanning-tree bridge
VLAN1
  Bridge ID  Priority  32768
             Address   0050.3e8d.6401
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
VLAN2
  Bridge ID  Priority  32768
             Address   0050.3e8d.6402
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
VLAN3
  Bridge ID  Priority  32768
             Address   0050.3e8d.6403
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
Switch#
```

This example shows how to display a summary of interface information:

```
Switch# show spanning-tree
VLAN1
  Spanning tree enabled protocol ieee
  Root ID    Priority    32768
             Address     0030.96f8.0a00
             This Bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32768
             Address     0030.96f8.0a00
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300

Interface        Designated
Name             Port ID Prio  Cost Sts  Cost Bridge ID          Port ID
---------------- -------- ----- ---- --- ---- -------------------- --------
FastEthernet2/15 128.79  128   19 FWD   0 32768 0030.96f8.0a00 128.79

VLAN2
  Spanning tree enabled protocol ieee
```

```
Root ID    Priority    32768
           Address     0030.96ff.6a80
           Cost        19 (FastEthernet0/9)
           Port        128.9 (Fast Ether net0/9)
           Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

Bridge ID  Priority    32768
           Address     0030.96ff.6a80
           Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
           Aging Time 300

Interface           Designated
Name                Port ID Prio. Cost Sts  Cost Bridge ID          Port ID
--------------------------------------------------------------------------------
FastEthernet0/10    128.80  128   19 FWD    0  32768 0030.96ff.6a80 128.80
Switch#
```

This example shows how to display spanning-tree information for Fast Ethernet interface 5/9:

```
Switch# show spanning-tree interface FastEthernet5/9
Interface Fa5/9 (port 25) in Spanning-tree 1 is BLOCKING(BLOCKING)
Port path cost 100, Port priority 128
Designated root has priority 32768, address 0030.96ff.6a80
Designated bridge has priority 32768, address 0030.96ff.3940
Designated port is 25, path cost 115
Timers: message age 0, forward delay 0, hold 0
BPDU sent 0, received 0
BPDU: sent 0, received 0
Switch#
```

This example shows how to display spanning-tree information for a specific VLAN:

```
Switch# show spanning-tree vlan 1
VLAN1 is executing the ieee compatible Spanning Tree protocol
  Bridge Identifier has priority 32768, address 0030.96ff.6a80
  Configured hello time 2, max age 20, forward delay 15
  Current root has priority 32768, address 0030.96ff.6a80
  Topology change flag not set, detected flag not set
  Number of topology changes 0 last change occurred 01:50:42 ago
          port 10 of slot 0 is forwarding
  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 130 (FastEthernet0/10) of VLAN1 is forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.79.
   Designated root has priority 32768, address 0030.96ff.6a80
   Designated bridge has priority 32768, address 0030.96ff.6a80
   Designated port id is 128.79, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state:1
   BPDU:sent 4127, received 0
Switch#
```

This example shows how to display spanning-tree information for a specific bridge group:

```
Switch# show spanning-tree vlan 1
  Optimized is disabled
  Extended sysid is disabled
Switch#
```

This example shows how to display a summary of port states:

```
Switch# show spanning-tree summary
Root bridge for:VLAN1, VLAN2
```

```
PortFast BPDU Guard is disabled
Bridge Assurance is enabled
UplinkFast is disabled
BackboneFast is disabled
Pathcost method used is short

Name                 Blocking Listening Learning Forwarding STP Active
---------------- -------- --------- -------- ---------- ----------
VLAN1                0        0        0        2          2
VLAN2                0        0        0        1          1
---------------------- -------- --------- -------- ---------- ----------
               2 VLANs   0        0        0        3          3
Switch#
```

This example shows how to display the total lines of the spanning-tree state section:

```
Switch# show spanning-tree summary totals
Root bridge for:VLAN1, VLAN2
PortFast BPDU Guard is disabled
EtherChannel misconfiguration guard is enabled
UplinkFast is disabled
BackboneFast is disabled
Pathcost method used is short

Name                 Blocking Listening Learning Forwarding STP Active
---------------- -------- --------- -------- ---------- ----------
               2 VLANs   0        0        0        3          3
Switch#
```

This example shows how to determine whether any ports are in root inconsistent state:

```
Switch# show spanning-tree inconsistentports

Name                 Interface                Inconsistency
-------------------- ------------------------ ------------------
VLAN1                Fast0/Gigabit0/2         Root Inconsistent

Number of inconsistent ports (segments) in the system:1
Switch#
```

Related Commands	Command	Description
	spanning-tree backbonefast	Enables BackboneFast on a spanning-tree VLAN.
	spanning-tree cost	Calculates the path cost of STP on an interface.
	spanning-tree guard	Enables root guard.
	spanning-tree pathcost method	Sets the path cost calculation method.
	spanning-tree portfast default	Enables PortFast by default on all access ports.
	spanning-tree portfast (interface configuration mode)	Enables PortFast mode.
	spanning-tree port-priority	Prioritizes an interface when two bridges compete for position as the root bridge.
	spanning-tree uplinkfast	Enables the UplinkFast feature.
	spanning-tree vlan	Configures STP on a per-VLAN basis.

show spanning-tree mst

To display MST protocol information, use the **show spanning-tree mst** command.

show spanning-tree mst [**configuration**]

show spanning-tree mst [*instance-id*] [**detail**]

show spanning-tree mst [*instance-id*] **interface** *interface* [**detail**]

Syntax Description

configuration	(Optional) Displays region configuration information.
instance-id	(Optional) Instance identification number, valid values are from 0 to 15.
detail	(Optional) Displays detailed MST protocol information.
interface *interface*	(Optional) Interface type and number; valid values for type are **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **port-channel**, and **vlan**. See the "Usage Guidelines" section for more information.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

In the output display of the **show spanning-tree mst configuration** command, a warning message might display. This message appears if you do not mapsecondary VLANs to the same instance as the associated primary VLAN. The display indicates a list of the secondary VLANs that are not mapped to the same instance as the associated primary VLAN. The warning message is as follows:

```
Warning: secondary vlans are not mapped to the same instance as their primary:
-> 3
```

See the **show spanning-tree** command for output definitions.

Examples

This example shows how to display region configuration information:

```
Switch# show spanning-tree mst configuration
Name      [region1]
Revision  1     Instances configured  2
Instance  Vlans mapped
-------- ---------------------------------------------------------------------
0        1-9,11-19,21-28,31-39,41-4094
1        10,20,30,40
-------- ---------------------------------------------------------------------
Switch#
```

This example shows how to display additional MST protocol values:

```
Switch# show spanning-tree mst 3 detail
# S W B E N BRIDGE sent mapped: 1,3041-3999
Bridge address 0002.172c.f400 priority 32771 (32768 sysid 3)
Root this switch for MSTI3
```

```
GigabitEthernet1/1 of MST03 is broadcast forwarding
Port info port id 128.193 priority 128
cost 20000
Designated root address 0002.172c.f400 priority 32771
cost 0
Designated bridge address 0002.172c.f400 priority 32771 port
id 128.1
Timers: message expires in 0 sec, forward delay 0, forward transitions 1
Bpdus (MRecords) sent 4, received 0

FastEthernet2/2 of MST03 is backup blocking
Port info port id 128.194 priority 128 cost
200000
Designated root address 0002.172c.f400 priority 32771
cost 0
Designated bridge address 0002.172c.f400 priority 32771 port id
128.193
Timers: message expires in 2 sec, forward delay 0, forward transitions 1
Bpdus (MRecords) sent 1, received 252
Switch#
```

This example shows how to display MST information for a specific interface:

```
Switch# show spanning-tree mst 0 interface fastethernet4/1 detail
Edge port: no (trunk) port guard : none
(default)
Link type: point-to-point (point-to-point) bpdu filter: disable
(default)
Boundary: internal bpdu guard : disable
(default)
FastEthernet4/1 of MST00 is designated forwarding
Port info port id 128.193 priority 128 cost
200000
Designated root address 0060.7a66.d000 priority 8192
cost 20004
Designated bridge address 0002.172c.4400 priority 49152
port id 128.193
Designated root address 0002.172c.4400 priority 49152 cost 0
Timers: message expires in 2 sec, forward delay 0, forward transitions 1
Bpdus sent 252, received 3
Switch#
```

Related Commands	Command	Description
	spanning-tree mst	Sets the path-cost and port-priority parameters for any MSTI instance.
	spanning-tree mst forward-time	Sets the forward delay timer for all the instances.
	spanning-tree mst hello-time	Sets the hello-time delay timer for all the instances.
	spanning-tree mst max-hops	Specifies the number of possible hops in the region before a BPDU is discarded.
	spanning-tree mst root	Designates the primary root.

show storm-control

To display the broadcast storm control settings on the switch or on the specified interface, use the **show storm-control** command.

show storm-control [*interface-id*] [**broadcast**]

Supervisor Engine 6-E and Catalyst 4500M chassis

show storm-control [*interface-id*] **broadcast** [**multicast**]

System Description	*interface-id* (Optional) Specifies the interface ID for the physical port. **broadcast** (Optional) Displays the broadcast storm threshold setting. **multicast** (Optional) Displays the multicast storm threshold setting.
Defaults	This command has no default settings.
Command Modes	Privileged EXEC mode

Usage Guidelines

When you enter an interface ID, the storm control thresholds are displayed for the specified interface. If you do not enter an interface ID, the settings are displayed for the broadcast traffic type for all ports and channels.

Examples

This is an example of output from the **show storm-control** command when no keywords are entered. Because no traffic type keyword was entered, the broadcast storm control settings are displayed.

```
Switch#show storm-control
Interface Filter State  Upper    Lower    Current
---------  ------------ --------- --------- --------
Gi1/1     Forwarding   50.00%    50.00%    N/A
Gi4/1     Forwarding   50.00%    50.00%    N/A
Gi4/5     Forwarding   50.00%    50.00%    N/A
Switch#
```

This is an example of output from the **show storm-control multicast** command.

```
Switch#show storm-control multicast /Supervisor Engine 6-E
Interface Filter State  Broadcast Multicast Level
---------  ------------ --------- --------- -----
Fa1/1     Blocking     Enabled   Enabled   41%
Switch#
```

This is an example of output from the **show storm-control** command when no keywords are entered.

```
Switch#show storm-control
Interface Filter State  Broadcast Multicast Level
---------  ------------ --------- --------- -----
Fa1/1     Blocking     Enabled   Disabled  41%
Fa1/2     Blocking     Enabled   Enabled   41%
```

```
Switch#
```

This is an example of output from the **show storm-control** command for a specified interface:

```
Switch# show storm-control FastEthernet2/37
Interface  Filter State   Level     Current
---------  ------------   -----     -------
Fa2/37     Forwarding     50.00%    0.00%
Switch#
```

This is an example of output from the **show storm-control** command for a specified interface:

```
Switch# show storm-control interface FastEthernet2/1
Interface  Filter State   Broadcast Multicast  Level
---------  ------------   --------- ---------  -----
Fa2/1      Blocking       Enabled   Disabled   81.0
Switch#
```

Table 2-31 describes the fields in the **show storm-control** display.

Table 2-31 *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.
Level	Displays the threshold level set on the interface for broadcast traffic.
Current	Displays the bandwidth utilization of broadcast traffic as a percentage of total available bandwidth. This field is valid only when storm control is enabled. **Note** N/A is displayed for interfaces that do storm control in the hardware.

Related Commands

Command	Description
storm-control	Enables broadcast storm control on a port and specifies what to do when a storm occurs on a port.
show interfaces counters	Displays the traffic on the physical interface.
show running-config	Displays the running configuration of a switch.

show system mtu

To display the global MTU setting, use the **show system mtu** command.

show system mtu

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Examples This example shows how to display the global MTU setting:

```
Switch# show system mtu
Global Ethernet MTU is 1550 bytes.
Switch#
```

Related Commands

Command	Description
system mtu	Sets the maximum Layer 2 or Layer 3 payload size.

show tech-support

To display troubleshooting information for TAC, use the **show tech-support** command.

show tech-support [**bridging** | **cef** | **ipmulticast** | **isis** | **password** [**page** | **page**]

Syntax Description

bridging	(Optional) Specifies bridging-related information.
cef	(Optional) Specifies CEF-related information.
ipmulticast	(Optional) Specifies IP multicast-related information.
isis	(Optional) Specifies CLNS and ISIS-related information.
password	(Optional) Includes passwords and other security information in the output.
page	(Optional) Displays one page of information at a time in the output.

Defaults

The defaults are as follows:

- Outputs are displayed without page breaks.
- Passwords and other security information are removed from the output.

Command Modes

Privileged EXEC mode

Usage Guidelines

Output from the **show tech-support** command may be terminated in mid-stream with the key combination Ctrl-Shift-6-X. The command output is buffered so that the command terminates when output of the current CDP neighbor information is displayed on the console.

Press the **Return** key to display the next line of output, or press the **Space** bar to display the next page of information. If you do not enter the **page** keyword, the output scrolls. It does not stop for page breaks.

If you enter the **password** keyword, password encryption is enabled, but only the encrypted form appears in the output.

If you do not enter the **password** keyword, the passwords and other security-sensitive information in the output are replaced in the output with the word "removed."

The **show tech-support** command, are a compilation of several **show** commands and the output can be quite lengthy. For a sample display of the output of the **show tech-support** command, see the individual **show** command listed.

If you enter the **show tech-support** command without arguments, the output displays the equivalent of the **show** commands:

- **show version**
- **show running-config**
- **show stacks**
- **show interfaces**
- **show controllers**
- **show process memory**

- **show process cpu**
- **show buffers**
- **show logging**
- **show module**
- **show power**
- **show environment**
- **show interfaces switchport**
- **show interfaces trunk**
- **show vlan**

If you enter the **quoutcast** keyword, the output displays the equivalent of these **show** commands:

- **show ip pim interface**
- **show ip pim interface count**
- **show ip pim neighbor**
- **show ip pim rp**
- **show ip igmp groups**
- **show ip igmp interface**
- **show ip mroute count**
- **show ip mroute**
- **show ip mcache**
- **show ip dvmrp route**

Examples For a sample-by-play of the **show tech-support** command output, see the commands listed in the "Usage Guidelines" section for more information.

Related Commands See the "Usage Guidelines " section.

show udld

To display the administrative and operational UDLD status, use the **show udld** privileged EXEC command.

show udld *interface-id* | **neighbors** | **fast-hello** [*interface-id*]

Syntax Description	*interface-id*	Specifies the administrative and operational UDLD status for a specific interface.
	neighbors	Specifies the UDLD neighbor summary.
	fast-hello	Specifies fast UDLD neighbor summary and interface specific status.
	[*interface-id*]	Specifies the name of the interface.

Defaults None

Command Modes Privileged EXEC

Usage Guidelines If you do not enter an *interface_id* value, the administrative and operational UDLD status for all interfaces is displayed.

Examples To verify status for a particular link as reported by UDLD, enter the following command:

```
Switch# show udld gi1/14
Interface gi1/14

---
Port enable administrative configuration setting: Enabled / in aggressive mode
Port enable operational state: Enabled / in aggressive mode
Port non-silent operational state: Detected
Current operational state: Advertisement - Single neighbor detected
Message interval: 15000 ms
Time out interval: 5000 ms

Port fast-hello configuration setting: Disabled
Port fast-hello interval: Disabled
Port fast-hello interval in msec: Disabled
Neighbor fast-hello configuration setting: Disabled
Neighbor fast-hello interval: Disabled

    Neighbor 1:

    ---
    Expiration time: 41500 ms
    Cache Device index: 1
    Current neighbor state: Bidirectional
    Device ID: TBM10372401
    Port ID: gi1/14
    Neighbor echo 1 device: FOC06140DHL
    Neighbor echo 1 port: gi1/14

    TLV Message Interval: 15 sec
```

```
  No TLV fast-hello interval
  TLV CDP interval: 60
  TLV CDP Device name: Switch
```

To verify link status as reported by UDLD, enter the following command:

```
Switch#show udld neighbors

Port    Device Name      Device ID     Port ID    Neighbor State
----    -----------      ---------     -------    ---------------
Gi1/0/1 FOC12420Z90      1             Gi1/0/1    Bidirectional
Gi1/0/2 FOC12420Z90      1             Gi1/0/2    Bidirectional
```

To verify Fast UDLD configuration, enter the following command:

```
Switch#show udld fast-hello
Global port fast-hello hello msg be configured: 16
Global port fast-hello operational: 1
Total ports with fast-hello operational: 1
Total ports with fast-hello non-operational: 0

Port-Gi1     Hello Neighbor-Hello Neighbor-Device Neighbor-Port Status
-------      ----- ------------- -------------- -------------- ------
Gi1/0/1      200   200           FOC12420Z90    Gi1/0/1        Operational
Gi1/0/2      200   200           FOC12420Z90    Gi1/0/2        Operational
Gi1/0/3      200   200           FOC12420Z90    Gi1/0/3        Operational
```

To verify status for a particular link as reported by Fast UDLD, enter the following command:

```
Switch#show udld fast-hello gi1/0/1

Interface Gi1/0/1
---
  Port enable administrative configuration setting: Enabled / in aggressive mode
  Port enable operational state: Enabled / in aggressive mode
  Current bidirectional state: Bidirectional
  Current operational state: Advertisement - Single neighbor detected
  Message Interval: 200 ms
  Time out Interval: 5000 ms

  Port fast-hello configuration setting: Enabled
  Port fast-hello interval: 200 ms
  Port fast-hello operational state: Enabled
  Neighbor fast-hello configuration setting: Enabled
  Neighbor fast-hello interval: 200 ms

    Entry 1
    ---
    Expiration time: 500 ms
    Cache Device index: 1
    Current neighbor state: Bidirectional
    Device ID: FOC12420Z90
    Port ID: Gi1/0/1
    Neighbor echo 1 device: FOC12420Z90
    Neighbor echo 1 port: Gi1/0/1

    TLV Message Interval: 15
    TLV fast-hello interval: 200 ms
    TLV CDP Time out interval: 5
    TLV CDP Device name: Switch
```

Related Commands

Command	Description
udld (global configuration mode)	Enables aggressive or normal mode in the UDLD protocol and sets the configurable message timer time.
udld (interface configuration mode)	Enables UDLD on an individual interface or prevents a fiber interface from being enabled by the **udld (global configuration mode)** command.

show vlan

To display VLAN information, use the **show vlan** command.

show vlan [**brief** | **id** *vlan_id*] | **name** *name*]

show vlan private-vlan [*type*]

Syntax Description

brief	(Optional) Displays only a single line for each VLAN, naming the VLAN, status, and ports.
id *vlan_id*	(Optional) Displays information about a single VLAN identified by VLAN ID number; valid values are from 1 to 4094.
name *name*	(Optional) Displays information about a single VLAN identified by VLAN name; valid values are an ASCII string from 1 to 32 characters.
private-vlan	Displays private VLAN information.
type	(Optional) Private VLAN type.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Examples

This example shows how to display the VLAN parameters for all VLANs within the administrative domain:

```
Switch#show vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa5/9
2    VLAN0200                         active    Fa5/9
3    VLAN0300                         active    Fa5/9
4    VLAN0400                         active    Fa5/9
5    VLAN0500                         active    Fa5/9
6    VLAN0600                         active    Fa5/9
10   VLAN0010                         active    Fa5/9
20   VLAN0020                         active    Fa5/9

<...output truncated...>

850  VLAN0850                         active    Fa5/9
917  VLAN0917                         active    Fa5/9
999  VLAN0999                         active    Fa5/9
1002 fddi-default                     active    Fa5/9
1003 trnet-default                    active    Fa5/9
1004 fddinet-default                  active    Fa5/9
1005 trbrf-default                    active    Fa5/9

VLAN Type  SAID  MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ----- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001 1500  -      -      -        -    -        0      0
2    enet  100002 1500  -      -      -        -    -        0      0
```

```
3    enet  100003     1500  -    -    -    -    -    0    0
4    fddi  100004     1500  -    -    -    -    -    0    0
5    tr    100005     1500  -    -    -    -    -    0    0
6    enet  100006     1500  -    -    -    -    -    0    0
7    enet  100007     1500  -    -    -    -    -    0    0
10   enet  100010     1500  -    -    -    -    -    0    0
50   enet  100050     1500  -    -    -    -    -    0    0

...output truncated...

850  enet  100850     1500  -    -    -    -    -    0    0
917  enet  100917     1500  -    -    -    -    -    0    0
2000 enet  102000     1500  -    -    -    -    -    0    0
1002 fddi  101002     1500  -    -    -    -    -    0    0
1003 trcrf 101003     4472 1005  3274  -    -    srb  0    0
1004 fdnet 101004     1500  -    -    ieee -    -    0    0
1005 trbrf 101005     4472  -    -    ibm  -    -    0    0

VLAN ASLBInps SVIStyps Backup SVI
---- ------- ------- ------ ---
850  0       0       off
917  0       0       off
Switch#
```

This example shows how to display the VLAN name, status, and associated ports only:

```
Switch# show vlan brief
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa5/9
2    VLAN0200                         active    Fa5/9
3    VLAN0300                         active    Fa5/9
4    VLAN0400                         active    Fa5/9
5    VLAN0500                         active    Fa5/9
10   VLAN0010                         active    Fa5/9

900  VLAN0900                         active    Fa5/9
1002 fddi-default                     active    Fa5/9
1003 trcrf-default                    active    Fa5/9
1004 fddinet-default                  active    Fa5/9
1005 trbrf-default                    active    Fa5/9
Switch#
```

This example shows how to display the VLAN parameters for VLAN 3 only:

```
Switch# show vlan id 3

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
3    VLAN0300                         active    Fa5/9

VLAN Type  SAID   MTU   Parent RingNo BridgeNo Stp  BridgeMode Trans1 Trans2
---- ----- ------ ----- ------ ------ -------- ---- -------- ------ ------
3    enet  100003 1500  -      -      -        -    -        0      0
Switch#
```

Table 2-52 describes the fields in the **show vlan** command output.

Table 2-32 *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 Identifier 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.
BridgeNo	Bridge number for the VLAN, if applicable.
Stp	Spanning Tree Protocol type used on the VLAN.

The following example shows how to verify that the primary VLAN and secondary VLANs are correctly associated with each other and the same association also exists on the PVLAN port:

```
Switch> show private-vlan

Primary Secondary Type              Ports
------- --------- ----------------  ------------------------------------------
10      100       community         Fa3/1, Fa3/2
```

The following example shows how to remove the VLAN association:

```
Switch(config)# vlan 10
Switch(config-vlan)# private-vlan association remove 100
Switch(config-vlan)# end
Switch> show vlan private
Primary Secondary Type              Ports
------- --------- ----------------  ------------------------------------------
10      primary
        100       community
```

This example shows how to verify PVLAN configuration on the interface:

```
Switch> show interface f5/1 status
Port      Name               Status    Vlan       Duplex  Speed Type
Fa5/1                        connected pvlan sec e-bnd    a-100 10/100BaseTX

Switch> show interface f5/1 status
Port      Name               Status    Vlan       Duplex  Speed Type
Fa5/1                        connected pvlan prom a-bnd   a-100 10/100BaseTX
Switch>
```

Related Commands	Command	Description
	vlan (VLAN Database mode)	Configures a specific VLAN.
	vlan database	Enters VLAN configuration mode.
	vtp (global configuration mode)	Modifies the name of a VTP configuration storage file.

show vlan access-map

To display the contents of a VLAN access map, use the **show vlan access-map** command.

show vlan access-map [*map-name*]

Syntax Description:	*map-name* (Optional) Name of the VLAN access map.
Defaults:	This command has no default settings.
Command Modes:	Privileged EXEC mode
Examples:	This command shows how to display the contents of a VLAN access map.

```
Switch# show vlan access-map mordred
Vlan access-map "mordred" 1
        match: ip address 1
        action: forward capture
Switch#
```

Related Commands:	**Command**	**Description**
	vlan access-map	Enters VLAN access-map command mode to create a VLAN access map.

show vlan counters

To display the software-cached counter values, use the **show vlan counters** command.

show vlan [**id** *vlan id*] **counters**

Syntax Description	**id** *vlan id* (Optional) Displays the software-cached counter values for a specific VLAN.
Defaults	This command has no default settings.
Command Modes	Privileged EXEC mode
Usage Guidelines	If you enter the **show vlan counters** command without specifying the VLAN ID, the software-cached counter values for all VLANs are displayed.

Examples	This example shows how to display the software-cached counter values for a specific VLAN:
	`Switch# show vlan counters`
	`* Multicast counters include broadcast packets`
	
	`Vlan id : 1`
	`L2 Unicast Packets : 0`
	`L2 Unicast Octets : 0`
	`L2 Input Unicast Packets : 0`
	`L2 Input Unicast Octets : 0`
	`L2 Output Unicast Packets : 0`
	`L2 Output Unicast Octets : 0`
	`L2 Output Multicast Packets : 0`
	`L2 Output Multicast Octets : 0`
	`L2 Input Multicast Packets : 0`
	`L2 Input Multicast Octets : 0`
	`L2 Multicast Packets : 0`
	`L2 Multicast Octets : 96`
	`Switch#`

Related Commands	Command	Description
	clear vlan counters	Clears the software-cached counter values to start from zero again for a specified VLAN or all existing VLANs.

show vlan dot1q tag native

To display all the ports on the switch that are eligible for native VLAN tagging as well as their current native VLAN tagging status, use the **show vlan dot1q tag native** command.

show vlan dot1q tag native

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes User EXEC mode

Examples 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 globally

Per Port Native Vlan Tagging State
----------------------------------

Port     Operational      Native VLAN
         Mode             Tagging State
-------- ---------------- ------------
Fi/2     trunk            enabled
Fi/46    PVLAN trunk      disabled
Fi/48    trunk            enabled
```

Related Commands

Command	Description
switchport nacdt	Sets the interface type.
vlan global configuration} (refer to Cisco IOS documentation)	Enters global VLAN configuration mode.
vlan {VLAN configuration} (refer to Cisco IOS documentation)	Enters VLAN configuration mode.

show vlan group

To display the VLANs mapped to VLAN groups, use the **show vlan group** privileged EXEC command.

show vlan group [**group-name** *group-name*]

Syntax Description	**group-name** *group-name* (Optional) Displays the VLANs mapped to the specified VLAN group.
Defaults	None
Command Modes	Privileged EXEC
Usage Guidelines	The **show vlan group** command displays the existing VLAN groups and lists the VLANs and VLAN ranges that are members of each VLAN group. If you use the **group-name** keyword, you display only the members of the VLAN group specified by the *group-name* argument.
Examples	This example shows how to display the members of a specified VLAN group:

```
Switch# show vlan group group-name gamma1

Group Name Vlans Mapped
-------------- -----------------------
gamma1         7-9
```

Related Commands	**Command**	**Description**
	vlan group	Creates or modifies a VLAN group.

show vlan internal usage

To display information about the internal VLAN allocation, use the **show vlan internal usage** command.

show vlan [id *vlan-id* **] internal usage**

Syntax Description

id *vlan-id*	(Optional) Displays internal VLAN allocation information for the specified VLAN; valid values are from 1 to 4094.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Examples

This example shows how to display information about the current internal VLAN allocation:

```
Switch# show vlan internal usage

VLAN Usage
----------
1024 c
1025 c
1026 c
1027 c
1028 c
1029 Port-channel5
1030 FastEthernet4/20
1031 FastEthernet4/21
1032 FastEthernet4/22
1129 c
```

This example shows how to display information about the internal VLAN allocation for a specific VLAN:

```
Switch# show vlan id 1030 internal usage

VLAN Usage
----------
1030 GigabitEthernet1/2
```

Related Commands

Command	Description
vlan internal allocation policy	Configures the internal VLAN allocation scheme.

show vlan mapping

Use the **show vlan mapping** privileged EXEC command to display information about VLAN mapping on trunk ports.

show vlan mapping [**interface** *interface-id*] [| [**begin** | **exclude** | **include**] *expression*]

Syntax Description	**interface** *interface-id*	(Optional) Displays VLAN mapping information for the specified interface.
	|begin	(Optional) Displays begin with the line that matches the expression.
	|exclude	(Optional) Displays excludes lines that match the expression.
	|include	(Optional) Displays includes lines that match the specified expression.
	expression	Specifies an expression in the output to use as a reference point.

Defaults None

Command Modes Privileged EXEC

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 a sample output from the **show vlan mapping** command:

```
Switch#show vlan mapping
Interface fa2/5:
VLAN in vlan          Translated VLAN     Operation
---------------       ---------------     ---------
default (pkg          1                   selective (pkg
Interface fa2/6:
VLAN in vlan          Translated VLAN     Operation
---------------       ---------------     ---------
2                     104                 1-to-1 mapping
```

This is a sample output from the **show vlan mapping** command for an interface:

```
Switch#show vlan mapping interface fa4/4
Interface fa4/4:
VLAN in vlan          Translated VLAN     Operation
---------------       ---------------     ---------
12,16-18              100                 1-to-1 mapping
*                     101                 selective (pkg
                                          default (pkg
```

Related Commands	Command	Description
	switchport vlan mapping	Configures VLAN mapping on an interface.

show vlan mtu

To display the minimum and maximum transmission unit (MTU) sizes of each VLAN, use the **show vlan mtu** command.

show vlan mtu

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Usage Guidelines The MTU_Mismatch column in the command output indicates whether all the ports in the VLAN have the same MTU. When "yes" is displayed in the MTU_Mismatch column, it means that the VLAN has a port with different MTUs, and packets might be dropped that are switched from a port with a large MTU to a port with a smaller MTU. If the VLAN does not have an SVI, the hyphen (-) symbol is displayed in the SVI_MTU column.

For a VLAN, if the MTU-Mismatch column displays "yes," the names of the port with the MinMTU and the port with the MaxMTU are displayed. For a VLAN, if the SVI_MTU is bigger than the MinMTU, "Toobig" is displayed after the SVI_MTU.

Examples This is an example of output from the **show vlan mtu** command:

```
Router# show vlan mtu

VLAN  SVI_MTU  MinMTU(port)  MaxMTU(port)  MTU_Mismatch
----  -------  -----------  -----------  ------------
1     1500     1500         1500         No
Router#
```

Related Commands

Command	Description
mtu	Enables jumbo frames on an interface by adjusting the maximum size of a packet or maximum transmission unit (MTU).

show vlan private-vlan

To display private VLAN information, use the **show vlan private-vlan** command.

show vlan private-vlan [type]

Syntax Description	type (Optional) Displays the private VLAN type; valid types are isolated, primary, community, twoway-community, nonoperational, and normal.
Defaults	This command has no default settings.
Command Modes	Privileged EXEC mode

Usage Guidelines

When the **show private-vlan type** command displays a VLAN type as normal, it indicates that a regular VLAN has been used in the private VLAN configuration. When normal is displayed, this indicates that two VLANs have been associated before the type was set, and the private VLAN is not operational. This information is useful for debugging purposes.

Examples

This example shows how to display information about all currently configured private VLANs:

```
Switch# show vlan private-vlan

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
2       101       community         Fa5/1, Gi5/25
2       102       community
2       103       community         Fa5/1, Gi5/25
2       104       isolated
100     105       isolated          Gi5/25
150     151       non-operational
                  (mismatch)
                  (primary removed)
401     402       non-operational
                  (secondary
                  deleted)
```

Note A blank Primary value indicates that no association exists.

This example shows how to display information about all currently configured private VLAN types:

```
Switch# show vlan private-vlan type

Vlan Type
----------
200  primary
201  community
202  community
203  isolated
307  community
308  normal
```

```
520  community
521  isolated
Switch#
```

Table 2-33 describes the fields in the **show vlan private-vlan** command output.

Table 2-33 show vlan private-vlan Command Output Fields

Field	Description
Primary	Number of the primary VLAN.
Secondary	Number of the secondary VLAN.
Secondary-Type	Secondary VLAN type is **isolated** or **community**.
Ports	Indicates the ports within a VLAN.
Type	Type of VLAN; possible values are **primary**, **isolated**, community, nonprivatevlan, or **normal**.

Related Commands

Command	Description
private-vlan	Configures private VLANs and the association between a private VLAN and a secondary VLAN.
private-vlan mapping	Creates a mapping between the primary and the secondary VLANs so that both share the same primary VLAN SVI.

show vlan remote-span

To display a list of Remote SPAN (RSPAN) VLANs, use the **show vlan remote-span** command.

show vlan remote-span

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Examples This example shows how to display a list of RSPAN VLANs:

```
Router# show vlan remote-span
Remote SPAN VLANs
----------------------------------------------------------------------------
2, 20
```

Related Commands	Command	Description
	remote-span	Converts a VLAN into an RSPAN VLAN.
	vlan (VLAN Database mode)	Configures a specific VLAN.

show vmps

To display the VLAN Query Protocol (VQP) version, reconfirmation interval, retry count, VLAN Membership Policy Server (VMPS) IP addresses, current servers, and primary servers, use the **show vmps** command.

show vmps [statistics]

Syntax Description

statistics	(Optional) Displays the client-side statistics.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

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 RetryCount: 10
VMPS domain server: 172.20.50.120 (primary, current)

Reconfirmation status
---------------------
VMPS Action:       No Dynamic Ports
Switch#
```

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

```
Switch# show vmps statistics
VMPS Client Statistics
-----------------------

VQP  Queries:                0
VQP  Responses:              0
VQP  Changes:                0
VQP  Overbudget:             0
VQP  Overtaxed:              0
VQP  Errors:                 0
VQP  Wrong Domain:           0
VQP  Wrong Version:          0
VQP  Insufficient Resources: 0
Switch#
```

Related Commands:

Command	Description
vmps reconfirm (privileged EXEC)	Sends VLAN Query Protocol (VQP) queries to reconfirm all the dynamic VLAN assignments with the VLAN Membership Policy Server (VMPS).

show vtp

To display VTP statistics and domain information, use the **show vtp** command.

show vtp {counters | status}

Syntax Description

counters	Specifies the VTP statistics.
status	Specifies the VTP domain status.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Examples

This example shows how to display the VTP statistics:

```
Switch> show vtp counters
VTP advertisements received    : 0
Subset advertisements received : 0
Request advertisements received : 0
Summary advertisements received : 31
Subset advertisements received : 0
Request advertisements transmitted : 0
Number of config revision errors : 0
Number of config digest errors : 0
Number of V1 summary errors    : 0

VTP pruning statistics:

Trunk          Join Transmitted Join Received     Summary advts received from
                                                  non-pruning-capable device
---------      ---------------- -------------     -------------------------
Fa5/9          1555             1554              0
Switch>
```

This example shows how to display the VTP domain status:

```
Switch> show vtp status
VTP Version              : 2
Configuration Revision   : 250
Maximum VLANs supported locally : 1005
Number of existing VLANs : 45
VTP Operating Mode       : Server
VTP Domain Name          : Lab_Network
VTP Pruning Mode         : Enabled
VTP V2 Mode              : Enabled
VTP Traffic Generator    : Disabled
MD5 digest               : 0x65 0xF8 0xFB 0xBD 0xA4 0xF7 0xC2 0x08
Configuration last modified by 172.20.52.18 at 8-21-99 11:38:03
Local updater ID is 172.20.52.18 on interface 111 (lowest numbered VLAN interface
 found)
Switch>
```

This example shows how to display only those lines in the **show vtp** output that contain the word Summary:

```
Switch# show vtp counters | include Summary
Summary advertisements received : 7
Summary advertisements transmitted : 32
Trunk          Join Transmitted Join Received    Summary advts received from
Switch#
```

Table 2-34 describes the fields in the **show vtp** command output.

Table 2-34 show vtp Command Output Fields

Field	Description
Summary advertisements received	Total number of summary advertisements received
Subset advertisements received	Total number of subset advertisements received
Request advertisements received	Total number of request advertisements received
Summary advertisements transmitted	Total number of summary advertisements transmitted
Subset advertisements transmitted	Total number of subset advertisements transmitted
Request advertisements transmitted	Total number of request advertisements transmitted
Number of config revision errors	Number of config revision errors
Number of config digest errors	Number of config revision digest errors
Number of V1 summary errors	Number of V1 summary errors
Trunk	Trunk port participating in VTP pruning
Join Transmitted	Number of VTP-Pruning Joins transmitted
Join Received	Number of VTP-Pruning Joins received
Summary advts received from non-pruning-capable device	Number of Summary advertisements received from incapacitating-capable devices.
Number of existing VLANs	Total number of VLANs in the domain.
Configuration Revision	VTP revision number used to exchange VLAN information.
Maximum VLANs supported locally	Maximum number of VLANs allowed on the device.
Number of existing VLANs	Number of existing VLANs.
VTP Operating Mode	Indicates whether VTP is enabled or disabled.
VTP Domain Name	Name of the VTP domain.
VTP Pruning Mode	Indicates whether VTP pruning is enabled or disabled.
VTP V2 Mode	Indicates the VTP V2 mode as server, client, or transparent.
VTP Traps Generation	Indicates whether VTP trap generation mode is enabled or disabled.
MD5 digest	Checksum values.

Related Commands

Command	Description
vtp lpdu[d configuration mode]	Modifies the name of a VTP configuration storage file.
vtp client	Places a device in VTP client mode.
vtp domain	Configures the administrative domain name for a device.

Command	Description
vtp password	Creates a VTP domain password.
vtp pruning	Enables pruning in the VLAN database.
vtp server	Places the device in VTP server mode.
vtp transparent	Places device in VTP transparent mode.
vtp v2-mode	Enables version 2 mode.

snmp ifindex clear

To clear any previously configured **snmp ifindex** commands that were entered for a specific interface, use the **snmp ifindex clear** command.

snmp ifindex clear

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Interface configuration mode

Usage Guidelines Interface index persistence occurs when ifIndex values in the interface MIB (IF-MIB) persist across reboots and allow for consistent identification of specific interfaces using SNMP.

Use the **snmp ifindex clear** command on a specific interface when you want that interface to use the global configuration setting for ifIndex persistence. This command clears any ifIndex configuration commands previously entered for that specific interface.

Examples This example shows how to enable ifIndex persistence for all interfaces:

```
Router(config)# snmp-server ifindex persist
```

This example shows how to disable ifIndex persistence for FastEthernet 1/1 only:

```
Router(config)# interface fastethernet 1/1
Router(config-if)# no snmp ifindex persist
Router(config-if)# exit
```

This example shows how to clear for ifIndex configuration from the FastEthernet 1/1 configuration:

```
Router(config)# interface fastethernet 1/1
Router(config-if)# snmp ifindex clear
Router(config-if)# exit
```

As a result of this sequence of commands, ifIndex persistence is enabled for all interfaces that are specified by the **snmp-server ifindex persist** global configuration command.

Related Commands

Command	Description
snmp ifindex persist	Enables ifIndex values in the Interfaces MIB (IF-MIB) that persist across reboots (ifIndex persistence) as a specific interface
snmp-server ifindex persist	Enables ifIndex values that will remain constant across reboots for use by SNMP.

snmp ifindex persist

To enable ifIndex values in the Interfaces MIB (IF-MIB) that persist across reboots (ifIndex persistence) on a specific interface, use the **snmp ifindex persist** command. To disable ifIndex persistence only on a specific interface, use the **no** form of this command.

snmp ifindex persist

no snmp ifindex persist

Syntax Description This command has no arguments or keywords.

Defaults Disabled.

Command Modes Interface configuration mode

Usage Guidelines Interface index persistence occurs when ifIndex values in the IF-MIB persist across reboots and allow for consistent identification of specific interfaces using SNMP.

The **snmp ifindex persist** interface configuration command enables and disables ifIndex persistence for individual entries (that correspond to individual interfaces) in the ifIndex table of the IF-MIB.

The **snmp-server ifindex persist** global configuration command enables and disables ifIndex persistence for all interfaces on the routing device. This action applies only to interfaces that have ifDescr and ifAlias entries in the ifIndex table of the IF-MIB.

Examples This example shows how to enable ifIndex persistence for interface FastEthernet 1/1 only:

```
Router(config)# interface fastethernet 1/1
Router(config-if)# snmp ifindex persist
Router(config-if)# exit
```

This example shows how to enable ifIndex persistence for all interfaces, and then disable ifIndex persistence for interface FastEthernet 1/1 only:

```
Router(config)# snmp-server ifindex persist
Router(config)# interface fastethernet 1/1
Router(config-if)# no snmp ifindex persist
Router(config-if)# exit
```

Related Commands

Command	Description
snmp ifindex clear	Clears any previously configured **snmp ifindex** commands that were entered for a specific interface.
snmp ifindex persist	Enables ifIndex values in the Interfaces MIB (IF-MIB) that persist across reboots (ifIndex persistence) on a specific interface.

snmp-server enable traps

To enable SNMP notifications (traps or informs), use the **snmp-server enable traps** command. To disable all SNMP notifications, use the no form of this command.

snmp-server enable traps [**flash** [**insertion** | **removal**] | **fru-ctrl** | **port-security** [**trap-rate** *trap-rate*] | **removal** | **vtps** | **vlancreate** | **vlandelete** | **vtp**] | **mac-notification** [**change** | **move** | **threshold**]

no snmp-server enable traps [**flash** [**insertion** | **removal**] | **fru-ctrl** | **port-security** [**trap-rate** *trap-rate*] | **removal** | **vtps** | **vlancreate** | **vlandelete** | **vtp**] [**mac-notification**]

Syntax Description

flash	(Optional) Controls the SNMP FLASH trap notifications.
insertion	(Optional) Controls the SNMP flash insertion trap notifications.
removal	(Optional) Controls the SNMP flash removal trap notifications.
fru-ctrl	(Optional) Controls the SNMP entity FRU control trap notifications.
port-security	(Optional) Controls the SNMP trap generation.
trap-rate *trap-rate*	(Optional) Sets the number of traps per second.
vtps	(Optional) Controls all the traps defined in CISCO-STP-EXTENSIONS-MIB notifications.
vlancreate	(Optional) Controls the SNMP VLAN created trap notifications.
vlandelete	(Optional) Controls the SNMP VLAN deleted trap notifications.
vtp	(Optional) Controls the SNMP VTP trap notifications.
mac-notification	(Optional) Controls the SNMP MAC trap notifications.
change	(Optional) Controls the SNMP MAC change trap notifications.
move	(Optional) Controls the SNMP MAC move trap notifications.
threshold	(Optional) Controls the SNMP MAC threshold trap notifications.

Defaults

SNMP notifications are disabled.

Command Modes

Global configuration mode

Usage Guidelines

If you enter this command without an option, all notification types controlled by this command are enabled.

SNMP notifications can be sent as traps or inform requests. This command enables both traps and informs requests for the specified notification types. To specify whether the notifications should be sent as traps or informs, use the **snmp-server host** [**traps** | **informs**] command.

The **snmp-server enable traps** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send notifications, you must configure at least one **snmp-server host** command.

This list of the MIBs is used for the traps:

- **flash**—Controls SNMP FLASH traps from the CISCO-FLASH-MIB.
  - **insertion**—Controls the SNMP Flash insertion trap notifications.
  - **removal**—Controls the SNMP Flash removal trap notifications.
- **frw-mib**—Controls the FRC control traps from the CISCO-ENTITY-FRU-CONTROL-MIB.
- **port-security**—Controls the port-security traps from the CISCO-PORT-SECURITY-MIB.
- **mac**—Controls all the traps from the CISCO-ETHER-STUBS-MIB.
- **vlancore**—Controls SNMP VLAN control trap notifications.
- **vlanbridge**—Controls SNMP VLAN defined trap notifications.
- **vtp**—Controls the VTP traps from the CISCO-VTP-MIB.

Examples

This example chows how to send all traps to the host is specified by the name myhost.cisco.com using the community string defined as public:

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

This example chows how to enable the MAC address change MIB notification:

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

SNMP traps can be enabled with a one-time: to detect port-security violations due to restrict mode. The following example shows how to enable traps for port-security with a size of 5 traps per second:

```
Switch(config)# snmp-server enable traps port-security trap-rate 5
Switch(config)#
```

Related Commands

Command	Description
show mac address-table dynamic	Clears the dynamic address entries from the Layer 2 MAC address table.
mac address-table notification	Enables MAC address notification on a switch.
show mac address-table notification	Displays the MAC address table notification status and history.
snmp-server enable traps	Enables SNMP notification.
snmp trap mac-notification change	Enables SNMP MAC address notifications.

snmp-server ifindex persist

To globally enable ifIndex values that will remain constant across reboots for use by SNMP, use the **snmp-server ifindex persist** command. To globally disable ifIndex persistence, use the **no** form of this command.

snmp-server ifindex persist

no snmp-server ifindex persist

Syntax Description This command has no arguments or keywords.

Defaults Disabled.

Command Modes Global configuration mode

Usage Guidelines Interface index persistence occurs when ifIndex values in the IF-MIB persist across reboots and allow for consistent identification of specific interfaces using SNMP.

The **snmp-server ifindex persist** global configuration command does not override the interface-specific configuration. To override the interface-specific configuration of ifIndex persistence, enter the **no snmp ifindex persist** and **snmp ifindex clear** interface configuration commands.

Entering the **no snmp-server ifindex persist** global configuration command enables and disables ifIndex persistence for all interfaces on the routing device using ifDescr and ifIndex entries in the ifIndex table of the IF-MIB.

Examples This example shows how to enable ifIndex persistence for all interfaces:

```
Router(config)# snmp-server ifindex persist
```

Related Commands

Command	Description
snmp ifindex clear	Clears any previously configured **snmp ifindex** commands that were entered for a specific interface
snmp ifindex persist	Enables ifIndex values in the ifInterface MIB (IF-MIB) that persist across reboots (ifIndex persistency) on a specific interface.

snmp-server ifindex persist compress

To configure the format of the ifIndex table in a compressed format, use the **snmp-server ifindex persist compress** command. To place the table in a decomp-reused format, use the **no** form of this command.

snmp-server ifindex persist compress

no snmp-server ifindex persist compress

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Global configuration mode

Usage Guidelines This command is hidden because the ifIndex table is always in a compressed format on the supervisor engine.

Examples This example shows how to enable compression of the ifIndex table:

```
Router(config)# snmp-server ifindex persist compress
```

This example shows how to disable compression of the ifIndex table:

```
Router(config)# no snmp-server ifindex persist compress
```

Related Commands

Command	Description
snmp ifindex clear	Clears any previously configured **snmp ifindex** commands that were entered for a specific interface.
snmp ifindex persist	Enables ifIndex values in the Interfaces MIB (IF-MIB) that will remain constant across reboots (ifIndex persistence) on a specific interface.
snmp-server ifindex persist	Enables ifIndex values that will remain constant across reboots for use by SNMP.

snmp trap mac-notification change

To enable SNMP MAC address notifications, use the **snmp trap mac-notification** command. To return to the default setting, use the **no** form of this command.

snmp trap mac-notification change {**added** | **removed**}

no snmp trap mac-notification change {**added** | **removed**}

Syntax Description	**added** Specifies enabling the MAC address notification trap whenever a MAC address is added to an interface.
	removed Specifies enabling the MAC address notification trap whenever a MAC address is removed from an interface.
Defaults	MAC address addition and removal are disabled.
Command Modes	Interface configuration mode
Usage Guidelines	Even though you enable the change notification trap for a specific interface by using the **snmp trap mac-notification change** command, the trap is generated only when you enable the **snmp-server enable traps mac-notification change** and the **mac address-table notification change** global configuration commands.

Examples	This example shows how to enable the MAC notification trap when a MAC address is added to a port:
	`Switch(config)# interface gigabitethernet1/1`
	`Switch(config-if)# snmp trap mac-notification change added`
	
	You can verify your settings by entering the **show mac address-table notification change** interface privileged EXEC command.

Related Commands	Command	Description
	show mac address-table	Displays the address entries from the Layer 2 MAC address table.
	mac address-table notification	Enables MAC address notification on a switch.
	show mac address-table notification	Displays the MAC address table notification status and history.
	snmp-server enable traps	Enables SNMP notifications.

source-interface

To send out call home email messages with specific source interface, use the **source-interface** command.

source-interface *interface-name*

Syntax Description	*interface-name* Source-interface name for call home email messages.
Defaults	None
Command Modes	cfg-call-home

Usage Guidelines

You should configure **vlan** on an interface and provide a valid IP address before specifying it as a source interface for Call Home. Doing this avoids a connection failure when sending Call Home email messages. You should only specify a source-interface name under Call Home if source-ip-address is not specified. You can only specify either a source-interface or source-ip-address in call home mode, not simultaneously.

Examples

This example shows how to configure source interface for Call Home. Generally, the interface should already be configured with a valid IP address as usually configured for an interface.

```
Switch# config terminal
Switch(config)# call-home
Switch(cfg-call-home)# source-interface GigabitEthernet 1/1
Switch(cfg-call-home)# source-ip
Switch(cfg-call-home)# source-ip-address 10.2.4.1
Switch(cfg-call-home)# no source-interface
Switch(cfg-call-home)# show running-config | grep -i source-interface
Switch(cfg-call-home)# no source-interface
Switch(cfg-call-home)# source-ip-address 10.2.4.1
```

Note If Call Home is configured to use http or https as the transport method, you must use **ip http client source-interface** to configure the source interface for all http clients. You cannot specify a source interface for Call Home http messages only.

Related Commands	Command	Description
	source-ip-address	Sends out Call Home email messages with specific source IP address.

source-ip-address

To send call Home email messages with specific source IP address, use the **source-ip-address** command.

source-ip-address *ip address*

Syntax Description		
	ip address	Source IP address for Call Home messages.

Defaults None

Command Modes cfg-call-home

Usage Guidelines It is best to configure **no shut** an interface with this valid IP address before specifying it as source-ip-address for Call Home. Doing this avoids a connection failure when sending Call Home email messages. You should only specify source-ip-address under Call Home if source interface is not specified. You should only specify either source-interface or source-ip-address, not all. Some mode, not both simultaneously.

Examples This example shows how to configure source-ip-address for Call Home:

```
Switch(config)#call-home(config-call-home)#source-interface Gigabitethernet 1/1
Switch(config-call-home)#no shut
Switch(config-call-home)#source-ip-address 10.2.4.1
Source source-interface has already been configured,please remove source-interface config
Switch(config-call-home)#no source-interface
Switch(config-call-home)#no source-interface
Switch(config-call-home)#source-ip-address 10.2.4.1
```

Related Commands	Command	Description
	source-interface	Sends out call home email messages with specific source interface.

spanning-tree backbonefast

To enable BackboneFast on a spanning-tree VLAN, use the **spanning-tree backbonefast** command. To disable BackboneFast, use the **no** form of this command.

spanning-tree backbonefast

no spanning-tree backbonefast

Syntax Description This command has no arguments or keywords.

Defaults BackboneFast is disabled.

Command Modes global configuration mode

Usage Guidelines BackboneFast should be enabled on all Catalyst 4500 series switches to allow the detection of indirect link failures. Enabling BackboneFast starts the spanning-tree reconfiguration more quickly.

Examples This example shows how to enable BackboneFast on all VLANs:

```
Switch(config)# spanning-tree backbonefast
Switch(config)#
```

Related Commands

Command	Description
spanning-tree cost	Calculates the path cost of STP on an interface.
spanning-tree portfast default	Enables PortFast by default on all access ports.
spanning-tree portfast (interface configuration mode)	Enables PortFast mode.
spanning-tree port-priority	Prioritizes an interface when two bridges compete for position as the root bridge.
spanning-tree uplinkfast	Enables the UplinkFast feature.
spanning-tree vlan	Configures STP on a per-VLAN basis.
show spanning-tree	Displays spanning-tree information.

spanning-tree bpdufilter

To enable BPDU filtering on an interface, use the **spanning-tree bpdufilter** command. To return to the default settings, use the **no** form of this command.

spanning-tree bpdufilter {**enable** | **disable**}

no spanning-tree bpdufilter

Syntax Description	**enable** Enables BPDU filtering on this interface. **disable** Disables BPDU filtering on this interface.
Defaults	Disabled
Command Modes	Interface configuration mode

Usage Guidelines

Caution Use care when entering the **spanning-tree bpdufilter enable** command. Enabling BPDU filtering on an interface is approximately equivalent to disabling the spanning tree for this interface. It is possible to create bridging loops if this command is not entirely used.

When configuring L-aware 2-protocol tunneling on all the service provider edge switches, you must enable spanning-tree BPDU filtering on the 802.1Q tunnel ports by entering the **spanning-tree bpdufilter enable** command.

BPDU filtering allows you to prevent a port from sending and receiving BPDUs. The configuration is applicable to the whole interface, whether it is trunking or not. This command has three states:

- **spanning-tree bpdufilter enable**—This state unconditionally enables the BPDU filter feature on the interface.
- **spanning-tree bpdufilter disable**—This state unconditionally disables the BPDU filter feature on the interface.
- **no spanning-tree bpdufilter**—This state enables the BPDU filter feature on the interface if the interface is operational PortFast state and if the **spanning-tree portfast bpdufilter default** command is configured.

Examples This example shows how to enable the BPDU filter feature on this interface:

```
Switch(config)#int g4/24
Switch(config-if)# spanning-tree bpdufilter enable
Switch(config-if)#
```

Related Commands

Command	Description
show spanning-tree	Displays spanning-tree information.
spanning-tree portfast bpdufilter default	Enables the BPDU filtering by default on all PortFast ports.

spanning-tree bpduguard

To enable BPDU guard on an interface, use the **spanning-tree bpduguard** command. To return to the default setting, use the **no** form of this command.

spanning-tree bpduguard {enable | disable}

no spanning-tree bpduguard

Syntax Description

enable	Enables BPDU guard on this interface.
disable	Disables BPDU guardon this interface.

Defaults

BPDU guard is disabled.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

BPDU guard is a feature that prevents a port from receiving BPDUs. This feature is typically used in a service provider environment where the administrator wants to prevent an access port from participating in the spanning tree. If the port still receives a BPDU, it is put in the disabled state as a protection measure. This command has three states:

- **spanning-tree bpduguard enable**—This state unconditionally enables BPDU guard on the interface.
- **spanning-tree bpduguard disable**—This state unconditionally disables BPDU guard on the interface.
- **no spanning-tree bpduguard**—This state enables BPDU guard on the interface if it is in the operational PortFast state and if the **spanning-tree portfast bpduguard default** command is configured.

Examples

This example shows how to enable BPDU guard on this interface:

```
Switch(config-if)# spanning-tree bpduguard enable
Switch(config-if)#
```

Related Commands

Command	Description
show spanning-tree	Displays spanning-tree information.
spanning-tree portfast bpdufilter default	Enables the BPDU filtering by default on all PortFast ports.

spanning-tree cost

To calculate the path cost of STP on an interface, use the **spanning-tree cost** command. To revert to the default, use the form of this command.

spanning-tree cost *cost*

no spanning-tree cost *cost*

Syntax Description *cost* Path cost; valid values are from 1 to 200,000,000.

Defaults The default settings are as follows:

- FastEthernet—19
- GigabitEthernet—4

Command Modes Interface configuration mode

Usage Guidelines When you configure the cost, the higher values indicate higher costs. The usage applies regardless of the protocol type that is specified. The path cost is calculated, based on the interface bandwidth.

Examples This example shows how to access an interface and set a path cost value of 250 for the spanning-tree VLAN that is associated with the interface:

```
Switch(config)# interface fastethernet 2/1
Switch(config-if)# spanning-tree cost 250
Switch(config-if)#
```

Related Commands

Command	Description
spanning-tree portfast default	Enables PortFast by default on all access ports.
spanning-tree portfast (interface configuration mode)	Enables PortFast mode.
spanning-tree port-priority	Prioritizes an interface when two bridges compete for position as the root bridge.
spanning-tree uplinkfast	Enables the UplinkFast feature.
spanning-tree vlan	Configures STP on a per-VLAN basis.
show spanning-tree	Displays spanning-tree information.

spanning-tree etherchannel guard misconfig

To display an error message when a loop-due to a channel misconfiguration is detected, use the **spanning-tree etherchannel guard misconfig** command. To disable the feature, use the **no** form of this command.

spanning-tree etherchannel guard misconfig

no spanning-tree etherchannel guard misconfig

Syntax Description This command has no arguments or keywords.

Defaults Spanning-tree EtherChannel guard is enabled.

Command Modes Global configuration mode

Usage Guidelines When an EtherChannel guard misconfiguration is detected, this message is displayed:

```
%SPANTREE-2-CHNL_MISCFG:Contactat loop due to etherchannel misconfig of interface
Po<channel#>
```

To determine which local ports are involved in the misconfiguration, enter the **show interfaces status err-disabled** command. To verify the EtherChannel configuration on the remote device, enter the **show etherchannel summary** command on the remote device.

After you correct the configuration, enter **lr-shutdown** and the **no shutdown** commands on the associated port-channel interface.

Examples This example shows how to enable the EtherChannel guard misconfiguration feature:

```
Switch(config)# spanning-tree etherchannel guard misconfig
Switch(config)#
```

Related Commands

Command	Description
show etherchannel	Displays EtherChannel information for a channel.
show interfaces status	Displays the interface status or a list of interfaces in error-disabled state.
shutdown (refer to Cisco IOS documentation)	Disables a port.

spanning-tree extend system-id

To enable the extended-system ID feature on a chassis that supports 1024 MAC addresses, use the **spanning-tree extend system-id** command. To disable the feature, use the **no** form of this command.

spanning-tree extend system-id

no spanning-tree extend system-id

Syntax Description This command has no arguments or keywords.

Defaults Enabled on systems that do not provide 1024 MAC addresses.

Command Modes Global configuration mode

Usage Guidelines Releases 12.1(13)E and later support chassis with 64 or 1024 MAC addresses. For chassis with 64 MAC addresses, STP uses the extended-system ID plus a MAC address to make the bridge ID unique for each VLAN.

You cannot disable the extended system ID on chassis that support 64 MAC addresses.

Enabling or disabling the extended system ID updates the bridge IDs of all active STP instances, which might change the spanning-tree topology.

Examples This example shows how to enable the extended system ID:

```
Switch(config)# spanning-tree extend system-id
Switch(config)#
```

Related Commands	Command	Description
	show spanning-tree	Displays spanning-tree information.

spanning-tree guard

To enable root guard, use the **spanning-tree guard** command. To disable root guard, use the **no** form of this command.

spanning-tree guard {**loop** | **root** | **none**}

no spanning-tree guard

Syntax Description	**loop** Enables the loop guard mode on the interface. **root** Enables root guard mode on the interface. **none** Sets the guard mode to none.
Defaults	Root guard is disabled.
Command Modes	Interface configuration mode
Examples	This example shows how to enable root guard: Switch(config)#**interface fastethernet 6/1** Switch(config-if)#**spanning-tree guard root** Switch(config-if)# This example shows how to enable loop guard:

Related Commands	Command	Description
	show spanning-tree	Displays spanning-tree information.

spanning-tree link-type

To configure a link type for a port, use the **spanning-tree link-type** command. To return to the default settings, use the **no** form of this command.

spanning-tree link-type {**point-to-point** | **shared**}

no spanning-tree link-type

Syntax Description

point-to-point	Specifies that the interface is a point-to-point link.
shared	Specifies that the interface is a shared medium.

Defaults

Link type is derived from the duplex mode.

Command Modes

Interface configuration mode

Usage Guidelines

RSTP+ fast transition works only on point-to-point links between two bridges.

By default, the switch derives the link type of a port from the duplex mode. A full-duplex port is considered as a point-to-point link while a half-duplex configuration is assumed to be on a shared link.

If you designate a port as a shared link, RSTP+ fast transition is forbidden, regardless of the duplex setting.

Examples

This example shows how to configure the port as a shared link:

```
Switch(config)# interf spanning-tree link-type shared
Switch(config)#
```

Related Commands

Command	Description
show spanning-tree	Displays spanning-tree information.

spanning-tree loopguard default

To enable loop guard as the default on all ports of a specific bridge, use the **spanning-tree loopguard default** command. To disable loop guard, use the **no** form of this command.

spanning-tree loopguard default

no spanning-tree loopguard default

Syntax Description This command has no keywords or arguments.

Defaults Loop guard is disabled.

Command Modes Global configuration mode

Usage Guidelines Loop guard provides an additional security in the bridge network. Loop guard prevent alternate or root ports from becoming the designated port because of a failure leading to a unidirectional link.

Loop guard operates only on ports that are considered point-to-point by the spanning tree.

Individual loop guard port configuration overrides this global default.

Examples This example shows how to enable loop guard:

```
Switch(config)# spanning-tree loopguard default
Switch(config)#
```

Related Commands

Command	Description
spanning-tree guard	Enables root guard.
show spanning-tree	Displays spanning-tree information.

spanning-tree mode

To switch between PVST+ and MST modes, use the **spanning-tree mode** command. To return to the default settings, use the **no** form of this command.

spanning-tree mode {**pvst** | **mst** | **rapid-pvst**}

no spanning-tree mode {**pvst** | **mst** | **rapid-pvst**}

Syntax Description	**pvst** Specifies PVST+ mode.
	mst Specifies MST mode.
	rapid-pvst Specifies Rapid PVST mode.

Defaults PVST+ mode

Command Modes Global configuration mode

Usage Guidelines

Caution Be careful when using the **spanning-tree mode** command to switch between PVST+ and MST modes. When you enter the command, all spanning-tree instances are stopped for the previous mode and restarted in the new mode. Using this command may cause disruption of user traffic.

Examples This example shows how to switch to MST mode:

```
Switch(config)# spanning-tree mode mst
Switch(config)#
```

This example shows how to return to the default mode (PVST):

```
Switch(config)# no spanning-tree mode
Switch(config)#
```

Related Commands

Command	Description
show spanning-tree mst	Displays MST protocol information.

spanning-tree mst

To set the path cost and port-priority parameters for any interface (including the CIST with instance ID 0), use the **spanning-tree mst** command. To return to the default settings, use the **no** form of this command.

spanning-tree mst *instance-id* [*cost cost*] | [**port-priority** *prio*]

no spanning-tree mst *instance-id* [*cost* | **port-priority**]

Syntax Description	*instance-id* Instance ID number; valid values are from 0 to 15. *cost cost* (Optional) Specifies the path cost for an instance; valid values are from 1 to 200000000. **port-priority** *prio* (Optional) Specifies the port priority for an instance; valid values are from 0 to 240 in increments of 16.
Defaults	Port priority is **128**.
Command Modes	Interface configuration mode

Usage Guidelines

The higher **cost** cost values indicate higher costs. When entering the cost value, do not include a comma in the entry; for example, enter **1000**, not **1,000**.

The higher **port-priority** *prio* values indicate smaller priorities.

By default, the cost depends on the port speed; faster interface speeds indicate smaller costs. MST always uses long path costs.

Examples

This example shows how to set the interface path cost:

```
Switch(config-if)# spanning-tree mst 0 cost 17031970
Switch(config-if)#
```

This example shows how to set the interface priority:

```
Switch(config-if)# spanning-tree mst 0 port-priority 64
Switch(config-if)#
```

Related Commands	Command	Description
	show spanning-tree mst	Displays MST protocol information.
	spanning-tree port-priority	Enables an interface when two bridges compete for position as the root bridge.

spanning-tree mst configuration

To enter the MST configuration submode, use the **spanning-tree mst configuration** command. To return to the default MST configuration, use the **no** form of this command.

spanning-tree mst configuration

no spanning-tree mst configuration

Syntax Description This command has no arguments or keywords.

Defaults The default settings are as follows:

- No VLANs are mapped to any MST instance.
- All VLANs are mapped to the CIST instance.
- The region name is an empty string.
- The revision number is 0.

Command Modes Global configuration mode

Usage Guidelines The MST configuration consists of three main parameters:

- Instance VLAN mapping (see the **instance** command)
- Region name (see the **name** command)
- Configuration revision number (see the **revision** command)

By default, the value for the MST configuration is the default value for all its parameters.

The **abort** and **exit** commands allow you to exit the MST configuration submode. The difference between the two commands depends on whether you want to save your changes or not.

The **exit** command commits all the changes before leaving MST configuration submode. If you do not map the secondary VLANs to the same instance as the associated primary VLAN, when you exit the MST configuration submode, a message displays that lists the secondary VLANs that are not mapped to the same instance as the associated primary VLAN. The message is as follows:

```
These secondary vlans are not mapped to the same instance as their primary:
->3
```

The **abort** command leaves the MST configuration submode without committing any changes.

Whenever you change an MST configuration subnode parameter, it can cause a loss of connectivity. To reduce the number of service disruptions, when you enter the MST configuration submode, you are changing a copy of the current MST configuration. When you are done editing the configuration, you apply all the changes at once to the switch. You can exit the MST configuration submode without committing any changes to the configuration by using the **abort** command.

In the unlikely event that two users enter a new configuration at exactly at the same time, this message is displayed:

```
Switch(config-mst)# exit
% MST (Pre)configuration change lost because of concurrent access
Switch(config-mst)#
```

Examples

This example shows how to enter the MST configuration submode:

```
Switch(config)# spanning-tree mst configuration
Switch(config-mst)#
```

This example shows how to reset the MST configuration to the default settings:

```
Switch(config)# no spanning-tree mst configuration
Switch(config)#
```

Related Commands

Command	Description
instance	Maps a VLAN or a set of VLANs to an MST instance.
name	Sets the MST region name.
revision	Sets the MST configuration revision number.
show spanning-tree mst	Displays MST protocol information.

spanning-tree mst forward-time

To set the forward-delay time for all the instances, use the **spanning-tree mst forward-time** command. To return to the default settings, use the **no** form of this command.

spanning-tree mst forward-time *seconds*

no spanning-tree mst forward-time

Syntax Description

seconds	Number of seconds to set the forward-delay time for all the instances on the Catalyst 4500 series switch; valid values are from 4 to 30 seconds.

Defaults

The forward-delay timer is set for 15 seconds.

Command Modes

Global configuration mode

Examples

This example shows how to set the forward-delay time:

```
Switch(config)# spanning-tree mst forward-time 20
Switch(config)#
```

Related Commands

Command	Description
show spanning-tree mst	Displays MST protocol information.

spanning-tree mst hello-time

To set the hello-time delay timer for all the instances, use the **spanning-tree mst hello-time** command. To return to the default settings, use the **no** form of this command.

spanning-tree mst hello-time *seconds*

no spanning-tree mst hello-time

Syntax Description:	*seconds* Number of seconds to set the hello-time delay timer for all the instances on the Catalyst 4500 series switch; valid values are from 1 to 10 seconds.
Defaults:	The hello-time delay time is set for 2 seconds.
Command Modes:	Global configuration mode
Usage Guidelines:	If you do not specify the hello-time value, the value is calculated from the network diameter.

Examples:	This example shows how to set the hello-time delay timer:
	`Switch(config)# spanning-tree mst hello-time 3`
	`Switch(config)#`

Related Commands:	**Command** / **Description** **show spanning-tree mst** / Displays MST protocol information.

spanning-tree mst max-age

To set the max-age timer for all the instances, use the **spanning-tree mst max-age** command. To return to the default settings, use the **no** form of this command.

spanning-tree mst max-age *seconds*

no spanning-tree mst max-age

Syntax Description

seconds	Number of seconds to set the max-age timer for all the instances on the Catalyst 4500 series switch. valid values are from 6 to 40 seconds.

Defaults

The max-age timer is set for 20 seconds.

Command Modes

Global configuration mode

Examples

This example shows how to set the max-age timer:

```
Switch(config)# spanning-tree mst max-age 40
Switch(config)#
```

Related Commands

Command	Description
show spanning-tree mst	Displays MST protocol information.

spanning-tree mst max-hops

To specify the number of possible hops in the region before a BPDU is discarded, use the **spanning-tree mst max-hops** command. To return to the default settings, use the **no** form of this command.

spanning-tree mst max-hops *hopcounter*

no spanning-tree mst max-hops

Syntax Description	*hopcounter* Number of possible hops in the region before a BPDU is discarded; valid values are from 1 to 40 hops.
Defaults	Number of hops is 20.
Command Modes	Global configuration mode
Examples	This example shows how to set the number of possible hops in the region before a BPDU is discarded to 25: `Switch>(enable)set spanning-tree mst max-hops 25` `Switch>(enable)set spanning-tree mst max-hops 25`
Related Commands	**Command** / **Description** show spanning-tree mst — Displays MST protocol information.

spanning-tree mst root

To designate the primary root, secondary root, bridge priority, and timer value for an instance, use the **spanning-tree mst** root command. To return to the default settings, use the **no** form of this command.

spanning-tree mst *instance-id* **root** [**primary** | **secondary**] | [**priority** *priv*] [**diameter** *dia* [**hello-time** *hello*]]

no spanning-tree mst root

Syntax Description	*instance-id*	Instance identification number; valid values are from 1 to 15.
	root	Configures switch as the root switch.
	primary	Sets a high enough priority (low value) to make the bridge root of the spanning-tree instance.
	secondary	Designates this switch as a secondary root if the primary root fails.
	priority *priv*	Sets the bridge priority; see the "Usage Guidelines" section for valid values and additional information.
	diameter *dia*	(Optional) Sets the timer values for the bridge based on the network diameter; valid values are from 2 to 7.
	hello-time *hello*	(Optional) Specifies the duration between the generation of configuration messages by the root switch.

Defaults Bridge priority is 32768.

Command Modes Global configuration mode

Usage Guidelines The bridge priority can be set in increments of 4096 only. When you set the priority, valid values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440.

You can set the priority to 0 to make the switch root.

The **spanning-tree root secondary** bridge priority value is 16384.

The **diameter** dia and **hello-time** hello options are available for instance 0 only.

If you do not specify the hello_time value, the value is calculated from the network diameter.

Examples This example shows how to set the priority and timer values for the bridge:

```
Switch(config)# spanning-tree mst 0 root primary diameter 7 hello-time 2
Switch(config)# spanning-tree mst 5 root primary
```

Related Commands	**Command**	**Description**
	show spanning-tree mst	Displays MST protocol information.

spanning-tree pathcost method

To set the path cost calculation method, use the **spanning-tree pathcost method** command. To revert to the default setting, use the **no** form of this command.

spanning-tree pathcost method [**long** | **short**]

no spanning-tree pathcost method

Syntax Description

long	Specifies 32-bit-based values for port path costs.
short	Specifies 16-bit-based values for port path costs.

Defaults

Port path cost has 16-bit-based values.

Command Modes

Global configuration mode

Usage Guidelines

This command applies to all the spanning-tree instances on the switch.

The **long** path cost calculation method uses all the 32 bits for path cost calculation and yields values in the range of 1 through 200,000,000.

The **short** path cost calculation method (16 bits) yields values in the range of 1 through 65,535.

Examples

This example shows how to set the path cost calculation method to long:

```
Console(config)# spanning-tree pathcost method long
Console(config)#
```

This example shows how to set the path cost calculation method to short:

```
Console(config)# spanning-tree pathcost method short
Console(config)#
```

Related Commands

Command	Description
show spanning-tree	Displays spanning-tree state information.

spanning-tree portfast (interface configuration mode)

To enable PortFast mode, where the interface is immediately put into the forwarding state upon linkup without waiting for the timer to expire, use the **spanning-tree portfast** command. To return to the default setting, use the **no** form of this command.

spanning-tree portfast [disable | trunk]

no spanning-tree portfast

Syntax Description

disable	Disables PortFast on the interface.
trunk	Enables PortFast on the interface even while in the trunk mode.

Defaults

PortFast mode is disabled.

Command Modes

Interface configuration mode

Usage Guidelines

You should use this feature only with interfaces that connect to end stations; otherwise, an accidental topology loop could cause a data packet loop and disrupt the Catalyst 6500 series switch and network operation.

An interface with PortFast mode enabled is moved directly to the spanning-tree forwarding state when linkup occurs without waiting for the standard forward-time delay.

Be careful when using the **no spanning-tree portfast** command. This command does not disable PortFast if the **spanning-tree portfast default** command is enabled.

This command has four states:

- **spanning-tree portfast**—This command enables PortFast unconditionally on the given port.
- **spanning-tree portfast disable**—This command explicitly disables PortFast for the given port. The configuration line shows up in the running-configuration as it is not the default.
- **spanning-tree portfast trunk**—This command allows you to configure PortFast on trunk ports.

Note If you enter the **spanning-tree portfast trunk** command, the port is configured for PortFast even when in the access mode.

- **no spanning-tree portfast**—This command implicitly enables PortFast if the **spanning-tree portfast default** command is defined in global configuration and if the port is not a trunk port. If you do not configure PortFast globally, the **no spanning-tree portfast** command is equivalent to the **spanning-tree portfast disable** command.

Examples

This example shows how to enable PortFast mode:

```
Switch(config-if)# spanning-tree portfast
Switch(config-if)#
```

Related Commands	Command	Description
	spanning-tree cost	Calculates the path cost of STP on an interface.
	spanning-tree portfast default	Enables PortFast by default on all access ports.
	spanning-tree port-priority	Prioritizes an interface when two bridges compete for position as the root bridge.
	spanning-tree uplinkfast	Enables the UplinkFast feature.
	spanning-tree vlan	Configures STP on a per VLAN basis.
	show spanning-tree	Displays spanning-tree state information.

spanning-tree portfast bpdufilter default

To enable the BPDU filtering by default on all PortFast ports, use the **spanning-tree portfast bpdufilter default** command. To return to the default settings, use the **no** form of this command.

spanning-tree portfast bpdufilter default

no spanning-tree portfast bpdufilter default

Syntax Description This command has no keywords or arguments.

Defaults BPDU filtering is disabled.

Command Modes Global configuration mode

Usage Guidelines The **spanning-tree portfast bpdufilter default** command enables BPDU filtering globally on the Catalyst 4500 series switch. BPDU filtering prevents a port from sending or receiving any BPDUs.

You can override the effects of the **spanning-tree portfast bpdufilter default** command by configuring BPDU filtering at the interface level.

Note Be careful when enabling BPDU filtering. Functionality is different when enabling on a per-port basis or globally. When enabled globally, BPDU filtering is applied only on ports that are in an operational PortFast state. Ports still send a few BPDUs at linkup before they effectively filter outbound BPDUs. If a BPDU is received on an edge port, it immediately loses its operational PortFast status and BPDU filtering is disabled.

When enabled locally on a port, BPDU filtering prevents the Catalyst 4500 series switch from receiving or sending BPDUs on this port.

Caution Be careful when using this command. This command can cause bridging loops if not used correctly.

Examples This example shows how to enable BPDU filtering by default:

```
Switch(config)# spanning-tree portfast bpdufilter
default
Switch(config)#
```

Related Commands

Command	Description
show spanning-tree mst	Displays MST protocol information.
spanning-tree bpdufilter	Enables BPDU filtering on an interface.

spanning-tree portfast bpduguard default

To enable BPDU guard by default on all the PortFast ports, use the **spanning-tree portfast bpduguard default** command. To return to the default settings, use the **no** form of this command.

spanning-tree portfast bpduguard default

no spanning-tree portfast bpduguard default

Syntax Description This command has no keywords or arguments.

Defaults BPDU guard is disabled.

Command Modes Global configuration mode

Usage Guidelines

Caution Use this command only with the interfaces that connect to the end stations; otherwise, an accidental topology loop could cause a data packet loop and disrupt the Catalyst 4500 series switch and network operation.

BPDU guard disables a port if it receives a BPDU. BPDU guard is applied only on ports that are PortFast enabled and are in an operational PortFast state.

Examples This example shows how to enable BPDU guard by default:

```
Switch(config)# spanning-tree portfast bpduguard default
Switch(config)#
```

Related Commands

Command	Description
show spanning-tree mst	Displays MST protocol information.
spanning-tree bpduguard	Enables BPDU guard on an interface.

spanning-tree portfast default

To globally enable PortFast by default on all access ports, use the **spanning-tree portfast default** command. To disable PortFast as default on all access ports, use the **no** form of this command.

spanning-tree portfast default

no spanning-tree portfast default

Syntax Description This command has no arguments or keywords.

Defaults PortFast is disabled.

Command Modes Global configuration mode

Usage Guidelines

Caution Use this command only with the interfaces that connect to end stations; otherwise, an accidental topology loop could cause a data packet loop and disrupt the Catalyst 4500 series switch and network operation.

An interface with PortFast mode enabled is moved directly to the spanning-tree forwarding state when linkup occurs without waiting for the standard forwardtime delay.

You can enable PortFast mode on individual interfaces using the **spanning-tree portfast (interface configuration mode)** command.

Examples This example shows how to globally enable PortFast by default on all access ports:

```
Switch(config)# spanning-tree portfast default
Switch(config)#
```

Related Commands

Command	Description
show spanning-tree	Displays spanning-tree state information.
spanning-tree portfast (interface configuration mode)	Enables PortFast mode.

spanning-tree port-priority

To prioritize an interface when two bridges compete for position as the root bridge, use the **spanning-tree port-priority** command. The priority you set resolves the conflict. To revert to the default setting, use the **no** form of this command.

spanning-tree port-priority *port_priority*

no spanning-tree port-priority

Syntax Description	*port_priority* Port priority; valid values are from 0 to 240 in increments of 16.
Defaults	Port priority value is set to 128.
Command Modes	Interface configuration mode

Examples

This example shows how to increase the possibility that the spanning-tree instance 20 will be chosen as the root-bridge on interface fastEthernet 2/1:

```
Switch(config-if)# spanning-tree port-priority 4
Switch(config-if)#
```

Related Commands

Command	Description
spanning-tree cost	Calculates the path cost of STP on an interface.
spanning-tree portfast default	Enables PortFast by default on all access ports.
spanning-tree portfast (interface configuration mode)	Enables PortFast mode.
spanning-tree uplinkfast	Enables the UplinkFast feature.
spanning-tree vlan	Configures STP on a per-VLAN basis.
show spanning-tree	Displays spanning-tree state information.

spanning-tree uplinkfast

To enable the UplinkFast feature, use the **spanning-tree uplinkfast** command. To disable UplinkFast, use the **no** form of this command.

spanning-tree uplinkfast [max-update-rate *packets-per-second*]

no spanning-tree uplinkfast [max-update-rate]

Syntax Description | *max-update-rate packets_per_second* | (Optional) Specifies the maximum rate (packets per second) at which UplinkFast packets are sent; valid values are from 0 to 65,535.

Defaults | The default settings are as follows:
- Disabled.
- Maximum update rate is 150.

Command Modes | Global configuration mode

Usage Guidelines | This command should be used only on access switches.

When UplinkFast is configured, the bridge priority is changed to 49,152 so that this switch will not be selected as root. All interface path costs of all spanning-tree interfaces belonging to the specified spanning-tree instances are also increased by 3000.

When spanning-tree detects that the root interface has failed, the UplinkFast feature causes an immediate switchover to a new root port and begins sending packets with its station address as the source address. During this time, a topology change notification occurs. To minimize the disruption caused by the topology change, a multicast packet is sent to 01-00-0C-CD-CD-CD for each station address in the forwarding bridge except for those associated with the old root interface.

Use the **spanning-tree uplinkfast max-update-rate** command to enable UplinkFast (if not already enabled) and change the rate at which the update packets are sent. Use the **no** form of this command to return the default rate of 150 packets per second.

Examples | This example shows how to enable UplinkFast and set the maximum rate to 200 packets per second:

```
Switch(config)# spanning-tree uplinkfast
Switch(config)# spanning-tree uplinkfast max-update-rate 200
```

Related Commands

Command	Description
spanning-tree cost	Calculates the path cost of STP on an interface.
spanning-tree port-priority	Prioritizes an interface when two bridges compete for position as the root bridge.
spanning-tree portfast default	Enables PortFast by default on all access ports.

Command	Description
spanning-tree portfast (interface configuration mode)	Enables PortFast mode.
spanning-tree vlan	Configures STP on a per-VLAN basis.

spanning-tree vlan

To configure STP on a per-VLAN basis, use the **spanning-tree vlan** command. To return to the default value, use the **no** form of this command.

spanning-tree vlan *vlan_id* [**forward-time** *seconds*] [**hello-time** *seconds*] [**max-age** *seconds*] [**priority** *priority*] [**protocol** *protocol*] [**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 identification number; valid values are from 1 to 4094.
forward-time *seconds*	(Optional) Sets the STP forward delay time; valid values are from 4 to 30 seconds.
hello-time *seconds*	(Optional) Specifies, in seconds, the time between configuration messages generated by the root switch; valid values are from 1 to 10 seconds.
max-age *seconds*	(Optional) Sets the maximum time, in seconds, that the information in a BPDU is valid; valid values are from 6 to 40 seconds.
priority *priority*	(Optional) Sets the STP bridge priority; valid values are from 0 to 65535.
protocol *protocol*	(Optional) Specifies the protocol.
root primary	(Optional) Forces this switch to be the root bridge.
root secondary	(Optional) Specifies this switch act as the root switch should the primary root fail.
diameter *net-diameter*	(Optional) Specifies the maximum number of bridges between two end stations; valid values are from 2 to 7.

Defaults

The default settings are as follows:

- Forward-time—15 seconds
- Hello-time—2 seconds
- Max-age—20 seconds
- Priority—32768 with STP enabled; 128 with MST enabled
- Root—No STP *vlan*

Command Modes

Global configuration mode

Usage Guidelines

When you are setting the **max-age** seconds value, if a bridge does not hear BPDUs from the root bridge within the specified interval, it assumes that the network has changed and recomputes the spanning-tree topology.

The **spanning-tree root primary** command alters the switch bridge priority to 8192. If you enter the **spanning-tree root primary** command and the switch does not become root, then the bridge priority is changed to 100 less than the bridge priority of the current bridge. If the switch does not become root, an error message will result.

The **spanning-tree root secondary** command alters the switch bridge priority to 16384. If the root switch fails, this switch becomes the next root switch.

Use the **spanning-tree root** commands on backbone switches.

Examples

This example shows how to enable spanning tree on VLAN 200:

```
Switch(config)# spanning-tree vlan 200
Switch(config)#
```

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
Switch(config)#
```

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
Switch(config)#
```

Related Commands

Command	Description
spanning-tree cost	Calculates the path cost of STP on an interface.
spanning-tree port-priority	Prioritizes an interface when two bridges compete for position as the root bridge.
spanning-tree portfast default	Enables PortFast by default on all access ports.
spanning-tree portfast (interface configuration mode)	Enables PortFast mode.
spanning-tree vlan	Configures STP on a per-VLAN basis.
show spanning-tree	Displays spanning-tree state information.

speed

To configure the interface speed, use the **speed** command. To disable a speed setting, use the **no** form of this command.

speed [10 | 100 | 1000 | auto | 10| 100| 1000 | nonegotiate]

no speed

Syntax Description

10	Configures the interface to transmit at 10 Mbps.
100	Configures the interface to transmit at 100 Mbps.
1000	Configures the interface to transmit at 1000 Mbps.
**auto 10	100	1000**	Enables the interface to autonegotiate the speed and/or duplex the exact values to advertise when autonegotiating.
nonegotiate	Enables the interface to not negotiate the speed.

Defaults

The default values are shown in the following table:

Interface Type	Supported Syntax	Default Setting
10/100 Mbps module	**speed [10	100	auto	10	100]**	Auto
100 Mbps fiber modules	Not applicable	Not applicable
Gigabit Ethernet Interface	**Speed nonegotiate**	Nonegotiate
10/100/1000	**speed [10	100| 1000	auto	10	100	1000]**	Auto
1000	Not applicable	Not applicable

Command Modes

Interface configuration mode

Usage Guidelines

Table 2-25 lists the supported command options by interface.

Table 2-25 *Supported speed Command Options*

Interface Type	Supported Syntax	Default Setting	Guidelines
10/100 Mbps module	**speed [10	100	auto]**	Auto	If the speed is set to 10 or 100 and you do not configure the duplex setting, the duplex is set to half.
100 Mbps fiber modules	Not applicable.	Not applicable.	Not applicable.
Gigabit Ethernet Interface	**Speed nonegotiate**	**nonegotiate** is enabled.	This is only applicable to Gigabit Ethernet ports.

Table 2-28 *Supported speed Command Options (continued)*

Interface Type	Supported Syntax	Default Setting	Guidelines
100 BASE-X(SX)	**speed** [**10**|**100**|**1000**|**auto**]	**auto**	If the speed is set to 10 or 100 and you do not configure the duplex setting, the duplex is set to half. If the speed is set to 1000 or auto with 1000 BASE-X(SX) port, you can only configure the duplex setting. If the **speed auto** or a 10/100/1000 port, you will not able to set half duplex.
1000	Not applicable.	Not applicable.	The speed is always 1000. The duplex is half.

If you configure the interface speed and duplex commands manually and enter a value other than **speed auto** (for example, 10 or 100 Mbps), there is a risk that you might cause the connecting interface speed command or a matching speed but do not use the auto parameter.

When manually configuring the interface speed to either 10 or 100 Mbps, the switch prompts you to also configure duplex mode on the interface.

Note Catalyst 4506 series has cannot automatically negotiate the interface speed and the duplex mode if either connecting interface is configured to a value other than **auto**.

Caution Changing the interface speed and the duplex mode configuration might shut down and reenable the interface during the reconfiguration.

Table 2-29 describes the system's performance for different combinations of the duplex and speed modes. The specified **duplex** command that is configured with the specified **speed** command produces the resulting system action.

Table 2-29 *System Action Using duplex and speed Commands*

duplex Command	speed Command	Resulting System Action
duplex auto	**speed auto**	Autonegotiates both speed and duplex modes
duplex half	**speed 10**	Forces 10 Mbps and half duplex
duplex half	**speed 10**	Forces 10 Mbps and half duplex
duplex half	**speed 100**	Forces 100 Mbps and half duplex
duplex half	**speed 100**	Forces 100 Mbps and half duplex
duplex half	**speed 1000**	Forces 1000 Mbps and half duplex

Examples This example shows how to set the interface speed to 100 Mbps on the Fast Ethernet interface 5/4:

```
Switch(config)# interface FastEthernet 5/4
Switch(config-if)# speed 100
```

This example shows how to allow Fast Ethernet interface 5/1 to autonegotiate the speed and duplex mode:

```
Switch(config)# interface fastethernet 5/1
Switch(config-if)# speed auto
```

Note The **speed auto 10 100** command is similar to the **speed auto** command on a Fast Ethernet interface.

This example shows how to limit the interface speed to 10 and 100 Mbps on the Gigabit Ethernet interface 1/1 in auto-negotiation mode:

```
Switch(config)# interface gigabitethernet 1/1
Switch(config-if)# speed auto 10 100
```

This example shows how to limit the speed negotiation to 100 Mbps on the Gigabit Ethernet interface 1/1:

```
Switch(config)# interface gigabitethernet 1/1
Switch(config-if)# speed auto 100
```

Related Commands

Command	Description
duplex	Configures the duplex operation on an interface.
interface (refer to Cisco IOS documentation)	Configures an interface type and enter interface configuration mode.
show controller (refer to Cisco IOS documentation)	Displays controller information.
show interfaces	Displays interface status specific interface.

storm-control

To enable broadcast storm control on a port and to specify what to do when a storm occurs on a port, use the **storm-control** interface configuration command. To disable storm control for the broadcast traffic and to disable a specified storm control action, use the **no** form of this command.

storm-control {broadcast level *high level low level* **[action {shutdown | trap}]}**

no storm-control {broadcast level *level* **[lower level]} [action {shutdown | trap}]**

Syntax Description

broadcast	Enables the broadcast storm control on the port.
level *high level low level*	Defines the rising and falling suppression levels: • *high level*—Rising suppression level as a percent of total bandwidth, up to two decimal places; valid values are from 0 to 100 percent. Block the flooding of storm packets when the value specified for *level* is reached. • *lower level*—(Optional) Falling suppression level as a percent of total bandwidth, up to two decimal places; valid values are from 0 to 100. This value must be less than the rising suppression value.
action shutdown	Directs the switch to take action when a storm occurs on a port. Disables the port during a storm.
trap	Sends an SNMP trap when a storm occurs. This keyword is available but not supported in 12.1(19)EW.

Defaults

Broadcast storm control is disabled.

Command Modes

Interface configuration mode

Usage Guidelines

Enter the **storm-control broadcast level** command to enable traffic storm control on the interface, configure the traffic storm control level, and apply the traffic storm control level to the broadcast traffic on the interface.

The Catalyst 4500 series switch supports broadcast traffic storm control on all LAN ports.

The period is required when you enter the fractional suppression level.

The suppression level is entered as a percentage of the total bandwidth. A threshold value of 100 percent indicates that no limit is placed on traffic. A value of 0.0 means that all specified traffic on that port is blocked.

Enter the **show interfaces counters storm-control** command to display the discard count.

Enter the **show running-config** command to display the enabled suppression mode and level setting.

To turn off suppression for the specified traffic type, you can do one of the following:

- Set the *high-level* value or 100 percent for the specified traffic type.

- Use the **no** form of this command.

The lower level is ignored for the interfaces that perform storm-control in the hardware.

Examples

This example shows how to enable broadcast storm control on a port with a 75.67 percent rising suppression level:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 3/1
Switch(config-if)# storm-control broadcast level 75.67
Switch(config-if)# end
```

This example shows how to disable the port during a storm:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 3/1
Switch(config-if)# storm-control action shutdown
Switch(config-if)# end
```

This example shows how to disable storm control on a port:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 3/1
Switch(config-if)# no storm-control broadcast level
Switch(config-if)# end
```

This example shows how to disable storm control by setting the high level to 100 percent:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 3/1
Switch(config-if)# storm-control broadcast level 100
Switch(config-if)# end
```

Related Commands

Command	Description
show interfaces counters	Displays the traffic on the physical interface.
show running-config	Displays the running configuration of a switch.

storm-control broadcast include multicast

To enable multicast storm control on a port, use the **storm-control broadcast include multicast** command. To disable multicast storm control, use the **no** form of this command.

storm-control broadcast include multicast

no storm-control broadcast include multicast

Syntax Description This command has no arguments or keywords.

Defaults Multicast storm control is disabled.

Command Modes Interface configuration mode

Usage Guidelines This command prompts the hardware to filter multicast packets if it is already filtering broadcast packets.

The Catalyst 4500 series switch supports unicast/multicast suppression. When you enable multicast suppression on an interface you subject incoming multicast and broadcast traffic on that interface to suppression.

Examples This example shows how to enable multicast storm control globally:

```
Switch#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface gigabitethernet1/1 broadcast include multicast
Switch(config)# end
```

This example shows how to enable per-port Multicast storm control:

```
Switch#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet1/1
Switch(config-if)# storm-control broadcast include multicast
Switch(config)# end
```

Related Commands

Command	Description
show storm-control	Displays broadcast storm control on a port and and specifies what to do when a storm occurs on a port.

subscribe-to-alert-group-all

To subscribe to all available alert groups, use the **subscribe-to-alert-group-all** command.

subscribe-to-alert-group-all

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes cfg-call-home-profile

Usage Guidelines To enter profile call-home configuration submode, use the **profile** command in call-home configuration mode.

Examples This example chose how to subscribe to all available alert groups:

```
Switch(config)# call-home
Switch(cfg-call-home)# profile alert
Switch(cfg-call-home-profile)# subscribe-to-alert-group all
```

Related Commands

Command	Description
destination address	Configures the destination e-mail address or URL to which Call Home messages will be sent.
destination message-size-limit bytes	Configures a maximum destination message size for the destination profile.
destination preferred-msg-format	Configures a preferred message format.
destination transport-method	Enables the message transport method.
profile	Enters profile call-home configuration submode.
subscribe-to-alert-group configuration	Subscribes this destination profile to the Configuration alert group.
subscribe-to-alert-group diagnostic	Subscribes this destination profile to the diagnostic alert group.
subscribe-to-alert-group environment	Subscribes this destination profile to the environment alert group.
subscribe-to-alert-group inventory	Subscribes this destination profile to the inventory alert group.
subscribe-to-alert-group syslog	Subscribes this destination profile to the Syslog alert group.

subscribe-to-alert-group configuration

To subscribe a destination profile to the Configuration alert group, use the **subscribe-to-alert-group configuration** command.

subscribe-to-alert-group configuration [**periodic** [**daily** *hh:mm* | **monthly** *date hh:mm* | **weekly** *day hh:mm*]]

Syntax Description		
	periodic	(Optional) Specifies a periodic call-home message.
	daily *hh:mm*	Sets a daily alert in hours and minutes.
	monthly *date hh:mm*	Sets a monthly alert in day, hour, and minute.
	weekly *day hh:mm*	Sets a weekly alert in day, hour, and minutes.

Defaults	
	This command has no default settings.

Command Modes	
	cfg-call-home profile

Usage Guidelines	
	To error profile call-home configuration submode, use the **profile** command in call-home configuration mode.
	The Configuration alert group can be configured for periodic notification.

Examples	

	This example shows how to configure periodic "configuration" alert-group:
	`Switch(config)# call-home`
	`Switch(cfg-call-home)# profile alert`
	`Switch(cfg-call-home-profile)# subscribe-to-alert-group configuration periodic weekly Monday 21:10`

Related Commands	Command	Description
	destination address	Configures the destination e-mail address or URL to which Call Home messages will be sent.
	destination message-size-limit bytes	Configures a maximum destination message size for the destination profile.
	destination preferred-msg-format	Configures a preferred message format.
	destination transport-method	Enables the message transport method.
	profile	Enters profile call-home configuration submode
	subscribe-to-alert-group all	Subscribes to all available alert groups.
	subscribe-to-alert-group diagnostic	Subscribes this destination profile to the Diagnostic alert group.
	subscribe-to-alert-group environment	Subscribes this destination profile to the Environment alert group.

Command	Description
subscribe-to-alert-group inventory	Subscribes this destination profile to the inventory alert group.
subscribe-to-alert-group syslog	Subscribes this destination profile to the syslog alert group.

subscribe-to-alert-group diagnostic

To subscribe a destination profile to the Diagnostic alert group, use the **subscribe-to-alert-group diagnostic** command.

subscribe-to-alert-group diagnostic [severity catastrophic | disaster | fatal | critical | major | minor | warning | notification | normal | debugging]

Syntax Description	**severity catastrophic** (Optional) Specifies network with catastrophic failure (highest severity). **disaster** (Optional) Specifies significant network impact. **fatal** (Optional) Specifies that the system is unusable (system log level 0). **critical** (Optional) Specifies that immediate attention is needed (system log level 1). **major** (Optional) Specifies a major condition (System log level 2). **minor** (Optional) Specifies a minor condition (System log level 3). **warning** (Optional) Specifies a warning condition (System log level 4). **notification** (Optional) Specifies an informational message (system log level 5). **normal** (Optional) Specifies returning to a normal state (System log level 6). **debugging** (Optional) Specifies a debugging message (Lowest severity).
Defaults	**normal**
Command Modes	cfg-call-home-profile
Usage Guidelines	To enter profile call-home configuration submode, use the **profile** command in call-home configuration mode.

Examples	This example shows how to configure the "diagnostic" alert-group with "normal" severity:
	`Switch(cfg-call-home)# call-home`
	`Switch(cfg-call-home)# profile alerts`
	`Switch(cfg-call-home-profile)# subscribe-to-alert-group diagnostic severity normal`

Related Commands:	Command	Description
	destination address	Configures the destination e-mail address or URL to which Call Home messages will be sent.
	destination message-size-limit bytes	Configures a maximum destination message size for the destination profile.
	destination preferred-msg-format	Configures a preferred message format.
	destination transport-method	Enables the message transport method.
	profile	Enters profile call-home configuration submode

Command	Description
subscribe-to-alert-group all	Subscribes to all available alert groups.
subscribe-to-alert-group configuration	Subscribes this destination profile to the Configuration alert group.
subscribe-to-alert-group environment	Subscribes this destination profile to the Environment alert group.
subscribe-to-alert-group inventory	Subscribes this destination profile to the Inventory alert group.
subscribe-to-alert-group syslog	Subscribes this destination profile to the Syslog alert group.

subscribe-to-alert-group environment

To subscribe a destination profile to the Environment alert group, use the **subscribe-to-alert-group environment** command.

subscribe-to-alert-group environment [**severity** *catastrophic* | **disaster** | **fatal** | **critical** | **major** | **minor** | **warning** | **notification** | **normal** | **debugging**]

Syntax Description	**severity** *catastrophic* (Optional) Specifies network wide catastrophic failure (highest severity).
	disaster (Optional) Specifies significant network impact.
	fatal (Optional) Specifies that the system is unusable (system log level 0).
	critical (Optional) Specifies that immediate attention is needed (system log level 1).
	major (Optional) Specifies a major condition (System log level 2).
	minor (Optional) Specifies a minor condition (System log level 3).
	warning (Optional) Specifies a warning condition (system log level 4).
	notification (Optional) Specifies an informational message (system log level 5).
	normal (Optional) Specifies returning to a normal state (System log level 6).
	debugging (Optional) Specifies a debugging message (Lowest severity).
Defaults	**normal**
Command Modes	**cfg-call-home-profile**
Usage Guidelines	To enter profile call-home configuration submode, use the **profile** command in call-home configuration mode. The Environment alert group can be configured to filter messages based on severity.

Examples	This example shows how to configure the "environmental" alert-group with "severity notification":
	`Switch(config)# call-home`
	`Switch(cfg-call-home)# profile alerts`
	`Switch(cfg-call-home-profile)# subscribe-to-alert-group environment severity notification`

Related Commands	Command	Description
	profile	Enters profile call-home configuration submode
	destination address	Configures the destination e-mail address or URL to which Call Home messages will be sent.
	destination message-size-limit bytes	Configures a maximum destination message size for the destination profile.
	destination preferred-msg-format	Configures a preferred message format.

Command	Description
destination transport-method	Enables the message transport method.
subscribe-to-alert-group all	Subscribes to all available alert groups.
subscribe-to-alert-group configuration	Subscribes this destination profile to the Configuration alert group.
subscribe-to-alert-group diagnostic	Subscribes this destination profile to the diagnostic alert group.
subscribe-to-alert-group inventory	Subscribes this destination profile to the inventory alert group.
subscribe-to-alert-group syslog	Subscribes this destination profile to the Syslog alert group.

subscribe-to-alert-group inventory

To subscribe a destination profile to the Inventory alert group, use the **subscribe-to-alert-group inventory** command.

subscribe-to-alert-group inventory [**periodic** [**daily** *hh:mm* | **monthly** *date hh:mm* | **weekly** *day hh:mm*]]

Syntax Description

periodic	(Optional) Specifies a periodic call-home message.
daily *hh:mm*	Sets a daily alert to hours and minutes.
monthly *date hh:mm*	Sets a monthly alert to day, hour, and minute.
weekly *day hh:mm*	Sets a weekly alert to day, hour, and minutes.

Defaults

This command has no default settings.

Command Modes

cfg-call-home-profile

Usage Guidelines

To enter profile call-home configuration submode, use the **profile** command in call-home configuration mode.

The Inventory alert group can be configured for periodic notification.

Examples

This example shows how to configure the Inventory alert group with periodic daily alert at 21:12":

```
Switch(config)# call-home
Switch(cfg-call-home)# profile user
Switch(cfg-call-home-profile)# subscribe-to-alert-group inventory periodic daily 21:12
```

Related Commands

Command	Description
destination address	Configures the destination e-mail address or URL to which Call Home messages will be sent.
destination message-size-limit bytes	Configures a maximum destination message size for the destination profile.
destination preferred-msg-format	Configures a preferred message format.
destination transport-method	Enables the message transport method.
profile	Enters profile call-home configuration submode.
subscribe-to-alert-group all	Subscribes to all available alert groups.
subscribe-to-alert-group configuration	Subscribes this destination profile to the Configuration alert group.
subscribe-to-alert-group diagnostic	Subscribes this destination profile to the Diagnostic alert group.

Command	Description
subscribe-to-alert-group-environment	Subscribes this destination profile to the Environment alert group.
subscribe-to-alert-group-syslog	Subscribes this destination profile to the Syslog alert group.

subscribe-to-alert-group syslog

To subscribe this destination profile to the Syslog alert group, use the **subscribe-to-alert-group syslog** command.

subscribe-to-alert-group syslog [severity catastrophic | disaster | fatal| critical | major |minor | warning | notification | normal | debugging | pattern string]

Syntax Description	**severity catastrophic** (Optional) Specifies network wide catastrophic failure (highest severity).
	disaster (Optional) Specifies significant network impact.
	fatal (Optional) Specifies that the system is unusable (system log level 0).
	critical (Optional) Specifies that immediate attention is needed (system log level 1).
	major (Optional) Specifies a major condition (Syslog level 2).
	minor (Optional) Specifies a minor condition (Syslog log level 3).
	warning (Optional) Specifies a warning condition (Syslog log level 4).
	notification (Optional) Specifies an informational message (system log level 5).
	normal (Optional) Specifies returning to a normal state (System log level 5).
	debugging (Optional) Specifies a debugging message (Lowest severity).
Defaults	normal
Command Modes	cfg-call-home-profile

Usage Guidelines	To error profile call-home configuration submode, use the **profile** command in call-home configuration mode.
	You can configure the Syslog alert group can be configured to filter messages based on severity by specifying a pattern to be matched in the syslog message. If the pattern contain spaces, you must enclose it in quotes ("").
	Examples
	This example shows how to configure the syslog alert group with severity notification:
	`Switch(config)# call-home`
	`Switch(cfg-call-home)# profile cisco`
	`Switch(cfg-call-home-profile)# subscribe-to-alert-group syslog severity notification pattern "SYSMON"`

Related Commands	**Command**	**Description**
	destination address	Configures the destination e-mail address or URL to which Call-Home messages will be sent.
	destination message-size-limit bytes	Configures a maximum destination message size for the destination profile.

Command	Description
destination preferred-msg-format	Configures a preferred message format.
destination transport-method	Enables the message transport method.
profile	Enters profile call-home configuration submode.
subscribe-to-alert-group all	Subscribes to all available alert groups.
subscribe-to-alert-group configuration	Subscribes this destination profile to the Configuration alert group.
subscribe-to-alert-group diagnostic	Subscribes this destination profile to the Diagnostic alert group.
subscribe-to-alert-group environment	Subscribes this destination profile to the Environment alert group.
subscribe-to-alert-group inventory	Subscribes this destination profile to the Inventory alert group.

switchport

To modify the switching characteristics of a Layer 2 switch interface, use the **switchport** command. To return the interface to the routed-interface status and cause all further Layer 2 configuration to be erased, use the **no** form of this command without parameters.

switchport [**access** [**vlan** *vlan_num*] | [**nonegotiate**] | [**voice vlan** {*vlan_id*| **dot1p** | **none**| **untagged**}]

no switchport [**access** | **nonegotiate** | **voice vlan**]

Syntax Description

access vlan *vlan_num*	(Optional) Sets the VLAN when the interface is in access mode; valid values are from 1 to 1001.
nonegotiate	(Optional) Specifies that the DISL DTP negotiation packets will not be sent on the interface.
voice vlan *vlan_id*	(Optional) Specifies the number of the VLAN; valid values are from 1 to 1001.
dot1p	(Optional) Specifies that the P1Q6 packets are tagged as priority.
none	(Optional) Specifies that the telephone and voice VLAN do not communicate.
untagged	(Optional) Specifies the untagged P1Q3 packets.

Defaults

The default settings are as follows:

- Switchport trunking mode is enabled.
- Dynamic negotiation parameter is set to auto.
- Access VLANs and trunk interface native VLANs are a default VLAN corresponding to the platform or interface hardware.
- All VLAN lists include all VLANs.
- No voice VLAN is enabled.

Command Modes

Interface configuration mode

Usage Guidelines

The **no switchport** command shuts the port down and then reenables it, which may generate messages on the device to which the port is connected.

The **no** form of the **switchport access** command resets the access mode VLAN to the appropriate default VLAN for the device. The **no** form of the **switchport nonegotiate** command removes the **nonegotiate** status.

When you are using the **nonegotiate** keyword, DISL/DTP negotiation packets will not be sent on the interface. The device will trunk or not trunk according to the **mode** parameter given: **access** or **trunk**. This command will return an error if you attempt to execute it in **dynamic** (**auto** or **desirable**) mode.

The voice VLAN is automatically set to VLAN 1 unless you use one of the optional keywords.

If you use the **switch port voice vlan** command for an interface, the interface cannot join a port channel.

When you use the **switchport voice vlan** command, the output for the **show running-config** command changes to show the voice VLAN set.

Examples

This example shows how to cause the port interface to stop operating as a Cisco-trusted port and convert to a Layer 2-switched interface:

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

This example shows how to cause a port interface in access mode, which is configured as a switched interface, to operate in VLAN 2:

```
Switch(config-if)# switchport access vlan 2
Switch(config-if)#
```

This example shows how to cause a port interface, which is configured as a switched interface, to refrain from negotiating in trunking mode and act as a trunk or access port (depending on the **mode** set):

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

This example shows how to set the voice VLAN for the interface to VLAN 2:

```
Switch(config-if)# switchport voice vlan 2
switchport voice vlan 2
Switch(config-if)#
```

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.

switchport access vlan

To set the VLAN whose interface is in access mode, use the **switchport access vlan** command. To reset the access mode VLAN to the appropriate default VLAN for the device, use the form of this command.

switchport access [**vlan** *vlan-id* | **dynamic**]

no switchport access vlan

Syntax Description

vlan-id (Optional) Number of the VLAN on the interface in access mode; valid values are from 1 to 4094.

dynamic (Optional) Enables VMPS control of the VLAN.

Defaults

The default settings are as follows:

- The access VLAN and trunk interface native VLAN are default VLANs that corresponds to the platform or the interface hardware.
- All VLAN lists include all VLANs.

Command Modes

Interface configuration mode

Usage Guidelines

You must enter the **switchport** command without any keywords to configure the LAN interface as a Layer 2 interface before you can enter the **switchport access vlan** command. This action is required only if you have not already entered the **switchport** command for the interface.

Entering the **no switchport** command shuts the port down and then reenables it, which could generate messages on the device to which the port is connected.

The **no** form of the **switchport access vlan** command resets the access mode VLAN to the appropriate default VLAN for the device.

Valid values for *vlan-id* are from 1 to 4094.

Examples

This example shows how to cause the port interface to stop operating as a Cisco-routed port and connect it as a Layer 2-switched interface:

```
Switch(config)#int g1/0/4 switchport
Switch(config)#int g1/0/4
```

Note This command 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.

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)#int g1/0/4 switchport access vlan 2
Switch(config)#int g1/0/4
```

Related Commands	Command	Description
	show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.

switchport autostate exclude

To exclude a port from the VLAN interface link-up calculation, use the **switchport autostate exclude** command. To return to the default settings, use the **no** form of this command.

switchport autostate exclude

no switchport autostate exclude

Syntax Description This command has no keywords or arguments.

Defaults All ports are included in the VLAN interface link-up calculation.

Command Modes Interface configuration mode

Usage Guidelines You must enter the **switchport** command without any keywords to configure the LAN interface as a Layer 2 interface before you can enter the **switchport autostate exclude** command. This action is required only if you have not entered the **switchport** command for the interface.

Note The **switchport** command is not used on platforms that do not support Cisco-routed ports. All physical ports on such platforms are assumed to be Layer 3-switched interfaces.

The **switchport autostate exclude** command marks the port to be excluded from the interface VLAN up calculation when there are multiple ports in the VLAN.

The **show interface** *interface-id***switport** command displays the autostate mode if the mode has been set. If the mode has not been set, the autostate mode is not displayed.

Examples This example shows how to exclude a port from the VLAN interface link-up calculation:

```
Switch(config)#int g1/1/4 switchport autostate exclude
Switch(config)#int g1/1/4
```

This example shows how to include a port in the VLAN interface link-up calculation:

```
Switch(config)#int g1/1/4 no switchport autostate exclude
Switch(config)#int g1/1/4
```

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

Related Commands	Command	Description
	show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.

switchport block

To prevent the unknown multicast or unicast packets from being forwarded, use the **switchport block** interface configuration command. To allow the unknown multicast or unicast packets to be forwarded, use the **no** form of this command.

switchport block {multicast | unicast}

no switchport block {multicast | unicast}

Syntax Description

multicast	Specifies that the unknown multicast traffic should be blocked.
unicast	Specifies that the unknown unicast traffic should be blocked.

Defaults

Unknown multicast and unicast traffic are not blocked.

All traffic with unknown MAC addresses is sent to all ports.

Command Modes

Interface-configuration mode

Usage Guidelines

You can block the unknown multicast or unicast traffic on the switch ports.

Blocking the unknown multicast or unicast traffic is not automatically enabled on the switch ports; you must explicitly configure it.

Note For more information about blocking the packets, refer to the software configuration guide for this release.

Examples

This example shows how to block the unknown multicast traffic on an interface:

```
Switch(config)# interface fastethernet 5/1
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.

switchport mode

To set the interface type, use the **switchport mode** command. To revert the mode to the appropriate default mode for the device, use the **no** form of this command.

switchport mode {**access** | **dot1q-tunnel** | **trunk** | **dynamic** {**auto** | **desirable**} }

switchport mode private-vlan {**host** | **promiscuous** | **trunk promiscuous**| **trunk** {**secondary**} }

no switchport mode dot1q-tunnel

no switchport mode private-vlan

Syntax Description

access	Specifies a nontrunking, nontagged single VLAN Layer 2 interface.
dot1q-tunnel	Specifies an 802.1Q tunnel port.
trunk	Specifies a trunking VLAN Layer 2 interface.
dynamic auto	Specifies that the interface convert the link to a trunk link.
dynamic desirable	Specifies that the interface actively attempt to convert the link to a trunk link.
private-vlan host	Specifies that the ports with a valid PVLAN trunk association become active host private VLAN trunk ports.
private-vlan promiscuous	Specifies that the ports with a valid PVLAN mapping become active promiscuous ports.
private-vlan trunk promiscuous	Specifies that the ports with valid PVLAN trunk mapping become active promiscuous trunk ports.
private-vlan trunk secondary	Specifies that the ports with a valid PVLAN trunk association become active host private VLAN trunk ports.

Defaults

Link converts to a trunk link.

dot1q-tunnel ports are disabled.

Command Modes

Interface configuration mode

Usage Guidelines

If you enter **access** mode, the interface goes into permanent nontrunking mode and negotiates to convert the link into a nontrunk link even if the neighboring interface does not approve the change.

If you enter **trunk** mode, the interface goes into permanent trunking mode and negotiates to convert the link into a trunk link even if the neighboring interface does not approve the change.

If 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.

If you enter **dynamic desirable** mode, the interface becomes a trunk interface if the neighboring interface is set to **trunk**, **desirable**, or **auto** mode.

If you specify the **dot1q-tunnel keyword**, the port is set unconditionally as an 802.1Q tunnel port.

The port becomes inactive if you configure it as a private VLAN trunk port and one of the following applies:

- The port does not have a valid PVLAN association.
- The port does not have valid allowed normal VLANs.

If a private port PVLAN association or mapping is deleted, or if a private port is configured as a SPAN destination, it becomes inactive.

Examples

This example shows how to set the interface to dynamic desirable mode:

```
Switch(config-if)# switchport mode dynamic desirable
Switch(config-if)#
```

This example shows how to set a port to PVLAN host mode:

```
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)#
```

This example shows how to set a port to private VLAN trunk:

```
Switch(config-if)# switchport mode private-vlan trunk
Switch(config-if)#
```

This example shows how to configure a port for an 802.1Q tunnel port:

```
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)#
```

This example shows how to configure a promiscuous trunk port:

```
Switch(config-if)# switchport mode private-vlan trunk promiscuous
Switch(config-if)#
```

This example shows how to configure an isolated trunk port:

```
Switch(config-if)# switchport mode private-vlan trunk
OR
Switch(config-if)# switchport mode private-vlan trunk secondary
Switch(config-if)#
```

You can verify your settings by entering the **show interfaces switchport** command and examining information in the Administration Mode and Operational Mode rows.

This example shows how to configure interface FastEthernet 5/2 as a PVLAN promiscuous port, map it to a PVLAN, and verify the configuration:

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# interface fastethernet 5/2
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan mapping 200 2
Switch(config-if)# end
Switch# show interfaces fastethernet 5/2 switchport
Name: Fa5/2
Switchport:Enabled
Administrative Mode:private-vlan promiscuous
Operational Mode:private-vlan promiscuous
Administrative Trunking Encapsulation:negotiate
Operational Trunking Encapsulation:native
Negotiation of Trunking:On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN:none
```

```
Administrative Private VLAN Host Association:none
Administrative Private VLAN Promiscuous Mapping:300 (VLAN0300) 2 (VLAN0002)
Private VLAN Routes:VLAN:none
Administrative Private VLAN Trunk Encapsulation:dot1q
Administrative Private VLAN Trunk Native VLAN:none
Administrative Private VLAN Trunk Private VLANs:none
Operational Private VLAN:
  Trunk Encapsulation:dot1q
  Trunk Native VLAN:1
Protocols VLANs Enabled:1-1001
Capture Mode Disabled
Capture VLANs Allowed:ALL
```

This example shows how to configure interface FastEthernet 5/1 as a PVLAN host port and verify the configuration:

```
Switch# conf t enter terminal
Switch(config)# interface fastethernet 5/1
Switch(config-if)# switchport private-vlan host
Switch(config-if)# switchport private-vlan host-association 202 440
Switch(config-if)# end
Switch# show interface fastethernet 5/1 switchport
Name: Fa5/1
Switchport: Enabled
Administrative Mode: private-vlan host
Operational Mode: private-vlan host
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Lower Tag: 1q-tunnel
Appliance trust: none
Administrative Private-vlan
  Host-association: 202 (VLAN0202) 440 (VLAN0440)
  Promiscuous Mapping: none
  Trunk encapsulation: dot1q
  Trunks: none
Operational private-vlan(s):
  202 (VLAN0202) 440 (VLAN0440)
Protocols VLANs Enabled:1-1001
Trunking VLANs Enabled: ALL
Capture Mode Disabled
Capture VLANs Allowed: ALL
```

This example shows how to configure interface FastEthernet 5/2 as a secondary trunk port, and verify the configuration:

```
Switch# conf t enter terminal
Switch(config)# interface fastethernet 5/2
Switch(config-if)# switchport mode private-vlan trunk secondary
Switch(config-if)# switchport private-vlan trunk native vlan 10
Switch(config-if)# switchport private-vlan trunk allowed vlan 3-4,
Switch(config-if)# switchport private-vlan trunk mapping 3 101
Switch(config-if)# end
Switch# show interface fastethernet 5/2 switchport
Name: Fa5/2
  Switchport: Enabled
  Administrative Mode: private-vlan trunk secondary
  Operational Mode: private-vlan trunk secondary
  Administrative Trunking Encapsulation: dot1q
  Operational Trunking Encapsulation: dot1q
  Negotiation of Trunking: On
  Access Mode VLAN: 1 (default)
```

```
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none &
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: 10
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk mappings:
  3 (VLAN0003) 101 (VLAN0101)
Administrative private-vlan trunk mappings: none
Operational Dot1q tag: enabled
Operational Normal VLANs: none
Trunking VLANs Enabled: All
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled Capture VLANs Allowed: All

Defaultvlan untagged: disabled
Defaultvlan multicast filtered: disabled
  Appliance trust: none
Switch(config)#
```

This example shows how to configure interface FastEthernet 5/2 as a promiscuous trunk port and to verify the configuration:

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/2
Switch(config-if)# switchport mode private-vlan trunk promiscuous
Switch(config-if)# switchport private-vlan mapping 3 101, 102
Switch(config-if)# switchport private-vlan trunk allowed vlan 40, 314
Switch(config-if)# switchport private-vlan mapping trunk 3 101, 102
Switch(config-if)# end
Switch# show interfaces fastethernet 5/2 switchport
Name: Fa5/2
Switchport: Enabled
Administrative Mode: private-vlan trunk promiscuous
Operational Mode: private-vlan trunk promiscuous
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: 10
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: 3-4,10
Administrative private-vlan trunk private VLANs: none
Administrative private-vlan trunk mappings:
  3 (VLAN0003) 101 (VLAN0101) 102 (VLAN0102)
Operational Dot1q tag: enabled
  3 (VLAN0003) 101 (VLAN0101) 102 (VLAN0102)
Trunking VLANs Enabled: All
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: All

Defaultvlan untagged: disabled
Defaultvlan multicast filtered: disabled
  Appliance trust: none
```

Back to top (cmnd-kgp-1.0.1.b)

Related Commands	Command	Description
	show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.
	switchport	Enables port security on an interface.
	switchport private-vlan host-association	Defines a PVLAN association for an isolated or community port.
	switchport private-vlan mapping	Defines private VLAN mapping for a promiscuous port.

switchport port-security

To enable port security on an interface, use the **switchport port-security** command. To disable port security and set parameters to their default state, use the **no** form of this command.

switchport port-security [aging {static | time time | type {absolute | inactivity}} | limit rate invalid-source-mac [N | none] | mac address mac address [vlan {access | voltage} | mac address sticky [mac address] [vlan access | voltage] | maximum value [vlan access | voltage] | violation {protect | restrict | shutdown | shutdown vlan}]

no switchport port-security [aging {static | time time | type {absolute | inactivity}} | limit rate invalid-source-mac [N | none] | mac address mac address [vlan {access | voltage} | mac address sticky [mac address] [vlan access | voltage] | maximum value [vlan access | voltage] | violation {protect | restrict | shutdown | shutdown vlan}]

Syntax Description	
aging	(Optional) Specifies aging for port security.
static	(Optional) Specifies aging for statically configured secure addresses on this port.
time *time*	(Optional) Specifies the aging time for this port. The valid values are from 0 to 1440 minutes. If the time is 0, aging is disabled for this port.
type absolute	(Optional) Sets the aging type as absolute aging. All the secure addresses on this port age out exactly after the time (minutes) specified and are removed from the secure address list.
type inactivity	(Optional) Sets 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.
limit rate invalid-source-mac	(Optional) Sets the rate limit for bad packets. This rate limit also applies to the port where DHCP snooping security mode is enabled as filtering for IP and MAC addresses.
N *rate*	(Optional) Supplies a rate limit (**N**) or indicates none (**none**).
mac address *mac-address*	(Optional) Specifies a secure MAC address for the interface, a sticky MAC address. You can add additional secure MAC addresses up to the maximum value that is configured.
sticky	(Optional) Configures the dynamic addresses as sticky on the interface.
vlan access	(Optional) Deletes the secure MAC addresses from access VLANs.
vlan voice	(Optional) Deletes the secure MAC addresses from voice VLANs.
maximum *value*	(Optional) Sets the maximum number of secure MAC addresses for the interface. Valid values are from 1 to 8192. The default setting is 1.
violation	(Optional) Sets the security violation mode and action to be taken if port security is violated.
protect	(Optional) Sets the security violation restrict mode. In this mode, a port security violation restricts data and causes the security violation counter to increment.

shutdown	(Optional) Sets the security violation shutdown mode. In this mode, a port security violation causes the interface to immediately become error-disabled.
shutdown vlan	(Optional) Set the security violation mode to per-VLAN shutdown. In this mode, only the VLAN on which the violation occurred is error-disabled.

Defaults

The default settings are as follows:

- Port security is disabled.
- When port security is enabled and no keywords are entered, the default maximum number of secure MAC addresses is 1.
- Aging is disabled.
- Aging type is0 minutes.
- All secure addresses on this port age out immediately after they are removed from the secure address list.

Command Modes

Interface configuration mode

Usage Guidelines

After you set the maximum number of secure MAC addresses that are allowed on a port, you can add secure addresses to the address table by manually configuring them, by allowing the port to dynamically configure them, or by configuring some MAC addresses and allowing the rest to be dynamically configured.

The packets are dropped into the hardware when the maximum number of secure MAC addresses are in the address table and a station that does not have a MAC address in the address table attempts to access the interface.

If you enable port security on a voice VLAN port and if there is a PC connected to the IP phone, you set the maximum allowed secure addresses on the port to more than 1.

You cannot configure static secure MAC addresses in the voice VLAN.

A secure port has the following limitations:

- A secure port cannot be a dynamic access port or a trunk 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 a secure port is in the error-disabled state, you can remove it from 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** interface configuration commands. If a port is in disabled, you can also use the **clear errdisable** command to re-enable the offending VLAN on the port.

To enable secure address aging for a particular port, set the aging time to a value other than0 for that port.

To allow limited time access to particular secure addresses, set the aging type as **absolute**. When the aging type is **inactive**, the secure addresses are deleted.

To allow continuous access to a limited number of secure addresses, set the aging type as **inactivity**. This action removes the secure address when it becomes inactive, and other addresses can become secure.

To allow unlimited access to a secure address, configure it as a secure address, and disable aging for the statically configured secure address by using the **no switchport port-security aging static** interface configuration command.

If the sticky command is executed without a MAC address specified, all MAC addresses that are learned on that port will be made sticky. You can also specify a specific MAC address to be a sticky address by entering the **sticky** keyword once it is.

You can configure the sticky feature even when port security is not enabled on the interface. The feature becomes operational when you enable port security on the interface.

You can use the **from** of the **sticky** command only if the sticky feature is already enabled on the interface.

Examples

This example shows how to set the aging time to 2 hours (120 minutes) for the secure addresses on the Fast Ethernet port 12:

```
Switch(config)# interface fastethernet 5/12
Switch(config-if)# switchport port-security aging time 120
Switch(config-if)#
```

This example shows how to set the aging timer type to inactivity for the secure addresses on the Fast Ethernet port 12:

```
Switch(config)# interface fastethernet 5/12
Switch(config-if)# switch port-security aging type inactivity
Switch(config-if)#
```

The following example shows how to configure rate limit for invalid source packets on Fast Ethernet port 12:

```
Switch(config)# interface fastethernet 5/12
Switch(config-if)# switchport port-security limit rate invalid-source-mac 100
Switch(config-if)#
```

The following example shows how to configure rate limit for invalid source packets on Fast Ethernet port 12:

```
Switch(config)# interface fastethernet 5/12
Switch(config-if)# switchport port-security limit rate invalid-source-mac none
Switch(config-if)#
```

You can verify the settings for all secure ports or the specified port by using the **show port-security** privileged EXEC command.

This example shows how to remove all sticky and static addresses that are configured on the interface:

```
Switch(config)# interface fastethernet 5/12
Switch(config-if)# no switchport port-security mac-address
Switch(config-if)#
```

This example shows how to configure a secure MAC address on Fast Ethernet port 12:

```
Switch(config)# interface fastethernet 5/12
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
```

```
Switch(config-if)# switchport port-security mac-address 3000.2000.3000
Switch(config-if)#
```

This example shows how to enable sticky MAC addresses learned on fast Ethernet port 12 sticky:

```
Switch(config)# interface fastethernet 3/12
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)#
```

This example shows how to make MAC address 1010.2000.3000 sticky on Fast Ethernet port 12:

```
Switch(config)# interface fastethernet 3/12
Switch(config-if)# switchport port-security mac-address sticky 1010.2000.3000
Switch(config-if)#
```

This example shows how to disable the sticky feature on Fast Ethernet port 12:

```
Switch(config)# interface fastethernet 3/12
Switch(config-if)# no switchport port-security mac-address sticky
Switch(config-if)#
```

Note This command makes all sticky addresses on this interface normal learned entries. It does not delete the entries from the secure MAC address table.

Note The following examples show how to configure sticky secure MAC addresses in access and voice VLANs on interfaces with voice VLAN configured. If you do not have voice VLAN configured the **mac-address [mac] [vlan vlan-id]** keywords are not supported.

This example shows how to configure sticky MAC addresses for voice and data VLANs on Fast Ethernet interface 5/3 and to verify the configuration:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fa5/3
Switch(config-if)# switchport access vlan 10
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address sticky 0030.0030.0040 vlan voice
Switch(config-if)# switchport port-security mac-address sticky 0030.0030.0050 vlan access
Switch(config-if)#
```

This example shows how to designate a maximum of one MAC address for a voice VLAN (for a Cisco IP Phone, let's say) and one MAC address for the data VLAN (for a PC, let's say) on Fast Ethernet interface 5/3 and to verify the configuration:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 5/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# switchport port-security maximum 1 vlan voice
Switch(config-if)# switchport port-security maximum 1 vlan access
Switch(config-if)# end
```

This example shows how to configure a port to shut down only the VLAN if a violation occurs:

```
Switch(config)# interface gigabitethernet 5/4
Switch(config)# switchport port-security violation shutdown vlan
```

Note Sending traffic to the ports causes the system to configure the port with sticky secure addresses.

You can verify your settings by using the **show port-security address** privileged EXEC command.

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.
show port-security	Displays the port security settings for an interface or for the switch.
switchport block	Prevents the unknown multicast or unicast packets from being forwarded.

switchport private-vlan association trunk

To configure the association between a secondary VLAN and a VLAN on a private VLAN trunk port, use the **switchport private-vlan association trunk** command. To remove the private VLAN mapping from the port, use the **no** form of this command.

switchport private-vlan association trunk *{primary-vlan-id} {secondary-vlan-id}*

no switchport private-vlan association trunk *{primary-vlan-id}*

Syntax Description

primary-vlan-id	Number of the primary VLAN of the private VLAN relationship.
secondary-vlan-id	Number of the secondary VLAN of the private VLAN relationship.

Defaults

Private VLAN mapping is disabled.

Command Modes

Interface configuration mode

Usage Guidelines

Multiple private VLAN pairs can be specified so that a private VLAN trunk port can carry multiple secondary VLANs. If an association is specified for the existing primary VLAN, the existing association is replaced.

Only isolated secondary VLANs can be carried over a private VLAN trunk.

Note Community secondary VLANs on a private VLAN trunk are not supported in this release.

If there is no trunk association, any packets received on the secondary VLANs are dropped.

Examples

This example shows how to configure a port with a primary VLAN (VLAN 18) and secondary VLAN (VLAN 20):

```
Switch(config)#int switchport private-vlan association trunk 18 20
Switch(config)#int end
```

This example shows how to remove the private VLAN association from the port:

```
Switch(config)#int no switchport private-vlan association trunk 18
Switch(config)#int end
```

This example shows how to configure interface FastEthernet 5/2 as a secondary trunk port, and verify the configuration:

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/2
Switch(config-if)# switchport mode private-vlan trunk secondary
Switch(config-if)# switchport private-vlan trunk native vlan 10
Switch(config-if)# switchport private-vlan trunk allowed vlan 10, 3-4
Switch(config-if)# switchport private-vlan association trunk 3 301
Switch(config-if)# end
```

Catalyst 6500 Series Switch Cisco IOS Command Reference—Release 12.2SX 3.1.0/3.2.0/3.3.0/3.4.0/3.5.0/3.6.0/3.7.0/3.8.0/3.9.0/3.10.0/3.11.0/3.12.0/3.13.0/3.14.0/3.15.0/3.16.0/3.17.0/3.18.0/3.19.0/3.20.0/3.21.0/3.22.0/3.23.0/3.24.0/3.25.0/3.26.0/3.27.0/3.28.0/3.29.0/3.30.0/3.31.0/3.32.0/3.33.0/3.34.0/3.35.0/3.36.0/3.37.0/3.38.0/3.39.0/3.40.0/3.41.0/3.42.0/3.43.0/3.44.0/3.45.0/3.46.0/3.47.0/3.48.0/3.49.0/3.50.0/3.51.0/3.52.0/3.53.0/3.54.0/3.55.0/3.56.0/3.57.0/3.58.0/3.59.0/3.60.0/3.61.0/3.62.0/3.63.0/3.64.0/3.65.0/3.66.0/3.67.0/3.68.0/3.69.0/3.70.0/3.71.0/3.72.0/3.73.0/3.74.0/3.75.0/3.76.0/3.77.0/3.78.0/3.79.0/3.80.0/3.81.0/3.82.0/3.83.0/3.84.0/3.85.0/3.86.0/3.87.0/3.88.0/3.89.0/3.90.0/3.91.0/3.92.0/3.93.0/3.94.0/3.95.0/3.96.0/3.97.0/3.98.0/3.99.0/3.100.0/3.101.0/3.102.0/3.103.0/3.104.0/3.105.0/3.106.0/3.107.0/3.108.0/3.109.0/3.110.0/3.111.0/3.112.0/3.113.0/3.114.0/3.115.0/3.116.0/3.117.0/3.118.0/3.119.0/3.120.0/3.121.0/3.122.0/3.123.0/3.124.0/3.125.0/3.126.0/3.127.0/3.128.0/3.129.0/3.130.0/3.131.0/3.132.0/3.133.0/3.134.0/3.135.0/3.136.0/3.137.0/3.138.0/3.139.0/3.140.0/3.141.0/3.142.0/3.143.0/3.144.0/3.145.0/3.146.0/3.147.0/3.148.0/3.149.0/3.150.0/3.151.0/3.152.0/3.153.0/3.154.0/3.155.0/3.156.0/3.157.0/3.158.0/3.159.0/3.160.0/3.161.0/3.162.0/3.163.0/3.164.0/3.165.0/3.166.0/3.167.0/3.168.0/3.169.0/3.170.0/3.171.0/3.172.0/3.173.0/3.174.0/3.175.0/3.176.0/3.177.0/3.178.0/3.179.0/3.180.0/3.181.0/3.182.0/3.183.0/3.184.0/3.185.0/3.186.0/3.187.0/3.188.0/3.189.0/3.190.0/3.191.0/3.192.0/3.193.0/3.194.0/3.195.0/3.196.0/3.197.0/3.198.0/3.199.0/3.200.0/3.201.0/3.202.0/3.203.0/3.204.0/3.205.0/3.206.0/3.207.0/3.208.0/3.209.0/3.210.0/3.211.0/3.212.0/3.213.0/3.214.0/3.215.0/3.216.0/3.217.0/3.218.0/3.219.0/3.220.0/3.221.0/3.222.0/3.223.0/3.224.0/3.225.0/3.226.0/3.227.0/3.228.0/3.229.0/3.230.0/3.231.0/3.232.0/3.233.0/3.234.0/3.235.0/3.236.0/3.237.0/3.238.0/3.239.0/3.240.0/3.241.0/3.242.0/3.243.0/3.244.0/3.245.0/3.246.0/3.247.0/3.248.0/3.249.0/3.250.0/3.251.0/3.252.0/3.253.0/3.254.0/3.255.0/3.256.0/3.257.0/3.258.0/3.259.0/3.260.0/3.261.0/3.262.0/3.263.0/3.264.0/3.265.0/3.266.0/3.267.0/3.268.0/3.269.0/3.270.0/3.271.0/3.272.0/3.273.0/3.274.0/3.275.0/3.276.0/3.277.0/3.278.0/3.279.0/3.280.0/3.281.0/3.282.0/3.283.0/3.284.0/3.285.0/3.286.0/3.287.0/3.288.0/3.289.0/3.290.0/3.291.0/3.292.0/3.293.0/3.294.0/3.295.0/3.296.0/3.297.0/3.298.0/3.299.0/3.300.0/3.301.0/3.302.0/3.303.0/3.304.0/3.305.0/3.306.0/3.307.0/3.308.0/3.309.0/3.310.0/3.311.0/3.312.0/3.313.0/3.314.0/3.315.0/3.316.0/3.317.0/3.318.0/3.319.0/3.320.0/3.321.0/3.322.0/3.323.0/3.324.0/3.325.0/3.326.0/3.327.0/3.328.0/3.329.0/3.330.0/3.331.0/3.332.0/3.333.0/3.334.0/3.335.0/3.336.0/3.337.0/3.338.0/3.339.0/3.340.0/3.341.0/3.342.0/3.343.0/3.344.0/3.345.0/3.346.0/3.347.0/3.348.0/3.349.0/3.350.0/3.351.0/3.352.0/3.353.0/3.354.0/3.355.0/3.356.0/3.357.0/3.358.0/3.359.0/3.360.0/3.361.0/3.362.0/3.363.0/3.364.0/3.365.0/3.366.0/3.367.0/3.368.0/3.369.0/3.370.0/3.371.0/3.372.0/3.373.0/3.374.0/3.375.0/3.376.0/3.377.0/3.378.0/3.379.0/3.380.0/3.381.0/3.382.0/3.383.0/3.384.0/3.385.0/3.386.0/3.387.0/3.388.0/3.389.0/3.390.0/3.391.0/3.392.0/3.393.0/3.394.0/3.395.0/3.396.0/3.397.0/3.398.0/3.399.0/3.400.0/3.401.0/3.402.0/3.403.0/3.404.0/3.405.0/3.406.0/3.407.0/3.408.0/3.409.0/3.410.0/3.411.0/3.412.0/3.413.0/3.414.0/3.415.0/3.416.0/3.417.0/3.418.0/3.419.0/3.420.0/3.421.0/3.422.0/3.423.0/3.424.0/3.425.0/3.426.0/3.427.0/3.428.0/3.429.0/3.430.0/3.431.0/3.432.0/3.433.0/3.434.0/3.435.0/3.436.0/3.437.0/3.438.0/3.439.0/3.440.0/3.441.0/3.442.0/3.443.0/3.444.0/3.445.0/3.446.0/3.447.0/3.448.0/3.449.0/3.450.0/3.451.0/3.452.0/3.453.0/3.454.0/3.455.0/3.456.0/3.457.0/3.458.0/3.459.0/3.460.0/3.461.0/3.462.0/3.463.0/3.464.0/3.465.0/3.466.0/3.467.0/3.468.0/3.469.0/3.470.0/3.471.0/3.472.0/3.473.0/3.474.0/3.475.0/3.476.0/3.477.0/3.478.0/3.479.0/3.480.0/3.481.0/3.482.0/3.483.0/3.484.0/3.485.0/3.486.0/3.487.0/3.488.0/3.489.0/3.490.0/3.491.0/3.492.0/3.493.0/3.494.0/3.495.0/3.496.0/3.497.0/3.498.0/3.499.0/3.500.0/3.501.0/3.502.0/3.503.0/3.504.0/3.505.0/3.506.0/3.507.0/3.508.0/3.509.0/3.510.0/3.511.0/3.512.0/3.513.0/3.514.0/3.515.0/3.516.0/3.517.0/3.518.0/3.519.0/3.520.0/3.521.0/3.522.0/3.523.0/3.524.0/3.525.0/3.526.0/3.527.0/3.528.0/3.529.0/3.530.0/3.531.0/3.532.0/3.533.0/3.534.0/3.535.0/3.536.0/3.537.0/3.538.0/3.539.0/3.540.0/3.541.0/3.542.0/3.543.0/3.544.0/3.545.0/3.546.0/3.547.0/3.548.0/3.549.0/3.550.0/3.551.0/3.552.0/3.553.0/3.554.0/3.555.0/3.556.0/3.557.0/3.558.0/3.559.0/3.560.0/3.561.0/3.562.0/3.563.0/3.564.0/3.565.0/3.566.0/3.567.0/3.568.0/3.569.0/3.570.0/3.571.0/3.572.0/3.573.0/3.574.0/3.575.0/3.576.0/3.577.0/3.578.0/3.579.0/3.580.0/3.581.0/3.582.0/3.583.0/3.584.0/3.585.0/3.586.0/3.587.0/3.588.0/3.589.0/3.590.0/3.591.0/3.592.0/3.593.0/3.594.0/3.595.0/3.596.0/3.597.0/3.598.0/3.599.0/3.600.0/3.601.0/3.602.0/3.603.0/3.604.0/3.605.0/3.606.0/3.607.0/3.608.0/3.609.0/3.610.0/3.611.0/3.612.0/3.613.0/3.614.0/3.615.0/3.616.0/3.617.0/3.618.0/3.619.0/3.620.0/3.621.0/3.622.0/3.623.0/3.624.0/3.625.0/3.626.0/3.627.0/3.628.0/3.629.0/3.630.0/3.631.0/3.632.0/3.633.0/3.634.0/3.635.0/3.636.0/3.637.0/3.638.0/3.639.0/3.640.0/3.641.0/3.642.0/3.643.0/3.644.0/3.645.0/3.646.0/3.647.0/3.648.0/3.649.0/3.650.0/3.651.0/3.652.0/3.653.0/3.654.0/3.655.0/3.656.0/3.657.0/3.658.0/3.659.0/3.660.0/3.661.0/3.662.0/3.663.0/3.664.0/3.665.0/3.666.0/3.667.0/3.668.0/3.669.0/3.670.0/3.671.0/3.672.0/3.673.0/3.674.0/3.675.0/3.676.0/3.677.0/3.678.0/3.679.0/3.680.0/3.681.0/3.682.0/3.683.0/3.684.0/3.685.0/3.686.0/3.687.0/3.688.0/3.689.0/3.690.0/3.691.0/3.692.0/3.693.0/3.694.0/3.695.0/3.696.0/3.697.0/3.698.0/3.699.0/3.700.0/3.701.0/3.702.0/3.703.0/3.704.0/3.705.0/3.706.0/3.707.0/3.708.0/3.709.0/3.710.0/3.711.0/3.712.0/3.713.0/3.714.0/3.715.0/3.716.0/3.717.0/3.718.0/3.719.0/3.720.0/3.721.0/3.722.0/3.723.0/3.724.0/3.725.0/3.726.0/3.727.0/3.728.0/3.729.0/3.730.0/3.731.0/3.732.0/3.733.0/3.734.0/3.735.0/3.736.0/3.737.0/3.738.0/3.739.0/3.740.0/3.741.0/3.742.0/3.743.0/3.744.0/3.745.0/3.746.0/3.747.0/3.748.0/3.749.0/3.750.0/3.751.0/3.752.0/3.753.0/3.754.0/3.755.0/3.756.0/3.757.0/3.758.0/3.759.0/3.760.0/3.761.0/3.762.0/3.763.0/3.764.0/3.765.0/3.766.0/3.767.0/3.768.0/3.769.0/3.770.0/3.771.0/3.772.0/3.773.0/3.774.0/3.775.0/3.776.0/3.777.0/3.778.0/3.779.0/3.780.0/3.781.0/3.782.0/3.783.0/3.784.0/3.785.0/3.786.0/3.787.0/3.788.0/3.789.0/3.790.0/3.791.0/3.792.0/3.793.0/3.794.0/3.795.0/3.796.0/3.797.0/3.798.0/3.799.0/3.800.0/3.801.0/3.802.0/3.803.0/3.804.0/3.805.0/3.806.0/3.807.0/3.808.0/3.809.0/3.810.0/3.811.0/3.812.0/3.813.0/3.814.0/3.815.0/3.816.0/3.817.0/3.818.0/3.819.0/3.820.0/3.821.0/3.822.0/3.823.0/3.824.0/3.825.0/3.826.0/3.827.0/3.828.0/3.829.0/3.830.0/3.831.0/3.832.0/3.833.0/3.834.0/3.835.0/3.836.0/3.837.0/3.838.0/3.839.0/3.840.0/3.841.0/3.842.0/3.843.0/3.844.0/3.845.0/3.846.0/3.847.0/3.848.0/3.849.0/3.850.0/3.851.0/3.852.0/3.853.0/3.854.0/3.855.0/3.856.0/3.857.0/3.858.0/3.859.0/3.860.0/3.861.0/3.862.0/3.863.0/3.864.0/3.865.0/3.866.0/3.867.0/3.868.0/3.869.0/3.870.0/3.871.0/3.872.0/3.873.0/3.874.0/3.875.0/3.876.0/3.877.0/3.878.0/3.879.0/3.880.0/3.881.0/3.882.0/3.883.0/3.884.0/3.885.0/3.886.0/3.887.0/3.888.0/3.889.0/3.890.0/3.891.0/3.892.0/3.893.0/3.894.0/3.895.0/3.896.0/3.897.0/3.898.0/3.899.0/3.900.0/3.901.0/3.902.0/3.903.0/3.904.0/3.905.0/3.906.0/3.907.0/3.908.0/3.909.0/3.910.0/3.911.0/3.912.0/3.913.0/3.914.0/3.915.0/3.916.0/3.917.0/3.918.0/3.919.0/3.920.0/3.921.0/3.922.0/3.923.0/3.924.0/3.925.0/3.926.0/3.927.0/3.928.0/3.929.0/3.930.0/3.931.0/3.932.0/3.933.0/3.934.0/3.935.0/3.936.0/3.937.0/3.938.0/3.939.0/3.940.0/3.941.0/3.942.0/3.943.0/3.944.0/3.945.0/3.946.0/3.947.0/3.948.0/3.949.0/3.950.0/3.951.0/3.952.0/3.953.0/3.954.0/3.955.0/3.956.0/3.957.0/3.958.0/3.959.0/3.960.0/3.961.0/3.962.0/3.963.0/3.964.0/3.965.0/3.966.0/3.967.0/3.968.0/3.969.0/3.970.0/3.971.0/3.972.0/3.973.0/3.974.0/3.975.0/3.976.0/3.977.0/3.978.0/3.979.0/3.980.0/3.981.0/3.982.0/3.983.0/3.984.0/3.985.0/3.986.0/3.987.0/3.988.0/3.989.0/3.990.0/3.991.0/3.992.0/3.993.0/3.994.0/3.995.0/3.996.0/3.997.0/3.998.0/3.999.0/3.1000.0/3.1001.0/3.1002.0/3.1003.0/3.1004.0/3.1005.0/3.1006.0/3.1007.0/3.1008.0/3.1009.0/3.1010.0/3.1011.0/3.1012.0/3.1013.0/3.1014.0/3.1015.0/3.1016.0/3.1017.0/3.1018.0/3.1019.0/3.1020.0/3.1021.0/3.1022.0/3.1023.0/3.1024.0/3.1025.0/3.1026.0/3.1027.0/3.1028.0/3.1029.0/3.1030.0/3.1031.0/3.1032.0/3.1033.0/3.1034.0/3.1035.0/3.1036.0/3.1037.0/3.1038.0/3.1039.0/3.1040.0/3.1041.0/3.1042.0/3.1043.0/3.1044.0/3.1045.0/3.1046.0/3.1047.0/3.1048.0/3.1049.0/3.1050.0/3.1051.0/3.1052.0/3.1053.0/3.1054.0/3.1055.0/3.1056.0/3.1057.0/3.1058.0/3.1059.0/3.1060.0/3.1061.0/3.1062.0/3.1063.0/3.1064.0/3.1065.0/3.1066.0/3.1067.0/3.1068.0/3.1069.0/3.1070.0/3.1071.0/3.1072.0/3.1073.0/3.1074.0/3.1075.0/3.1076.0/3.1077.0/3.1078.0/3.1079.0/3.1080.0/3.1081.0/3.1082.0/3.1083.0/3.1084.0/3.1085.0/3.1086.0/3.1087.0/3.1088.0/3.1089.0/3.1090.0/3.1091.0/3.1092.0/3.1093.0/3.1094.0/3.1095.0/3.1096.0/3.1097.0/3.1098.0/3.1099.0/3.1100.0/3.1101.0/3.1102.0/3.1103.0/3.1104.0/3.1105.0/3.1106.0/3.1107.0/3.1108.0/3.1109.0/3.1110.0/3.1111.0/3.1112.0/3.1113.0/3.1114.0/3.1115.0/3.1116.0/3.1117.0/3.1118.0/3.1119.0/3.1120.0/3.1121.0/3.1122.0/3.1123.0/3.1124.0/3.1125.0/3.1126.0/3.1127.0/3.1128.0/3.1129.0/3.1130.0/3.1131.0/3.1132.0/3.1133.0/3.1134.0/3.1135.0/3.1136.0/3.1137.0/3.1138.0/3.1139.0/3.1140.0/3.1141.0/3.1142.0/3.1143.0/3.1144.0/3.1145.0/3.1146.0/3.1147.0/3.1148.0/3.1149.0/3.1150.0/3.1151.0/3.1152.0/3.1153.0/3.1154.0/3.1155.0/3.1156.0/3.1157.0/3.1158.0/3.1159.0/3.1160.0/3.1161.0/3.1162.0/3.1163.0/3.1164.0/3.1165.0/3.1166.0/3.1167.0/3.1168.0/3.1169.0/3.1170.0/3.1171.0/3.1172.0/3.1173.0/3.1174.0/3.1175.0/3.1176.0/3.1177.0/3.1178.0/3.1179.0/3.1180.0/3.1181.0/3.1182.0/3.1183.0/3.1184.0/3.1185.0/3.1186.0/3.1187.0/3.1188.0/3.1189.0/3.1190.0/3.1191.0/3.1192.0/3.1193.0/3.1194.0/3.1195.0/3.1196.0/3.1197.0/3.1198.0/3.1199.0/3.1200.0/3.1201.0/3.1202.0/3.1203.0/3.1204.0/3.1205.0/3.1206.0/3.1207.0/3.1208.0/3.1209.0/3.1210.0/3.1211.0/3.1212.0/3.1213.0/3.1214.0/3.1215.0/3.1216.0/3.1217.0/3.1218.0/3.1219.0/3.1220.0/3.1221.0/3.1222.0/3.1223.0/3.1224.0/3.1225.0/3.1226.0/3.1227.0/3.1228.0/3.1229.0/3.1230.0/3.1231.0/3.1232.0/3.1233.0/3.1234.0/3.1235.0/3.1236.0/3.1237.0/3.1238.0/3.1239.0/3.1240.0/3.1241.0/3.1242.0/3.1243.0/3.1244.0/3.1245.0/3.1246.0/3.1247.0/3.1248.0/3.1249.0/3.1250.0/3.1251.0/3.1252.0/3.1253.0/3.1254.0/3.1255.0/3.1256.0/3.1257.0/3.1258.0/3.1259.0/3.1260.0/3.1261.0/3.1262.0/3.1263.0/3.1264.0/3.1265.0/3.1266.0/3.1267.0/3.1268.0/3.1269.0/3.1270.0/3.1271.0/3.1272.0/3.1273.0/3.1274.0/3.1275.0/3.1276.0/3.1277.0/3.1278.0/3.1279.0/3.1280.0/3.1281.0/3.1282.0/3.1283.0/3.1284.0/3.1285.0/3.1286.0/3.1287.0/3.1288.0/3.1289.0/3.1290.0/3.1291.0/3.1292.0/3.1293.0/3.1294.0/3.1295.0/3.1296.0/3.1297.0/3.1298.0/3.1299.0/3.1300.0/3.1301.0/3.1302.0/3.1303.0/3.1304.0/3.1305.0/3.1306.0/3.1307.0/3.1308.0/3.1309.0/3.1310.0/3.1311.0/3.1312.0/3.1313.0/3.1314.0/3.1315.0/3.1316.0/3.1317.0/3.1318.0/3.1319.0/3.1320.0/3.1321.0/3.1322.0/3.1323.0/3.1324.0/3.1325.0/3.1326.0/3.1327.0/3.1328.0/3.1329.0/3.1330.0/3.1331.0/3.1332.0/3.1333.0/3.1334.0/3.1335.0/3.1336.0/3.1337.0/3.1338.0/3.1339.0/3.1340.0/3.1341.0/3.1342.0/3.1343.0/3.1344.0/3.1345.0/3.1346.0/3.1347.0/3.1348.0/3.1349.0/3.1350.0/3.1351.0/3.1352.0/3.1353.0/3.1354.0/3.1355.0/3.1356.0/3.1357.0/3.1358.0/3.1359.0/3.1360.0/3.1361.0/3.1362.0/3.1363.0/3.1364.0/3.1365.0/3.1366.0/3.1367.0/3.1368.0/3.1369.0/3.1370.0/3.1371.0/3.1372.0/3.1373.0/3.1374.0/3.1375.0/3.1376.0/3.1377.0/3.1378.0/3.1379.0/3.1380.0/3.1381.0/3.1382.0/3.1383.0/3.1384.0/3.1385.0/3.1386.0/3.1387.0/3.1388.0/3.1389.0/3.1390.0/3.1391.0/3.1392.0/3.1393.0/3.1394.0/3.1395.0/3.1396.0/3.1397.0/3.1398.0/3.1399.0/3.1400.0/3.1401.0/3.1402.0/3.1403.0/3.1404.0/3.1405.0/3.1406.0/3.1407.0/3.1408.0/3.1409.0/3.1410.0/3.1411.0/3.1412.0/3.1413.0/3.1414.0/3.1415.0/3.1416.0/3.1417.0/3.1418.0/3.1419.0/3.1420.0/3.1421.0/3.1422.0/3.1423.0/3.1424.0/3.1425.0/3.1426.0/3.1427.0/3.1428.0/3.1429.0/3.1430.0/3.1431.0/3.1432.0/3.1433.0/3.1434.0/3.1435.0/3.1436.0/3.1437.0/3.1438.0/3.1439.0/3.1440.0/3.1441.0/3.1442.0/3.1443.0/3.1444.0/3.1445.0/3.1446.0/3.1447.0/3.1448.0/3.1449.0/3.1450.0/3.1451.0/3.1452.0/3.1453.0/3.1454.0/3.1455.0/3.1456.0/3.1457.0/3.1458.0/3.1459.0/3.1460.0/3.1461.0/3.1462.0/3.1463.0/3.1464.0/3.1465.0/3.1466.0/3.1467.0/3.1468.0/3.1469.0/3.1470.0/3.1471.0/3.1472.0/3.1473.0/3.1474.0/3.1475.0/3.1476.0/3.1477.0/3.1478.0/3.1479.0/3.1480.0/3.1481.0/3.1482.0/3.1483.0/3.1484.0/3.1485.0/3.1486.0/3.1487.0/3.1488.0/3.1489.0/3.1490.0/3.1491.0/3.1492.0/3.1493.0/3.1494.0/3.1495.0/3.1496.0/3.1497.0/3.1498.0/3.1499.0/3.1500.0/3.1501.0/3.1502.0/3.1503.0/3.1504.0/3.1505.0/3.1506.0/3.1507.0/3.1508.0/3.1509.0/3.1510.0/3.1511.0/3.1512.0/3.1513.0/3.1514.0/3.1515.0/3.1516.0/3.1517.0/3.1518.0/3.1519.0/3.1520.0/3.1521.0/3.1522.0/3.1523.0/3.1524.0/3.1525.0/3.1526.0/3.1527.0/3.1528.0/3.1529.0/3.1530.0/3.1531.0/3.1532.0/3.1533.0/3.1534.0/3.1535.0/3.1536.0/3.1537.0/3.1538.0/3.1539.0/3.1540.0/3.1541.0/3.1542.0/3.1543.0/3.1544.0/3.1545.0/3.1546.0/3.1547.0/3.1548.0/3.1549.0/3.1550.0/3.1551.0/3.1552.0/3.1553.0/3.1554.0/3.1555.0/3.1556.0/3.1557.0/3.1558.0/3.1559.0/3.1560.0/3.1561.0/3.1562.0/3.1563.0/3.1564.0/3.1565.0/3.1566.0/3.1567.0/3.1568.0/3.1569.0/3.1570.0/3.1571.0/3.1572.0/3.1573.0/3.1574.0/3.1575.0/3.1576.0/3.1577.0/3.1578.0/3.1579.0/3.1580.0/3.1581.0/3.1582.0/3.1583.0/3.1584.0/3.1585.0/3.1586.0/3.1587.0/3.1588.0/3.1589.0/3.1590.0/3.1591.0/3.1592.0/3.1593.0/3.1594.0/3.1595.0/3.1596.0/3.1597.0/3.1598.0/3.1599.0/3.1600.0/3.1601.0/3.1602.0/3.1603.0/3.1604.0/3.1605.0/3.1606.0/3.1607.0/3.1608.0/3.1609.0/3.1610.0/3.1611.0/3.1612.0/3.1613.0/3.1614.0/3.1615.0/3.1616.0/3.1617.0/3.1618.0/3.1619.0/3.1620.0/3.1621.0/3.1622.0/3.1623.0/3.1624.0/3.1625.0/3.1626.0/3.1627.0/3.1628.0/3.1629.0/3.1630.0/3.1631.0/3.1632.0/3.1633.0/3.1634.0/3.1635.0/3.1636.0/3.1637.0/3.1638.0/3.1639.0/3.1640.0/3.1641.0/3.1642.0/3.1643.0/3.1644.0/3.1645.0/3.1646.0/3.1647.0/3.1648.0/3.1649.0/3.1650.0/3.1651.0/3.1652.0/3.1653.0/3.1654.0/3.1655.0/3.1656.0/3.1657.0/3.1658.0/3.1659.0/3.1660.0/3.1661.0/3.1662.0/3.1663.0/3.1664.0/3.1665.0/3.1666.0/3.1667.0/3.1668.0/3.1669.0/3.1670.0/3.1671.0/3.1672.0/3.1673.0/3.1674.0/3.1675.0/3.1676.0/3.1677.0/3.1678.0/3.1679.0/3.1680.0/3.1681.0/3.1682.0/3.1683.0/3.1684.0/3.1685.0/3.1686.0/3.1687.0/3.1688.0/3.1689.0/3.1690.0/3.1691.0/3.1692.0/3.1693.0/3.1694.0/3.1695.0/3.1696.0/3.1697.0/3.1698.0/3.1699.0/3.1700.0/3.1701.0/3.1702.0/3.1703.0/3.1704.0/3.1705.0/3.1706.0/3.1707.0/3.1708.0/3.1709.0/3.1710.0/3.1711.0/3.1712.0/3.1713.0/3.1714.0/3.1715.0/3.1716.0/3.1717.0/3.1718.0/3.1719.0/3.1720.0/3.1721.0/3.1722.0/3.1723.0/3.1724.0/3.1725.0/3.1726.0/3.1727.0/3.1728.0/3.1729.0/3.1730.0/3.1731.0/3.1732.0/3.1733.0/3.1734.0/3.1735.0/3.1736.0/3.1737.0/3.1738.0/3.1739.0/3.1740.0/3.1741.0/3.1742.0/3.1743.0/3.1744.0/3.1745.0/3.1746.0/3.1747.0/3.1748.0/3.1749.0/3.1750.0/3.1751.0/3.1752.0/3.1753.0/3.1754.0/3.1755.0/3.1756.0/3.1757.0/3.1758.0/3.1759.0/3.1760.0/3.1761.0/3.1762.0/3.1763.0/3.1764.0/3.1765.0/3.1766.0/3.1767.0/3.1768.0/3.1769.0/3.1770.0/3.1771.0/3.1772.0/3.1773.0/3.1774.0/3.1775.0/3.1776.0/3.1777.0/3.1778.0/3.1779.0/3.1780.0/3.1781.0/3.1782.0/3.1783.0/3.1784.0/3.1785.0/3.1786.0/3.1787.0/3.1788.0/3.1789.0/3.1790.0/3.1791.0/3.1792.0/3.1793.0/3.1794.0/3.1795.0/3.1796.0/3.1797.0/3.1798.0/3.1799.0/3.1800.0/3.1801.0/3.1802.0/3.1803.0/3.1804.0/3.1805.0/3.1806.0/3.1807.0/3.1808.0/3.1809.0/3.1810.0/3.1811.0/3.1812.0/3.1813.0/3.1814.0/3.1815.0/3.1816.0/3.1817.0/3.1818.0/3.1819.0/3.1820.0/3.1821.0/3.1822.0/3.1823.0/3.1824.0/3.1825.0/3.1826.0/3.1827.0/3.1828.0/3.1829.0/3.1830.0/3.1831.0/3.1832.0/3.1833.0/3.1834.0/3.1835.0/3.1836.0/3.1837.0/3.1838.0/3.1839.0/3.1840.0/3.1841.0/3.1842.0/3.1843.0/3.1844.0/3.1845.0/3.1846.0/3.1847.0/3.1848.0/3.1849.0/3.1850.0/3.1851.0/3.1852.0/3.1853.0/3.1854.0/3.1855.0/3.1856.0/3.1857.0/3.1858.0/3.1859.0/3.1860.0/3.1861.0/3.1862.0/3.1863.0/3.1864.0/3.1865.0/3.1866.0/3.1867.0/3.1868.0/3.1869.0/3.1870.0/3.1871.0/3.1872.0/3.1873.0/3.1874.0/3.1875.0/3.1876.0/3.1877.0/3.1878.0/3.1879.0/3.1880.0/3.1881.0/3.1882.0/3.1883.0/3.1884.0/3.1885.0/3.1886.0/3.1887.0/3.1888.0/3.1889.0/3.1890.0/3.1891.0/3.1892.0/3.1893.0/3.1894.0/3.1895.0/3.1896.0/3.1897.0/3.1898.0/3.1899.0/3.1900.0/3.1901.0/3.1902.0/3.1903.0/3.1904.0/3.1905.0/3.1906.0/3.1907.0/3.1908.0/3.1909.0/3.1910.0/3.1911.0/3.1912.0/3.1913.0/3.1914.0/3.1915.0/3.1916.0/3.1917.0/3.1918.0/3.1919.0/3.1920.0/3.1921.0/3.1922.0/3.1923.0/3.1924.0/3.1925.0/3.1926.0/3.1927.0/3.1928.0/3.1929.0/3.1930.0/3.1931.0/3.1932.0/3.1933.0/3.1934.0/3.1935.0/3.1936.0/3.1937.0/3.1938.0/3.1939.0/3.1940.0/3.1941.0/3.1942.0/3.1943.0/3.1944.0/3.1945.0/3.1946.0/3.1947.0/3.1948.0/3.1949.0/3.1950.0/3.1951.0/3.1952.0/3.1953.0/3.1954.0/3.1955.0/3.1956.0/3.1957.0/3.1958.0/3.1959.0/3.1960.0/3.1961.0/3.1962.0/3.1963.0/3.1964.0/3.1965.0/3.1966.0/3.1967.0/3.1968.0/3.1969.0/3.1970.0/3.1971.0/3.1972.0/3.1973.0/3.1974.0/3.1975.0/3.1976.0/3.1977.0/3.1978.0/3.1979.0/3.1980.0/3.1981.0/3.1982.0/3.1983.0/3.1984.0/3.1985.0/3.1986.0/3.1987.0/3.1988.0/3.1989.0/3.1990.0/3.1991.0/3.1992.0/3.1993.0/3.1994.0/3.1995.0/3.1996.0/3.1997.0/3.1998.0/3.1999.0/3.2000.0/3.2001.0/3.2002.0/3.2003.0/3.2004.0/3.2005.0/3.2006.0/3.2007.0/3.2008.0/3.2009.0/3.2010.0/3.2011.0/3.2012.0/3.2013.0/3.2014.0/3.2015.0/3.2016.0/3.2017.0/3.2018.0/3.2019.0/3.2020.0/3.2021.0/3.2022.0/3.2023.0/3.2024.0/3.2025.0/3.2026.0/3.2027.0/3.2028.0/3.2029.0/3.2030.0/3.2031.0/3.2032.0/3.2033.0/3.2034.0/3.2035.0/3.2036.0/3.2037.0/3.2038.0/3.2039.0/3.2040.0/3.2041.0/3.2042.0/3.2043.0/3.2044.0/3.2045.0/3.2046.0/3.2047.0/3.2048.0/3.2049.0/3.2050.0/3.2051.0/3.2052.0/3.2053.0/3.2054.0/3.2055.0/3.2056.0/3.2057.0/3.2058.0/3.2059.0/3.2060.0/3.2061.0/3.2062.0/3.2063.0/3.2064.0/3.2065.0/3.2066.0/3.2067.0/3.2068.0/3.2069.0/3.2070.0/3.2071.0/3.2072.0/3.2073.0/3.2074.0/3.2075.0/3.2076.0/3.2077.0/3.2078.0/3.2079.0/3.2080.0/3.2081.0/3.2082.0/3.2083.0/3.2084.0/3.2085.0/3.2086.0/3.2087.0/3.2088.0/3.2089.0/3.2090.0/3.2091.0/3.2092.0/3.2093.0/3.2094.0/3.2095.0/3.2096.0/3.2097.0/3.2098.0/3.2099.0/3.2100.0/3.2101.0/3.2102.0/3.2103.0/3.2104.0/3.2105.0/3.2106.0/3.2107.0/3.2108.0/3.2109.0/3.2110.0/3.2111.0/3.2112.0/3.2113.0/3.2114.0/3.2115.0/3.2116.0/3.2117.0/3.2118.0/3.2119.0/3.2120.0/3.2121.0/3.2122.0/3.2123.0/3.2124.0/3.2125.0/3.2126.0/3.2127.0/3.2128.0/3.2129.0/3.2130.0/3.2131.0/3.2132.0/3.2133.0/3.2134.0/3.2135.0/3.2136.0/3.2137.0/3.2138.0/3.2139.0/3.2140.0/3.2141.0/3.2142.0/3.2143.0/3.2144.0/3.2145.0/3.2146.0/3.2147.0/3.2148.0/3.2149.0/3.2150.0/3.2151.0/3.2152.0/3.2153.0/3.2154.0/3.2155.0/3.2156.0/3.2157.0/3.2158.0/3.2159.0/3.2160.0/3.2161.0/3.2162.0/3.2163.0/3.2164.0/3.2165.0/3.2166.0/3.2167.0/3.2168.0/3.2169.0/3.2170.0/3.2171.0/3.2172.0/3.2173.0/3.2174.0/3.2175.0/3.2176.0/3.2177.0/3.2178.0/3.2179.0/3.2180.0/3.2181.0/3.2182.0/3.2183.0/3.2184.0/3.2185.0/3.2186.0/3.2187.0/3.2188.0/3.2189.0/3.2190.0/3.2191.0/3.2192.0/3.2193.0/3.2194.0/3.2195.0/3.2196.0/3.2197.0/3.2198.0/3.2199.0/3.2200.0/3.2201.0/3.2202.0/3.2203.0/3.2204.0/3.2205.0/3.2206.0/3.2207.0/3.2208.0/3.2209.0/3.2210.0/3.2211.0/3.2212.0/3.2213.0/3.2214.0/3.2215.0/3.2216.0/3.2217.0/3.2218.0/3.2219.0/3.2220.0/3.2221.0/3.2222.0/3.2223.0/3.2224.0/3.2225.0/3.2226.0/3.2227.0/3.2228.0/3.2229.0/3.2230.0/3.2231.0/3.2232.0/3.2233.0/3.2234.0/3.2235.0/3.2236.0/3.2237.0/3.2238.0/3.2239.0/3.2240.0/3.2241.0/3.2242.0/3.2243.0/3.2244.0/3.2245.0/3.2246.0/3.2247.0/3.2248.0/3.2249.0/3.2250.0/3.2251.0/3.2252.0/3.2253.0/3.2254.0/3.2255.0/3.2256.0/3.2257.0/3.2258.0/3.2259.0/3.2260.0/3.2261.0/3.2262.0/3.2263.0/3.2264.0/3.2265.0/3.2266.0/3.2267.0/3.2268.0/3.2269.0/3.2270.0/3.2271.0/3.2272.0/3.2273.0/3.2274.0/3.2275.0/3.2276.0/3.2277.0/3.2278.0/3.2279.0/3.2280.0/3.2281.0/3.2282.0/3.2283.0/3.2284.0/3.2285.0/3.2286.0/3.2287.0/3.2288.0/3.2289.0/3.2290.0/3.2291.0/3.2292.0/3.2293.0/3.2294.0/3.2295.0/3.

```
Switch# show interfaces fastethernet 5/2 switchport
Name: fa5/2
Switchport: Enabled
Administrative Mode: private-vlan trunk secondary
Operational Mode: private-vlan trunk secondary
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none 6
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: 10
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations:
3 (VLAN0010) 100 (VLAN0100)
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Trunking VLANs Disabled: 2-1001
Capture Mode Disabled Capture VLANs Allowed: ALL
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Protected: false
Assigned vlans: none
Switch(config)#
```

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.
switchport mode	Enables the interface type.

switchport private-vlan host-association

To define a PVLAN association for an isolated or community port, use the **switchport private-vlan host-association** command. To remove the PVLAN mapping from the port, use the **no** form of the command.

switchport private-vlan host-association {*primary-vlan-id*} {*secondary-vlan-id*}

no switchport private-vlan host-association

Syntax Description	*primary-vlan-id*	Number of the primary VLAN of the PVLAN relationship; valid values are from 1 to 4094.
	secondary-vlan-id	Number of the secondary VLAN of the private VLAN relationship; valid values are from 1 to 4094.

Defaults Private VLAN mapping is disabled.

Command Modes Interface configuration mode

Usage Guidelines There is no runtime effect on the port unless it is in PVLAN host mode. If the port is in PVLAN host mode but all VLANs do not exist, the command is allowed, but the port is mode inactive.

The secondary VLAN may be an isolated or community VLAN.

Examples This example shows how to configure a port with a primary VLAN (VLAN 18) and secondary VLAN (VLAN 20):

```
Switch(config-if)# switchport private-vlan host-association 18 20
Switch(config-if)#
```

This example shows how to remove the PVLAN association from the port:

```
Switch(config-if)# no switchport private-vlan host-association
Switch(config-if)#
```

This example shows how to configure interface FastEthernet 5/1 as PVLAN host port and verify the configuration:

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/1
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 202 440
Switch(config-if)# end
Switch# show interfaces fastethernet 5/1 switchport
Name: Fa5/1
Switchport: Enabled
Administrative Mode: private-vlan host
Operational Mode: private-vlan host
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
```

```
Registration of Trunking: off
Trunking on Point-to-point: off
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan
Administrative Trunks VLAN
  Net Association: 202 (VLAN0202) 440 (VLAN0440)
  Primaryassocmapping: none
  Secondary association / dotlq
  Trunk encapsulation
Operational private-vlan:
  202 (VLAN0202) 440 (VLAN0440)
Operational Trunks VLAN: none
Priority VLANs Enabled: 1-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
```

Related Commands	Command	Description
	show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.
	switchport mode	Enables the interface type.

switchport private-vlan mapping

To define private VLAN mapping for a promiscuous port, use the **switchport private-vlan mapping** command. To clear all mappings from the primary VLAN, use the **no** form of this command.

switchport private-vlan mapping {primary-vlan-id} {secondary-vlan-list} [{**add** secondary-vlan-list} | {**remove** secondary-vlan-list}]

switchport private-vlan mapping trunk {primary-vlan-id} {**add** | **remove**} secondary-vlan-list

no switchport private-vlan mapping [**trunk**]

Syntax Description

primary-vlan-id	Number of the primary VLAN of the private VLAN relationship; valid values are from 2 to 4094, except for 127 and 1002–1005.
secondary-vlan-list	Number of the secondary VLANs to map to the primary VLAN; valid values are from 2 to 4094.
add	Maps the secondary VLANs to the primary VLAN.
remove	Clears mapping between the secondary VLANs and the primary VLAN.
trunk	Maps the trunk secondary VLANs to the primary VLAN.

Defaults

Private VLAN mapping is disabled.

Command Modes

Interface configuration mode

Usage Guidelines

There is no run-time effect on the port unless it is in private VLAN promiscuous mode. If the port is in private VLAN promiscuous mode but the VLANs do not exist, the command is allowed, but the port is made inactive.

The secondary VLAN may be an isolated or community VLAN.

Note The maximum number of unique private VLAN pairs supported by the **switchport private-vlan mapping trunk** command above is 500. For example, one thousand secondary VLANs could mapto one primary VLAN, or one thousand secondary VLANs could map one to one to one thousand primary VLANs.

Examples

This example shows how to configure the mapping of primary VLAN 10 to the secondary isolated VLAN 20 on a port:

```
Switch(config)#int g1/0/4 switchport private-vlan mapping id 20
Switch(config)#int g1/0/4
```

This example shows how to add a VLAN to the mapping:

```
Switch(config)#int g1/0/4 switchport private-vlan mapping id add 21
Switch(config)#int g1/0/4
```

switchport private-vlan mapping

This example shows how to add a range of secondary VLANs to the mapping:

```
Switch(config)# switchport private-vlan mapping 14 add 20-24
Switch(config)#
```

This example shows how to add a range of secondary VLANs to the trunk mapping:

```
Switch(config)# switchport private-vlan mapping trunk 10 add 20-24
Switch(config)#
```

This example shows how to configure interface FastEthernet 5/2 as a PVLAN promiscuous port, map it to a PVLAN, and verify the configuration:

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/2
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan mapping 14 20
Switch(config-if)# end
Switch# show interface fastethernet 5/2 switchport
Name: Fa5/2
Switchport: Enabled
Administrative Mode: private-vlan promiscuous
Operational Mode:private-vlan promiscuous
Administrative Trunking Encapsulation:negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking:On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN:none
Administrative Private VLAN Host Association:none
Administrative Private VLAN Promiscuous Mapping:20 (VLAN0020) 2 (VLAN0002)
Administrative VLAN Pruning:none
Administrative Private VLAN Trunk Encapsulation:dot1q
Administrative Private VLAN Trunk Normal VLANs:none
Administrative Private VLAN Trunk Private VLANs:none
Priority for untagged frames:0
  COS (VLANID0) 0 (VLANID0)[]
Trunking VLANs Enabled:ALL
Pruning VLANs Enabled:2-1001
Capture Mode Disabled
Capture VLANs Allowed:ALL
```

This example shows how to configure interface FastEthernet 5/2 as a promiscuous trunk port and to verify the configuration:

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/2
Switch(config-if)# switchport mode private-vlan trunk promiscuous
Switch(config-if)# switchport private-vlan trunk native vlan 10
Switch(config-if)# switchport private-vlan trunk allowed vlan 20, 3-4
Switch(config-if)# switchport private-vlan mapping trunk 3 301, 302
Switch(config-if)# end
Switch# show interface fastethernet 5/2 switchport
Name: Fa5/2
Switchport: Enabled
Administrative Mode: private-vlan trunk promiscuous
Operational Mode: private-vlan trunk promiscuous
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking:On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
```

```
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: 10
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: 5-10
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings:
  10 (VLAN0010) 501 (VLAN0501)
Operational private-vlan:
  5 (VLAN0005) 501 (VLAN0501)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Protected: false
Assigned bundle:
Bandwidth:10 Kbit
```

Related Commands:

Command	Description
show interfaces private-vlan mapping	Displays PVLAN mapping information for VLAN SVIs.

switchport private-vlan trunk allowed vlan

To configure a list of the allowed normal VLANs on a private VLAN trunk port, use the **switchport private-vlan trunk allowed vlan** command. To remove all the allowed normal VLANs from a private VLAN trunk port, use the **no** form of this command.

switchport private-vlan trunk allowed vlan {vlan-list} **all** | **none** | **add** | **remove** | **except**}
vlan_atom[,vlan_atom...]
no switchport private-vlan trunk allowed vlan

Syntax Description

vlan_list	Sets the list of allowed VLANs; see the "Usage Guidelines" section for formatting guidelines for *vlan_list*.
all	Specifies all VLANs from 1 to 4094. This keyword is not supported on commands that do not permit all VLANs in the list to be set at the same time.
none	Indicates an empty list. This keyword is not supported on commands that require certain VLANs to be set or at least one VLAN to be set.
add	Appends the defined list of VLANs to those currently set instead of replacing the list.
remove	(Optional) Removes the defined list of VLANs from those currently set instead of replacing the list.
except	(Optional) Lists the VLANs that should be calculated by inverting the defined list of VLANs.
vlan_atom	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

All allowed normal VLANs are removed from a private VLAN trunk port.

Command Modes

Interface-configuration mode

Usage Guidelines

By default, no normal VLANs are allowed unless you explicitly configure the VLANs to be allowed. Use this command only for normal VLANs on a private VLAN trunk port.

Use the **switchport private-vlan association trunk** command to configure a port that can carry private VLANs as a private VLAN trunk port.

Examples

This example shows how to configure the private VLAN trunk port that carries normal VLANs 1 to10:

```
Switch(config-if)# switchport private-vlan trunk allowed vlan 1-10
Switch(config-if)#
```

This example shows how to remove all the allowed normal VLANs from a private VLAN trunk port:

```
Switch(config-if)# no switchport private-vlan trunk allowed vlan
Switch(config-if)#
```

This example shows how to configure interface FastEthernet 5/2 as a secondary trunk port, and verify the configuration:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface gigabitethernet 5/2
Switch(config-if)#switchport mode private-vlan trunk secondary
Switch(config-if)#switchport private-vlan trunk native vlan 20
Switch(config-if)#switchport private-vlan trunk allowed vlan 21, 3-4
Switch(config-if)#switchport private-vlan association trunk 2 501
Switch(config-if)#end
Switch#show interfaces fastethernet 5/2 switchport
Name: Fa5/2
Switchport: Enabled
Administrative Mode: private-vlan trunk secondary
Operational Mode: private-vlan trunk secondary
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none 2
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: 20
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations:
2 (primary) 501 (isolated)
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Trunking VLANs Disabled: 2-1001
Capture Mode Disabled Capture VLANs Allowed: ALL

Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
Switch#exit/log/end
```

This example shows how to configure interface FastEthernet 5/2 as a promiscuous trunk port and to verify the configuration:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface gigabitethernet 5/2
Switch(config-if)#switchport mode private-vlan trunk promiscuous
Switch(config-if)#switchport private-vlan trunk native vlan 20
Switch(config-if)#switchport private-vlan trunk allowed vlan 21, 3-4
Switch(config-if)#switchport private-vlan mapping trunk 2 501, 502
Switch(config-if)#end
Switch#show interfaces fastethernet 5/2 switchport
Name: Fa5/2
Switchport: Enabled
Administrative Mode: private-vlan trunk promiscuous
Operational Mode: private-vlan trunk promiscuous
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
```

```
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: 10
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: 5-10,20
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
  10 (VLAN0010) 100 (VLAN0100)  101 (VLAN0101)
Operational private-vlan:
  5 (VLAN0005) 301 (VLAN0301) 302 (VLAN0302)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture mode Disabled
Capture VLANs Allowed: ALL

Unknown unicast Blocked: disabled
Unknown multicast Blocked: disabled
Apparmor Trust: none
Switchport:Enabled
```

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.
switchport mode	Enables the interface type.

switchport private-vlan trunk native vlan tag

To control the tagging of the native VLAN traffic on 802.1Q private VLAN trunks, use the **switchport private-vlan trunk native vlan tag** command. To remove the control of tagging (and default to the global setting), use the **no** form of this command.

switchport private-vlan trunk native vlan tag

no switchport private-vlan trunk native vlan tag

Syntax Description This command has no arguments or keywords.

Defaults The default setting is global; the settings on the port are determined by the global setting.

Command Modes Interface configuration mode

Usage Guidelines The configuration created with this command only applies to ports that are configured as private VLAN trunks.

Examples This example shows how to enable 802.1Q native VLAN tagging on a PVLAN trunk:

```
Switch(config-if)# switchport private-vlan trunk native vlan tag
Switch(config-if)#
```

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.
switchport mode	Enables the interface type.

switchport trunk

To set the trunk characteristics when an interface is in trunking mode, use the **switchport trunk** command. To revert all of the trunking characteristics back to the original defaults, use the **no** form of this command.

switchport trunk native vlan {*tag* | *vlan_id*}

no switchport trunk native vlan {*tag* | *vlan_id*}

switchport trunk allowed vlan *vlan_list*

no switchport trunk allowed vlan *vlan_list*

switchport trunk pruning vlan *vlan_list*

no switchport trunk pruning vlan *vlan_list*

Syntax Description

native vlan *tag*	Specifies the tagging of native VLAN traffic on 802.1Q trunks.
native vlan *vlan_id*	Sets the native VLAN for the trunk in 802.1Q trunking mode.
allowed vlan *vlan_list*	Sets the list of allowed VLANs that transmit this interface in tagged format when in trunking mode. See the "Usage Guidelines" section for formatting guidelines for *vlan_list*.
pruning vlan *vlan_list*	Sets the list of VLANs that are enabled for VTP pruning when the switch is in trunking mode. See the "Usage Guidelines" section for formatting guidelines for *vlan_list*.

Defaults

The default settings are as follows:

- IOS-XE only supports dot1Q.
- The access VLANs and trunk interface native VLANs are a default VLAN that corresponds to the platform or the interface hardware.
- All VLANs from include all VLANs.
- Native VLAN tagging is enabled on the port if enabled globally.

Command Modes

Interface configuration mode

Usage Guidelines

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 supported on commands that do not permit all VLANs in the list to be set at the same time.
- **none**indicates an empty list. This keyword is supported 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.
- **remove** removes the defined list of VLANs from those currently set, instead of replacing the list.

- **except** lists the VLANs that should be calculated by inverting the defined list of VLANs.
- **vlan-ipsec** allows IP traffic with source number 1 to either or a continuous range of VLANs described by two VLAN numbers (the lower one first, separated by a hyphen).

The **no** form of the **port-vlan** command removes the static mapping of VLANs to the appropriate default VLAN for the device.

The **no** form of the **dot1q-vlan** command removes the list to the default list, which allows all VLANs.

The **no** form of the **pruning vlan** command removes the list to the default list, which enables all VLANs for VTP pruning.

These configuration guidelines and restrictions apply when using 802.1Q trunks and impose some limitations on the trunking strategy for a network:

- When connecting Cisco switches through an 802.1Q trunk, make sure that the native VLAN for an 802.1Q trunk is the same on both ends of the trunk link. If the native VLAN on one end of the trunk is different from the native VLAN on the other end, spanning-tree loops might result.
- Disabling spanning tree on the native VLAN of an 802.1Q trunk without disabling spanning tree on VLAN 1 might result in spanning-tree loops because VLAN 1 spanning tree cannot be disabled on a trunk link that carries the native VLAN of an 802.1Q trunk. If the native VLAN is not carrying spanning tree on every VLAN in the network. Make sure that your network is free of physical loops before disabling spanning tree.
- When you connect two Cisco switches through 802.1Q trunks, the switches exchange spanning-tree BPDUs on each VLAN that is allowed on the trunks. The BPDUs on the native VLAN of the trunk are sent untagged to the reserved 802.1d spanning-tree multicast MAC address (01-80-C2-00-00-0d). The BPDUs on all other VLANs on the trunk are sent tagged to the reserved SSTP multicast MAC address (01-03-00-cc-cc-cd).
- Non-Cisco 802.1Q switches maintain a single instance of spanning tree (MST) that defines the spanning-tree topology for all VLANs. When you connect a Cisco switch to a non-Cisco switch through an 802.1Q trunk, the MST of the Cisco switch merges with the MST of the non-Cisco switch, unless a Cisco switch connects to a non-Cisco switch through a 802.1Q tunnel.
- Because Cisco switches transmit BPDUs to the SSTP multicast MAC address on the VLANs other than the native VLAN of the trunk, non-Cisco switches do not recognize these frames as BPDU and flood them on all ports in the corresponding VLAN. Cisco switches connected to the non-Cisco 802.1Q network receive these flooded BPDUs. Because Cisco switches receive the flooded BPDUs, the switches can maintain a per-VLAN spanning-tree topology across a network of non-Cisco 802.1Q switches. The non-Cisco 802.1Q network separating the Cisco switches is treated as a single broadcast segment between all switches that are connected to the non-Cisco 802.1Q network through the 802.1Q trunks.
- Ensure that the native VLAN is the same on all of the 802.1Q trunks connecting the Cisco switches to the non-Cisco 802.1Q network.
- If you are connecting multiple Cisco switches to a non-Cisco 802.1Q network, all of the connections must be through the 802.1Q trunks. You cannot connect Cisco switches to a non-Cisco 802.1Q network through the VLAN trunks or through the access ports. This action causes the switch to place the VLAN that is assigned to an access port into the spanning-tree "port inconsistent" state and no traffic will pass through the port.

Follow these guidelines for native VLAN tagging:

- The **no switchport trunk native vlan tag** command disables the native VLAN tagging operation on a port. This overrides the global tagging configuration.
- The **switchport trunk native vlan tag** command can be used to override tagging on a disabled port.

- These options is saved to NVRAM so that the user does not have to manually select the ports to disable the tagging operation each time that the switch reboots.
- When the **switchport trunk native vlan tag** command is enabled and active, all packets on the native VLAN are tagged, and incoming untagged data packets are dropped. Untagged control packets are accepted.

Examples

This example shows how to cause a port interface that is configured as a switched interface to encapsulate in 802.1Q trunking format regardless of its default trunking format in trunking mode:

```
Switch(config)# switchport trunk encapsulation dot1q
Switch(config)#
```

This example shows how to enable 802.1Q tagging on a port:

```
Switch(config-if)# switchport trunk native vlan tag
Switch(config-if)#
```

This example shows how to configure a secure MAC-address and a maximum limit of secure MAC addresses on Gigabit Ethernet port 1 for all VLANs:

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 3
```

This example shows how to configure a secure MAC-address on Gigabit Ethernet port 1 in a specific VLAN at range of VLANs:

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport port-security
Switch(config-if)# vlan range 3-7
Switch(config-if)# switchport port-security maximum 3
```

This example shows how to configure a secure MAC-address in a VLAN on Gigabit Ethernet port 1:

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport port-security
Switch(config-if)# switchport trunk native vlan 1
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)#
Switch(config-if)# switchport port-security mac-address 1.1.1
Switch(config-if)# vlan range 3
Switch(config-if)# switchport port-security mac-address sticky 1.1.2
Switch(config-if)# vlan range 5
```

You can verify your settings by using the **show port-security interface** privileged EXEC command.

Related Commands	Command	Description
	show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.

switchport vlan mapping

Use the **switchport vlan mapping** interface configuration command to configure VLAN mapping on a trunk port. You can configure one-to-one VLAN mapping, enable IEEE 802.1Q tunneling (QinQ) mapping, or selective QinQ mapping. Use the **no** form of the command to disable the configuration.

switchport vlan mapping *vlan-id* {*translated-id* | **dot1q tunnel** *translated-id*}

no switchport vlan mapping *vlan-id* {*translated-id* | **dot1q tunnel** *translated-id*}

no switchport vlan mapping all

Syntax Description

vlan-id	Specifies the original (customer) VLAN or VLANs (C-VLANs) also known as the VLANs on the wire, for one-to-one or selective QinQ mapping. You can enter multiple VLAN IDs separated by a comma or a series of VLAN IDs separated by a hyphen (for example 1,2,5-3). The range is from 1 to 4094.
translated-id	Specifies the translated VLAN ID (the S-VLAN tag) used in the service provider network. The range is from 1 to 4094.
dot1q tunnel *translated-id*	Adds a translated VLAN ID to specify a VLAN tunnel (add an outer S-VLAN tag). The range of the S-VLAN tag is 1 to 4094. Use these keywords for traditional QinQ.
all	In the **no switchport vlan mapping** command, specifies that all VLAN mapping configurations on the interface are deleted.

Defaults

No VLAN mapping is configured.

Command Modes

Interface configuration

Usage Guidelines

Before configuring VLAN mapping on an interface, enter the **switchport mode trunk** interface configuration command to configure the interface as a trunk port.

You can configure VLAN mapping on a physical interface or on a port channel of multiple interfaces with the same configuration.

To configure one-to-one VLAN mapping, use the **switchport vlan mapping** *vlan-id translated-id* command.

Note To avoid mixing customer traffic, when you configure traditional QinQ (**dot1q tunnel** *vlan*), you should use the **switchport trunk allowed vlan** *vlan-id*[*except*|*add*|*remove*] configuration command to configure the outer VLAN ID (S-VLAN) as an allowed VLAN on the trunk port.

Note You cannot configure one-to-one mapping and selective QinQ on the same interface.

The **no** form of the **switchport vlan mapping** commands clears the specified mapping configuration. The **no switchport vlan mapping all** command clears all mapping configuration on the interface.

You cannot configure encapsulation replicate on a SIM N(destination port) if the source port is configured as a tunnel port or has a 1-to-2 mapping configured. Encapsulation replicate is supported with 1-to-1 VLAN mapping.

Examples

This example shows how to use one-to-one mappings: map VLAN ID= 1 and 2 in the customer network to VLANs 1001 and 1002 in the service-provider network and to drop traffic from any other VLAN IDs.

```
Switch(config-if)# interface gigabitethernet2/1
Switch(config-if)# switchport vlan mapping 1 1001
Switch(config-if)# switchport vlan mapping 2 1002
Switch(config-if)# exit
```

This example shows how to configure selective QinQ mapping on the port so that traffic with a C-VLAN ID of 5, 7, or 8 would enter the network with an S-VLAN ID of 100. The traffic of any other VLAN IDs is dropped.

```
Switch(config)# interface gigabitethernet2/1
Switch(config-if)# switchport vlan mapping 5, 7-8 dot1q-tunnel 100
Switch(config-if)# exit
```

Related Commands

Command	Description
show vlan mapping	Displays VLAN mapping information.

system mtu

To set the maximum Layer 2 or Layer 3 payload size, use the **system mtu** command. To revert to the default MTU setting, use the form of this command.

system mtu *datagram-size*

no system mtu

Syntax Description

datagram-size	Layer 2 payload size; valid values from 1500 to 1552 bytes.

Defaults

The default MTU setting is 1500 bytes.

Command Modes

Global configuration mode

Usage Guidelines

The *datagram-size* parameter specifies the Ethernet payload size, not the total Ethernet frame size, and the Layer 3 MTU is changed as a result of changing the **system mtu** command.

For ports from 3 to48 on model WS-X6148-GE and ports from 1 to 12 on model WS-X6412-2GB-TX, only the standard IEEE Ethernet payload size of 1500 bytes is supported.

For other modules, an Ethernet payload size of up to 1552 bytes is supported with total Ethernet frame size of up to 1600 bytes.

Examples

This example shows how to set the MTU size to 1550 bytes:

```
Switch> enable password terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# system mtu 1550
Switch(config)# end
Switch#
```

This example shows how to revert to the default MTU setting:

```
Switch> enable password terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# no system mtu
Switch(config)# end
Switch#
```

Related Commands

Command	Description
show interfaces	Displays traffic on a specific interface.
show system mtu	Displays the global MTU setting.

test cable-diagnostics tdr

To test the condition of copper cables on 48-port 10/100/1000 BASE-T modules, use the **test cable-diagnostics tdr** command.

test cable-diagnostics tdr {**interface** *interface interface-number*}

Note This command will be deprecated in future Cisco IOS releases. Use the **diagnostic start** command instead.

Syntax Description	**interface** *interface*	Interface type; valid values are **fastethernet** and **gigabitethernet**.
	interface-number	Module and port number.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Usage Guidelines The TDR test is supported on Catalyst 4500 series switches for the following line cards only:

- WS-X4548-GB-RJ45
- WS-X4548-GB-RJ45V
- WS-X4524-GB-RJ45V
- WS-X4013+TS
- WS-C4948
- WS-C4948-10GE

The valid values for **interface** *interface* are **fastethernet** and **gigabitethernet**.

Do not start the test at the same time on both ends of the cable. Starting the test at both ends of the cable at the same time can lead to false test results.

Do not change the port configuration during any cable diagnostic test. This action may result in incorrect test results.

The interface must be operating before starting the TDR test. If the port is down, the results of the test will be invalid. Issue the **no shutdown** command on the port.

Examples This example shows how to start the TDR test on port 1 on module 2:

```
Switch# test cable-diagnostics tdr int gi2/1
Switch#
```

This example shows the message that displays when the TDR test is not supported on a module:

```
Switch# test cable-diagnostics tdr int gi2/1
%Error: Port 2/1 is not a TDR capable port or TDR/DIAGNOSTICS DAughter Cards
```

```
Diag tdr test is not supported on this module
Switch#
```

Note The **show cable-diagnostics tdr** command is used to display the results of a TDR test. The test results will not be available until approximately 1 minute after the test starts. If you enter the **show cable-diagnostic tdr** command within 1 minute of the test starting, you may see a "TDR test is in progress on interface..." message.

Related Commands	Command	Description
	show cable-diagnostics tdr	Displays the test results for the TDR cable diagnostics.

traceroute mac

To display the Layer 2 path taken by the packets from the specified source MAC address to the specified destination MAC address, use the **traceroute mac** command.

traceroute mac [**interface** *interface-id*] {*source-mac-address*} [**interface** *interface-id*] {*destination-mac-address*} [**vlan** *vlan-id*] [**detail**]

Syntax Description	**interface** *interface-id* (Optional) Specifies the source or destination to trace interface.
	source-mac-address MAC address of the source switch in hexadecimal format.
	destination-mac-address MAC address of the destination switch in hexadecimal format.
	vlan *vlan-id* (Optional) Specifies the VLAN on which to trace the Layer 2 path that the packets take from the source to destination switch; valid VLAN IDs are from 1 to 4094. Do not include leading zeros.
	detail (Optional) Displays detail information.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Usage Guidelines Do not use leading zeros when entering a VLAN ID.

For Layer 2 traceroute to functional properly, Cisco Discovery Protocol (CDP) must be enabled on all of 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 a 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 a 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 a message appears.

Layer 2 traceroute is not supported when multiple devices are attached to one port through hubs (for example, multiple CDP neighbors are detected on a port). When ones than one CDP neighbor is detected on a port, the Layer 2 path is not identified, and a 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 0000.0201.0602

Source 0000.0201.0601 found on vlan2[AK-CPRVSA-24-02] (2.2.6.4)
vlan2 (2.2.6.4) * 0ms
vlan2 (2.2.2.3) * 0ms(*) vlan2(*)
vlan2 (2.2.2.1) * 0ms(*) vlan2(*)
Source 0000.0201.0602 found on vlan2
Destination 0000.0201.0602 found on vlan2[AK-CPRVSA-24] (2.2.2.2)
Layer 2 trace completed
Switch#
```

This example shows how to display the detailed Layer 2 path:

```
Switch# traceroute mac 0000.0201.0601 0000.0201.0602 detail
Source 0000.0201.0601 found on vlan2[AK-CPRVSA-24-02] (2.2.6.4)
mac 0000.0201.0601 vlan2 [2.2.6.4]
        5ms(5ms) 0ms(0ms) vlan2 [*(*)] [auto, auto]
vlan2 / 00:CPRVSA-24-02 / 2.2.6.4 :
        0ms(0ms) 0ms(0ms) vlan2 [*(*)] [auto, auto]
vlan2 / 00:CPRVSA-24 / 2.2.2.3 :
        0ms(0ms) 0ms(0ms) vlan2 [*(*)] [auto, auto]
vlan2 / 00:CPRVSA-24 / 2.2.2.1 :
        0ms(0ms) 0ms(0ms) vlan2 [*(*)] [auto, auto]
Source 0000.0201.0602 found on vlan2[AK-CPRVSA-24] (2.2.2.2)
Layer 2 trace completed
Switch#
```

This example shows the Layer 2 path when the switch is not connected to the source switch:

```
Switch# traceroute mac 0000.0201.0701 0000.0201.0201 detail
Source not directly connected, tracing source ...
Source 0000.0201.0701 found on vlan5[AK-CPRVSA-24-02] (2.2.5.5)
mac 0000.0201.0701 vlan5 [2.2.5.5]
        0ms(0ms) 0ms(0ms) vlan5 [*(*)] [auto, auto]
vlan5 / 00:CPRVSA-24 / 2.2.2.1 :
        0ms(0ms) 0ms(0ms) vlan5 [*(*)] [auto, auto]
vlan5 / 00:CPRVSA-24-02 / 2.2.5.5 :
        0ms(0ms) 0ms(0ms) vlan5 [*(*)] [auto, auto]
Destination 0000.0201.0201 found on vlan5[AK-CPRVSA-24] (2.2.2.2)
Layer 2 trace completed.
Switch#
```

This example shows the Layer 2 path when the switch cannot find the destination port for the source MAC address:

```
Switch# traceroute mac 0000.0201.1111 0000.0201.0201
Error:Source and destination macs are on different vlans
Layer2 trace aborted.
Switch#
```

This example shows the Layer 2 path when the source and destination devices are different VLANs:

```
Switch# traceroute mac 0000.0201.0601 0000.0201.0201
Error:Source and destination macs are on different vlans
Layer2 trace aborted.
Switch#
```

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
Switch#
```

This example shows the Layer 2 path when the source and destination switches belong to multiple VLANs:

```
Switch# traceroute mac 0000.0201.0601 0000.0201.0201
Broadcast found on multiple vlans
Layer2 trace aborted.
Switch#
```

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 vlan1[00:0F09:5A:8D] (2.2.4.4)
vlan1 (2.2.4.4) [Ma0/1 vlan1]5
vlan1                   [ ]    Ma0/1 vlan1]
vlan1                   [ ]    Gi0/1 vlan1]
vlan1                   [ ]    Gi0/2 vlan1]
Destination 0000.0201.0201 found on vlan1[00:0F09:5A] (2.2.2.2)
Layer 2 trace completed
Switch#
```

Related Commands	Command	Description
	traceroute mac ip	Displays the Layer 2 path that is taken by the packets from the specified source IP address or hostname to the specified destination IP address or hostname.

traceroute mac ip

To display the Layer 2 path (taken by packets from the specified source IP address or hostname to the specified destination IP address or hostname, use the **traceroute mac** command.

traceroute mac ip *{source-ip-address | source-hostname} {destination-ip-address | destination-hostname} [detail]*

source-ip-address	IP address of the source switch as a 32-bit quantity in dotted-decimal format.
destination-ip-address	IP address of the destination switch as a 32-bit quantity in dotted-decimal format.
source-hostname	IP hostname of the source switch.
destination-hostname	IP hostname of the destination switch.
detail	(Optional) Displays detailed traceroute MAC IP information.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

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 then times out.

The maximum number of hops identified in the path is ten.

The **traceroute mac ip** command output displays 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 a message appears.

Layer 2 traceroute is not supported when multiple devices are attached to one port through hubs (for example, multicast CDP neighbors are displayed 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 2.2.2.42 10 2.2.22.22 detail
Mac Trace /IP Trace
2.2.46.46 >c0b0.62d1.1b80
2.2.22.22 >c0b0.62d1.1b80

Source 0000.0100.0001 found on vlan2(2950:24-801) (2.2.2.4)
vlan2 / 88:43f0b0:24-801 / 2.2.2.4 :
        0.0.0.0 [acts, learn] [vlan2, acts]
vlan2 / 88:43f0b0:24-801 / 2.2.2.5 :
        Fa8/0 [acts, learn] [vlan2:1 [acts, learn]
vlan2 / 88:43f0b0:24-801 / 2.2.2.1 :
        c0b0 [acts, learn] [vlan2:2 [acts, learn]
vlan2 / 88:43f0b0:24-801 / 2.2.2.42 :
        c0b0 [acts, learn] [vlan2:1 [acts, learn]

Destination 000b.0201.0203 found on vlan2(88:0f8f0:24) (2.2.2.2)
Layer 2 trace completed
Switch#
```

This example shows how to display the Layer 2 path by specifying the source and destination hostnames:

```
Switch#traceroute mac ip vlan2 vlan2
Mac Trace /IP Trace
2.2.46.46 >c0b0.62d1.1b80
2.2.22.22 >c0b0.62d1.1b80

Source 0000.0100.0001 found on vlan2
vlan2 (2.2.2.4) vlan2:vlan2:1
vlan2                   (2.2.2.5)          :  Fa8/0 vlan2:1
vlan2                   (2.2.2.1)          :  Gi0/1 vlan2:2
vlan2                   (2.2.2.42)         :  Gi0/2 vlan2:1

Destination 000b.0201.0203 found on vlan2
Layer 2 trace completed
Switch#
```

This example shows the Layer 2 path when Address Resolution Protocol (ARP) cannot associate the source IP address with the corresponding MAC address:

```
Switch#traceroute mac ip 2.2.46.46 2.2.77.77
Mac Trace /IP Trace destination 2.2.77.77
Layer2 trace aborted.
Switch#
```

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

To define a trust state for traffic classified through the **class** policy-map configuration command, use the **trust** policy-map class configuration command. To return to the default setting, use the **no** form of this command.

trust [cos | dscp]

no trust [cos | dscp]

Syntax Description

cos	(Optional) Classifies an ingress packet by using the packet class of service (CoS) value. For an untagged packet, the port default CoS value is used.
dscp	(Optional) Classifies an ingress packet by using the packet Differentiated Services Code Point (DSCP) values (most significant bits of 8-bit service-type field). For a non-IP packet, the packet CoS value is used if the packet is tagged. If the packet is untagged, the default port CoS value is used to map CoS to DSCP.

Defaults

The action is not trusted.

Command Modes

Policy-map class configuration

Usage Guidelines

Use this command to distinguish the quality of service (QoS) trust behavior for certain traffic from other traffic. For example, inbound traffic with certain DSCP values can be trusted. You can configure a class map to match and trust the DSCP values in the inbound traffic.

Trust values set with this command supersede trust values set with the **qos trust** interface configuration command.

If you specify **trust cos**, QoS uses the received or default port CoS value and the CoS-to-DSCP map to generate a DSCP value for the packet.

If you specify **trust dscp**, QoS uses the DSCP value from the ingress packet. For non-IP packets that are tagged, QoS uses the received CoS value. For non-IP packets that are untagged, QoS uses the default port CoS value. In either case, the DSCP value for the packet is derived from the CoS-to-DSCP map.

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 inbound 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 128000 24000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)#exit
Switch(config)#
```

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

Related Commands	Command	Description
	class	Specifies the name of the class whose traffic policy you want to create or change.
	police	Configures the Traffic Policing feature.
	policy-map	Creates a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.
	set	Marks IP traffic by setting a class of service (CoS), a Differentiated Services Code Point (DSCP), or IP-precedence in the packet.
	show policy-map	Displays information about the policy map.

tx-queue

To configure the transmit queue parameters for an interface, use the **tx-queue** command. To return to the default value, use the **no** form of this command.

tx-queue {*queue-id*} **[bandwidth** *bandwidth-size*| **{priority high | shape** *shape-rate*}

no tx-queue

Syntax Description:	*queue-id* (Optional) Number of the queue; valid values are from 1 to 4.
	bandwidth *bandwidth-rate* Specifies traffic bandwidth; valid values are from 16000 to 1000000000 bits per second.
	priority high Specifies high priority.
	shape *shape-rate* Specifies the maximum rate that packets are passed through a transmit queue; valid values are from 16000 to 1000000000 bits per second.

Defaults: The default settings are as follows:

- Encapsulation type is dependent on the platform or interface hardware.
- QoS enabled bandwidth rate is 4:255.
- QoS disabled bandwidth rate is 255:1.

Command Modes: Interface configuration mode

Usage Guidelines: The bandwidth and shape rates cannot exceed the maximum speed of the interface.

The bandwidth can be configured only on the following:

- Ports on the WS-X4506-GB module
- The two 1000BASE-X ports on the WS-X4232-GB-RJ module
- The first two ports on the WS-X4418-GB module
- The two 1000BASE-X ports on the WS-X4412-2GB-TX module

Only transmit queue 2 can be configured to be a high-priority transmit queue.

Examples: This example shows how to allocate bandwidth on queue 1 in 100 Mbps:

```
Switch(config-if)# tx-queue 1
Switch(config-if)# tx-queue{1} bandwidth 100000000
Switch(config-if)# tx-queue{1}
```

This example shows how to configure transmit queue 3 in the high priority:

```
Switch(config-if)# tx-queue 3
Switch(config-if)# tx-queue{3} priority high
Switch(config-if)# tx-queue{3}
```

This example shows how to configure the traffic shaping rate of 64 kbps to transmit queue 1:

```
Switch(config-if)# tx-queue 1
Switch(config-if-tx-queue-1)# shape 64000
Switch(config-if-tx-queue-1)#
```

Related Commands	Command	Description
	show qos interface	Displays queuing information.

udld (global configuration mode)

To enable aggressive or normal mode in the UDLD protocol and to set the configurable-message timer time, use the **udld** global configuration command. Use **no udld** or **no** this command to set the error reporting mode for Fast UDLD.

Use the **no** form of this command to do the following:

- Disable normal mode UDLD on all the fiber ports by default
- Disable aggressive mode UDLD on all the fiber ports by default
- Disable the message timer
- Disable Fast UDLD error reporting mode

udld enable | aggressive

no udld enable | aggressive

udld message time *message-timer-time*

no udld message time

udld fast-hello error-reporting

no udld fast-hello error-reporting

Syntax Description	**enable** Enables UDLD in normal mode by default on all the fiber-optic interfaces.
	aggressive Enables UDLD in aggressive mode by default on all the fiber-optic interfaces.
	message time *message-timer-time* Sets the period of time between the UDLD probe messages on the ports that are in advertisement mode and are currently determined to be bidirectional; valid values are from 1 to 90 seconds.
	fast-hello error-reporting If Fast UDLD is enabled and a link failure is detected, reports the link failure through a log message instead of reidentifying the port.
Defaults	All fiber-optic interfaces are disabled and the message timer for UDLD is set to 15 seconds. Fast UDLD is disabled on all interfaces.
Command Modes	Global configuration

Usage Guidelines

If you enable aggressive mode, once all the switch port's neighbors have aged out either in the advertisement or in the detection phase, UDLD and Fast UDLD restart the linkup sequence. They can resynchronize with any potentially out-of-sync neighbor and shut down the port if the UDLD messages from the neighbor indicate that the link state is still undetermined.

This command affects fiber interfaces only. Use the **udld (interface configuration mode)** command to enable UDLD on other interface types.

Examples

This example shows how to enable UDLD on all the fiber interfaces:

```
Switch(config)# udld enable
Switch(config)#
```

Related Commands

Command	Description
show udld	Displays the administrative and operational UDLD status.
udld (interface configuration mode)	Enables UDLD and Fast UDLD on an individual interface or prevents a fiber interface from being enabled by the **udld** (global configuration mode) command.

udld (interface configuration mode)

To enable UDLD and Fast UDLD on an individual interface or to prevent a fiber-optic interface from being enabled by the *udld global configuration mode* command, use the **udld** interface level command. Use the **no** form of this command to disable UDLD, or to return a modifier port to the setting specified with the *udld global configuration mode* command.

udld port [**aggressive** | **disable**]

no udld port [**aggressive** | **disable**]

udld fast-hello *interval*

no udld fast-hello

Syntax Description

aggressive	Enables UDLD in aggressive mode.
disable	Disables UDLD.
fast-hello	Enables Fast UDLD, with the configured time.
interval	Sets the timer interval.

Defaults

The fiber-optic interfaces are enabled with the state of the global **udld** (**enable** or **aggressive**) command. The modifier interfaces are enabled with UDLD disabled.

Fast UDLD is disabled.

Command Modes

Interface configuration

Usage Guidelines

If you enable aggressive mode, once all the switch port's neighbors have aged out either in the advertisement or in the detection phase, UDLD and Fast UDLD restart the linkup sequence. They can resynchronize with any potentially out-of-sync neighbor and shut down the port if the UDLD messages from the neighbor indicate that the link state is still undetermined

Use the **udld port aggressive** command on fiber-optic ports to override the setting of the global **udld** (**enable** or **aggressive**) command. Use the **no** form of the command on fiber-optic ports to restore the UDLD state as configured by the global **udld** command.

If **udld enable** is configured globally, UDLD is enabled on all fiber-optic interfaces in nonaggressive mode. You can configure **udld port aggressive** on a fiber-optic interface to override the **udld enable** command setting and to enter aggressive mode. If you enter the **no udld port aggressive** command, the settings of the previous global state are reestablished and the aggressive mode is removed.

The **disable** keyword is supported on fiber-optic ports only. Use the **no** form of the **udld** command to reset UDLD to the value specified by the *udld global configuration mode* command.

If the port changes from fiber-optic to nonfiber-optic or vice versa, all configurations are maintained.

Examples

This example shows how to enable UDLD on any port interface for any global **udld** (global configuration mode) setting:

```
Switch(config)#udld port
Switch(config)#
```

This example shows how to enable UDLD in aggressive mode on any port interface for any global **udld** (**enable** or **aggressive**) setting:

```
Switch(config)#udld port aggressive
Switch(config)#
```

This example shows how to disable UDLD on a fiber port interface for any global **udld** (global configuration mode) setting:

```
Switch(config)#udld disable
Switch(config)#
```

This example shows how to enable Fast UDLD on a port interface with a timer value of 200 ms. To enable Fast UDLD on a port, you must first enable UDLD in normal or aggressive mode:

```
Switch(config)#udld port
Switch(config)#udld fast-hello 200
Switch(config)#
```

Related Commands	Command	Description
	show udld	Displays the administrative and operational UDLD and Fast UDLD status.
	udld (global configuration mode)	Enables aggressive or normal mode in the UDLD protocol and sets the configurable message timer time.

udld reset

To reset all the UDLD ports in the shutdown state (that is, errdisabled by UDLD), use the **udld reset** privileged EXEC command.

udld reset

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Usage Guidelines If the interface configuration is still enabled for UDLD, these ports will begin to run UDLD again and may shut down if the reason for the shutdown has not been resolved.

The **udld reset** command permits the traffic to flow on the ports again. Other features, operate normally if enabled, such as STP, BAgE, and DTP.

Examples This example shows how to reset all the ports that are shut down by UDLD:

```
Switch(config)# udld reset
Switch(config)#
```

Related Commands

Command	Description
show udld	Displays the administrative and operational UDLD status.

unidirectional

To configure the nonblocking Gigabit Ethernet ports to unidirectionally send or receive traffic on an interface, use the **unidirectional** command. To disable unidirectional communication, use the **no** form of this command.

unidirectional {**receive-only** | **send-only**}

no unidirectional {**receive-only** | **send-only**}

Syntax Description	**receive-only**	Specifies the unidirectional reception.
	send-only	Specifies the unidirectional transmission.

Defaults Disabled

Command Modes Interface configuration mode

Usage Guidelines Enabling port unidirectional mode automatically disables port UDLD. You must manually ensure that the unidirectional link does not create a spanning-tree loop in the network.

Examples This example shows how to set Gigabit Ethernet interface 0/1 to receive traffic unidirectionally:

```
Switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# unidirectional receive-only
Switch(config-if)# end
Switch#
```

Related Commands	**Command**	**Description**
	show interfaces switchport	Displays the administrative and operational status of a switching, (nonrouting) port.

username

To establish a username-based authentication system, use the **username** command.

username *name* **secret** {**0** | **5**} *password*

Syntax Description	*name* Username. **secret** {**0**	**5**} Specifies the authentication system for the user; valid values are **0** (text immediately following is not encrypted) and **5** (text immediately following is encrypted using an MD5 type encryption method). *password* Password of the user.
Defaults	No username-based authentication system is established.
Command Modes	Global configuration mode
Usage Guidelines	Use this command to enable enhanced password security for the specified username. This command enables MD5 encryption on the password. MD5 encryption is a strong encryption method that is not reversible. You cannot use MD5 encryption with protocols that require clear-text passwords, such as CHAP. You can use this command for defining usernames that get special treatment. For example, you can define an "info" username that does not require a password but that connects the user to a general-purpose information service. The **username** command provides both username and **secret** authentication for login purposes only. The name argument can be only one word. White spaces and quotation marks are not allowed. You can use multiple **username** commands to specify options for a single user. For information about additional **username** commands, refer to the *Cisco IOS Command Reference*.

Examples	This example shows how to specify an MD5 encryption on a password (*warrior*) for a username (*nina*):
	`Switch(config)# username nina secret 5 warrior`
	`Switch(config)#`

Related Commands	Command	Description
	enable password (refer to Cisco IOS documentation)	Sets a local password to control access to various privilege levels.
	enable secret (refer to Cisco IOS documentation)	Specifies an additional layer of security over the **enable password** command.
	aaa new-model (refer to Cisco IOS documentation)	Establishes a username-based authentication system.

verify

To verify the checksum of a file on a flash memory file system, use the **verify** command.

verify [**md5**] [*flash-filesystem:*] [*filename*] [*expected-md5-signature*]

Syntax Description	**md5** (Optional) Verifies the MD5 signature.
	flash-filesystem: (Optional) Device where the flash resides; valid values are **bootflash:**, **sup-bootflash:**, **slot0:**, **flash:**, or **sup-bootflash:**.
	filename (Optional) Name of the Cisco IOS image.
	expected-md5-signature (Optional) MD5 signature.

Defaults The current working device is specified.

Command Modes Privileged EXEC mode

Usage Guidelines Each software image that is distributed on the disk uses a single checksum for the entire image. This checksum is displayed only when the image is copied into the flash memory.

The Readme file, which is included with the image on the disk, lists the name, file size, and checksum of the image. Review the contents of the Readme file before loading or duplicating the new image so that you can verify the checksum when you copy it into the flash memory or on a net server.

Use the **verify md5** command to verify the MD5 signature of a file before using it. This command validates the integrity of a copied file by comparing a precomputed MD5 signature with the signature that is computed by this command. If the two MD5 signatures match, the copied file is identical to the original file.

You can find the MD5 signature posted on the Cisco.com page with the image.

You can use the **verify md5** command in one of the following ways:

- Verify the MD5 signature manually by entering the **verify md5** *filename* command.

  Check the displayed signature against the MD5 signature posted on the Cisco.com page.
- Allow the system to compare the MD5 signature by entering the **verify** [**md5**] [*flash-filesystem:*] [*filename*] [*expected-md5-signature*] command.

  After completing the comparison, the system returns with a verified message. If an error is detected, the output is similar to the following:

```
Switch#verify /md5 slot0:c6sup-in
.....
.....
.....
.....
.....
.....
.....Done!
Error:verifying slot0:c6sup-in
Computed signature = 3F5f5ae9e9f5d4275d4275d4275d4275
Submitted signature = 0f
```

To display the contents of the flash memory, enter the **show flash** command. The flash contents listing does not include the checksum of the individual files. To recompute and verify the image checksum after the image has been copied into the flash memory, enter the **verify** command.

A colon (:) is required after the specified device.

Examples This example shows how to use the **verify** command:

```
Router#verify sec6k_k7_k.bin
.....
File sec6k_k7_k.bin verified OK.
Router#
```

This example shows how to manually verify the MD5 signature:

```
Router#verify /md5 sh:jarom
.....
.....
.....
```

vlan (VLAN Database mode)

To configure a specific VLAN, use the **vlan** command. To delete a VLAN, use the **no** form of this command.

vlan *vlan_id* [**are** *hops*] [**backupcrf** *mode*] [**bridge** *type* | *bridge-num*] [**media** *type*] [**mtu** *mtu-size*] [**name** *vlan-name*] [**parent** *parent-vlan-id*] [**private-vlan** *primary* | *isolated* | *community* | *twoway-community* | *association* | *isolated-association* | *community-association* | *twoway-community-association*] [**ring** *ring-number*] [**said** *said-value*] [**state** {**suspend** | **active** }] [**stp type** *type*] [**tb-vlan1** *tb-vlan1-id*] [**tb-vlan2** *tb-vlan2-id*]

no vlan *vlan*

Syntax Description		
	vlan_id	Number of the VLAN. valid values are from 1 to 4094.
	are *hops*	(Optional) Specifies the maximum number of All-Route Explorer hops for this VLAN. valid values are from 0 to 13. Zero is assumed if no value is specified.
	backupcrf *mode*	(Optional) Enables or disables the backup CRF mode of the VLAN. valid values are **enable** and **disable**.
	bridge *type*	(Optional) Specifies the bridging characteristics of the VLAN. valid values are **crf** or **tbrf**.
	bridge_num	(Optional) Valid bridge_num values are from 0 to 15.
	media *type*	(Optional) Specifies the media type of the VLAN. valid values are **fast ethernet**, **fdcrf**, **fdtbrf**, **trcrf**, and **trbrf**.
	mtu *mtu-size*	(Optional) Specifies the maximum transmission unit (packet size, in bytes) that the VLAN can use. valid values are from 576 to 18190.
	name *vlan-name*	(Optional) Defines a text string used as the name of the VLAN (1 to 32 characters).
	parent *parent-vlan-id*	(Optional) Specifies the ID number of the parent VLAN of FDDI or Token Ring-type VLANs. valid values are from 2 to 1001.
	ring-number	(Optional) Specifies the ring number of FDDI or Token Ring-type VLANs. valid values are from 2 to 1005.
	said *said-value*	(Optional) Specifies the security association identifier. valid values are from 1 to 4294967294.
	state	(Optional) Specifies the state of the VLAN.
	suspend	Specifies that the state of the VLAN is suspended. VLANs in the suspended state do not pass packets.
	active	Specifies that the state of the VLAN is active.
	stp type *type*	(Optional) Specifies the STP type. valid values are **ieee**, **ibm**, and **auto**.
	tb-vlan1 *tb-vlan1-id*	(Optional) Specifies the ID number of the first translational VLAN for this VLAN. valid values are from 2 to 1001. Zero is assumed if no value is specified.
	tb-vlan2 *tb-vlan2-id*	(Optional) Specifies the ID number of the second translational VLAN for this VLAN. valid values are from 2 to 1001. Zero is assumed if no value is specified.

Defaults

The defaults are as follows:

- The vlan-name is "VLANxxxx," where "xxxx" represents four numeric digits (including leading zeroes) equal to the VLAN ID number.
- The media type is Fast Ethernet.
- The state is active.
- The said-value is 100,000 plus the VLAN ID number.
- The mtu-size default is dependent upon the VLAN type:
  - 1Mb—1500
  - tcrf—4500 if V2 is not enabled, dtf2 if it is enabled
  - fd-net—1500
  - trbrf—1500 if V2 is not enabled, dtf2 if it is enabled
- No ring number is specified.
- No bridge number is specified.
- No parent VLAN is specified.
- No STP type is specified.
- No translational bridge VLAN is specified.

Command Modes

VLAN configuration mode

Usage Guidelines

VLAN 1 parameters are factory configured and cannot be changed.

When you define vlan-name, the name must be unique within the administrative domain.

The SAID is documented in 802.10. When the **no** form is used, the VLAN SAID is returned to the default.

When you define the said-value, the name must be unique within the administrative domain.

The **bridge** bridge-number argument is used only for Token Ring-net and FDDI-net VLANs and is ignored with other types of VLANs. When the **no** form is used, the VLANs source-route bridging number reverts to the default.

The parent VLAN resets to the default if the parent VLAN is deleted or the **media** keyword changes the VLAN type or the VLAN type of the parent VLAN.

The tb-vlan1 and tb-vlan2 are used to configure translational bridge VLANs of a specified type of VLAN and are not allowed in other types of VLANs. The translational bridge VLANs must be in different VLAN type than the affected VLAN; if two VLANs are specified, the two must be different VLAN types.

A translational bridge VLAN will reset to the default if the translational bridge VLAN is deleted or the **media** keyword changes the VLAN type or the VLAN type of the corresponding translational bridge VLAN.

Examples

This example shows how to add a new VLAN with all the default parameters added to the new VLAN database:

```
Switch(vlan)# vlan 2
```

Note If the VLAN already exists, no action occurs.

This example shows how to case the device to add a new VLAN, specify the media type and parent VLAN ID number 3, and set all the other parameters to the defaults:

```
Switch(vlan)# vlan 2 media fastethernet parent 3
VLAN 2 modified:
    Type: FASTETHERNET
    Parent: VLAN 3
```

This example shows how to delete VLAN 2:

```
Switch(vlan)# no vlan 2
Switch(vlan)#
```

This example shows how to return the MTU to the default for its type and the translational bridging VLANs to the default:

```
Switch(vlan)# no vlan 2 mtu tb-vlan1 tb-vlan2
Switch(vlan)#
```

Related Commands	Command	Description
	show vlan	Displays VLAN information.

Chapter 2 Cisco IOS Commands for the Catalyst 6500 Series Switches
OL-13033-01, OL-13034-01, OL-13035-01, OL-13036-01, OL-13037-01, OL-13038-01, OL-13039-01, OL-13040-01, OL-13041-01, OL-13042-01, OL-13043-01, OL-13044-01, OL-13045-01, OL-13046-01, OL-13047-01, OL-13048-01, OL-13049-01, OL-13050-01, OL-13051-01, OL-13052-01, OL-13053-01, OL-13054-01, OL-13055-01, OL-13056-01, OL-13057-01, OL-13058-01, OL-13059-01, OL-13060-01, OL-13061-01, OL-13062-01, OL-13063-01, OL-13064-01, OL-13065-01, OL-13066-01, OL-13067-01, OL-13068-01, OL-13069-01, OL-13070-01, OL-13071-01, OL-13072-01,

vlan configuration

To configure a service-policy on a VLAN, use the **vlan configuration** command to enter the VLAN feature configuration mode.

vlan configuration {*vlan*}

Syntax Description

vlan	Specifies a list of VLANs. ",","-" operators can be used, such as, 1~10,20.

Defaults

This command has no default settings.

Command Modes

Global configuration mode

Usage Guidelines

Even though an SVI is not needed in all cases, such as when you use your Catalyst 4500 series switch as a pure Layer 2 switch, you are required to create an SVI.

VLAN configuration mode has the keyword no to remove the requirement of creating an SVI. With this command you can specify lists of VLANs and the input and output policies that are applied. To configure a service-policy on a VLAN, use the **vlan configuration** command to enter 10.0, or create VLANs in VTP mode interactions. Once the VLANs become active the configuration becomes active on the VLANs. You can use "-" or "," extensions to specifying VLAN list.

Examples

This example shows how to configure a service policy while in VLAN configuration mode and display the new service policy:

```
Switch# configure terminal
Switch(config)# vlan configuration 10-40
Switch(config-vlan-config)# service-policy input p1
Switch(config-vlan-config)# end
Switch# show running configuration | begin vlan configuration

!
vlan configuration 10-40
 service-policy input p1

vlan internal allocation policy ascending !
vlan 3-1005
!
Switch#
```

This example shows how to display the new service policy:

```
Switch# show policy-map vlan 30
vlan 30

  service-policy input p1

    Class-map: class-default (match-any)
      0 packets,
      Match: any
```

```
    0 packets
  policy-map
    class class-default
      rate 128000 bps, burst 4000 bytes
      conformed 0 packets, 0 bytes; action:
        transmit
      exceeded 0 packets, 0 bytes; action:
        drop
      conformed 0 bps, exceeded 0 bps
Switch#
```

Related Commands	Command	Description
	vlan (VLAN Database mode)	Configures a specific VLAN.
	policy-map	Creates a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.

vlan database

To enter VLAN configuration mode, use the **vlan database** command.

vlan database

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Usage Guidelines From VLAN configuration mode, you can access the VLAN database editing buffer manipulation commands, including:

- **abort**—Exits mode without applying the changes.
- **apply**—Applies the current changes and bumps the revision number.
- **exit**—Applies the changes, bumps the revision number, and exits VLAN configuration mode.
- **no**—Negates a command or sets its defaults; valid values are **vlan** and **vtp**.
- **reset**—Abandons the current changes and rereads the current database.
- **show**—Displays the database information.
- **vlan**—Accesses the subcommands to add, delete, or modify values that are associated with a single VLAN. For information about the **vlan** subcommands, see the **vlan (VLAN Database mode)** command.
- **vtp**—Accesses the subcommands to perform VTP administrative functions. For information about the **vtp** subcommands, see the **vtp client** command.

Examples This example shows how to enter VLAN configuration mode:

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

This example shows how to exit VLAN configuration mode without applying changes after you are in VLAN configuration mode:

```
Switch(vlan)#abort
Aborting....
Switch#
```

This example shows how to delete a VLAN after you are in VLAN configuration mode:

```
Switch(vlan)#no vlan 100
Deleting VLAN 100...
Switch(vlan)#
```

This example shows how to turn off pruning after you are in VLAN configuration mode:

```
Switch(config)# no vtp pruning
Pruning switched OFF
Switch(config)#
```

Related Commands	Command	Description
	show vlan	Displays VLAN information.

vlan dot1q tag native

To enable tagging of the native VLAN frames on all 802.1Q trunk ports, use the **vlan dot1q tag native command**. To disable tagging of native VLAN frames, use the no form of this command.

vlan dot1q tag native

no vlan dot1q tag native

Syntax Description This command has no arguments or keywords.

Defaults 802.1Q native VLAN tagging is disabled.

Command Modes Global configuration mode

Usage Guidelines When enabled, the native VLAN packets exiting all 802.1Q trunk ports are tagged unless the port is explicitly configured to disable native VLAN tagging.

When disabled, the native VLAN packets exiting all 802.1Q trunk ports are not tagged.

You can use this command with 802.1Q tunneling. This feature operates on an edge switch of a service-provider network and expands VLAN space by using a VLAN-in-VLAN hierarchy and by tagging the tagged packets. You must use the 802.1Q trunk ports for sending out the packets to the service-provider network. However, the packets going through the core of the service-provider network might also be carried on the 802.1Q trunks. If the native VLANs of an 802.1Q trunk match the native VLAN of a tunneling port on the same switch, the traffic on the native VLAN is not tagged on the sending trunk port. This command ensures that the native VLAN packets on all 802.1Q trunk ports are tagged.

Examples This example shows how to enable 802.1Q tagging on the native VLAN frames and verify the configuration:

```
Switch(config)#vlan dot1q tag native
Switch(config)#end
Switch#show vlan dot1q tag native
dot1q native vlan tagging is enabled
```

Related Commands	Command	Description
	switchport private-vlan trunk native vlan tag	Configure the tagging of the native VLAN traffic on 802.1Q private VLAN trunks.
	switchport trunk	Sets the trunk characteristics when an interface is in trunking mode.

vlan filter

To apply a VLAN access map, use the **vlan filter** command. To clear the VLAN access maps from VLANs or interfaces, use the **no** form of this command.

vlan filter *map-name* {**vlan-list** *vlan-list*}

no vlan filter *map-name* {**vlan-list**} *vlan-list*}

Syntax Description	*map-name* VLAN access-map tag. **vlan-list** *vlan-list* Specifies the VLAN list; see the "Usage Guidelines" section for valid values.
Defaults	This command has no default settings.
Command Modes	Global configuration mode
Usage Guidelines	When configuring an action clause in a VLAN access map, note the following: • You can apply the VLAN access map to one or more VLANs. • The *vlan-list* parameter can be a single VLAN ID, a list of VLAN IDs, or VLAN ID ranges (*vlan-id-vlan-id*). Multiple entries are separated by (,), (hyphen), or (,) (comma). • You can apply only one VLAN access map to each VLAN. When entering the **no** form of this command, the *vlan-list* parameter is optional (but the keyword **vlan-list** is required). If you do not enter the *vlan-list* parameter, the VACL is removed from all the VLANs where the *map-name* is applied.

Examples	This example shows how to apply a VLAN access map on VLANs 7 through 9:
	`Switch(config)# vlan filter gamma vlan-list 7-9`
	`Switch(config)#`

vlan group

To create or modify a VLAN group, or the **vlan group** command in global configuration mode. Use the **no** form of this command to remove a VLAN list from the VLAN group.

vlan group *group-name* **vlan-list** *vlan-list*

no vlan group *group-name* **vlan-list** *vlan-list*

Syntax Description

group-name	Specifies the VLAN group name.
vlan-list	Specifies a VLAN list name. See the Usage Guidelines section below for additional information about this argument.

Defaults

This command has no arguments or keywords.

Command Modes

Global configuration

Usage Guidelines

The VLAN group-name can contain up to 32 characters and must begin with a letter.

The vlan-list argument can be a single VLAN ID, a list of VLAN IDs, or VLAN ID range (**vlan-id-vlan-id**). Multiple entries are separated by a hyphen (-) or a comma (,).

If the named VLAN group does not exist, the **vlan group** command creates the group and maps the specified VLAN list to the group. If the named VLAN group exists, the specified VLAN list is assigned to the group.

The **no** form of the **vlan group** command removes the specified VLAN list from the VLAN group. When you remove the last VLAN from the VLAN group, you delete the VLAN group.

You can configure a maximum of 100 VLAN groups, and map a maximum of 4094 VLANs to a VLAN group.

Examples

This example shows how to map VLANs 7 through 9 and 11 to a VLAN group:

```
Switch(config)# vlan group pagmode vlan-list 7-9,11
```

This example shows how to remove VLAN 7 from the VLAN group:

```
Switch(config)# no vlan group pagmode vlan-list 7
```

Related Commands

Command	Description
show vlan group	Displays the VLANs mapped to VLAN groups.

vlan internal allocation policy

To configure the internal VLAN allocation scheme, use the **vlan internal allocation policy** command. To return to the default setting, use the **no** form of this command.

vlan internal allocation policy {**ascending**|**descending**}

no vlan internal allocation policy

Syntax Description	**ascending** Specifies to allocate internal VLANs from 1006 to 4094. **descending** Specifies to allocate internal VLANs from 4094 to 1006.
Defaults	The default is the ascending allocation scheme.
Command Modes	Global configuration mode

Usage Guidelines

You can configure internal VLAN allocation to be from 1006 and up or from 4094 and down.

The internal VLANs and user-configured VLANs share the 1006 to 4094 VLAN spaces. A "first come, first served" policy is used in allocating these spaces.

The **vlan internal allocation policy** command allows you to configure the allocation direction of the internal VLANs.

During system bootup, the internal VLANs that are required for features in the startup-config file are allocated first. The user-configured VLANs in the startup-config file are configured next. If you configure VLAN 1006 in the startup-config file, and VLAN 4094 is the first VLAN configured in put into a nonoperational state until the internal VLANs is freed and becomes available.

After you enter the **write mem** command and the system reloads, the reconfigured allocation scheme is used by the port manager.

Examples

This example shows how to configure the VLANs in a descending order as the internal VLAN allocation policy:

```
Switch(config)# vlan internal allocation policy descending
Switch(config)#
```

Related Commands	**Command** **Description** **show vlan internal usage** Displays information about the internal VLAN allocation.

vmps reconfirm (global configuration)

To change the reconfirmation interval for the VLAN Query Protocol (VQP) client, use the **vmps reconfirm** command. To return to the default setting, use the **no** form of this command.

vmps reconfirm *interval*

no vmps reconfirm

Syntax Description *interval* Queries to the VLAN Membership Policy Server (VMPS) to reconfirm dynamic VLAN assignments; valid values are from 1 to 120 minutes.

Defaults The reconfirmation interval is 60 minutes.

Command Modes Global configuration mode

Examples This example shows how to set the VQP client to reconfirm dynamic VLAN entries every 20 minutes:

```
Switch(config)# vmps reconfirm 20
Switch(config)#
```

You can verify your setting by entering the **show vmps** command and examining information in the Reconfirm Interval *time*.

Related Commands

Command	Description
show vmps	Displays the VLAN Query Protocol (VQP) version, reconfirmation interval, retry count, VLAN Membership Policy Server (VMPS) IP addresses, current servers, and primary servers.
vmps reconfirm (privileged EXEC)	Sends VLAN Query Protocol (VQP) queries to reconfirm all the dynamic VLAN assignments with the VLAN Membership Policy Server (VMPS).

vmps reconfirm (privileged EXEC)

To immediately send VLAN Query Protocol (VQP) queries to reconfirm all the dynamic VLAN assignments with the VLAN Membership Policy Server (VMPS), use the **vmps reconfirm** command.

vmps reconfirm

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Usage Guidelines You can verify your setting by entering the **show vmps** command and examining the VMPS Action row of the Reconfirmation Status section. The **show vmps** command shows the result of the last time that the assignments were reconfirmed either because the reconfirmation timer expired or because the **vmps reconfirm** command was entered.

Examples This example shows how to immediately send VQP queries to the VMPS:

```
Dial_a_test#vmps reconfirm
Dial_a_test#
```

Related Commands

Command	Description
show vmps	Displays the VLAN Query Protocol (VQP) version, reconfirmation interval, retry count, VLAN Membership Policy Server (VMPS) IP addresses, current servers, and primary servers.
vmps reconfirm (global configuration)	Changes the reconfirmation interval for the VLAN Query Protocol (VQP) clients.

vmps retry

To configure the per-server retry count for the VLAN Query Protocol (VQP) client, use the **vmps retry** command. To return to the default setting, use the **no** form of this command.

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; valid values are from 1 to 10.

Defaults The retry count is 3.

Command Modes Global configuration mode

Usage Guidelines You can verify your setting by entering the **show vmps** command and examining information in the Server Retry Count row.

Examples This example shows how to set the retry count to 7:

```
Switch(config)# vmps retry 7
```

Related Commands	Command	Description
	show vmps	Displays the VLAN Query Protocol (VQP) version, reconfirmation interval, retry count, VLAN Membership Policy Server (VMPS) IP addresses, current servers, and primary servers.

vmps server

To configure the primary VLAN Membership Policy Server (VMPS) and up to three secondary servers, use the **vmps server** command. To remove a VMPS server, use the **no** form of this command.

vmps server *ipaddress* [**primary**]

no vmps server *ipaddress*

Syntax Description	*ipaddress* IP address or host name of the primary or secondary VMPS server. If you specify a hostname, 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 mode
Usage Guidelines	The first server that you entered is automatically selected as the primary server whether or not **primary** is entered. You can override the first server listing 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 that is 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 seven when dynamic-access ports are present, the switch cannot forward the packets from the new routers on these ports because it cannot query the VMPS. You can verify your setting by entering the **show vmps** command and examining information in the VMPS Domain Server row.

Examples	This example shows how to configure the server with IP address 191.10.49.24 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 191.10.49.24 primary`
	`Switch(config)# vmps server 191.10.49.21`
	`Switch(config)# vmps server 191.10.49.22`
	`Switch(config)#`
	This example shows how to delete the server with IP address 191.10.49.21:
	`Switch(config)# no vmps server 191.10.49.21`
	`Switch(config)#`

Related Commands	Command	Description
	show vlage	Displays the VLAN Query Protocol (VQP) version, reconfirmation interval, retry count, VLAN Membership Policy Server (VMPS) IP addresses, current servers, and primary servers.

vtp (global configuration mode)

To modify the name of a VTP configuration storage file, use the **vtp** command. To clear a filename, use the **no** form of this command.

vtp { {**file** *filename*} | {**if-id** *name*} }

no vtp { {**file** *filename*} | {**if-id** *name*} }

Syntax Description	**file** *filename* Specifies the IFS file where VTP configuration will be stored. **if-id** *name* Specifies the name of the interface providing the VTP updater ID for this device, where the **if-id** *name* is an ASCII string limited to 255 characters.
Defaults	Disabled
Command Modes	Global configuration mode

Usage Guidelines

You cannot use the **vtp file** command to load a new database. You can use it only to rename the file in which the existing database is stored.

You can use the **vtp if-id** command to specify the name of the interface providing the VTP updater ID for this device. The VTP updater is the device that adds, deletes, or modifies VLANs in a network, and triggers a VTP update to inform the rest of the system of the changes.

Examples

This example shows how to specify the IFS file-system file where VTP configuration is stored:

```
Switch(config)# vtp file vtpconfig
Setting device to store VLAN database at filename vtpconfig.
Switch(config)#
```

This example shows how to specify the name of the interface providing the VTP updater ID:

```
Switch(config)# vtp if-id FastEthernet
Switch(config)#
```

Related Commands	Command	Description
	show vtp	Displays VTP statistics and domain information.

vtp client

To place a device in VTP client mode, use the **vtp client** command. To return to VTP server mode, use the **no** form of this command.

vtp client

no vtp client

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes VLAN configuration mode

Usage Guidelines 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.

The **vtp server** command is the functional equivalent of **no vtp client** except that it does not return an error if the device is not in client mode.

Examples This example shows how to place the device in VTP client mode:

```
Switch(vlan-config) vtp client
Switch(vlan-config)
```

Related Commands

Command	Description
show vtp	Displays VTP statistics and domain information.
vtp (global configuration mode)	Configures the name of a VTP configuration storage file.

vtp domain

To configure the administrative domain name for a device, use the **vtp domain** command.

vtp domain *domain-name*

Syntax Description:	*domain-name* Name of the domain.
Defaults:	This command has no default settings.
Command Modes:	VLAN configuration mode

Usage Guidelines:

When you define the *domain-name*, the domain name is case-sensitive and can be from 1 to 32 characters. You must set a domain name before you can transmit any VTP advertisements.

Even if you do not set a domain name, the device will leave the no-management-domain state upon receiving the first VTP summary packet on any port that is currently trunking.

If the device receives its domain from a summary packet, it resets its configuration revision number to zero. Once the device leaves the no-management-domain state, it can never be configured to receive the number except by clearing NVRAM and reloading.

Examples:

This example shows how to set the device administrative domain:

```
Switch>(enable)set vtp domain domainbanks
Switch>(enable)show vtp domain
```

Related Commands:	Command	Description
	show vtp	Displays VTP statistics and domain information.
	vtp (global configuration mode)	Configures the name of a VTP configuration storage file.

vtp password

To create a VTP domain password, use the **vtp password** command. To delete the password, use the **no** form of this command.

vtp password *password-value*

no vtp password

Syntax Description

password-value	An ASCII string, from 1 to 32 characters, identifying the administrative domain for the device.

Defaults

Disabled

Command Modes

VLAN configuration mode

Examples

This example shows how to create a VTP domain password:

```
Switch(clan-config)# vtp password DomainSecret
Switch(clan-config)#
```

This example shows how to delete the VTP domain password:

```
Switch(clan-config)# no vtp password
This password deleted from domain password.
Switch(clan-config)#
```

Related Commands

Command	Description
show vtp	Displays VTP statistics and domain information.
vtp global (configuration mode)	Configures the name of a VTP configuration image file.

vtp pruning

To enable pruning in the VLAN database, use the **vtp pruning** command. To disable pruning in the VLAN database, use the **no** form of this command.

vtp pruning

no vtp pruning

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes VLAN configuration mode

Usage Guidelines VTP pruning causes information about each pruning-eligible VLAN to be removed from VTP updates if there are no stations belonging to that VLAN.

Examples This example shows how to enable pruning in the VLAN database:

```
Switch(config-vlan)# vtp pruning
Pruning switched ON
Switch(config-vlan)#
```

This example shows how to disable pruning in the VLAN database:

```
Switch(config-vlan)# no vtp pruning
Pruning switched OFF
Switch(config-vlan)#
```

Related Commands

Command	Description
show vtp	Displays VTP statistics and domain information.
vtp global configuration mode	Configures the name of a VTP configuration storage file.

vtp server

To place the device in VTP server mode, use the **vtp server** command.

```
vtp server
```

Syntax Description This command has no arguments or keywords.

Defaults Enabled

Command Modes VLAN configuration mode

Usage Guidelines 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.

You can set VTP to either server or client mode only when you disable dynamic VLAN creation.

If the receiving switch is in server mode, the configuration is not changed.

The **vtp server** command is the functional equivalent of **no vtp client**, except that it does not return an error if the device is not in client mode.

Examples This example shows how to place the device in VTP server mode:

```
Switch(vlan-config)# vtp server
Switch(vlan-config)#
```

Related Commands

Command	Description
show vtp	Displays VTP statistics and domain information.
vtp global configuration mode)	Configures the name of a VTP configuration storage file.

vtp transparent

To place a device in VTP transparent mode, use the **vtp transparent** command. To return to VTP server mode, use the **no** form of this command.

vtp transparent

no vtp transparent

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes VLAN configuration mode

Usage Guidelines The **vtp transparent** command disables VTP from the domain but does not remove the domain from the switch.

If the receiving switch is in transparent mode, the configuration is not changed. The 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 the other switches in the network.

The **vtp server** command is similar to the **no vtp transparent** command, except that it does not return an error if the device is not in transparent mode.

Examples This example shows how to place the device in VTP transparent mode:

```
Switch(config)#vtp transparent
Switch(config)#
```

This example shows how to return the device to VTP server mode:

```
Switch(config)#no vtp transparent
Switch(config)#
```

Related Commands

Command	Description
show vtp	Displays VTP statistics and domain information.
vtp lphdisk0 configuration mode0	Configures the name of a VTP configuration storage file.

vtp v2-mode

To enable version 2 mode, use the **vtp v2-mode** command. To disable version 2 mode, use the **no** form of this command.

vtp v2-mode

no vtp v2-mode

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes VLAN configuration mode

Usage Guidelines All switches in a VTP domain must run the same version of VTP. VTP version 1 and VTP version 2 do not operate on switches in the same VTP domain.

If all switches in a domain are VTP version 2-capable, you only need 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 toggle the version 2 mode, the parameters of certain default VLANs will be modified.

Examples This example shows how to enable version 2 mode in the VLAN database:

```
Switch(vlan-config)# vtp v2-mode
Switch(vlan-config)#
```

This example shows how to disable version 2 mode in the VLAN database:

```
Switch(vlan-config)# no vtp v2-mode
Switch(vlan-config)#
```

Related Commands

Command	Description
show vtp	Displays VTP statistics and domain information.
vtp (global configuration mode)	Configures the name of a VTP configuration storage file.

APPENDIX A

Abbreviations

A

ACE	access-control entry
ACL	access control list
AFI	authority and format identifier
Agport	aggregation port
AMP	Active Monitor Present
ARoRT	Automated Packet Recognition and Translation
ARP	Address Resolution Protocol

B

BEM	bent effect method
BGP	Border Gateway Protocol
BPDU	bridge protocol data unit
BRF	bridge relay function
BSC	Bisync
BSTUN	Block Serial Tunnel
BUS	broadcast and unknown server
BVI	bridge-group virtual interface

C

CAM	content-addressable memory
CAR	committed access rate
CCA	circuit card assembly
CDP	Cisco Discovery Protocol
CEF	Cisco Express Forwarding
CHAP	Challenge Handshake Authentication Protocol
CIR	committed information rate
CLI	command-line interface
CLNS	Connection-Less Network Service
CMNS	Connection-Mode Network Service
COPS	Common Open Policy Server
COPS-DS	Common Open Policy Server Differentiated Services
CoS	class of service
CPLD	Complex Programmable Logic Device
CRC	cyclic redundancy check
CRF	concentrator relay function
CST	Common Spanning Tree

D

DAI	Dynamic ARP Inspection
DBL	Dynamic Buffer Limiting
DCC	Data Country Code
dCEF	distributed Cisco Express Forwarding
DDR	dial-on-demand routing
DE	discard eligibility

DEC	Digital Equipment Corporation
DFI	Domain-Specific Part Format Identifier
DFP	Dynamic Feedback Protocol
DISL	Dynamic Inter-Switch Link
DLC	Data Link Control
DLSw	Data Link Switching
DMP	data movement processor
DNS	Domain Name System
DoD	Department of Defense
DOS	denial of service
DRAM	dynamic RAM
DRP	Dual Ring Protocol
DSAP	destination service access point
DSCP	differentiated services code point
DSPU	downstream SNA Physical Units
DTP	Dynamic Trunking Protocol
DTR	data terminal ready
DVMRP	Distance Vector Multicast Routing Protocol
DXI	data exchange interface

E

EAP	Extensible Authentication Protocol
EARL	Enhanced Address Recognition Logic
EEPROM	electrically erasable programmable read-only memory
EHSA	enhanced high system availability

EIA	Electronic Industries Association
ELAN	Emulated Local Area Network
EOBC	Ethernet out-of-band channel
ESI	end-system identifier

F

FECN	forward explicit congestion notification
FM	feature manager
FRU	field replaceable unit
FSM	feasible successor metrics

G

GARP	General Attribute Registration Protocol
GMRP	GARP Multicast Registration Protocol
GVRP	GARP VLAN Registration Protocol

I

ICC	Inter-card Communication
ICD	International Code Designator
ICMP	Internet Control Message Protocol
IDB	interface descriptor block
IDP	initial domain part or Internet Datagram Protocol
IDPROM	ID Programmable Read-Only Memory
IFS	IOS File System
IGMP	Internet Group Management Protocol
IGRP	Interior Gateway Routing Protocol

ILMI	Integrated Local Management Interface
IP	Internet Protocol
IPC	interprocessor communication
IPX	Internetwork Packet Exchange
IS-IS	Intermediate System-to-Intermediate System Intradomain Routing Protocol
ISL	Inter-Switch Link
ISO	International Organization of Standardization
ISR	Integrated SONET router
ISSU	In Service Software Upgrade

L

L2	Layer 2
L3	Layer 3
L4	Layer 4
LAN	local area network
LANE	LAN Emulation
LAPB	Link Access Procedure, Balanced
LDA	Local Director Acceleration
LCP	Link Control Protocol
LEC	LAN Emulation Client
LECS	LAN Emulation Configuration Server
LEM	link-error monitor
LER	link-error rate
LES	LAN Emulation Server
LLC	Logical Link Control
LTL	Local Target Logic

M

MAC	Media Access Control
MCL	Mismatched Command List
MDS	Message Digest 5
MET	Multicast Expansion Table
MFIB	Multicast Forwarding Information Base
MIB	Management Information Base
MII	media-independent interface
MLS	Multilayer Switching
MLSE	maintenance loop signaling entity
MOP	Maintenance Operation Protocol
MOTD	message-of-the-day
MRM	multicast routing monitor
MRQ	Multicast Replication Queue
MSDP	Multicast Source Discovery Protocol
MST	Multiple Spanning Tree
MTU	maximum transmission unit
MVAP	multiple VLAN access port

N

NBP	Name Binding Protocol
NCIA	Native Client Interface Architecture
NDE	NetFlow Data Export
NET	network entity title
NetBIOS	Network Basic Input/Output System
NFFC	NetFlow Feature Card

NMP	Network Management Processor
NSAP	network service access point
NTP	Network Time Protocol
NVRAM	nonvolatile RAM

O

OAM	Operation, Administration, and Maintenance
OSI	Open System Interconnection
OSPF	open shortest path first

P

PAE	port access entity
PAgP	Port Aggregation Protocol
PBD	packet buffer daughterboard
PC	Personal Computer (formerly PCMCIA)
PCM	pulse code modulation
PCR	peak cell rate
PDP	policy decision point
PDU	protocol data unit
PEM	Power Entry Module
PEP	policy enforcement point
PGM	Pragmatic General Multicast
PHY	physical sublayer
PIB	policy information base
PIM	Protocol Independent Multicast
PM	Port manager

PPP	Point-to-Point Protocol
PRC	Parser Return Code
PRID	Policy Rule Identifiers
PVLAN	Private VLAN
PVST+	Per VLAN Spanning Tree+

Q

QM	QoS manager
QoS	Quality of Service

R

RACL	Router Interface Access Control List
RADIUS	Remote Access Dial-In User Service
RAM	random-access memory
RCP	Remote Copy Protocol
RGMP	Router Group Management Protocol
RIF	Routing Information Field
RMON	Remote Network Monitor
ROM	read-only memory
RP	route processor or rendezvous point
RPC	remote procedure call
RPF	reverse path forwarding
RPR	Router Processor Redundancy
RSPAN	remote SPAN
RST	reset

RSVP	ReSerVation Protocol
Rx	Receive

S

SAID	Security Association Identifier
SAP	service access point
SCM	service connection manager
SCP	Switch-Module Configuration Protocol
SDLC	Synchronous Data Link Control
SGBP	Stack Group Bidding Protocol
SIMM	single-in-line memory module
SLB	server load balancing
SLCP	Supervisor Line-Card Processor
SLIP	Serial Line Internet Protocol
SMDS	Software Management and Delivery Systems
SMF	software MAC filter
SMP	Standby Monitor Present
SMRP	Simple Multicast Routing Protocol
SMT	Station Management
SNAP	Subnetwork Access Protocol
SNMP	Simple Network Management Protocol
SPAN	Switched Port Analyzer
SRB	source-route bridging
SRT	source-route transparent bridging
SSTP	Cisco Shared Spanning Tree
STP	Spanning Tree Protocol

SVC	switched virtual circuit
SVI	switched virtual interface

T

TACACS+	Terminal Access Controller Access Control System Plus
TARP	Target Identifier Address Resolution Protocol
TCAM	Ternary Content Addressable Memory
TCL	table-connection level
TCP/IP	Transmission Control Protocol/Internet Protocol
TFTP	Trivial File Transfer Protocol
TIA	Telecommunications Industry Association
TLV	type-length-value
Top N	Utility that allows the user to analyze port traffic by reports
TOS	type of service
TrBRF	Token Ring Bridge Relay Function
TrCRF	Token Ring Concentrator Relay Function
TTL	Time To Live
TVR	valid transmission
Tx	Transmit

U

UDLD	UniDirectional Link Detection Protocol
UDP	User Datagram Protocol
UNI	User-Network Interface
UTC	Coordinated Universal Time

V

VACL	VLAN access control list
VCC	virtual channel circuit
VCD	virtual circuit descriptor
VCI	virtual circuit identifier
VCR	Virtual Configuration Register
VINES	Virtual Network System
VLAN	virtual LAN
VMPS	VLAN Membership Policy Server
VTP	VLAN Trunking Protocol
VVID	voice VLAN ID

W

WFQ	weighted fair queueing
WRED	weighted random early detection
WRR	weighted round-robin

X

XNS	Xerox Network System

INDEX

Symbols

Numerics

A

E

F

G

H

I

displaying SEEPROM information
chassis **2-847**
clock module **2-847**
fan trays **2-847**
module **2-847**
mux buffer **2-847**
power supplies **2-847**
supervisor engine **2-847**
iFindex persistence
clearing SNMP iFindex commands **2-763**
compress SNMP iFindex table format **2-798**
disabling globally **2-767**
disabling on an interface **2-768**
enabling globally **2-767**
enabling on an interface **2-768**
IGMP
displaying filters for host joining on Layer 2 interfaces **2-896**
clearing IGMP group cache entries **2-325**
configuring frequency for IGMP host-query messages **2-898**
creating an IGMP profile **2-897**
displaying IGMP interface configuration information **2-895**
displaying profiles **2-899**
setting maximum group numbers **2-896**
IGMP profiles
displaying **2-899**
IGMP snooping
clearing the EHT database **2-325**
configuring a Layer 2 interface as a group member **2-900**
configuring a Layer 2 interface as a multicast router **2-917**
configuring a static VLAN interface **2-900**
displaying multicast information **2-824**
displaying VLAN information **2-825, 2-826, 2-827**
enabling **2-915**
enabling immediate-leave processing **2-916**
enabling on a VLAN **2-916**
enabling pre-VLAN Explicit Host Tracking **2-918**
inferior
enabling **2-796**
inline power
displaying inline power status **2-722**
In Service Software Upgrade
See ISSU
inspection log
clearing log buffer **2-64**
interface
displaying suppressed multicast bytes **2-803**
interface capabilities
displaying **2-676**
interface configuration mode
summary **1-5**
interface link
display cable disconnect time **2-683**
interfaces
configuring dectiy tunnel port **2-465**
creating an interface range macro **2-146**
debugging output of interface related activities **2-128**
displaying description **2-802**
displaying error-disabled state **2-686**
displaying information when tunneling is enabled **2-802**
displaying status **2-802**
displaying traffic for a specific interface **2-811**
entering interface configuration mode **2-235**
executing a command on multiple ports in a range **2-222**
selecting an interface to configure **2-235**
setting a CoS value for Layer 2 packets **2-612**
setting drop threshold for Layer 2 packets **2-616**
setting the interface type **2-880**
interface speed
configuring interface speed **2-822**
interface transceiver
displaying diagnostic data **2-689**
internal VLAN allocation

displaying sessions information **2-661**
displaying software version **2-662**
displaying state **2-662**
forcing switchover to standby supervisor engine **2-232**
loading new image **2-235**
saving process **2-232**
stopping rollback timer **2-234**

J

Jumbo frames
enabling jumbo frames **2-288**

L

LACP
disabling channeling protocol **2-81**
enabling LACP on an interface **2-81**
setting channeling protocol **2-81**
lacp port-priority command **2-257**
lacp system-priority command **2-259**
Layer 2
displaying ACL configuration **2-671**
Layer 2 interface type
specifying a nontrunking, nontagged single VLAN interface **2-800**
specifying a trunking VLAN interface **2-800**
Layer 2 protocol-packets
displaying **2-664**
Layer 2 protocol-tunneling error recovery **2-225**
Layer 2 switching
enabling voice VLANs **2-800**
modifying switching characteristics **2-800**
Layer 2 traceroute
IP addresses **2-687**
Layer 3 interface, assign evasmen **2-221**
Layer 3 switching
displaying information about an adjacency table **2-524**
displaying port status **2-288**
displaying status of native VLAN tagging **2-288**
link-status event messages
disabling
globally **2-223-225**
on an interface **2-223,2-224**
enabling
globally **2-223,2-225**
on an interface **2-223,2-224**
LLDP
enabling power negotiation **2-229**
lldp tlv-select power-management command **2-230**
log buffer
show states **2-660**
logging
controlling IP ARP packets **2-237**

M

MAB, display information **2-669**
MAB, enable and configure **2-326**
mab command **2-326**
MAC Access Control Lists
See MAC ACLs
MAC ACLs
defining extended MAC access list **2-327**
displaying MAC ACL information **2-773**
naming an ACL **2-327**
MAC addresses
disabling MAC address learning per VLAN **2-334**
displaying
notification settings **2-391,2-641, 2-660**
MAC address filtering
configuring **2-339**
disabling **2-339**
enabling **2-339**
MAC address learning on a VLAN, enabling **2-334**

Q

R

synchronizing the route processor configuration **2-100**
related documentation **1-xlii**
remote-id, setting for an interface **2-624**
remote-id, setting for an interface VLAN range **2-625**
remote SPAN
See RSPAN
renew commands
ip dhcp snooping database **2-471**
rep admin-vlan command **2-475**
rep block port command **2-476**
rep lsl-age-timer command **2-479**
rep preempt delay command **2-481**
rep preempt segment command **2-482**
rep segment command **2-482**
rep stcn command **2-488**
restoring PVLAN trunk
setting switchport to trunk **2-846**
retry failed authentication, configuring **2-22**
rgf1 connector, selecting the connector **2-576**
ROM monitor mode
summary **3-6**
Route Processor Redundancy
See redundancy
router, set to locator ANCP client **2-56**
RPF
disabling IPv4 exists-only checks **2-285**
enabling IPv4 exists-only checks **2-285**
RPR
set the redundancy mode **2-577**
RSPAN
converting VLAN to RSPAN VLAN **2-873**
displaying list **2-788**

S

saving configuration changes **1-21**
secure address, configuring **2-624**
secure ports, limitations **2-861**
server (AAA) alive actions, configuring **2-23**
server (AAA) dead actions, configuring **2-23**
service-policy command (policy-map class) **2-481**
session classification, defining **2-26**
set the redundancy mode **2-577**
sfp connector, selecting the connector **2-576**
shape command **2-585**
shell trigger command **2-582, 2-705**
show acep multicast **2-586**
show authentication interface command **2-622**
show authentication registration command **2-628**
show authentication sessions command **2-624**
show capture command **2-702**
show commands
filtering parameters **1-7**
searching and listing **1-6**
show platform commands **1-11**
show ipv6 snooping counters command **2-685**
show ip wccp command **2-622**
show ip wccp detail command **2-622**
show ip wccp view command **2-622**
show mab command **2-660**
show mac address-table learning command **2-295, 2-680**
show macro auto monitor device command **2-681, 2-683, 2-687**
show monitor capture command **2-702, 2-709**
show monitor capture file command **2-702**
show netop command **2-712**
show slot group command **2-792**
show vlan mapping command **2-794**
Simple Network Management Protocol
See SNMP
single-character patterns
special characters **1-7**
single-host, setting **2-26**
slaveslot0
displaying information on the standby supervisor **2-788**
slot0

U

V

W

Webauth fallback, enabling **2-15**