Catalyst 4500 Series Switch Cisco IOS Command Reference

Release 12.2(52)SG

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-16702-02

CHAPTER

Catalyst 4500 Series IOS Commands

New Commands

diagnostic fpga soft-error recover

ip multicast multipath

Revised Commands

A Commands

C Commands

D Commands

E Commands

F Commands

H Commands

I Commands

ip igmp max-groups
ip igmp profile
ip igmp query-interval
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 mdfs fastdrop
ip multicast multicast
ip route-cache flow
ip source binding
ip sticky-arp
ip verify header vlan all
ip verify source
ip verify unicast source reachable-via
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 mrouterless variable
ipv6 mld snooping tcn
ipv6 mld snooping vlan
issu abortversion
issu acceptversion
issu commitversion
redundancy config-sync mismatched-commands
issu loadversion
issu runversion
issu set rollback-timer

L. Commands

l2protocol-tunnel
l2protocol-tunnel cos

M Commands

N Commands

P Commands

Q Commands

R Commands

S Commands

spanning-tree ethertherself guard mincostlg
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 bpdugard default
spanning-tree portfast default
spanning-tree port-priority
spanning-tree uplinkfast
spanning-tree vlan
speed
storm-control
storm-control broadcast include multicast
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
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
system mtu

Show Commands

show access-group mode interface
show adjacency
show aeq mac4ccnt
show aq access-list
show authentication
show auto install status
show auto qos
show bootflash:
show bootvar
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 evaluate detect
show evaluate recovery
show erlert hunnel
show flowcontrol
show hw-module port-group
show hw-module uplink
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 inspectioning
show ip cef 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 ipc
show ipv6 mld snooping
show ipv6 mld snooping mrouter
show ipv6 mld snooping querier
show issu capability
show issu clients
show issu comp-matrix
show issu endpoints
show issu sessions
show issu fim
show issu message
show issu negotiated

T Commands

U Commands

V Commands

CONTENTS

CONTENTS A

INDEX I

Preface

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

Audience

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

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/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html.

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:

Convention	Description
boldface font	Boldface text indicates commands and keywords that you enter literally as shown.
italic font	*Italic* text indicates arguments for which you supply values.
[x]	Square brackets enclose an optional element (keyword or argument).
|	A vertical line indicates a choice within an optional or required set of keywords or arguments.
[x | y]	Square brackets enclosing keywords or arguments separated by a vertical line indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a vertical line indicate a required choice.
x {x | x}	Braces and a vertical line within square brackets indicate a required choice within an optional element.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
screen font	Terminal sessions and information the system displays are in screen font.
boldface screen font	Information you must enter is in **boldface screen** font.
italic screen font	Arguments for which you supply values are in *italic screen* font.
^ or Ctrl	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means Hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords, are in angle brackets.

Convention	Description
[ ]	Indicates an optional or optional parameter in square brackets.
! , #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

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 notice 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. 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.

2. All advertising materials mentioning features or use of this software must display the following acknowledgment: "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 acknowledgment: "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 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 Binary License

Copyright © 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 Netscape 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 the RC4, RSA, Bnlib, 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 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.

8. 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 cryptography-related.

9. 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/en/US/docstore/general/whatnew/whatnew.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* help 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 ?` `Enable|disable|network|rasnetwork|dial-in|dial-out`	Enter the **arap ?** command and get access 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)#? Switch(config-if)#? Switch(config-vlan)#? Switch(config-line)#? Switch(config-ipx-router)#? Switch(config-router)#? Switch(config-if)#channel-group ? Switch(config-if)#channel-group	Enter a Pro display a list of all the interface configuration commands available for the Gigabit Ethernet interface. Enter the command that you want to configure for the controller. In this example, the **channel-group** command is used. Enter a Pro display what you must enter next on the command line. In this example, you must enter the **group** keyword. Because `<cr>` is not displayed, it indicates that you must enter more information to complete the command.
access-expression Build a bridge boolean access expression apollo Apollo router commands arp Set arp entry interface arp-server Set arp type (arpa, probe, snap) or timeout backup Modify backup parameters bandwidth Set bandwidth informational parameter bridge-group Transparent bridging interface parameters bridge-group Transparent bridging interface parameters carrier-delay Specify delay for interface transitions cdp CDP interface subcommands channel-group EtherChannel/port bundling configuration cline CLNS interface subcommands clock Clock command custom-queue-list Assign a custom queue list to an interface darnet Interface DARnet config commands default Set a command to its defaults delay Specify interface throughput delay description Interface specific description dhcp DHCp Interface Pro dmps Dmps Stream PC dot1q IEEE 802.1Q encapsulation dot1qnative Enable Pro tunneling on an Interface dtscontrol Configure Cisco operation. dtsdata Enable Cisco operation. help Description of the interactive help system hold-queue Set hold queue depth ip Interface Internet protocol config commands ipx Novell IPX interface subcommands lata LD-LS commands lmi-type IEC-LMI interface subcommands . . .	

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

Command	Purpose
Switch(config)#**channel-group ?** channel-group Channel group number Switch(config)#channel-group	After you enter the **group** keyword, enter a *?* to display what you must enter 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.
Switch(config)#**channel-group 1 ?** mode Ethernet/Fast Mode of the interface Switch(config)#**1d** Switch(config)#**channel-group 1 mode ?** auto Enable PAgP only if a PAgP device is detected desirable Enable PAgP unconditionally on Enable Etherchannel only Switch(config)#**1d**	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. 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.
Switch(config)#**1d channel-group 1 mode auto ?** `<cr>` Switch(config)#**1d**	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 Return to complete the command. If additional keywords are listed, you can enter more keywords or press Return to complete the command.
Switch(config)#**channel-group 1 mode auto** Switch(config)#**1d**	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. You can obtain a list of commands available for each command mode by entering 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 1-3 Summary of Main Command Modes (continued)

Access Method	Prompt	Exit Method
Subinterface configuration	Router(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	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) and then enters privileged EXEC mode. To boot 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 enable 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 resets the command settings to default settings. Most commands are disabled by default, so the **default** form is the same as the **no** form. However, many **default** commands are enabled by default, so the **default** form is the same as the **default** form. Enter the **default** form of the command enables the command and restores 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 need 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[0-4], ..(ip|ipx).

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>** prompts.

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 hinting, 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 ({), right brace (}), 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

[abcdefhkl]

matches any one of the first four letters of the lowercase alphabet, or **l**.

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

[a-ek-l]

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

[a-ek-l\-]

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

[a-ek-l\-]]

The precise example matches any one of the first four letters of the lowercase 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 cannot create a regular expression by joining letters, digits, or keyboard characters that do not have special meaning. For example, **a**f**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 pattern, order is important. The regular expression **a**f**b** matches the character **a** followed by **a**, followed by **f**, followed by **b**. Matching does not have offs, 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 **a#** will match 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:

wildcat 1107 v123ts

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 1-5 lists the special characters that specify "multipliers" of a regular expression.

Table 1-5 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 ladbaqcone:

a*

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

a+

This pattern matches the string lib or bab:

ba?b

This string matches any number of asterisks (*):

i

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-Za-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 AB0a1, but not SA1d 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 telecodes, but not both codes and telecodes.

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(.)d\1e\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 d again. So, the regular expression can match abCzDzE. The software remembers that character 1 is Z and character 2 is E and then uses Z and E 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#, copy system:running-config nvram:startup-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 copy saves the configuration to NVRAM. On the Class A Flash file system platforms, this copy 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, set the **#macro keywords** command.

#macro keywords [*keyword1*] [*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

Command History

Release	Modification
12.2(50)SEW	Support for this command was introduced on the Catalyst 4500 series switch.

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 syntax valid.

Examples

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

```
Switch(config)# macro name test
Enter macro, '@' to end.
Macro macro commands one per line. End with the character '@'.
#macro keywords DTAGS DMAC
macro(config)
@
Switch(config)# lan g12.15
Switch(config-if)# macro apply test ?
  DTAGS  Keyword to replace with a value e.g DTAGS, DMAC   <-- It is always on 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

Command History	Release	Modification
	12.2(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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-LOGOFF, 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

Command History	Release	Modification
	12.2(18)SXF	Support for this command was introduced on the Catalyst 6500 series switch.

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 (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 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 overrides 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

Command History

Release	Modification
12.2(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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 shows how to make the PACL mode on the switch take effect:

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

This example shows 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

Command History	Release	Modification
	12.2(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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 unless all the pre-class CAM entries are programmed in hardware.

You must ensure that any access control configuration a member port or VLAN does not deny or drop the control packets from being forwarded 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)# end
Switch#
```

access-list hardware entries

To designate how ACLs are programmed into the switch 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 ACEs 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 ACEs in an ACL.

Defaults

The ACLs are programmed as packed.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(2)EW	Support for this command was introduced on the Catalyst 6500 series switch.

Usage Guidelines

Two types of hardware resources are used when ACLs are programmed: entries and masks. If one of the 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 compute 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 80 percent of the masks to program only 49 percent of the ACL entries.

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# access-list hardware entries packed
Switch(config)# end
Switch#
%SYS-5-CONFIG_I: Configured from console by console
Switch#
Switch# show platform hardware acl statistics utilization brief
Berkeley(Total)/Mask(Total)

        Input  Acl(Used+Free)  256 / 4096 (6%)  440 / 512 ( 8%)
        Input  Ace(Used+Free)    6 / 4096 ( 0%)    4 / 512 ( 0%)
        Input  Lou(Used+Free)    0 / 4096 ( 0%)    0 / 512 ( 0%)
```

```
          Input  (pps/BroadcastCast)     0 / 4294 ( 0)     0 / 512 ( 0)
          Output (pps/BroadcastCast)     0 / 4294 ( 0)     0 / 512 ( 0)
          Output (pps/DroppedBlast)      0 / 4294 ( 0)     0 / 512 ( 0)
          Output (pps/DroppedCast)       0 / 4294 ( 0)     0 / 512 ( 0)
          Output (pps/BroadcastCast)     0 / 4294 ( 0)     0 / 512 ( 0)

          L2Spc: used 2 out of 64

Switch#
```

This example shows how to reserve space (ternary hardware ACL entries in the hardware. The number of masks required to program 48 percent of the entries has decreased to 25 percent.

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#access-list hardware entries scattered
Switch(config)#end
Switch#
01:39:07: %SYS-5-CONFIG_I: Configured from console by console
Switch#show platform hardware acl statistics utilization brief
Detailed(%): Masks/Total(%)
                                   Used/Free/Max/Min
          Input  Acl(BroadcastCast)  2014 / 494 / 252 / 112 ( 80)
          Input  Acl(BroadcastCast)     0 / 4294 ( 0)     0 / 512 ( 0)
          Output (pps/BroadcastCast)    0 / 4294 ( 0)     0 / 512 ( 0)
          Output (pps/DroppedBlast)     0 / 4294 ( 0)     0 / 512 ( 0)
          Output (pps/DroppedCast)      0 / 4294 ( 0)     0 / 512 ( 0)
          Output (pps/BroadcastCast)    0 / 4294 ( 0)     0 / 512 ( 0)
          Output (pps/DroppedBlast)     0 / 4294 ( 0)     0 / 512 ( 0)
          Output (pps/DroppedCast)      0 / 4294 ( 0)     0 / 512 ( 0)

          L2Spc: used 2 out of 64

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** {*bal-num*}

Syntax Description	**feature** Specifies adjustment of region balance for ACLs.
	qos Specifies adjustment of region balance for QoSs.
	input Specifies adjustment of region balance for input ACL and QoSs.
	output Specifies adjustment of region balance for output ACL and QoSs.
	balance *bal-num* Specifies relative sizes of the PandV and PorV 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

Command History	**Release**	**Modification**
	12.2(25.SG)	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

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

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

A balance of 1 allocates the minimum number of PandV region entries and the maximum number of PorV region entries. A balance of 99 allocates the maximum number of PandV region entries and the minimum number of PorV region entries. A balance of 50 allocates equal numbers of PandV and PorV 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 to a port:

```
Switch(config)#snmp-server enable traps mac-notification change
Switch(config)#snmp-server host 172.20.135.110 public mac-notification
Switch(config)#mac address-table notification change interval 30
Switch(config)#mac address-table notification change history-size 100
Switch(config)#interface fastethernet 5/2
Switch(config-if)#snmp trap mac-notification change added
Switch(config-if)#exit
Switch(config)#exit
Switch#show snmp mib
ifMIB.1.3.6.1.2.1.31.1.1.1.18.0
ifMIB.1.3.6.1.2.1.31.1.1.1.18.1
ifMIB.1.3.6.1.2.1.31.1.1.1.18.2
ifMIB.1.3.6.1.2.1.31.1.1.1.18.3
ifMIB.1.3.6.1.2.1.31.1.1.1.18.4
ifMIB.1.3.6.1.2.1.31.1.1.1.18.5
ifMIB.1.3.6.1.2.1.31.1.1.1.18.6
ifMIB.1.3.6.1.2.1.31.1.1.1.18.7
ifMIB.1.3.6.1.2.1.31.1.1.1.18.8
ifMIB.1.3.6.1.2.1.31.1.1.1.18.9
ifMIB.1.3.6.1.2.1.31.1.1.1.18.10
ifMIB.1.3.6.1.2.1.31.1.1.1.18.11
ifMIB.1.3.6.1.2.1.31.1.1.1.18.12
ifMIB.1.3.6.1.2.1.31.1.1.1.18.13
ifMIB.1.3.6.1.2.1.31.1.1.1.18.14
ifMIB.1.3.6.1.2.1.31.1.1.1.18.15
ifMIB.1.3.6.1.2.1.31.1.1.1.18.16
ifMIB.1.3.6.1.2.1.31.1.1.1.18.17
ifMIB.1.3.6.1.2.1.31.1.1.1.18.18
ifMIB.1.3.6.1.2.1.31.1.1.1.18.19
ifMIB.1.3.6.1.2.1.31.1.1.1.18.20
ifMIB.1.3.6.1.2.1.31.1.1.1.18.21
ifMIB.1.3.6.1.2.1.31.1.1.1.18.22
ifMIB.1.3.6.1.2.1.31.1.1.1.18.23
ifMIB.1.3.6.1.2.1.31.1.1.1.18.24
ifMIB.1.3.6.1.2.1.31.1.1.1.18.25
ifMIB.1.3.6.1.2.1.31.1.1.1.18.26
ifMIB.1.3.6.1.2.1.31.1.1.1.18.27
ifMIB.1.3.6.1.2.1.31.1.1.1.18.28
ifMIB.1.3.6.1.2.1.31.1.1.1.18.29
ifMIB.1.3.6.1.2.1.31.1.1.1.18.30
ifMIB.1.3.6.1.2.1.31.1.1.1.18.31
ifMIB.1.3.6.1.2.1.31.1.1.1.18.32
ifMIB.1.3.6.1.2.1.31.1.1.1.18.33
ifMIB.1.3.6.1.2.1.31.1.1.1.18.34
ifMIB.1.3.6.1.2.1.31.1.1.1.18.35
ifMIB.1.3.6.1.2.1.31.1.1.1.18.36
ifMIB.1.3.6.1.2.1.31.1.1.1.18.37
ifMIB.1.3.6.1.2.1.31.1.1.1.18.38
ifMIB.1.3.6.1.2.1.31.1.1.1.18.39
ifMIB.1.3.6.1.2.1.31.1.1.1.18.40
ifMIB.1.3.6.1.2.1.31.1.1.1.18.41
ifMIB.1.3.6.1.2.1.31.1.1.1.18.42
ifMIB.1.3.6.1.2.1.31.1.1.1.18.43
ifMIB.1.3.6.1.2.1.31.1.1.1.18.44
ifMIB.1.3.6.1.2.1.31.1.1.1.18.45
ifMIB.1.3.6.1.2.1.31.1.1.1.18.46
ifMIB.1.3.6.1.2.1.31.1.1.1.18.47
ifMIB.1.3.6.1.2.1.31.1.1.1.18.48
ifMIB.1.3.6.1.2.1.31.1.1.1.18.49
```

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

Command History	Release	Modification
	12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

In a VLAN access map, if at least one ACL is configured for a packet type (IP or MAC), the default action for the packet type is **drop** (deny).

If an ACL is not configured for a packet type, the default action for the packet type is **forward** (permit).

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 shows how to define a drop action:

```
Switch(config)#vlan access-map ip action drop
Switch(config)#vlan access-map ip #
```

This example shows how to define a forward action:

```
Switch(config)#vlan access-map ip action forward
Switch(config)#vlan access-map ip #
```

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

Command History	Release	Modification
	12.2(52)SG	Support was introduced on the Catalyst 4500 series switches.

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 xiaoo
Switch(cfg-call-home-profile)# active
```

Related Commands

Command	Description
destination address	Configure the destination e-mail address or URL to which Call Home messages will be sent.
destination message-size-limit bytes	Configure a maximum destination message size for the destination profile.
destination preferred-msg-format	Configure 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.

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.

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	*identifier name* — Identifier that is 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

Command History	**Release**	**Modification**
	12.2(50)SG	Support for this command was introduced on the Catalyst 4500 series switch.

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 (no [vlan] 0x0100000d) hex[port]. For example, VLAN 10 and interface Fast Ethernet 2/1 will pass the field 0x0100000d1302f01. 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 *loc* 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 NAmetestag:

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

Related Commands	**Command**	**Description**
	ancp mode client	Sets the router to become 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 | server* **interface** *interface*

Syntax Description	*ipaddr	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

Command History	**Release**	**Modification**
	12.2(25)SG	Support for this command was introduced on the Catalyst 4500 series switch.

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 3/1
```

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 No keywords

Defaults This command has no default settings.

Command Modes Global configuration mode

Command History	Release	Modification
	12.2(50)SG	Support for this command was introduced on the Catalyst 4500 series switch.

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 shows how to set the router to become an ANCP client:

```
Switch# ancp mode client
```

Related Commands	Command	Description
	ancp client server	Displays multicast streams 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

Command History	Release	Modification
	12.1(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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

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.

Command	Description
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

Command History	**Release**	**Modification**
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples

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

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

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 applies 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

Command History	Release	Modification
	12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

This command applies only to the Access Gateway Module on Catalyst 4500 series switches.

The valid values for *mod* depend on the chassis that are used. For example, if you have a Catalyst 4506 chassis, valid values for the module are fm in 2 to 6. If you have a 4507R chassis, valid values are from 2 to 7.

When you execute the **attach module** *mod* command, the prompt changes to Gateway#.

This command is identical in the resulting action to 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:

```
Router#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 standby 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

Command History	Release	Modification
	12.2(25)SG	Support for this command was introduced.

Usage Guidelines The **authentication control-direction** command replaces the following dot1x command, which is deprecated in Cisco IOS Release 12.2(25)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 authenticates each user device that connects to a switch port. Depending on the EAP-based authentication that is exchanged between the client and the switch or the LAN, Extended 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 controlled port is enabled, the connected host is no longer node or power-down state. The host does not exchange traffic with other devices in the network. If the host connected to the unidirectional port that cannot send traffic to the network, the host cannot 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 only 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 parameters, 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

Command History	**Release**	**Modification**
	12.2(50)SG	Support for this command was introduced.

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 2000
Switch(config)#
```

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

authentication event

To configure the actions for authentication events, 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*]]

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.
action authorize vlan *vlan*	When authentication fails due to wrong user credentials, authorizes the port in particular VLAN.
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.
dead action authorize	Configures the (AAA) server dead action to authorize the port for authentication events.
vlan *vlan* **no-response action authorize**	(Optional) When the client does not support 802.1x, authorizes the port in a particular VLAN.

Command Default

The default settings are as follows:

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

Command Modes

Interface configuration mode

Command History

Release	Modification
12.2(50)SG	Support for this command was introduced.

Usage Guidelines

The **authentication event fail** command replaces the following dot1x 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 dot1x to signal authentication failures. By default, this type of failure triggers the authentication method to be retried. You can configure to either authorize the port in the configured VLAN or 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 dot1x 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 dhcp 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 dot1x 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)#interface gigabitethernet 1/1
Switch(config-if)#authentication event fail action next-method
Switch(config-if)#
```

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

```
Switch(config)#interface gigabitethernet 1/1
Switch(config-if)#authentication event server alive action reinitialize
Switch(config-if)#
```

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

```
Switch(config)#interface gigabitethernet 1/1
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)#interface gigabitethernet 1/1
Switch(config-if)#authentication event no-response action authorize
vlan 10
Switch(config-if)#
```

Related Commands

Command	Description
show authorization	Displays Authentication Manager information.

authentication fallback

To enable Web Auth fallback and to specify the fallback profile to use when failing over to Web Auth, 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*	The fallback profile name to use when failing over to Web Auth (maximum of 200 characters).

Command Default Disabled

Command Modes Interface configuration mode

Command History	**Release**	**Modification**
	12.2(20)EW	Support for this command was introduced.

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(18)SE and later releases:

[no] dot1x fallback *profile*

The WebAuth fallback feature allows you to have those 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 fallbackprofile1
Switch(config-if)#
```

This example shows how to disable WebAuth fallback:

```
Switch(config-if)# no authentication fallback fallbackprofile1
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

Command History	**Release**	**Modification**
	12.2(33)SXI	Support for this command was introduced.

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 downloaded for the client 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 will be authenticated and the rest will inherit the same access as the first client. 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 environment refers to the VLAN. The VLAN membership of a port is assigned to the RADIUS authentication server after a client is allowed on a particular domain. So, only one client MAC per port per VLAN is supported. Each one is required to authenticate separately. Any policies that are downloaded for the client will be applied to that client's MAC/IP only and will not affect the other on the same port. This client can be authenticated using different methods (such as 802.1X for PC, MAB for IPphone, or vice versa). No restriction exists on the authentication order.

The only consent with the above statement is that web-based authentication is only available for data devices because a user is probably operating the device and HTTP capability exists. Also, if web-based authentication is configured in MDA mode, the only form of enrollment for all types of devices is web-based authentication. The only exception to this is that voice devices can be enrolled without a web-based authentication. Furthermore, if you use dACLs for data devices and not for voice devices, when the user's data falls back to network, voice traffic is affected by the ACL that is applied based on the fallback policy. Therefore if network is configured as a fallback on an MDA enabled port, dACL is the only supported enforcement method.

Multi-authmode classifies the session as a MAC-based. No limit exists for the number of clients allowed on a port data domain. Only one client is allowed in a voice domain and each one is required to authenticate separately. Any policies that are downloaded for the client are applied for that client's MAC or IP only and do not affect others 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 use case, where a device needs to access the network before PXE times out and downloads a bootable image possibly containing a supplicant.

The configuration of 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. Multi-authentication host-mode allows the port to be in open access mode. 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 user and is only restricted 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 VLAN. You can verify your settings with the **show authentication** 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)#
Switch(config)# authentication host-mode single-host
Switch(config)#
```

Related Commands	Command	Description
	show authentication	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.

Note With Cisco IOS Release 12.2(50)SG, the **authentication open** command operates on a per-port rather than global basis.

```
authentication open
no authentication open
```

Syntax Description This command has no arguments or keywords.

Command Default Disabled.

Command Modes Interface configuration mode

Command History	Release	Modification
	12.2(50)SG	Support for this command was introduced.

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.

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

```
Switch(config)# int gi1/0/1
Switch(config-if)# authentication open
Switch(config-if)#
```

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

```
Switch(config)# int gi1/0/1
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 retrieve 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 methods 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

Command History	**Release**	**Modification**
	12.2(25)FZ(s)	Support for this command was introduced.

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 new 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. If authentication fails, then, subject to the **ssm** authentication method *occurs (subject to the configuration* of authentication failure handler).

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

Command History

Release	Modification
12.2(20)EW	Support for this command was introduced.

Usage Guidelines The **authentication periodic** command replaces the following dot1x command, which is deprecated in Cisco IOS Release 12.2(20)EW and later releases:

[no] dot1x reauthentication

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

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

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

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 802.1x 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

Command History	**Release**	**Modification**
	12.2(33)SXI	Support for this command was introduced.

Usage Guidelines The **authentication port-control** command replaces the following dot1x command, which is deprecated in Cisco IOS Release 12.2(33)SXI and later releases:

[no] dot1x port-control [auto | force-authorized | force-unauthorized]

The following guidelines apply to Ethernet switch network modules:

- The 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 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.
  - 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 or on an active port in an EtherChannel, an error message appears, and 802.1X is not enabled. If you enable 802.1X on a not yet active 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 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 authentication** 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 status 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

Command History

Release	Modification
12.2(33)SXI	Support for this command was introduced.

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 allowed 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

Command History	**Release**	**Modification**
	12.2(33)SXI	Support for this command was introduced.

Usage Guidelines — Reauthentication only occurs if it is enabled on the interface.

The **authentication timer reauthenticate** value command replaces the following dot1x commands that is deprecated in Cisco IOS Release 12.2(33)SX1 and later releases:

[**no**] **dot1x timeout** {**reauth-period** *seconds*| **quiet-period** *seconds* | **tx-period** *seconds* | **supp-timeout** *seconds*| **server-timeout** *seconds*}

Note 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)# authentication timer reauthenticate server
Switch(config)#
```

Related Commands	Command	Description
	show authenticatio	Displays Authentication Manager information.

authentication violation

Use the **authentication violation** interface configuration command to configure the violation modes: restrict and shutdown.

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**]

no authentication violation [**restrict**| **shutdown**]

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.

Defaults

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

Command Modes

Interface configuration

Command History	**Release**	**Modification**
	12.2(52)SG	Command introduced on the Catalyst 4500 series switch.

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 trigger on shutdown mode. The following syslog messages displays:

```
%AUTHMGR-5-SECURITY_VIOLATION: Security violation on the interface interface name, new
MAC address mac-address is seen.
%PM-4-ERR_DISABLE: psecure-violation error detected on interface name, putting
interface name in err-disable state
```

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	Connects the interface to a Cisco IP phone and automatically configures QoS for VoIP. The CoS labels of incoming packets are trusted only when the 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

Command History		
	Release	**Modification**
	12.2(25)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

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

Use the **cisco-phone** keyword on the ports at the edge of the network that are connected to Cisco IP phones. The switch detects the telephone through the Cisco Discovery Protocol (CDP) and trusts the QoS labels it parses that are received from the telephone.

Use the **trust** keyword on the ports that are connected to the interior of the network. Because it is assumed that the traffic has already been classified by the other edge devices, 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 old 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 trust** interface configuration command, the ingress classification on the specified interface is set to trust the CoS label that is received in the packet if the specified interface is configured as Layer 2 (and is set to trust DSCP if the interface is configured as Layer 3).

You can enter 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. Use the **debug auto qos** privileged EXEC command to enable auto QoS debugging.

To disable auto QoS on an interface, use the **no auto qos** 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 0/1 is a trusted device:

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

This example shows how to enable auto QoS and to trust the 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-if)# 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 on Supervisor Engines other than a Supervisor Engine 6-E:

```
Switch# debug auto qos
AutoQoS debugging is on
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# auto qos voip trust
Switch(config-if)#
00:00:07:gos
00:00:07:gos map cos 5 to dscp 46
00:00:07:gos map cos 3 to dscp 40
00:00:07:gos map dscp 32 to tx-queue 1
00:00:08:gos dbl
00:00:08:gos dbl map acl-name voip-policy
00:01:00:(1) class class-default:
00:01:00:(1) dbl
00:01:00:(1) interface Gigabitethernet1/1
00:01:00:gos trust cos
00:01:00:(1) tx-queue 3
00:01:00:(1) bandwidth 250 -1
00:01:00:(1) shape percent 33
00:01:00:(1) service-policy output acl-name voip-policy
Switch(config-if)# interface gigabitethernet1/1
Switch(config-if)# auto qos voip cisco-phone
Switch(config-if)#
00:00:07:gos
00:00:07:gos map cos 5 to dscp 26
00:00:07:gos map cos 3 to dscp 26
00:00:07:gos map dscp 32 to tx-queue 1
00:00:08:gos dbl
00:00:08:gos dbl map acl-name voip-policy
```

```
00:00:09: class class-default
00:00:09: dscp af21
00:00:09:interface GigabitEthernet1/1
00:00:09: qos trust device cisco-phone
00:00:09: qos trust cos
00:00:09: tx-queue 3
00:00:09: priority high
00:00:09: shape percent 33
00:00:09: bandwidth percent 33
00:00:09:service-policy output autoqos-voip-policy
```

This example shows how to display the QoS configuration that is automatically generated when auto QoS is enabled on an interface on a Supervisor II slot 1:

```
Switch#show interface ten/slot
Switch#show interface GigabitEthernet1/1 ten plus | Red with (MTU|E.
Switch#show interfaces GigabitEthernet1/1/0
Switch#show interfaces gig **auto qos voip trust
GigabitEthernet1/1/0
[AdMin: service-policy input AutoQos-VoIP-Input-Cos-Policy
[AdMin: service-policy output AutoQos-VoIP-Output-Policy
Switch#show interfaces GigabitEthernet1/1/0
Switch#show int gig **auto qos voip
GigabitEthernet1/1/0
Switch#show int gig
[AdMin: qos trust device cisco-phone
[AdMin: service-policy input AutoQos-VoIP-Input-Cos-Policy
[AdMin: service-policy output AutoQos-VoIP-Output-Policy
Switch#show int gig **load
Switch#
```

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 map cos	Defines the ingress CoS-to-DSCP mapping for the trusted interfaces.
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 operating information.
show qos maps	Displays QoS map information.

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 mate-sys mode

Command History	**Release**	**Modification**
	12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch (Catalyst 4507R only).

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

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

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

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 10,000000.
	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 one-limited.

Defaults No bandwidth is specified.

Command Modes Policy-map class configuration mode

Command History	Release	Modification
	12.2(40)SG	This command was introduced on the Catalyst 4500 series switch using a Supervisor Engine 6E.

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 this 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 of any unallocated bandwidth on the port.

If there is no unallocated bandwidth for the new queue or if the unalloc ated 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 cannot allot 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(config)# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# policy-map policy1
Switch(config-pmap)# class silver-class
Switch(config-pmap-c)# bandwidth 2000
Switch(config-pmap-c)# end
```

This example shows how to guarantee 30 percent of the bandwidth for class1 and 25 percent of the bandwidth for class2 when 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-pmap)# class class1
Switch(config-pmap-c)# bandwidth percent 60
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class2
Switch(config-pmap-c)# bandwidth percent 25
Switch(config-pmap-c)# exit
Switch(config-pmap)# end
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# service-policy input policy1
Switch(config-if)# end
```

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 voice.

```
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)# bandwidth remaining percent 50
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class2
Switch(config-pmap-c)# bandwidth remaining percent 25
Switch(config-pmap-c)# exit
Switch(config-pmap)# class voice
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# exit
Switch(config-pmap)# end
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
	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 or modifies 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 [policy-map class]	Creates a service policy that is a quality of service (QoS) policy within a policy map.
	shape [class-list-of-queuing]	Enables traffic shaping a class of traffic on a policy map attached to a physical port.
	show policy-map	Displays administrators 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

Command History

Release	Modification
12.2(52)SG	This command was introduced on the Catalyst 4500 series switch, Supervisor Engine 6-E, and Catalyst 4900M chassis.

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**—Enables or disables an alert group, See the **alert-group** command.
- **contact-email-addr** *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.
- **contact-id** *alphanumeric*—Specifies the customer contact identification for Cisco AutoNotification. 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** *text*—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 default.
- **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. You can specify up to four e-mail servers, using 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 set 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*—Specifies 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 shows how to configure the contact information:

```
Switch(config)# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# call-home
Switch(cfg-call-home)# contact-email-addr user@companyxyz.com
Switch(cfg-call-home)# phone-number +1-800-555-4567
Switch(cfg-call-home)# street-address "1234 Picaboo Street, Any city, Any state, 12345"
Switch(cfg-call-home)# customer-id Customer1234
Switch(cfg-call-home)# site-id Site1dot1abc1def2
Switch(cfg-call-home)# contract-id Company1234
Switch(cfg-call-home)# exit
Switch(config)#
```

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

```
Switch(config)# call-home
Switch(cfg-call-home)# rate-limit 50
```

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

```
Switch(config)# call-home
Switch(cfg-call-home)# default rate-limit
```

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

```
Switch(config)# call-home
Switch(cfg-call-home)# copy profile profile1 profile2
```

This example shows 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(cfg-call-home)# mail-server smtp.example.com priority 1
Switch(cfg-call-home)# mail-server 192.168.0.1 priority 2
Switch(cfg-call-home)# sender from username@example.com
Switch(cfg-call-home)# sender reply-to username@example.com
Switch(cfg-call-home)# exit
Switch(config)#
```

This example shows how to specify MgmtVrf as the vrf name where the call-home email message is forwarded:

```
Switch(cfg-call-home)# vrf MgmtVrf
```

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** *ccid*|*cid*]

Syntax Description		
	output analysis	Sends the output of the specified CLI show command for analysis. The show command must be contained in quotes (").
	show-command	
	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** (standalone) or **show module switch all** (VS system) commands, is sent to Cisco for analysis.
	bugs-list	
	command-reference	
	product-advisor	
	profile *name*	(Optional) Specifies an existing profile to which this request is sent. If no profile is specified, the request is sent to the Cisco TAC profile.
	send *ccid*|*cid*	(Optional) Specifies the identifier of a registered Smart Call Home user. If a *user-id* is specified, the resulting analysis report is sent to the e-mail address of the specified *user-id*. If a *contract-id* is 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

Command History	Release	Modification
	12.2(52)SG	This command was introduced on the Catalyst 4500 series switch, Supervisor Engine 6-E, and Catalyst 4500E Series.

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 Teams (PSIRT) notices, End-of-Life (EoL) or End of Sales (EoS) notices, or field notices (FNs) 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 slot2 test 5"
```

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 CLI 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. When e-mail delivery 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

Command History	**Release**	**Modification**
	12.2(25)EW.	This command was introduced on the Catalyst 4500 series switch. Supported Engine 5.4, and Catalyst 4500M chassis.

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 one 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 the 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@mycompany.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

Command History	Release	Modification
	12.2(52)SG	This command was introduced on the Catalyst 4500 series switch, Supervisor Engine 6-E, and Catalyst 4900M chassis.

Usage Guidelines

When you enter the module number, you can enter the number of the module.

If you do not specify the **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 destination profiles for a specific module number:

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

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) Test message text. **profile** *profile-name* Specifies the name of the destination profile.
Command Default	This command has no default settings.
Command Modes	Privileged EXEC mode

Command History	**Release**	**Modification**
	12.2(52)SG	This command was introduced on the Catalyst 4500 series switch, Supervisor Engine 6-E, and Catalyst 4900M chassis.

Usage Guidelines This command sends a test message to the specified destination profile. If you enter text-message text, 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# call-home test "test of the day" profile CiscoTac1
```

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 within 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

Command History	*Release*	*Modification*
	12.1(5c)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW	Support for LACP was added.

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 Layer 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 Layer 2 or vice versa if 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 interfaces. Do not assign bridge groups on the physical EtherChannel interfaces 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)#int gi1/1 channel-group 45 mode on
Creating a port-channel interface Port-channel45
Switch(config)#int gi1/1
```

Related Commands

Command	Description
interface port-channel	Accesses or creates a port-channel interface.
show interface 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

Command History

Release	Modification
12.2(31)SG	Support for this command was introduced on the Catalyst 4500 series switches.

Usage Guidelines

This command is not supported on systems that are configured with a Supervisor Engine 1.

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 **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 EtherChannel" 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)#interface gigabitethernet 1/1
Switch(config-if)#
```

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

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

Command History

Release	Modification
12.2(18)ZJ0W	Support for this command was introduced on the Catalyst 4500 series switches.

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 identify the policy map and to enter policy-map configuration mode. After specifying 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. After you are in policy-map configuration mode, in addition to the **class** keyword, you can choose from the **class-map** global configuration command. You attach the policy map to 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. This command is available on the Supervisor Engine 6-E and the Catalyst 4500M chassis.
- **dbl** Enables dynamic buffer limiting for traffic hitting this class. For details on **dbl** parameters refer to the **dbcm qos 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 policer specifies the bandwidth limitations and the action to take when the limits are exceeded. For

more information, see the **police** command. For more information about the two-rate policer, see the **police rate-limit** (per-flow policer) command. The two-rate traffic policer is supported on a Supervisor Engine 6-E and the Catalyst 6500M chassis.

- **priority**: Enables the strict-priority queue for a class of traffic. For more information, see the **priority** command. This command is supported in the Supervisor Engine 6-E and the Catalyst 6500M chassis.
- **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 rate limit for traffic transmission (shaping). For more information, see the **shape [class-based queuing]** command. This command is supported on the Supervisor Engine 6-E and the Catalyst 6500M chassis.
- **trust**: Defines a trust state for a traffic class. For more information, see the **trust** command. This command is not supported on the Supervisor Engine 6-E and the Catalyst 6500M chassis.

The switch supports up to 256 classes, including the default class, in a policy map. Packets that fail to meet any of the matching criteria are classified to 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 ingress 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 DSCP value obtained from the policed-DSCP map and then sent.

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# set ip dscp 10
Switch(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet1/0/4
Switch(config-if)# service-policy input 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

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switches.

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 with one match criterion, which is an access list called 103:

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

This example shows how to delete the client class map:

```
Switch(config)# configure terminal
Switch(config)# no class-map client
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 4094.
Defaults	This command has no default settings.
Command Modes	Privileged EXEC mode

Command History	**Release**	**Modification**
	12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW	Support for extended VLAN addresses was added.

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 use 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 (refer to Cisco IOS documentation)	Displays interface counter information.

clear energywise neighbors

Use the **clear energywise neighbors** privileged EXEC command to delete the EnergyWise neighbor tables.

clear energywise neighbors

Syntax Description This command has no arguments or keywords.

Defaults No default is defined.

Command Modes Privileged EXEC

Command History

Release	Modification
12.2(33)SG	This command was introduced.

Examples This example shows how to delete the neighbor tables:

```
Switch# clear energywise neighbors
Cleared all node and/or domain/role neighbors
```

You can verify that the tables were deleted by entering the **show energywise neighbors** privileged EXEC command.

Note The **clear energywise neighbors** command clears all discovered neighbors.

Related Commands

Command	Description
show energywise	Displays the EnergyWise settings and status of the entity and PoE ports.

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 re-enable.
	vlan	Specifies all VLANs on the interface be recovered.
	range	(Optional) Specifies the VLAN range to be recovered.

Defaults	
	This command has no default settings.

Command Modes	
	Global configuration mode

Command History		
	Release	**Modification**
	12.2(50)SG	Added support for per-VLAN error-disable detection.

Usage Guidelines

If a VLAN range is not specified, all VLANs on the specified interface are re-enabled. The **clear errdisable** command recovers 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(config)# clear errdisable interface ethernet1/slot 1/6-10
Switch(config)
```

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

Command History

Release	Modification
12.2(18)SXF	Support for this command was introduced on the Catalyst 6500 series switch.

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:

```
Dat>enb
Dat>clear hw-module slot 5 password
Dat>exit
```

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 On a Catalyst 4500 series switch, this command does not increment **interface resets** as it 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

Command History	**Release**	**Modification**
	12.2(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to clear the hardware logic from a Gigabit Ethernet IEEE 802.3z interface:

```
Switch#clear interface gigabitethernet 1/1
Switch#
```

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

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

Command History

Release	Modification
5.5 (3)CSX(9)	Support for this command was introduced on the Catalyst 6500 series switch.
5.5 (4) CSX(16)	Support for extended VLAN addresses added.

Examples

This example shows how to clear the hardware logic from a specific VLAN:

```
Console> (enable) clear interface vlan 5
Console>(enable)
```

Related Commands

Command	Description
show interface 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

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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

Command History	Release	Modification
	12.1(19)E1w	Support for this command was introduced on the Catalyst 4500 series switch.

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	

Command History		
	Release	**Modification**
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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   ACL Drops
----     ---------   -------     ----------   ---------
   1           0         0              0           0

Vlan     DHCP Permits  ACL 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

Command History	**Release**	**Modification**
	12.2(14)SX1	Support for this command was introduced on the Catalyst 6500 series switches.

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 1.1.1.1
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

Command History

Release	Modification
12.1(19)E1W	Support for this command was introduced on the Catalyst 4500 series switch.

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 gives you a DHCP binding configuration to assure binding 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 statistics

To clear the DHCP binding database statistics, use 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

Command History	Release	Modification
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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 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 4094.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 6500 series switch.

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(enable) clear ip igmp group 224.0.100.1
Switch(enb)
```

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 Internet Group Management Protocol (IGMP), see the **show ip igmp groups** command in IOS CMD 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

Command History	Release	Modification
	12.1(2)E1W	Support for this command was introduced on the Catalyst 6500 series switch.

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

Command History	Release	Modification
	12.1(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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

```
Switch#clear ip mfib counters
Switch#
```

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

Command History

Release	Modification
12.1(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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:

```
Switch#clear ip mfib fastdrop
Switch#
```

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 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

Command History

Release	Modification
12.2(12)EW	Support for this command was introduced on the Catalyst 4500 series switches.

Usage Guidelines

This command is not supported on systems that are configured with a Supervisor Engine I.

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#clear lacp 1 counters
Switch#
```

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*}] [**{vlan** *vlan_id*}] **notification}**

Syntax Description

dynamic	Specifies dynamic entry types.
address *mac_addr*	(Optional) Specifies the MAC address.
interface *interface*	(Optional) Specifies an interface and clears the entries associated with it; valid values are **Fastethernet** and **Gigabitethernet**.
vlan *vlan_id*	(Optional) Specifies the VL-MAN, 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

Command History

Release	Modification
12.1(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.1(12c)EW	Support for extended VL-MN addresses added.
12.2(17)SG	Support for MAC address notification global counters added.

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.
	mode cpu	Enters the mode CPU submode and manually synchronize the configurations on the two supervisor engines.
	show mac-address-table address	Displays the information about the MAC address table.
	snmp-server enable traps	Enables SNMP notification.

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 to clear the entries associated with it; valid values are **FastEthernet** and **GigabitEthernet**.
vlan *vlan_id*	(Optional) Specifies the VLANs; valid values are from 1 to 4094.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.1(12c)EW	Support for extended VLAN addresses added.

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 Layer 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 synchronize the configurations on the two supervisor 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

Command History	Release	Modification
	12.2(54)SG	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to clear NMSP statistics:

```
Switch# clear nmsp statistics
NMSP statistics cleared.
```

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

Command History	**Release**	**Modification**
	3.2.1(SG)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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| voice]**

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

Command History	Release	Modification
	12.2(20)EW	This command was first introduced on the Catalyst 4500 series switch.
	12.2(25)EW	Add support for sticky port security.

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 0000.0070.0007
```

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

```
Switch(config)# clear port-security dynamic interface gi2/6(ethernet0/1)
```

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

Command History	Release	Modification
	12.2(50)SG	Support for this command was introduced on the Catalyst 4500 series switch.

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*}}

aggregate-policer name	(Optional) Specifies an aggregate policer.	
interface	(Optional) Specifies an interface.	
fastethernet	(Optional) Specifies the Fast 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

Command History	Release	Modification
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

This command is not supported on the Supervisor Engine 6-E and the Catalyst 4500M chassis.

Note When you enter the **clear qos** command, the way that 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

Command History	**Release**	**Modification**
	12.1(12)EW	Support for this command was introduced on the Catalyst 4500 series switches.

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 hardware 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

Command History	Release	Modification
	12.2(31)SG	Support for this command was introduced on the Catalyst 4500 series switches.

Examples This example shows how to clear the VMPS statistics:

```
Switch> clear vmps statistics
Switch>
```

Related Commands	Command	Description
	show vmps	Displays VMPS information.
	vmps reconfirm (privileged EXEC)	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 named "system-cpp-policy" is attached.

Command Modes Global configuration mode

Command History	Release	Modification
	12.2(25)S1	Support for this command was introduced on Cisco7 Series supervisor engines and switches.
	12.2(25)SG	Support on Supervisor 6-E, and Catalyst 4500M was introduced.
	12.2(52)SG	Support on Supervisor 6E-E introduced.

Usage Guidelines After you enter the **control-plane** command, you can define control plane services for your main processor. For example, you can associate a 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 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
! Allow 10.1.1.2 traffic from rlogin
Switch(config)# access-list 140 deny tcp host 10.1.1.2 any eq telnet
! Allow all other traffic to be policed
Switch(config)# access-list 140 permit tcp any any eq telnet
! Define class-map to match traffic
Switch(config)# class-map match-any 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 1500 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)# service 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 the *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 a counter set to a switch port, use the **counter** command. To remove a counter assignment, use the **no** form of this command.

```
counter
no counter
```

Syntax Description This command has no arguments or keywords.

Defaults This command has no default setting.

Command Modes Interface configuration mode

Command History	Release	Modification
	12.2(18)SXF	Support for this command was introduced.

Usage Guidelines This command is supported on the Supervisor Engine 6-E and the Catalyst 4500M chassis.

The total number of switch ports that can have transmit and receive counters is 4096.

When a Layer 3 port with counter assigned is changed to a Layer 2 port or removed, the hardware counters are freed. This action is similar to entering the **no counter** command.

Examples This example shows how to assign a counter set to a switch port:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface vlan 20
Switch(config-if)# counter
Switch(config-if)# end
Switch#
```

dbl

To enable active queue management on a traffic class or 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

Command History	Release	Modification
	12.1(20)EW	This command was introduced on the Catalyst 4500 series switch.
	12.2(40)SG	Added support for the Supervisor Engine 6E.

Usage Guidelines The semantics of the DBL configuration is similar to the CSOSED 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(config)#policy-map testdbl
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config-pmap)#policy-map policy1
Switch(config-pmap-c)#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.

Command	Description
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 **form** 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

Command History	Release	Modification
	12.2(25)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples | This example shows how to display the information in the adjacency database:

```
Switch#debug adjacency
4d02h: add 172.20.52.34 [0]ip@GigabitEthernet1/1; via ARP w11 expires: 04:00:00
4d02h: del: add 172.20.52.34 [0]ip@GigabitEthernet1/1; via ARP w11 expires: 04:00:00
4d02h: del: add 172.20.52.34 [0]ip@GigabitEthernet1/1; via ARP w11 expires: 04:00:00
4d02h: add 172.20.52.34 [0]ip@GigabitEthernet1/1; via ARP w11 expires: 04:00:00
4d02h: del: add 172.20.52.34 [0]ip@GigabitEthernet1/1; via ARP w11 expires: 04:00:00
4d02h: del: add 172.20.52.34 [0]ip@GigabitEthernet1/1; via ARP w11 expires: 04:00:00
4d02h: add 172.20.52.34 [0]ip@GigabitEthernet1/1; via ARP w11 expires: 04:00:00
4d02h: del: add 172.20.52.34 [0]ip@GigabitEthernet1/1; via ARP w11 expires: 04:00:00
<... output truncated; ...>
Switch#
```

Related Commands

Command	Description
undebug adjacency (same as no debug 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

Command History

Release	Modification
12.1(11b)E9	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to debug the backup events:

```
Switch# debug backup
Backup events debugging is on
Switch#
```

Related Commands

Command	Description
undebug backup (same as the 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 to64. **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

Command History	Release	Modification
	12.1(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW	Support for extended VLAN addresses added.

Examples

This example shows how to limit the debugging output to VLAN interface 1:

```
Switch#debug condition interface vlan 1
Condition 2 set
Switch#
```

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** *module/port* | **GigabitEthernet** *module/port* | **port-channel** *interface-num* | **vlan** *vlan_id group-number*}

no debug condition standby {**fastethernet** *module/port*| **GigabitEthernet** *module/port* | **port-channel** *interface-num* | **vlan** *vlan_id group-number*}

Syntax Description	**fastethernet** Limits the debugging to Fast Ethernet interface. *module/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

Command History	**Release**	**Modification**
	12.1(2)EW	Support for this command was introduced on the Catalyst 6500 series switch.
	12.1(12c)EW	Support for extended VLAN addresses added.

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 entered 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#debug condition standby vlan 1 0
condition 1 set
Switch#
```

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.
Stopping all extensive debugging (possibly many debugging
messages to come), 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

Command History

Release	**Modification**
12.1(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.4(1)EW	Support for extended VLAN addresses added.

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 condition set.
Removing it will enable debug output of all debugging
messages in result, unless specific debugging flags
are first removed.

Proceed with removal? [yes/no] : 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

Command History	**Release**	**Modification**
	12.1(11)b,EW	Support for this command was introduced on the Catalyst 6500 series switch.

Examples This example shows how to enable the 802.1X debugging for all conditions:

```
Dot1x#debug dot1x all
Dot1x#
```

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) Displays 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

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 6500 series switch.

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 Shim/PM debugging is on
22:42:31:PAG:removing agport Po5 for port [Fa2/1]
22:42:31:PAG:port_delete [Fa2/1] port_ifidx [5]
22:42:31:PAG:computing id values of Fa2/1: Ifidx 5 ; i 1
22:42:31:PAG:port_delete:Fa2/1: Fa2/1 name =
22:42:31:PAG:SP - active incompatible for Fa2/1: displays of Fa2/1 is held, Fa2/1 is fol
22:42:31:PAG:page_active_change_ok:agport:Fa2/1, port Fa2/1 is agport Po5 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(config)# no debug ethernet-lb
Switch(config)#
```

Related Commands

Command	Description
undebug ethernet-lb (same as no debug ethernet-lb)	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*[/ | **GigabitEthernet** *module*[/ | **null**} | **port-channel** *interface-num*[| **vlan** *vlan_id*]

no debug interface {**FastEthernet** *module*[/ | **GigabitEthernet** *module*[/ | **null** | **port-channel** *interface-num*[| **vlan** *vlan_id*]

Syntax Description	**FastEthernet** Limits the debugging to Fast Ethernet interfaces. *module*[/ 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

Command History	Release	Modification
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.2(52)SG	Support for extended VLAN addresses added.

Examples

This example shows how to limit the debugging to interface VLAN 1:

```
Switch#debug interface vlan 1
Switch#debug condition interface vlan 1
Switch#dir
Switch#
```

Related Commands	Command	Description
	debug condition interface	Limits the debugging output of interface-related activities.
	undebug ethernet-lmi (same as **debug ethernet-lmi**)	Disables debugging output.

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**| **headers**| **packets**| **ports**| **seats**}

no debug ipc {**all**| **errors**| **events**| **headers**| **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

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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 ipc)	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

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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

Command History	Release	Modification
	12.1(11)b EW	Support for this command was introduced on the Catalyst 4500 series switch.

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

Command History	Release	Modification
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to enable debugging for the IP source guard:

```
Switch#debug ip verify source packet
Switch#clock
```

This example shows how to disable debugging for the IP source guard:

```
Switch#no debug ip verify source packet
Switch#clock
```

Related Commands	Command	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

Command History	**Release**	**Modification**
	12.1(12)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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
Port Aggregation Protocol Miscellaneous debugging is on
Switch#
```

Related Commands	**Command**	**Description**
	undebug pagp (same as no debug pagp)	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 messages.
	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

Command History	**Release**	**Modification**
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples

This example shows how to debug the monitoring errors:

```
Switch#debug monitor errors
SPAN error detail 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

Command History	Release	Modification
	12.2(52)SG	Support for this command was introduced on the Catalyst 4500 series switch.

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

Command History

Release	Modification
12.1(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to debug NVRAM:

```
Switch# debug nvram
NVRAM 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

Command History	**Release**	**Modification**
	12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines This command is taggered 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 PAgP miscellaneous debugging:

```
Switch# debug pagp misc
Port Aggregation Protocol Miscellaneous debugging is on
Switch#
*Sep 30 10:10:01: SP: PAgP: pagp_h_Ref-0. enqueued
*Sep 30 10:10:01: SP: PAgP: 135 bytes out Fa5/6
*Sep 30 10:10:01: SP: PAgP: Fa5/6 PAgP0/13 c/a/p/m/v/d/t/s/i/f/u/ifnum partner
*Sep 30 10:10:01: SP: PAgP: timer pagp_h_Ref-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 packets VLAN debugging functions.

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.

Examples	This example shows how to enable all PM debugging:
	`Router#debug platform packet protocol lacp`
	`Router#debug`

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 function. **transmit** (Optional) Enables the platform packet transmission debugging function. **vlan** (Optional) Enables the platform packet VLAN debugging function.
Defaults	This command has no default settings.
Command Modes	Privileged EXEC mode

Command History	**Release**	**Modification**
	12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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	Disables debugging output.
	show [**debug**] **platform packet protocol pagp** [**counters**	**flags**]	Displays the platform packet protocol pagp information.

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** | **etherchnl** | **messages** | **port**| **registry** | **vcp** | **sm** | **span** | **split** | **vlan** | **vp**}

no debug pm {**all** | **card**| **cookies** | **etherchnl** | **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.
	etherchnl Debugs the EtherChannel-related events.
	messages Debugs the PM messages.
	port Debugs the port-related events.
	registry Debugs the PM registry interaction.
	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

Command History	**Release**	**Modification**
	12.1(15c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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

Command History	Release	Modification
	12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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** Turns on event debugging
	packet Turns on packet debugging
	all Turns on both event and packet debugging

Defaults All debugging is turned off.

Command Modes Privileged EXEC mode

Command History	**Release**	**Modification**
	12.2(18)SXD	Support for this command was introduced on the Catalyst 6500 series switch.

Examples This example shows how to turn on packet debugging:

```
Switch# debug pppoe intermediate-agent packet
PPPOE IA Packet Debugging is on
*Aug 2 20:12:36.137: PPPOE_IA: Process new PPPoE packet, Message type: PADI, Input
interface: Gi3/3, vlan : 2 MAC dst: ffff.ffff.ffff, MAC src: aabb.cc00.0300
*Aug 2 20:12:36.137: PPPOE_IA: curr\all tag PPPOE packet from Input\Output
Gi3\gi3\0\0\0\0\0
*Aug 2 20:12:36.137: PPPOE_IA: curr\all tag PPPOE packet from Input\Output
Gi3\gi3\0\0\0\0\0
*Aug 2 20:12:36.137: PPPOE_IA: Process new PPPoE packet, Message type: PADO, Input
interface: Gi3/3, vlan : 2 MAC dst: aabb.cc00.0300, MAC src: 0014.a8ce.8512
*Aug 2 20:12:36.137: PPPOE_IA: curr\all tag PPPOE packet from Input\Output
Gi3\gi3\0\0\0\0\0, vlan : 2 MAC dst: aabb.cc00.0300, MAC src: aabb.cc00.0300
*Aug 2 20:12:36.137: PPPOE_IA: curr\all tag PPPOE packet from Input\Output
Gi3\gi3\0\0\0\0\0
*Aug 2 20:12:36.137: PPPOE_IA: Process new PPPoE packet, Message type: PADR, Input
interface: Gi3/3, vlan : 2 MAC dst: 0014.a8ce.8512, MAC src: aabb.cc00.0300
*Aug 2 20:12:36.140: PPPOE_IA: curr\all tag PPPOE packet from Input\Output
Gi3\gi3\0\0\0\0\0
*Aug 2 20:12:36.140: PPPOE_IA: Process new PPPoE packet, Message type: PADS, Input
interface: Gi3/3, vlan : 2 MAC dst: aabb.cc00.0300, MAC src: 0014.a8ce.8512
*Aug 2 20:12:36.140: PPPOE_IA: curr\all tag PPPOE packet from Input\Output
Gi3\gi3\0\0\0\0\0
```

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 the supervisor engine redundancy, use the **debug redundancy** command. To disable the debugging output, use the **no** form of this command.

debug redundancy {**errors** | **fsm** | **hpa** | **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.
	hpa 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

Command History	Release	Modification
	12.2(52)SG	Support for this command was introduced on the Catalyst 4500 series switch (Catalyst 4507R only).

Examples This example chose 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** | **etherchannel** | **config** | **events** | **exceptions** | **general** | **ha** | **mstp** | **pvst** | **root** | **snmp** | **switch** | **synchronization** | **uplinkfast**}

no debug spanning-tree {**all** | **bpdu** | **bpdu-opt** | **etherchannel** | **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 switchfabrics 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

Command History

Release	Modification
7.6.1(GBIW)	Support for this command was introduced on the Catalyst 4500 series switch.

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

Command History	**Release**	**Modification**
	12.1(8)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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 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 receive errors of the spanning-tree switch shim.
interrupt	Enables the shim ISR 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

Command History	Release	Modification
	12.1(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

This command is supported only by the supervisor engine and can be entered 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: STP SHM Tx: bpdu of type 1ser-st sent VL0 on FastEthernet5/9.101
*Sep 30 08:27:13: STP SHM Tx: bpdu of type 1ser-st sent VL0 on FastEthernet5/9.102
*Sep 30 08:27:13: STP SHM Tx: bpdu of type 1ser-st sent VL0 on FastEthernet5/9.105
*Sep 30 08:27:13: STP SHM Tx: bpdu of type 1ser-st sent VL0 on FastEthernet5/9.149
*Sep 30 08:27:13: STP SHM Tx: bpdu of type 1ser-st sent VL0 on FastEthernet5/9.152
*Sep 30 08:27:13: STP SHM Tx: bpdu of type 1ser-st sent VL0 on FastEthernet5/9.153
*Sep 30 08:27:13: STP SHM Tx: bpdu of type 1ser-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

Command History	Release	Modification
	12.1(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines | This command is supported only by the supervisor engine and can be 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 spanning-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

Command History	**Release**	**Modification**
	12.1(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples

This example shows how to debug the software VLAN events:

```
Switch# debug sw-vlan events
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

Enables 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

Command History	Release	Modification
	12.1(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines The following are four types of file read operations:

- Operation1—Reads the file header, which contains the header verification word and the file version number.
- Operation2—Reads the main body of the file, which contains most of the domain and VLAN information.
- Operation3—Reads TLV descriptor structures.
- Operation4—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 errors debugging is on
Switch#
```

Related Commands	Command	Description
	undebug vlan-vlan-lib (same as no debug)	Disables debugging output.
	(no vlan-lib)	

debug sw-vlan notification

To enable debugging of the messages that trace the activation and deactivation of the ISL 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 {**acrfwdchange** | **allowedvlanchgchange**| **fwdchange** | **linkchange**| **modechange**| **pruningchgchange** | **statechange**}

no debug sw-vlan notification {**acrfwdchange** | **allowedvlanchgchange**| **fwdchange** | **linkchange** | **modechange** | **pruningchgchange** | **statechange** }

Syntax Description

acrfwdchange	Enables the VLAN manager notification of aggregated access interface STP forward changes.
allowedvlanchgchange	Enables the VLAN manager notification of changes to 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.
pruningchgchange	Enables the VLAN manager notification of changes to pruning configurations.
statechange	Enables the VLAN manager notification of interface state changes.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.1(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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**|**pruning**|**packets**|**xmit**|**xmit**}

no debug sw-vlan vtp {**events**|**packets**|**pruning**|**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. **pruning** 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 the Cisco IOS VTP platform-dependent layer to send. **xmit** Displays the contents of all outgoing VTP pruning packets that the VTP code will request that the Cisco IOS VTP platform-dependent layer to send, but not include pruning packets.
Defaults	This command has no default settings.
Command Modes	Privileged EXEC mode

Command History	**Release**	**Modification**
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines If you do not enter any more parameters after entering **pruning**, the VTP pruning debugging messages are displayed.

Examples This example shows how to debug the software VLAN managing 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 sw-vlan vtp)	Disables debugging output.

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**}

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

Command History	Release	Modification
	12.2(25)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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 debug the UDLD events:

```
Switch> debug udld events
UDLD process debugging is on
Switch>
```

This example shows how to debug the UDLD packets:

```
Switch> debug udld packets
UDLD packets debugging is on
Switch>
```

This example shows how to debug the UDLD registry events:

```
Switch> debug udld registries
UDLD registries debugging is on
Switch>
```

Related Commands	Command	Description
	undebug vdb (same as no debug vdb)	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

Command History	Release	Modification
	12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to enable all VQP debugging:

```
Switch> enable
Switch# debug vqpc all
Switch#
```

Related Commands	Command	Description
	vmps reconfirm (privileged-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

Command History	Release	Modification
	12.1(6)EW	Support for this command was introduced on the Catalyst 6500 series switch.

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 3/1-5
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** | **host** *sender-ip*} *sender-ip-mask* {**mac** | **host** *sender-mac* [*sender-mac sender-mac-mask*]} [**request ip** | **host** *target-ip*] *target-ip-mask* {**mac** | **host** *target-mac* [*target-mac target-mac-mask*]} [**log** | **log-text** *log-text-string*] [**log-interval** *log-interval-seconds*]

no deny {**request**} {**ip** | **host** *sender-ip* | *sender-ip sender-ip-mask*} **mac** {**any** | **host** *sender-mac* | *sender-mac sender-mac-mask*} [**request ip** | **host** *target-ip* | *target-ip target-ip-mask*] **mac** {**any** | **host** *sender-mac* | *sender-mac sender-mac-mask*} [**request ip** | **host** *target-ip* | *target-ip target-ip-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.
request	Specifies a match for the ARP request.
ip	Specifies the IP address values for the ARP requests.
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 requests.
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

Command History	Release	Modification
	12.1(3)XH	Support for this command was introduced on the Catalyst 6500 series switch.

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 0000.0000.abcd 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 access-list static-hosts
Switch(config-arp-nacl)# deny ip host 1.1.1.1 mac host 0000.0000.abcd
Switch(config-arp-nacl)# end
Switch# show arp access-list

ARP access list static-hosts
    deny ip host 1.1.1.1 mac host 0000.0000.abcd
Switch#
```

Related Commands	Command	Description
	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 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 to 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.

Defaults This command has no default settings.

Command Modes cfg-call-home-profile

Command History	Release	Modification
	12.2(50)SG	Support was introduced on the Catalyst 4500 series switches.

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	Configure a maximum destination message size for the destination profile.
	destination preferred-msg-format	Configure a preferred message format.
	destination transport-method	Enable the message transport method.
	profile	Enter 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 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 3145728 bytes.

Command Modes cfg-call-home-profile

Command History	Release	Modification
	12.2(52)SG	Support was introduced on the Catalyst 4500 series switches.

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 xtest
Switch(cfg-call-home-profile)# destination message-size-limit 3000000
Switch(cfg-call-home-profile)#
```

Related Commands

Command	Description
destination address	Configure the destination e-mail address or URL to which Call Home messages will be sent.
destination preferred-msg-format	Configure 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.

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.

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

Command History	Release	Modification
	12.2(54)SG	Support was introduced on the Catalyst 4500 series switches.

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 state
Switch(cfg-call-home-profile)# destination preferred-msg-format long-text
Switch(cfg-call-home-profile)#exit
```

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 max 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.

Command	Description
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

Command History	Release	Modification
	12.2(52)SG	Support was introduced on the Catalyst 4500 series switches.

Usage Guidelines To enter profile call-home configuration submodes, 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 alex
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	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 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.

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.

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, Rather it issues a console error message once an hour. You should reload 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 error 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 S90, the default behavior is aggressive. In all other switches, the default behavior is conservative.

Command Modes

Global config mode

Command History	**Release**	**Modification**
	12.2(50)SG, 12.2(50)SG, 15.0(2)SG, XE 3.1.0SG	Support for this command was provided on the Catalyst 6500 series switch.
	12.2(50)SG, 15.0(2)SG, XE 3.3.0SG	Support for the **conservative** option was added.

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 revert 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 errors, 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 a normal mode, except that a bootup failure only 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

Command History	Release	Modification
	12.2(18)EW	This command was introduced on the Catalyst 4500 series switch.

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-diagnostic 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

Command History	Release	Modification
	12.2(25)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to run the specified diagnostic test at the specified module:

```
This exec command starts the TDR test on specified interface
Switch#diagnostic start module 1 test cable-diag port 3
diagnostic start module 1 test cable-diag port 3
diagnostic cable-diag for module 1 port 3 will be run
module 1: Running test(s) 5 may disrupt normal system operation
Do you want to continue? [n]: yes
yes
Switch#
2d18h: %CAT4-6-TEST_RUNNING: module 1: Running sw(cable-diag)tr [5=5] ...
2d18h: %CAT4-6-TEST_OK: module 1: sw(cable-diag)tr [5=5] has completed successfully
Switch#
```

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 a "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

Command History	**Release**	**Modification**
	12.2(33)SXI	Support for this command was introduced on the Catalyst 6500 series switch.

Examples

This example shows how to configure the maximum number of attempts before the port is moved to the auth-fail VLAN on Fast Ethernet interface 4/3:

```
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 dot1x 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

Command History	Release	Modification
	Cat4500 IOS	Support for this command was introduced on the Catalyst 4500 series switch.

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 inbound and out-bound traffic will be controlled.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.2(31)SG	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

You can manage remote systems in unauthenticated control. Unidirectional control enables you to turn on systems remotely using a specific Ethernet packet, listen to at 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 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

Command History

Release	Modification
12.2(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to enable 802.1x critical authentication:

```
Switch(config)# int 3
Switch(config-if)# dot1x critical
Switch(config-if)#
```

Related Commands

Command	Description
dot1x critical eapol	Enables sending EAPOL success packets when a port is critically authenticated partway through an EAP exchange.
dot1x critical recovery delay	Sets the time interval between port reinitialization.
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/gateway 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

Command History

Release	Modification
12.2(31)SG	Support for this command was introduced on the Catalyst 4500 series switch.

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 reinitialization when AAA unavailable occurs; valid values are from 1 to 10,000 milliseconds.
Defaults	Delay time is set to 100 milliseconds.
Command Modes	Global configuration mode

Command History	**Release**	**Modification**
	12.2(54)SG	Support for this command was introduced on the Catalyst 4500 series switch.

Examples

This example chose how to set the 802.1x critical recovery delay time to 500:

```
Switch(config)# dot1x critical recovery delay 500
Switch(config)#
```

Related Commands	**Command**	**Description**
	dot1x control	Enables the 802.1X critical authentication on a port.
	dot1x critical eapol	Enables sending EAPOL success packets when a port is critically authorized partners 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

Command History	Release	Modification
	12.2(33)SXI	Support for this command was introduced on the Catalyst 6500 series switch.

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 300
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 authorized partway through an EAP exchange.
	dot1x critical recovery delay	Sets the time interval between port reinitializations.
	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

Command History	Release	Modification
	12.2(25)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.2(25)EWA	Support for secondary VLAN at the configured guest VLAN ID was added.

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 with 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#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface fastethernet4/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#dot1x guest-vlan 10
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 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

Command History	Release	Modification
	12.2(25)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines With Cisco Release 12.2(25)EWA, you can use the **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 tag pkt pkt pkt pkt pkt pkt is enabled, the Catalyst 4500 series switch does not maintain EAPOL packet history. The switch allows clients that fail 802.1X authentication to access 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
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#dot1x guest-vlan supplicant
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 stack 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}

no 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

Command History	Release	Modification
	12.2(25)FX	Support for this command was introduced on the Catalyst 6500 series switch.
	12.2(37)SG	Added support for multiple domains.

Usage Guidelines Use this command to limit an IEEE 802.1x-enabled port to a single client or to attach multiple clients to an IEEE 802.1x-enabled port. In multiple-hosts mode, only one of the attached hosts needs to be successfully authorized for all hosts to be granted network access. If the port becomes unauthorized (re-authentication fails or an Extensible Authentication Protocol over LAN [EAPOL] logoff message is received), all attached clients are denied access to the network.

Use the **multi-domain** keyword to enable MDA on a port. MDA divides the port into both a data domain and a voice domain. MDA allows both a data device and a voice device, such as an IP phone (Cisco or non-Cisco), on the same IEEE 802.1x-enabled port.

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

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 server. 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(config)# dot1x
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# dot1x pipgaliforkeeset1
Switch(config)# dot1x port-control auto
Switch(config)# dot1x host-mode multi-host
Switch(config)# end
Switch#
```

This example shows how to enable MDA and to allow both a host and a voice device on the port:

```
Switch# configure t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface FastEthernet4/1
Switch(config-if)# switchport access vlan 12
Switch(config-if)# switchport mode access
Switch(config-if)# switchport voice vlan 10
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

Command History	Release	Modification
	12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines Use this command to initialize state machines and to set up the environment for fast authentication.

Examples This example shows how to initialize the 802.1X state machines on an interface:

```
Switch# dot1x initialize
Switch#
```

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

Command History	**Release**	**Modification**
	12.2(31)SG	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

The removal of the **dot1x mac-auth-bypass** configuration from a port does not affect the authorization or unauthorization state of a port. If the port is in unauthorized state, it remains unauthorized, 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

Command History	**Release**	**Modification**
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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 15.

Defaults

The switch sends a maximum of two retransmissions.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.1(19)EW	This command was modified to control an EAP-Request/Identity retransmission limit.

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-if)# dot1x max-req 5
Switch(config-if)#
```

This example shows how to return to the default setting:

```
Switch(config-if)# no dot1x max-req
Switch(config-if)#
```

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

Command History	**Release**	**Modification**
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines The 802.1X protocol is supported on both the Layer 2 static-access ports and the Layer 3-routed port. 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 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 or on an active port in an EtherChannel, an error message appears, and 802.1X is not 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 3/1:

```
Switch(config)# interface gigabitethernet1/1
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

Command History

Release	Modification
12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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 shows how to enable the periodic reauthentication of the client:

```
Switch(config-if)# no dot1x re-authentication
Switch(config-if)#
```

This example shows how to enable the periodic reauthentication and set the number of seconds between the reauthentication attempts is 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 times.
	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

Command History

Release	Modification
12.1(11)b	Support for this command was introduced on the Catalyst 4500 series switch.

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 guest-vlan[number]** 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	Manualization 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 to65535. See the "Usage Guidelines" section for more information.
reauth-period server	Number of seconds between reauthentication attempts; valid values are from 1 to65535 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 1 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

Command History

Release	Modification
12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switches.
12.2(25)EWA	Support for selecting the reauthentication timer from the "server" was added.

Usage Guidelines

The periodic reauthentication must be enabled before entering the **dot1x timeout re-authperiod** 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(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)# interface fastethernet3/1
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

Command History	**Release**	**Modification**
	12.1(8)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

Table 2-3 lists the supported command options by interface.

Table 2-3 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 **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 10**	Forces 10 Mbps and half duplex
duplex half	**speed 100**	Forces 100 Mbps and half 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:

```
Dub(config)#conf int g1/2/2 duplex full
Dub(config)#conf int g1/2/2
```

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.

energywise (global configuration)

Use the **energywise** global configuration command to enable and configure EnergyWise on an entity. Use the **no** form of this command to disable EnergyWise on the entity and remove the EnergyWise configuration.

energywise [**importance** *importance* | **keywords** *word,word,...* | **level** *level* | **management** *ip-port-number* | **name** *name* | **neighbor** *hostname* | *ip-address udp-port-number* | **role** *role*]

no energywise [**importance** | **keywords** | **level** | **management** | **name** | **neighbor** | **role**]

Syntax Description	**importance** *importance*	Sets the importance of the entity. The range is from 1 to 100.
	keywords *word,word,...*	Assigns at least one keyword for the entity. When assigning multiple keywords, separate the keywords with commas, and do not use spaces between keywords. For the word value: • You can enter alphanumeric characters and symbols such as #, (, %, ! or &. • Do not use an asterisk (*) or a blank space between the characters and symbols.
	level *level*	Sets the power level of the entity. The only valid value is 10.
	management *ip-port-number*	Specifies the TCP port that connects to the management station. The range is from 1 to 65000.
	name *name*	Specifies the EnergyWise specific entity name. For the name value: • You can enter alphanumeric characters and symbols such as #, (, %, ! or &. • Do not use an asterisk (*) or a blank space between the characters and symbols.
	neighbor *hostname* | *ip-address udp-port-number*	Assigns a static neighbor. • Hostname (hostname) or IP address (*ip-address*). • UDP port (*udp-port-number*) that sends and receives queries. The range is from 1 to 65000.
	role *role*	Specifies the role of the entity in the EnergyWise domain. For example: lobby.320. For the role value: • You can enter alphanumeric characters and symbols such as #, (, %, ! or &. • Do not use an asterisk (*) or a blank space between the characters and symbols.

Defaults

The importance is 1.

No keywords are defined.

The power level is 10.

The *top-port-number* is 43440.

The name is the hostname.

No neighbors are assigned.

The role is the model number.

Command Modes

Configuration

Command History

Release	Modification
12.2(52)SG	This command was introduced.

Usage Guidelines

When you add an entity to a domain, EnergyWise is enabled on the entity and in PoE ports.

Examples

This example shows how to enable EnergyWise, assign the entity to a domain, and set the password:

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#energywise domain cisco secret class protocol udp port 43440 ip 2.2.2.30
Switch(config)#energywise importance 50
Switch(config)#energywise keywords device
Switch(config)#energywise keepalive 60180
Switch(config)#energywise name Switch1
Switch(config)#energywise neighbor 4500-21 43440
Switch(config)#energywise role role.lobbyroom
Switch(config)#end
```

Related Commands

Command	Description
show energywise	Displays the EnergyWise settings and status.

energywise (interface configuration)

Use the **energywise** interface configuration command to configure EnergyWise on the power over Ethernet (PoE) port. Use **no** form of this command to disable EnergyWise on the port and remove the EnergyWise configuration.

energywise [importance *importance* **| keywords** *word,word,...* **| level** *level* **| recurrence at** *minute hour day_of_month month day_of_week* **| name** *name* **| role** *role*]

no energywise

Syntax Description	**importance** *importance* (Optional) Sets the importance of the port. The range is from 1 to 100.
	keywords *word,word,...* (Optional) Assigns at least one keyword for the port. When assigning multiple keywords, separate the keywords with commas, and do not use spaces between keywords. For the word value: • You can enter alphanumeric characters and special characters such as #, (, %, ! or &. • Do not use an asterisk (*) or a blank space between the characters and symbols.
	level *level* (Optional) Sets the power level of the port. The only valid values are 0 and 10.
	recurrence [at *minute hour day_of_month month day_of_week*] (Optional) Schedules the power-on or power-off recurrence. • **importance** *importance*—Sets the importance of the port in the domain. The range is from 1 to 100. • *minute*—The range is from 0 to 59. Use * for the wildcard. • *hour*—The range is from 0 to 23. Use * for the wildcard. • *day_of_month*—The range is from 1 to 31. Use * for the wildcard. • *month*—The range is from 1 to 12. You can also enter **jan**, **feb**, **mar**, **apr**, and so on. Use * for the wildcard. • *day_of_week*—The range is from 0 to 7 (0 and 7 both represent Sunday). Use * for the wildcard. **Note** The specified times are local times based on the PoE-entity time zone. **Note** If the day of the month and day of the week are both specified, (that is, are not wildcards), the recurrence is exercised when either field matches the current time. **Note** Recurrence takes effect within the minute specified, rather than exactly on the minute; it could occur as soon as 60 seconds late.

name name	(Optional) Specifies the EnergyWise-specific port name. Ru: the name value: • You can enter alphanumeric characters and symbols such as #, (, %, ! or &. • Do not use an asterisk (*) or a blank space between the characters and symbols.
role role	(Optional) Specifies the role of the port in the domain. For example, building6. Ru: the role value: • You can enter alphanumeric characters and symbols such as #, (, %, ! or &. • Do not use an asterisk (*) or a blank space between the characters and symbols.

Defaults

The importance is 1.

No keywords are defined.

The power level is 10.

The name is the short version of the interface name; for example, Gi 2 For Gigabit Ethernet 1/2.

Command Modes

Interface Configuration

Command History

Release	Modification
12.2(33)SXI	This command was introduced.

Usage Guidelines

To return the **importance** *value* keyword values to the default settings, use the **default energywise importance** and the **default energywise level** commands.

Examples

This example shows how to enable and configure EnergyWise on the PoE port:

```
Switch# conf term terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# energywise domain cisco secret cisco protocol udp port 43440 ip 2.2.2.30
Switch(config)# interface Gi1/2
Switch(config-if)# energywise level 10 recurrence importance 50 at 0 0 * * *
Switch(config-if)# energywise level 20 recurrence importance 50 at 0 20 * * *
Switch(config-if)# energywise importance 50
Switch(config-if)# energywise name hobbyinterface.1
Switch(config-if)# energywise role hobbyroom
Switch(config-if)#
```

Note Recurrence values effect within the minute specified, rather than exactly on the minute or could occur as much as 60 seconds late.

■ energywise (interface configuration)

Related Commands	Command	Description
	show energywise	Displays the EnergyWise settings and status.

energywise domain

Use the **energywise domain** global configuration command to enable EnergyWise on the entity, assign the entity to a domain, and set the password for secure communication among the entities in the domain. Use the **no** form of this command to disable EnergyWise on the entity and to remove the EnergyWise configuration.

energywise domain *domain-name* **secret** [0 | 7] *password* [**protocol udp** *port-number* [**interface** *interface-id*] | **ip** *ip-address*] |

no energywise domain

Syntax Description

domain-name	Assigns the entity to a domain with the specified domain-name. • You can enter alphanumeric characters and symbols such as @, %, ! or &. • Do not use an asterisk (*) or a blank space between the characters and symbols.
secret [0 | 7] *password*	Sets the *password* for secure communication among the entities in the domain. • (Optional) **0**—Use an unencrypted password. • (Optional) 7—Use an hidden password. This requires service *password-encryption* to be enabled. If you do not enter **0** or 7, the entity uses the default value of 0. For the *password* value: • You can enter alphanumeric characters and symbols such as @, %, ! or &. • Do not use an asterisk (*) or a blank space between the characters and symbols.
port *udp-port-number*	(Optional) Specifies the UDP port that sends and receives queries. The range is from 1 to 65000.
interface *interface-id*	(Optional) In a bridged network, specifies the interface that you would prefer for communicating with other EnergyWise entities rather than letting the switch select an interface by default.
ip *ip-address*	(Optional) In a routed network, specifies the IP address to be used while communicating with EnergyWise peers instead of letting the system choose a default. The **interface** and **ip** options are mutually exclusive.

Defaults

The entity is not assigned to a domain.

The *password* is not set.

The *udp-port-number* is 43401.

Command Modes Configuration

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

Usage Guidelines If you enter the **energywise domain** *domain-name* **secret** [**0** | **7**] *password* command, the entity selects the first available interface is communicate with the network and with management applications.

Examples This example shows how to enable EnergyWise and how to set the *domain-name* and *password* values.

```
Switch(config)# energywise domain cisco secret cisco protocol udp port 43440 ip 2.2.4.30
```

This example shows how to enable EnergyWise and to specify the route in the management applications:

```
Switch(config)# energywise domain cisco secret 0 cisco protocol udp port 43440 ip
192.168.1.2
```

Related Commands

Command	Description
show energywise	Displays the EnergyWise settings and status.

energywise query

Use the **energywise query** privileged EXEC command to run a query to display power information or to power the entities or PoE ports.

energywise query importance *importance* {**keywords** *word,word,...*} **name** *name* {**collect** {**delta** | **usage** }

energywise query importance *importance* {**keywords** *word,word,...*} **name** *name* {**set level** *level*

energywise query importance *importance* {**keywords** *word,word,...*} **name** *name* {**sum** {**delta** | **usage** }

Syntax Description

importance *importance*	Sets the importance of the entity or ports. The range is from 1 to 100.
keywords *word,word,...*	Specifies one of more keywords to use in the query. When specifying multiple keywords, separate the keywords with commas, and do not use spaces between keywords. For the *word* value: • You can enter alphanumeric characters and symbols such as #, {, %, ! or &. • Do not use an asterisk (*) or a blank space between the characters and symbols.
name *name*	Name to use in the query. For the *wildcard*, use * or *name** with the asterisk at the end of the name. For the *name* value: • You can enter alphanumeric characters and symbols such as #, {, %, ! or &. • Do not use an asterisk (*) or a blank space between the characters and symbols.
collect {**delta**	**usage** }	Displays the delta or usage values for the entity or PoE ports. • **delta**—Displays only the differences between the current and available power levels. • **usage**—Displays only the current power usage.
set level *level*	Sets the power level of the entity or the PoE ports. For the entity, the only valid value is 10. For the ports, the valid values are 0 and 10.
sum {**delta**	**usage** }	Displays the sum of the delta or usage values for the entity or PoE ports. • **delta**—Displays only the sum of the differences between the current and available power levels. • **usage**—Displays only the sum of the current power usage.

Command Modes Privileged EXEC

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

Usage Guidelines To power on or power off ports, enter the **energywise query** {**keywords** *word*,*word*,...} {**name** *name*} **set level**{*level* command.

> **Caution** Use this query with care because it affects the entity on which you enter the command and other devices in the domain that match the query criteria.

Examples These examples show how to filter with the entity name:

```
Switch# energywise query importance 100 name phone* collect usage
Energywise query, timeout is 5 seconds:

Host          Name          Usage
=====         =====         =====
2.3.2.21      phone         0.0 (W)
2.3.2.22      phone         0.0 (W)
2.3.2.23      phone         0.0 (W)
2.3.2.24      phone         0.0 (W)
2.3.2.25      phone         0.0 (W)
2.3.2.26      phone         19.4 (W)
2.3.2.31      phone         0.0 (W)
2.3.2.32      phone         0.0 (W)
2.3.2.33      phone         0.0 (W)

Query(ref): 9   Responder(ref): 9   Time: 0.28 seconds

Switch# energywise query importance 100 name * usage
Energywise query, timeout is 5 seconds:

Host
=====
144.3 (W)

Query(ref): 147   Responder(ref): 147   Time: 0.125 seconds

Switch# energywise query importance 100 name lobby* collect usage
Energywise query, timeout is 5 seconds:

Host          Name          Usage
=====         =====         =====
2.2.4.30      lobby1ceiling 17.15.3 (W)

Query(ref): 1   Responder(ref): 1   Time: 0.7 seconds

Switch# energywise query importance 100 name Fal.0.4* sum usage
Energywise query, timeout is 5 seconds:

Total Usage
```

```
12.0 (0)

Queries: 10   Responded: 10   Time: 0.4 seconds
```

This example shows the state of the delta values and the potential power change in the domain:

```
Switch# energywise query importance 100 name * use delta
Energywise query: timeout is 3 seconds:

Level  Label        Delta Power (W)
-----  -----        ---------------
0      Show         -12.0
1      Alternate    -723.0
2      Sleep        -723.0
3      Hibernate    -723.0
4      Ready        -723.0
5      Low          -723.0
6      Medium       -723.0
7      Critical     -723.0
8      Redundant    -723.0
9      Essential    -723.0
10     Full         -723.0

Queries: 48   Responded: 48   Time: 0.25 seconds
```

This example shows the power levels in the domain:

```
Switch# show energywise children
Interface  Role                Name                  Usage      Lvl  Imp  Type
---------  ----                ----                  -----      ---  ---  ----
Gi2/0/1    common              Switch                84.0 (W)   10   10   phone
Gi2/0/1    interface           Gi1.0.1               0.0 (W)    10   20   cable2

Gi2/0/6    interface           Gi1.0.6               0.0 (W)    10   20   cable2
Gi2/0/7    relaimportance      LabsInterface.7       0.0 (W)    10   50   cable2
Gi2/0/8    interface           Gi1.0.8               0.0 (W)    10   20   cable2
(output truncated)
```

```
Switch# energywise query importance 100 name * set level 2
Energywise query: timeout is 3 seconds:

Success rate is 100 percent (10/10) setting setlevel
!!!!!!!!!!
```

```
 energywise importance 30
 energywise keywords lobby temperature
 energywise keywords lobby satellite public
 energywise name lobbyGreater.2
end

Switch# energywise query keyword lobby collect usage
Energywise query, timeout is 5 seconds:

Host            Name            Usage
====            ====            =====
2.2.4.10        lobbyInterface.17 15.4 (W)

QueryId: 1    ResponseNum: 1    Time: 0.2 seconds

Switch# energywise query keyword satellite sum usage
Energywise query, timeout is 5 seconds:

Total Usage
===========
15.4 (W)

QueryId: 1    ResponseNum: 1    Time: 0.11 seconds
```

erase

To erase a file system, use the **erase** command.

erase {**all** [**non-default**] | **nvram:** | **cat4000_flash:** | **nvram:** | **startup-config**}

Syntax Description

all [**non-default**]	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 Catalyst 4500 series switch.
cat4000_flash:	Erases the VLAN database configuration file.
nvram:	Erases the startup-config and private-config file in NVRAM.
startup-config:	Erases the startup-config and private-config file in NVRAM.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.2(25)SG	Support for this command was introduced on the Catalyst 4500 series switch.

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 slave:cat4000_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 file.

The **erase all** [**non-default**] 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 states stored in the nonvolatile storage and resets the Catalyst 4500 series switch to the factory default settings. The default settings include those modified in the Cisco IOS library as well as those set by the **erase all non-default** command (vtp mode=transparent, and the NOMRON variables: Config0=9x2101, Pb1=~~hostnam~~, ~~~~ and BootAutoConfig=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_4/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/configuration/command/reference/cfr_book/

Caution The **erase all new-default** command can erase Cisco IOS images in bootflash. Ensure that a Cisco IOS image can be copied back to the bootflash (**rm/cos**, from a accessible 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 new-default
Switch#
Erase and format operation will destroy all data in non-volatile storage. [confirm]
[confirm]
Formatting bootflash: ...

Format of bootflash complete
Erasing nvram:
Erasing cat4000_flash:
Erasing bootflash:
Clearing the last power failure timestamp
Clearing all NVRAM variables
Erasing of nvram:,cat4000_flash:,bootflash: complete
Switch#
%SYS-5-RELOAD: Reload requested
%SYS-6-BOOTTIME: time taken to reload 0 seconds
%ENVMON-2- Please reboot the system for the changes to take effect
Switch#
%C6K-2-NOTICE:%%SYS-2-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#
```

This example shows how to erase the contents in nvram:

```
Switch# erase nvram:
Erasing the nvram filesystem will remove all files! [confirm] [confirm]
[OK]
Erase of nvram: complete
Switch#
%SYS-2-NOTICE:%%SYS-2-NV_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! [confirm] [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 bootvar	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**] | **dp-flap** | **gbic-invalid** | **lipvlgard** | **link-flap** | **psp-flap**}

no errdisable detect cause {**all** | **arp-inspection** [**action shutdown vlan**] | **bpduguard shutdown vlan** | **dhcp-rate-limit** [**action shutdown vlan**] | **dp-flap** | **gbic-invalid** | **lipvlgard** | **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.
	dp-flap Specifies the detection for the DTP flap error-disable cause.
	gbic-invalid Specifies the detection for the GBIC module error-disable cause.
	lipvlgard 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

Command History	**Release**	**Modification**
	12.2(18)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.2(52)SG	Added support for per-VLAN error-disable detection.

Usage Guidelines A cause (dp-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 **shutdown** command and then the **no shutdown** command to recover an interface manually from the error-disable state.

To prevent the port from shutting 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: bpdugaard, 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 bpdugaard 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 Detect        Detect[en, dis]    Mode
-----------------        ---------------    ----
arp-inspection           Disabled           port
bpdugaard                Enabled            vlan
channel-misconfig        Enabled            port
dhcp-rate-limit          Enabled            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 | hitpktgrd | link-flap | psp-flap |
    pvcreate-validate | security-violation | storm-control | udld | unicastflood | vmps}
    [arp-inspection] [interval {interval}]]

no errdisable recovery [cause {all | arp-inspection | bpdugaurd | channel-mismatch |
    dhcp-rate-limit | dtp-flap | gbic-invalid | hitpktgrd | link-flap | psp-flap |
    pvcreate-validate | security-violation | storm-control | udld | unicastflood | vmps}
    [arp-inspection] [interval {interval}]]
```

Syntax Description		
	cause	(Optional) Enables the error-disable recovery to recover from a specific cause.
	all	(Optional) Enables the recovery times for all error-disable causes.
	arp-inspection	(Optional) Enables the recovery time for the ARP inspection cause.
	bpdugaurd	(Optional) Enables the recovery time for the BPDU guard error-disable cause.
	channel-mismatch	(Optional) Enables the recovery time for the channel mismatching error-disable cause.
	dhcp-rate-limit	(Optional) Enables the recovery time for the DHCP rate limit error-disable cause.
	dtp-flap	(Optional) Enables the recovery time for the DTP flap error-disable cause.
	gbic-invalid	(Optional) Enables the recovery time for the GBIC module error-disable cause.
	l2pugaurd	(Optional) Enables the recovery time for the Layer 2 protocol-tunnel error-disable cause.
	link-flap	(Optional) Enables the recovery time for the link flap error-disable cause.
	psp-flap	(Optional) Enables the recovery time for the PAgP flap error-disable cause.
	pvcreate-validate	(Optional) Enables the recovery time for pvcreate validate 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 to recover from storm-control error-disable state.
	udld	(Optional) Enables the recovery time for the UDLD error-disable cause.
	unicastflood	(Optional) Enables the recovery time for the unicast flood error-disable cause.
	vmps	(Optional) Enables the recovery time for the VMPS error-disable cause.
	arp-inspection	(Optional) Enables the ARP inspection cause and recovery interval.
	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

Command History	Release	Modification
	12.1(3a)EW	Support for this command was introduced on the Catalyst 6500 series switch.
	12.1(19)EW	Support for the storm-control feature.

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 error-disabled state is a form of shutdown) and OSPF packets will not be sent or received. Unless enabled 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 can reset 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
security-violatio    Disabled
channel-misconfig    Disabled
vmps                 Disabled
pagp-flap            Disabled
dtp-flap             Disabled
link-flap            Disabled
l2protocol           Disabled
pverror-violation    Disabled
mac-limit            Disabled
dhcp-rate-limit      Disabled
storm-control        Disabled
unicast-flood        Disabled
arp-inspection       Enabled
```

```
Timer interval: 300 seconds

Interfaces that will be enabled at the next timeout:

Gi1:r4k4
```

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-X4418-GB and WS-X4412-2GB-TX	All ports except for the oversubscribed ports	Off
WS-X4418-GB	Uplink ports (1-2)	Off
WS-X4412-2GB-TX	Oversubscribed ports (3-148)	On
WS-X4412-2GB-TX	Uplink ports (13-14)	Off
WS-X4412-2GB-TX	Oversubscribed ports (1-12)	On
WS-X4418-2GB-TX	Uplink ports (17-18)	Off

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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 2-4 describes the guidelines for using the different configurations of the **send** and **receive** keywords with the **flowcontrol** command.

Table 2-4 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 2-5 identifies how the flow control will be forced or negotiated on the Gigabit Ethernet interfaces based on their speed settings.

Table 2-5 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
1000BASE-X	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)#interface gigabitethernet 1/1
Switch(config-if)# flowcontrol receive on
Switch(config-if)#
```

This example shows how to disable send flow control:

```
Switch(config)#interface gigabitethernet 1/1
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 (of the same type).
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

Command History	Release	Modification
	12.2(20)EW	Support for the Supervisor Engine 6-E and the Catalyst 4900M chassis is introduced.

Usage Guidelines The Supervisor Engine 6-E and Catalyst 4900 M chassis TCAM hardware doesn't have enough hardware statistics entries for every classification/QoS ca n entry. Therefore, the statistics for each ca n entry needs to be enabled as needed.

Examples This example shows how to enable TCAM hardware statistics in your ACLs as ce:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# hardware statistics
Switch(config)# ipv4acl ip any any
Switch(config)# ipv6acl ip any any
Switch(config)# mac acl ip any any
Switch(config)# 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 port-group

To select either Gigabit Ethernet or 10-Gigabit Ethernet interfaces on your module, use the **hw-module port-group** command.

hw-module module *number* **port-group** *number* **select [gigabitethernet | tengigabitethernet]**

Syntax Description

module *number*	Specifies a line module. Specifies a module which supports TwinGig converter.
port-group *number*	Port group number on a switch.
select	Specifies an interface type, valid values are Gigabit Ethernet and 10-Gigabit Ethernet.
gigabitethernet	(Optional) Specifies Gigabit Ethernet.
tengigabitethernet	(Optional) Specifies 10-Gigabit Ethernet.

Defaults

10 Gigabit.

Command Modes

Global configuration mode

Command History

Release	Modification
12.2(40)SG	Support for TwinGig converter module introduced.

Usage Guidelines

Support for this command is available on the Cisco Catalyst 4500 modules that support TwinGig converter modules, such as the Supervisor Engine 6-E and WS-X4606-10GE-E.

Examples

This example shows how to select Gigabit Ethernet interfaces on a WS-X4606-10GE-E using the TwinGig Converter:

```
Switch# conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# hw-module module 1 port-group 1 select gigabitethernet
Switch(config)# exit
```

Use the **show interfaces status** command to display your configuration.

Related Commands

Command	Description
show hw-module port-group	Displays how the X2 holes on a module are grouped.
show interfaces status	Displays the interface status or a list of interfaces in error-disabled state.

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

Command History	Release	Modification
	12.1(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.2(25)EW	Add slot and module keywords.

Examples

This example shows how to shut off power to a module in slot 5:

```
Router(config)# no hw-module slot 5 power
Router(config)#
```

Related Commands	Command	Description
	clear hw-module slot password	Clears the password on an intelligent line module.

hw-module uplink mode shared-backplane

To change the uplink mode so that you can use all four 10-Gigabit Ethernet ports as blocking ports on the Supervisor Engine 6-E and Catalyst 4500E chassis when operating in redundant mode, use the **hw-module uplink mode shared-backplane** command. To disable a shared-backplane uplink mode, use the **no** form of the command.

hw-module uplink mode shared-backplane

no hw-module uplink mode shared-backplane

Syntax Description This command has no keywords or arguments.

Defaults Only two 10-Gigabit Ethernet ports or four 1-Gigabit Ethernet ports can be used on the supervisor engine.

Command Modes Global configuration mode

Command History	Release	Modification
	12.2(40)SG	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines When changing the uplink mode using the **hw-module uplink mode shared-backplane** command, you must reload the system. A message is printed on the console to inform this.

Examples This example shows how to enable shared-backplane uplink mode:

```
Switch(config)# hw-module uplink mode shared-backplane
A reload of the active supervisor is required to apply the new configuration.
Switch(config)#do write
Switch#
```

This example shows how to disable shared-backplane uplink mode:

```
Switch(config)# no hw-module uplink mode shared-backplane
A reload of the active supervisor is required to apply the new configuration.
Switch(config)#do write
Switch#
```

This example shows how to display the current state of uplink mode:

```
Switch #show hw-module uplink
Active uplink mode configuration is Default
(will be Shared-backplane after next reload)

A reload of active supervisor is required to apply the new configuration.
```

Related Commands	Command	Description
	show fan-module uplink	Displays fan-fan-module uplink information.

hw-module uplink select

To select the 10-Gigabit Ethernet uplinks, enter this command on the Supervisor Engine V-10GE within the VS-C6509-E chassis, use the **hw-module uplink select** command.

hw-module uplink select {tengigabitethernet | gigabitethernet | all}

Syntax Description

tengigabitethernet	(Optional) Specifies the 10-Gigabit Ethernet uplinks.
gigabitethernet	(Optional) Specifies the Gigabit Ethernet uplinks.
all	(Optional) Specifies all uplinks (10-Gigabit Ethernet and Gigabit Ethernet).

Defaults

tengigabitethernet

Command Modes

Global configuration mode

Command History

Release	Modification
12.2(33)SXI	Support for this command was introduced on the Catalyst 6500 series switch.
12.2(50)SG	Support for the **all** keyword was added.

Usage Guidelines

On a Supervisor Engine V-10GE (WS-X6516-10GE) in a 10-slot chassis (Catalyst 6509 and 6509-E), if a stateful configuration with a new uplink mode is copied into flash memory and the system is power cycled, the system will not come up with the new uplink mode. After copying the startup configuration with the new uplink mode into flash memory, the uplink mode must be changed to the new uplink mode manually using the command before the system is power cycled. This ensures that the system comes up in the new uplink mode.

Supervisor Engine V-10GE and Supervisor Engine II+10GE support 10-Gigabit Ethernet and Gigabit Ethernet uplink ports. On the Supervisor Engine V-10GE, all uplink ports are always available. Similarly, when a Supervisor Engine V-10GE is plugged into a WS-C6503, WS-C6506, or WS-C6509 chassis, all uplink ports are always available. When a Supervisor Engine V-10GE is plugged into a WS-C6509 chassis, you can choose to use the 10-Gigabit Ethernet uplink ports, the Gigabit Ethernet uplink ports, or all uplink ports. If you choose to use all uplink ports, then the tests this will support only the WS-X6192-GE-TX switching linecard. Be aware that this command takes effect only after a *reload* (after you have executed the **redundancy reload shelf** command).

Because the uplink selection is programmed into hardware during initialization, changing the active uplinks requires saving the configuration and reloading the switch. When you are configuring a change to the uplinks, the system responds with a message informing you that the switch must be reloaded and suggesting the appropriate command (depending on redundancy mode) to reload the switch.

If you select the **all** keyword, ensure that the switch can either swap or fail over to a WS-X6192-GE switching module.

A **no** form of this command does not exist. To undo the configuration, you must configure the uplinks.

Examples

This example shows how to select the Gigabit Ethernet uplinks:

```
Switch(config)# hw-module uplink select gigabitethernet
A reload of the active supervisor is required to apply the new configuration.
Switch(config)# exit
Switch#
```

Note The Gigabit Ethernet uplinks will be active after the next reload.

This example shows how to select the Gigabit Ethernet uplinks in a redundant system in SSO mode:

```
Switch(config)# hw-module uplink select gigabitethernet
A 'redundancy reload shelf' or power-cycle of chassis is required to apply the new
configuration.
Switch(config)# exit
Switch#
```

Note The Gigabit Ethernet uplinks will be active after the next reload of the chassis/shelf. Use the **redundancy reload shelf** command to reload the chassis/shelf.

This example shows how to select the Gigabit Ethernet uplinks in a redundant system in RPR mode:

```
Switch(config)# hw-module uplink select gigabitethernet
A reload of the active supervisor is required to apply the new configuration.
Switch(config)# exit
Switch#
```

Note The Gigabit Ethernet uplinks will be active on a switchover or reload of the active supervisor engine.

This example shows how to select all the uplinks in a redundant system in SSO mode:

```
Switch(config)# hw-module uplink select all
Warning: This configuration mode may disarm sim12.
A 'redundancy reload shelf' or power-cycle of chassis is required to apply the new
configuration.
Switch(config)# exit
Switch#
```

Note If you select the **all** keyword, only the Dnome board will be supported in the tenth slot of the supervisor engine.

Related Commands

Command	Description
show hw-module uplink	Displays hardware module uplink information.

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 to 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

Command History

Release	Modification
12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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 1100
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.
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

Command History

Release	Modification
12.2(25)EW	Extended to include the 10-Gigabit Ethernet interface.

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.
ge-wan	Gigabit Ethernet WAN IEEE 802.3z interface; supported on Catalyst 4500 series switches that are configured with a Supervisor Engine 2 only.
pos	Packet OC-3 interface on the 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 fastethernet 2/4
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

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 6500 series switch.

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 never create 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:

```
Router(config)# interface port-channel 64
Router(config)#
```

Related Commands	Command	Description
	channel-group	Assigns and configures an EtherChannel interface to an EtherChannel group.
	show ethernet 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 id - vlan id*| *port-range* | **macro** *name*}

Syntax Description		
	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 *name*	Specifies the name of a macro.

Defaults	
This command has no default settings.	

Command Modes	
Global configuration mode	
Interface configuration mode	

Command History	Release	Modification
	12.1(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW	Support for extended VLAN addresses added.

Usage Guidelines

You can use the **interface range** command on the existing VLANSVIs only. To display the VLANSVIs, 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 configurations 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 -24, gigabitethernet4/5 -48.
```

Use these formats when entering the *port-range*:

- *interface-type* {*mod*}/{*first-port*} - {*last-port*}
- *interface-type* {*mod*}/{*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 HL 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 Command Reference for a switch 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

Command History	Release	Modification
	12.1(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.2(52)SG	Support for extended addressing was added.

Usage Guidelines The SVIs are created the first time that you enter the **interface vlan** *vlan_id* command for a particular VLAN. The *vlan_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 10
%I Creating vlan VLAN0010
Switch(config)#
```

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

Command History	Release	Modification
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

When an ARP access control list is applied to a VLAN for dynamic ARP inspection, the ARP packets containing only 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 neither permit nor deny (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
----     -------------   ---------  ---------          ----------
   2     Enabled         Active     arp-acl-foo-bar    No

Vlan     ACL Logging     DHCP Logging
----     -----------     ------------
   2     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 arp inspection limit (interface)

To limit the rate of incoming ARP requests and responses on an interface and prevent DAI 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 series 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 all of the trusted interfaces.

The burst interval is set to 1 second by default.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(27b)E	Support for this command was introduced on the Catalyst 6500 series switch.
12.2(25)SEW	Added support for interface monitoring.

Usage Guidelines

The trunk 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 internal feature can be used to remove the port from the error-disabled state. The rate applies to both the trusted and untrusted interfaces. Configure appropriate rates on trunks to handle the packets across multiple DAI-enabled VLANs or set the **none** keyword to make the rate unlimited.

The rate of the incoming ARP packets onthe 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 switchover,no more than 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#conf t terminal
Switch(config)# interface fa4/1
Switch(config-if)# ip arp inspection limit rate 25
Switch(config-if)# end
Switch#show ip arp inspection interfaces FastEthernet 4/3
Interface      Trust State     Rate (pps)
-------------  -----------     ----------
Fa4/3          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#conf t terminal
Switch(config)# interface fa4/1
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

Use the **ip arp inspection log-buffer** commands to set and modify 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 0to 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

Command History

Release	Modification
12.1(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

The first dropped packet of a given flow is logged immediately. The subsequent packets for the same flow are registered but 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 terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip arp inspection log-buffer entries 45
Switch(config)# end
Switch# show ip arp inspection log
Total\ Buffer\ Size\ : 45
Syslog rate : 5 entries per 1 seconds.
No entries in log buffer.
Switch#
```

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)# end
Switch# show ip arp inspection log
Total 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 interface 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

Command History	Release	Modification
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to configure an interface to be trusted:

```
Switch# conf t terminal
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 interfaces 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 a **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 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

Command History	Release	Modification
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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 show how to enable the source MAC validation:

```
Switch(config)# ip arp inspection validate src-mac
Switch(config)# end
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
----  -------------   ---------  ---------          ----------
   1  Enabled         Active

Vlan  ACL Logging     DHCP Logging
----  -----------     ------------
   1  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 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

Command History	Release	Modification
	12.2(18)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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** {**matchlog** | **none** } | **dhcp-bindings** {**permit** | **all** | **none** }}

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.
matchlog	Specifies that logging of packets matched against ACLs is controlled by the **matchlog** keyword in the permit and deny access control entries of the ACLs. **Note** By default, the **matchlog** keyword is not available on the ACEs. When the keyword is used, denied packets are not logged. Packets are logged only when they match against an ACE that has the **matchlog** keyword.
none	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.
none	Prevents all logging of packets permitted or denied by DHCP bindings.

Defaults

All denied or dropped packets are logged.

Command Modes

Global configuration mode

Command History

Release	Modification
12.2(18)SXF	Support for this command was introduced on the Catalyst 6500 series switch.

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 exceptions 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 compared is reset to log on deny

Examples

This example shows how to configure an ARP inspection on VLAN 1 to add packets to a log on matching against the ACL with the **logging** keyword:

```
Switch# conf t terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip arp inspection vlan 1 logging acl-match matching
Switch(config)# end
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
----  -------------    ---------  ---------          ----------
   1  Enabled          Active
   2  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 port in the load-balancing hash functions.
destination *dest*	Specifies the destination port in the hash-distancing hash. Uses the source and destination in hash functions.
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

Command History

Release	Modification
12.1(2)E(EW)	Support for this command was introduced on the Catalyst 6500 series switch.

Usage Guidelines

The original algorithm, tunnel algorithm, and universal algorithm are stated through the hardware. For software-routed packets, the algorithms are handled by the software. The **include-ports** option does not apply to the software-switched traffic.

Examples

This example shows how to configure the IP CEF load-sharing algorithm that includes Layer 4 ports:

```
Switch(config)# ip cef load-sharing algorithm include-ports
Switch(config)#
```

This example shows how to configure the IPCEF load-sharing algorithm that includes Layer 4 tunneling ports:

```
Switch(config)# ip cef load-sharing algorithm include-ports tunnel
Switch(config)#
```

Related Commands

Command	Description
show ip cef 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 untrusted Layer 2 interfaces, 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 2048.

Defaults

This command has no default settings.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.2(17d)SXB	Support for this command was introduced on the Catalyst 6500 series switch.

Examples

This example chose 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 gigabitethernet 4/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 1
Switch(config-if)# ip device tracking maximum 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)# 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

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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.
ip-address	Specifies an IP address.
interface *interface*	Specifies an interface type and number.
expiry *seconds*	Specifies interface (in seconds) after which binding is no longer valid.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History	Release	Modification
	12.2(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.2(25)EW	Support for the 10 Gigabit Ethernet interface was introduced on the Catalyst 4500 series switch.

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 1800 seconds:

```
Switch# ip dhcp snooping binding 0001.1074.1234 vlan 1 172.20.50.5 interface gi1/1 expiry 1800
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.

Command	Description
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: • flash:/<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

Command History

Release	Modification
12.1(19)EW	Support for this command was introduced on the Catalyst 6500 series switch.

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 (flash fills quickly). In addition, due to the nature of the file system used in the flash, a large number of files causes access to be considerably slowed. When a file is stored in a remote location accessible through TFTP, or RPR+SSO (standby supervisor engine cascade over the binding file 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 version4
Switch(config)# ip dhcp snooping database tftp://10.1.1.1/directory/file
Switch(config)# exit
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 Succeed Time : None
Last Failed Time : None
Last Failed Reason : No failure recorded.

Total Attempts      :   1  Startup Failures :   0
Successful Transfers :   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 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.

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 remote-id	Specifies the option 82 information format.
hostname	Specifies the remote ID for option 82.
string *word*	Specifies the user-configured hostname for the remote ID. The word string can be from 4 to 63 characters long with no spaces.

Defaults

DHCP option 82 data insertion is enabled.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.2(40)SG	Added **remote-id** keyword to support option 82 enhancement.

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# sh run | begin ip dhcp
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 ascii123
Switch(config)# interface GigabitEthernet 5/5
Switch(config-if)# ip dhcp snooping trust
Switch(config-if)# ip dhcp snooping limit rate 100
Switch(config-if)# ip dhcp snooping vlan 500 information option format-type circuit-id
string customer-001
Switch(config-if)# interface FastEthernet 2/1
Switch(config-if)# ip dhcp snooping vlan 555 information option format-type circuit-id
string customer-001
Switch(config-if)# end
```

Related Commands:	Command	Description
	ip dhcp snooping	Globally enables DHCP snooping.
	ip dhcp snooping binding	Sets up and gives zero 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	Enables create of an sub-option of DHCP snooping option-82's 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

Command History	Release	Modification
	12.2(25)SXWA	Support for this command was introduced on the Catalyst 6500 series switch.

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

Command History	**Release**	**Modification**
	12.1(13)E5	Support for this command was introduced on the Catalyst 6500 series switch.

Usage Guidelines Typically, the rate limit applies to the untrusted interfaces. If you want to set up rate limiting for the trusted interfaces, note that the trusted interface 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)# ip dhcp snooping limit rate 150
Switch(config)#
```

This example shows how to disable the DHCP message rate limiting:

```
Switch(config)# 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 vlan	Enables DHCP snooping on a trusted VLAN.
ip dhcp snooping vlan	Enables DHCP snooping on a VLAN or 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

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to enable DHCP snooping trust on an interface:

```
Switch(config)# int g 4/1
Switch(config-if)# ip dhcp snooping trust
Switch(config-if)#
```

This example shows how to disable DHCP snooping trust on an interface:

```
Switch(config)# int g 4/1
Switch(config-if)# no ip dhcp snooping trust
Switch(config-if)#
```

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 ip 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

Command History

Release	Modification
12.1(11b)EW	Support for this command was introduced on the Catalyst 6500 series switch.

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	Enables circuit-id/ip-subnet-id/hostname 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

To enable circuit-id (suboption of DHCP snooping option 82) on a VLAN, use the **ip dhcp snooping vlan information option format-type** 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 string** *string*

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

Syntax Description	*number*	Single VLAN number or a range of VLANs; valid values are from 1 to 4094.
	circuit-id	Specifies using the string as the circuit ID.
	string	Specifies a user-defined string for the circuit ID.

Defaults

VLAN-mod-port, if DHCP snooping option-82 is disabled.

Command Modes

Interface configuration mode

Command History	**Release**	**Modification**
	12.2(18)SXD2	Support for this command was introduced on the Catalyst 6500 series switch.

Usage Guidelines

The circuit-id suboption of DHCP option-82 is supported only when DHCP snooping is globally enabled and also VLANs using DHCP option 82.

Examples

The following example shows how to enable DHCP snooping on VLANS 500 through 555 and option 82 circuit-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 3/4
Switch(config)#if# ip dhcp snooping trust
Switch(config)#if# ip dhcp snooping vlan 500
Switch(config)#if# ip dhcp snooping vlan 500 information option format-type circuit-id
string customer-555
Switch(config)# interface FastEthernet 2/1
Switch(config)#if# ip dhcp snooping vlan 500 information option format-type circuit-id
string customer-555
Switch(config)# end
```

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

Command History	**Release**	**Modification**
	12.1(13)E9	Support for this command was introduced on the Catalyst 6500 series switch.

Usage Guidelines

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

An IGMP profile can be applied to one or more switch port interfaces, but one port can have only one profile applied to it.

Examples

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

```
Switch(config)# interface 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

Command History	Release	Modification
	12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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 the 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

Command History	Release	Modification
	12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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 2 interfaces, but each interface can have only one profile applied to it.

Examples

This example shows how to configure IGMP profile 40 that permits the specified range of IP multicast addresses:

```
Switch(config)# ip igmp profile 40
Switch(config-igmp-profile)# permit
Switch(config-igmp-profile)# range 233.1.1.1 233.255.255.255
Switch(config-igmp-profile)#
```

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

Command History	Release	Modification
	12.1(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

If you use the default IGMP snooping configuration, the valid query interval values are from 1 to 65535 seconds. If you have changed 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 LAN 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 **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-if)# ip igmp query-interval 120
Switch(config-if)#
```

Related Commands

Command	Description
ip igmp query-interval (refer to Cisco IOS documentation)	Configures the interval period before the router takes over as the querier for the interface after the previous querier has stopped querying.
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

Command History

Release	Modification
12.1(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.2(31)SGA	Support for flooding the spanning tree table was added.

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 command** 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 mac topology changes have occurred:

```
Switch(config)# ip igmp snooping tcn flood query count 3
Switch(config)#
```

This example shows how to disable the flooding of the spanning tree table to the network:

```
Switch(config)# no ip igmp snooping tcn flood
Switch(config)#
```

This example shows how to enable an IGMP general query:

```
Switch(config)# ip igmp snooping tcn query solicit
Switch(config)#
```

This example shows how to disable an IGMP general query:

```
Switch(config)# no ip igmp snooping tcn 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

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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 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
  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

Command History	Release	Modification
	12.1(20)EW	Support for five-command was introduced on the Catalyst 4500 series switch.
	12.2(31)SGA	Support for extended addressing was added.

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	Enables 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

Command History

Release	Modification
12.1(2)EW	Support for this command was introduced on the Catalyst 6500 series switch.

Examples

This example shows how to disable IGMP explicit host tracking on interface VLAN 200 and how to verify the configuration:

```
Switch>enable
Switch#configure terminal
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 igmp snooping querier mode  : fixed
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 Layer 2 interface as a static or router interface for a VLAN.

Command	Description
ip igmp snooping vlan static	Configures a Layer 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

Command History	**Release**	**Modification**
	12.1(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW	Support for extended addressing was added.

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.

Command	Description
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

Command History

Release	Modification
12.1(2)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.1(12c)EW	Support for extended addressing was added.
12.2(25)EW	Support for the 10-Gigabit Ethernet interface was introduced on the Catalyst 4500 series switch.

Usage Guidelines

You 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 400 mrouter interface fastethernet 5/6
Switch(config-if)#
```

This example shows how to specify the multicast switch learning method:

```
Switch(config-if)# ip igmp snooping 400 mrouter learn cgmp
Switch(config-if)#
```

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 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 zero-hop interface in 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

Command History	**Release**	**Modification**
	12.1(11)b(EW)	Support for this command was introduced on the Catalyst 6500 series switch.
	12.2(52)SG	Support for the 10-Gigabit Ethernet interface was introduced on the Catalyst 4500 series switch.

Examples

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

```
Switch(config)# ip igmp snooping vlan 1 static 0100.5e02.0203 interface fastethernet 5/11
Configuring port fastethernet5/11 on group 0100.5e02.0203 vlan 1
Switch(config)#
```

Related Commands	**Command**	**Description**
	ip igmp snooping	Enable IGMP snooping.
	ip igmp snooping vlan immediate-leave	Enable IGMP immediate-leave processing.

Command	Description
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

Command History

Release	Modification
12.1(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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 interfaces where the local proxy ARP feature is enabled.

Examples This example shows how to enable the local proxy ARP feature:

```
Switch(config)#int g1/1/4
Switch(config-if)#ip local-proxy-arp
Switch(config-if)#int g1/1/4
```

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

Command History	Release	Modification
	12.1(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to enable MFIB fast drops:

```
Switch#conf t
Switch#ip mfib fastdrop
Switch#end
```

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 functionality, use the **no** form of this command.

ip multicast [*vrf vrf-name*] **multipath** [**g-g-hash** | **basic** | **next-hop-hash**]

no ip multicast [*vrf vrf-name*] **multipath** [**g-g-hash** | **basic** | **next-hop-hash**]

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.
	g-g-hash | **next-hop-hash** (Optional) Enables IP 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-hash** keyword enables a more complex hash based on source, group, and next-hop address. This algorithm is referred to as the next-hop-hashed 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)

Command History	Release	Modification
	12.2(33)SXI	The **g-g-hash** keyword was introduced on the Catalyst 6500 switch.

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 there are more one neighbor but 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 invert to 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 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 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 **ip hash** keyword and multiple equal-cost paths exist, load splitting will occur across equal-cost paths based on source and group addresses using a hash-based algorithm. Unlike the default source-based hashing or the source-based load splitting IP multicast traffic, you must select the algorithm order to calculate the equal-cost paths by specifying one of the following keywords:

- **basic**—The basic S-G-hash algorithm is preferable for non-randomization in a network cabling 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 preferable because no randomization is used to determine the hash value. Unlike the S-hash and basic S-G-hash algorithms, 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:

```
Switch(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:

```
Switch(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:

```
Switch(config)# ip multicast multipath s-g-hash next-hop-based
```

ip route-cache flow

To enable NetFlow statistics for IP routing, use the **ip route-cache flow** command. To disable NetFlow statistics, use the **no** form of this command.

ip route-cache flow [infer-fields]

no ip route-cache flow [infer-fields]

Syntax Description	**infer-fields** (Optional) Includes the NetFlow fields as inferred by the software: Input identifier, Output identifier, and Routing information.
Defaults	NetFlow statistics is disabled. Inferred information is excluded.
Command Modes	Global configuration mode

Command History	**Release**	**Modification**
	12.1(12)EW	Support for this command was introduced on the Catalyst 4500 series switches.
	12.1(12)EW	Command enhanced to support infer fields.

Usage Guidelines

To use these commands, you need to install the Supervisor Engine IV and the NetFlow Service Card.

The NetFlow statistics feature captures a set of traffic statistics. These traffic statistics include the source IP address, destination IP address, Layer 4 port information, protocol, input and output identifiers, and other routing information that can be used for network analysis, planning, accounting, billing and identifying DoS attacks.

NetFlow switching is supported on IP and IP-encapsulated traffic over all interface types.

If you enter the **ip route-cache flow infer-fields** command after the **ip route-cache flow** command, you will purge the existing cache, and vice versa. This action is done to avoid having flows with and without inferred information in the cache simultaneously.

For additional information on NetFlow switching, refer to the *Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide*.

Note NetFlow consumes additional memory and CPU resources compared to other switching modes. You need to know the resources required on your switch before enabling NetFlow.

Examples This example shows how to enable NetFlow switching on the switch:

```
Switch#conf t terminal
Switch(config)# ip route-cache flow
Switch(config)# end
Switch#sh
```

Note This command does not work on individual interfaces.

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

Command History

Release	Modification
12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

The **ip source binding** command is used to add a static IP source binding entry only.

The **no** form of this command deletes 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 terminal
Switch(config)# ip source binding 11.0.0.1 0100.0100.0100 vlan 10 interface
gigabitethernet2/18
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

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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# conf 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# conf 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

Command History	Release	Modification
	12.1(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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 IPv6 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 terminal
Switch(config)# no ip verify header vlan all
Switch(config)# end
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 to learn static IP address binding on a port. **port-security** (Optional) Filters both source IP and MAC addresses using the port security feature.

Defaults

IP source guard is disabled.

Command Modes

Global configuration mode

Command History	**Release**	**Modification**
	12.2(18)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.2(17b)AF	Added support for IP port security and tracking.

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)# ip dhcp snooping vlan 10 20
Switch(config)# interface fastethernet 6/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 10
Switch(config-if)# switchport trunk allowed vlan 10-20
Switch(config-if)# no ip dhcp snooping trust
Switch(config-if)# ip verify source vlan dhcp-snooping
Switch(config-if)# end
Switch# show ip verify source interface f6/1
Interface  Filter-type  Filter-mode  IP-address       Mac-address       Vlan
---------------------------------------------------------------------------
Fa6/1      ip-vlan      active       10.5.5.1                           10
Fa6/1      ip-vlan      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 configure commands, one per line.  End with CNTL/Z.
Switch(config)# interface fastethernet 5/36
Switch(config)# interface FastEthernet 4/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# ip device tracking maximum 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)# end
```

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 deletes 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 filters on a particular interface.

ip verify unicast source reachable-via

To enable and configure unicast RPF checks on a Supervisor Engine 6-E and Catalyst 4500M chassis 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

Command History

Release	Modification
12.2(40)SG	Support for this command was introduced on the Catalyst 4500 with a Supervisor Engine 6-E and the Catalyst 4500M chassis.

Usage Guidelines

In basic RX mode, unicast RPF ensures a source address must be reachable on the arrived interface. For example, the source must be reachable without load balancing.

Note Uses per RPF in 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 strict-only checking mode:

```
Switch(config)# 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.

ipv6 mld snooping

In multicast 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 4001 and 1006 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

Command History

Release	Modification
12.2(50)SG	This command was introduced on the Catalyst 4500.

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# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ipv6 mld snooping
Switch(config)# end
Switch#
```

This example shows how to disable MLD snooping on a VLAN:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# no ipv6 mld snooping vlan 11
Switch(config)# end
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 (MASQs) 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

Command History	**Release**	**Modification**
	12.2(40)SG	This command was introduced on the Catalyst 4500.

Usage Guidelines In MLD snooping, the IPv6 multicast switch periodically sends out queries in hosts belonging to the multicast group. If a host wants to leave a multicast group, it can identify leave or it can respond to the query within 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 the same port), the configured last-listener query count determines the number of MASQs that are sent before an MLD client is aged out.

When the last-listener query count is set for a VLAN, this count overrides the value configured globally. When the VLAN count is not configured (set to the default of 0), the global count is used.

VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in MLD snooping.

Examples

This example shows how to globally set the last-listener query count:

```
Switch(config)#ipv6 mld snooping last-listener-query-count 3
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#configure 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	Configure 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 VLAN.
show ipv6 mld snooping querier	Displays IP version6 (IPv6) MLD snooping querier related information most recently received by the switch or the VLAN.

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 issuing a MASQ before deleting a port from the multicast group. The range is 100 to 32,768. The default is 1000 (1 second).

Command Default

The default global query interval (maximum response time) is 1000 (1 second).

The default VLAN query interval (maximum response time) is 0 (the global count is used).

Command Modes

Global configuration mode

Command History

Release	Modification
12.2(20)EW	This command was introduced on the Catalyst 4500.

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 overridden. 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)#exit
Switch#wr
```

This example shows how to set the last-listener query interval for VLAN 1 to 5.5 seconds:

```
Switch#configure terminal
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#wr
```

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	Configure 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 version6 (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

Command History	Release	Modification
	12.2(52)SG	This command was introduced on the Catalyst 4500.

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-forwarding time. This prevents the forwarding of duplicate reports.

Examples This example shows how to enable MLD snooping listener message suppression:

```
Switch# configure 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# configure 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, use 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 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

Command History	**Release**	**Modification**
	12.2(50)SG	This command was introduced on the Catalyst 4500.

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 waits before deleting a listener that does not respond, and it applies to all VLANs that do not have a VLAN value set.

The robustness value configured for a VLAN overrides the global value. If the VLAN robustness value is 0 (the default), the global value is used.

VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in MLD snooping.

Examples

This example shows how to configure the global robustness variable so that the switch sends out three queries before it deletes a listener port that does not respond:

```
Switch(config)# ipv6 mld snooping robustness-variable 3
Switch(config)# end
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 1
Switch(config)# end
Switch#
```

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	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

Command History	Release	Modification
	12.2(25)EW	This command was introduced on the Catalyst 4500.

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** | **mrouter interface** *interface-id* | **static** *ipv6-multicast-address* **interface** *interface-id*]

no ipv6 mld snooping vlan *vlan-id* [**immediate-leave** | **mrouter interface** *interface-id*| **static** *ipv6-multicast-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. **mrouter interface** — (Optional) Configures a multicast switch port. The **no** form of the command removes the configuration. **static** *ipv6-multicast-address* — (Optional) Configures a multicast group with the specified IPv6 multicast address. **interface** *interface-id* — Adds a 3-port or 5-port to the group. The mrouter 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

Command History	Release	Modification
	12.2(18)SXD	This command was introduced on the Catalyst 6500.

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#conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ipv6 mld snooping vlan 1 immediate-leave
Switch(config)#end
Switch#
```

This example shows how to disible MLD immediate-Leave processing on VLAN 1:

```
Switch#conf 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#
```

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

```
Switch#conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ipv6 mld snooping vlan 1 mrouter interface gigabitethernet1/0/2
Switch(config)#end
Switch#
```

This example shows how to configure a static multicast group:

```
Switch#conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ipv6 mld snooping vlan 1 static FF12::10 interface gigabitethernet1/0/2
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 network (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

Command History	**Release**	**Modification**
	12.2(31)SG3	This command was introduced on the Catalyst 4500 series switch.

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 in the new version (EV) state.

When the **issu abortversion** command is entered before the **issu runversion** command, the standby supervisor engine is reset and reloaded 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(config)# issu abortversion 2
Switch(config)#
```

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
ioss supervisor-state	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 ioss 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 SSO 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.
Defaults	Rollback timer resets automatically 45 minutes after you enter the **issu runversion** command.
Command Modes	Privileged EXEC mode

Command History	Release	Modification
	12.2(52)SG	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

After you are satisfied with the new image and have confirmed the new supervisor engine is reachable by both the console and the network, enter the **issu acceptversion** command to halt the rollback timer. If the **issu acceptversion** command is not entered within 45 minutes from the time the **issu runversion** command is entered, the entire SSO process is automatically rollebacked 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 extended period, the rollback timer automatically stops. If the standby state is not, 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 SSU process to continue:

```
Switch(config)#issu acceptversion 2
Switch#
```

Table continued from

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 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.
	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-new*]

Syntax Description

standby-slot	Specifies the slot number for the currently active supervisor engine.
standby-image-new	(Optional) Name of the new image on the currently active supervisor engine.

Defaults

Enabled by default.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.2(17)SXA	This command was introduced on the Catalyst 6500 series switch.

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 *ios* version (RF) 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 Hot*ios* 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 Switchover Software Upgrade (SSU) process. This process cannot be stopped or reverted in original state without starting a new ISSU process.

Entering the **issu commitversion** command without entering the **issu acceptversion** command is allowed. The system will automatically accept the version after the **issu commitversion** command. 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 1
Switch#
```

Related Commands

Command	Description
ios as-rightversion	Halts the rollback timer and ensures that the new Cisco IOS software image is not automatically stopped during the ISSU process.
ios commitversion	Loads the new Cisco IOS software image into the new standby supervisor engine.
ios loadversion	Starts the ISSU process.
ios 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 iosu 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 detected to be incompatible.

Defaults	
This command has no default settings.	

Command Modes	
Privileged EXEC mode	

Command History	Release	Modification
	12.2(25)SG	This command was introduced on the Catalyst 4500 series switch.

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 onto 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:cmaa-image.2 4 slavehost:flash:cmm-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.

Command	Description
force-reload/reversion	Loads the new Cisco IOS software image into the new standby supervisor engine.
force-switchover	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 **issu loadversion** command, use the **issu runversion** command.

issu runversion *standby-slot* [*standby-image-name*]

Syntax Description	*standby-slot* Specifies the standby slot on the networking device. *standby-image-name* (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

Command History	**Release**	**Modification**
	12.2(17)SCA	This command was introduced on the Catalyst 6500 series switch.

Usage Guidelines

The **issu runversion** command changes the currently active supervisor engine to standby-supervisor engine and the 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 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:

```
Dual-active-known# issu runversion 2
Dual-active#
```

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 load-version	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

Command History	**Release**	**Modification**
	12.2(1)SX1A	This command was introduced on the Catalyst 6500 series switch.

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 uni state.

Examples This example shows how you can set the rollback timer value to 3600 seconds, or 1 hour:

```
Switch#configure terminal
Enter configuration commands, one per line.
Switch(config)#issu set rollback-timer 3600
Switch(config)#end
Switch#
```

Related Commands	**Command**	**Description**
	issu acceptversion	Holds 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

Command History

Release	Modification
12.2(18)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

You must store this command, with or without protocol types, to tunnel Layer 2 packets.

Layer 2 protocol tunneling across a service-provider network ensures that Layer 2 information is propagated across the network to all customer locations. When protocol tunneling is enabled, protocol packets are encapsulated and sent across the service-provider network. Encapsulated packets do not enter 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 g 1/1/1  l2protocol-tunnel cdp
Switch(config)# int g 1/1/1#
```

Related Commands

Command	Description
l2protocol-tunnel cos	Configures the class of service (CoS) value for all tunneled Layer 2 protocol packets.

Command	Description
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

Command History

Release	Modification
12.1(12EW)	This command was first introduced on the Catalyst 4500 series switch.

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 in 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

Command History	**Release**	**Modification**
	12.2(18)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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-if)# l2protocol-tunnel drop-threshold cdp 50
Switch(config-if)#
```

Related Commands

Command	Description
ipv6 protocol-tunnel	Enables protocol tunneling on an interface.
ipv6 protocol-tunnel cos	Configures the class of service (CoS) value for all tunneled Layer 2 protocol packets.
ipv6 protocol-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

Command History	**Release**	**Modification**
	12.2.18SX-F	Support for this command was introduced on the Catalyst 4500 series switch.

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 is specified with the keyword, the threshold is applied to each of the tunneled Layer 2 protocol types. If you also set a drop threshold 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 error is brought out of the error-disabled state and allowed to retry the operation again when 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 an **no shutdown** commands.

Examples This example shows how to configure the maximum rate:

```
Switch(config-if)# l2protocol-tunnel shutdown-threshold stp 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 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

Command History	Release	Modification
	12.1(12c)EW	This command was introduced on the Catalyst 4500 series switches.

Usage Guidelines

This command is not supported on the systems that are configured with a Supervisor Engine I.

You must assign no/lport in the switch lan 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 gi1/0/4 lacp port-priority 17063
Switch(config)#int gi1/0/4
```

Related Commands

Command	Description
channel-group	Assigns and configure 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.

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

Command History	Release	Modification
	12.1(13)EW	This command was introduced on the Catalyst 4500 series switches.

Usage Guidelines

This command is not supported on systems that are configured with a Supervisor Engine I.

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 27543
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 port-priority	Sets the priority of the system for LACP.
show lacp	Displays LACP information.

lldp run

To enable processing of received LLDP control packets and enable transmission of LLDP packets with default or configured TLVs,

lldp run

Syntax Description This command has no arguments or keywords.

Defaults LLDP is disabled.

Command Modes global configuration mode

Command History

Release	Modification
12.2(33)SXI	Support was introduced on the Catalyst 6500 series switch.

Usage Guidelines Configuring this command enables LLDP protocol on the switch. Unconfiguring it disables processing or transmit of LLDP protocol packets from the switch.

Examples This example shows how to enable LLDP on the switch:

```
Switch(config)# lldp run
```

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

Command History	Release	Modification
	12.2(25)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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# config 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

Command History

Release	Modification
12.2(25)SG	Support for this command was introduced on the Catalyst 6500 series switch.

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 gi1/1:

```
Switch# conf t terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface gi1/1
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 gi1/1
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 gi1/1:

```
Switch# conf t terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gi1/1
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

Command History	Release	Modification
	12.2(25)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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)# end
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

Command History	Release	Modification
	12.2(52)SG	Support for this command was introduced on the Catalyst 6500 series switch.

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 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 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 gi1/1:

```
Switch#conf t terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface gi1/1
Switch(config-if)#logging event trunk-status enw(global)
Switch(config-if)#end
Switch#
```

Related Commands	Command	Description
	logging event trunk-status global (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

Command History

Release	Modification
12.2(25)EW	Support for this command was introduced.

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 authentication frames 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 authorization	Displays Authorization 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

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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 enter the following subset to create or delete entries in a MAC layer access list:

{**permit**|**deny**} {*protocol-number* |**any**} [*dscp-value mask*] | {**protocol-family** {**appletalk** | **arp-non-ipv4**| **decnet** |**ips** | **ipx**|**rarp-ipv4**| **sarp-non-ipv4** | **vines**| **xns**} | <*arbitrary offset*><*/ name-called offset*>]

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 offset<*/ name-called offset*>	Optionally Specifies an arbitrary offset/name in the range 1 bits to 65535. (Internal or Ethernet)
deny	Prevents access if the conditions are matched.

Table 2-7 mac access-list extended Subcommands (continued)

Subcommand	Description
dest-mac mask	(Optional) Specifies a destination MAC address of the form: *dest-mac address dest-mac-address mask*.
name-value ethertype	(Optional) Denotes a predefined name-valued ethertype for common protocols: arp—AppleTalk ARP ether—DEC-Ether applerait—AppleTalk ElterTalk 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 lsc-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
no	(Optional) Deletes a statement from an 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 assigned 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-Ip-v4	0x0806 and protocol header of Arp is a non-Ip protocol family
Decnet	0x6000-0x6009, 0x8038-0x8042

Table 2-6 Mapping an Ethernet Packet to a Protocol Family

Protocol Family	Ethertype in Packet Header
Ipx	0x8137 0x8138
Ipv6	0x86DD
Rarp-Ipv4	0x8035 and protocol header of Rarp-Ipv4
Rarp-Non-Ipv4	0x8035 and protocol header of Rarp-a non-Ipv4 protocol family
Vines	0x0BAD, 0x0BAE, 0x0BAF
Xns	0x0600, 0x0807

When you enter the *src-mac mask* or *dest-mac mask* value, follow these guidelines:

- Enter the MAC addresses as three 4-byte values in dotted hexadecimal format such as 0110.2222.0001.
- Enter the MAC address masks as three 4-byte values in dotted hexadecimal format. Use 1 for as a wildcard. For example, to match an address exactly, use 0000.0000.0000 (can be entered as 0110).
- For the optional *protocol* parameter, you can enter either the EtherType or the keyword.
- Entries without a protocol parameter match any protocol.

The access list 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 in 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 0000.4700.0000, which is going to 0000.4700.0000, and permits all other traffic:

```
Switch(config)# mac access-list extended mac_layer
Switch(config-ext-macl)# deny 0000.4700.0000 0.0.0 0000.4700.0000 0.0.0 protocol-family
appletalk
Switch(config-ext-macl)# permit any any
Switch(config-ext-macl)# 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

Command History	**Release**	**Modification**
	12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW	Support for extended addressing was added.

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)# no 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 in both 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

Command History	**Release**	**Modification**
	12.2(18)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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
Mcast State:
vlan  mac address     type        protocols          port
-----+---------------+--------+---------------+--------------------
1     0001.0000.0001  dynamic  ip,other       Gigabit Ethernet 1/1
1     0001.0204.0850  dynamic  ip             Gigabit Ethernet 1/1
1     0001.0236.a0c4  dynamic  ip,mcast grnd  Gigabit Ethernet 1/1
1     0001.4700.0b14  dynamic  ip             Gigabit Ethernet 1/1
1     0001.4700.0b15  dynamic  other          Gigabit Ethernet 1/1
1     0001.4700.0b16  dynamic  ip             Gigabit Ethernet 1/1
1     0001.4700.0b41  dynamic  ip             Gigabit Ethernet 1/1
1     0001.4700.0b42  dynamic  ip             Gigabit Ethernet 1/1
```

```
1    0015.9a06.4538  dynamic  ip          10.gabri03c3ecsw1/1:1
1    0016.3e8a.4a40  dynamic  ip          10.gabri03c3ecsw1/1:1
1    0016.3f26.3ac2  dynamic  ip          10.gabri03c3ecsw1/1:1
1    0016.5e5b.8e03  dynamic  ip          10.gabri03c3ecsw1/1:1
1    0016.5e5b.8e04  dynamic  ip          10.gabri03c3ecsw1/1:1
1    0016.5e5b.8e05  dynamic  ip          10.gabri03c3ecsw1/1:1
1    0016.5e5f.0437  dynamic  ip          10.gabri03c3ecsw1/1:1
1    0016.5e5f.0438  dynamic  ip          10.gabri03c3ecsw1/1:1
1    0016.5e5f.0439  dynamic  ip          10.gabri03c3ecsw1/1:1
1    0016.5e5f.0996  dynamic  ip          10.gabri03c3ecsw1/1:1
1    0016.5e8b.4a70  dynamic  ip          10.gabri03c3ecsw1/1:1
1    0016.c16d.2b40  dynamic  ip          10.gabri03c3ecsw1/1:1
1    0017.3f9a.0a00  dynamic  ip          10.gabri03c3ecsw1/1:1
1    0018.c1d5.b400  dynamic  ip          10.gabri03c3ecsw1/1:1
1    0037.a997.7b88  dynamic  ip          10.gabri03c3ecsw1/1:1
1    0037.a9a0.5a00  dynamic  ip          10.gabri03c3ecsw1/1:1
1    0037.a9a8.5a00  dynamic  ip          10.gabri03c3ecsw1/1:1
1    0038.5f5a.f148  dynamic  ip          10.gabri03c3ecsw1/1:1
1    0038.5f5a.f149  dynamic  ip          10.gabri03c3ecsw1/1:1
1    0039.7ba6.f14f  dynamic  ip          10.gabri03c3ecsw1/1:1
1    0012.d3b2.c078  dynamic  ip          10.gabri03c3ecsw1/1:1
1    0012.d3b2.c079  dynamic  ip          10.gabri03c3ecsw1/1:1
1    0012.d3b2.c07a  dynamic  ip          10.gabri03c3ecsw1/1:1
1    0012.da2c.91ab  dynamic  ip          10.gabri03c3ecsw1/1:1
1    0012.da2c.d3f0  dynamic  ip          10.gabri03c3ecsw1/1:1
1    0040.ce6f.2faa  dynamic  ip          10.gabri03c3ecsw1/1:1
1    0040.d0b8.4a00  dynamic  ip          10.gabri03c3ecsw1/1:1
1    0040.5f3d.4e00  dynamic  ip          10.gabri03c3ecsw1/1:1
1    0040.b771.e9ac  dynamic  ip          10.gabri03c3ecsw1/1:1
1    0040.b7f8.1f00  dynamic  ip          10.gabri03c3ecsw1/1:1
1    0040.b7f8.1f80  dynamic  ip          10.gabri03c3ecsw1/1:1
1    0040.b7fa.4f00  dynamic  ip          10.gabri03c3ecsw1/1:1
1    0040.bc9a.0f00  dynamic  ip          10.gabri03c3ecsw1/1:1
1    0040.bc9b.0f00  dynamic  ip          10.gabri03c3ecsw1/1:1
1    0040.d4bc.a040  dynamic  ip          10.gabri03c3ecsw1/1:1
1    0040.d5c4.d07a  dynamic  ip          10.gabri03c3ecsw1/1:1
1    0050.2012.40a6  dynamic  ip          10.gabri03c3ecsw1/1:1
Switch#
```

This example shows how to assign MAC addresses that belong to either the "ip" or the "other" bucket to both buckets:

```
Switch#conf t mac-address-table dynamic group protocols ip other
Enter configuration commands, one per line.
Switch#show mac-address-table dynamic
Unicast Entries
 vlan  mac address     type        protocols   port
-------+---------------+--------+-----------+----------------
 1     0000.0000.5000  dynamic  ip,other   10.gabri03c3ecsw1/1:1
 1     0000.0000.5001  dynamic  ip,other   10.gabri03c3ecsw1/1:1
 1     0000.4700.3a40  dynamic  ip,other   10.gabri03c3ecsw1/1:1
 1     0000.4716.0475  dynamic  ip,other   10.gabri03c3ecsw1/1:1
 1     0000.4716.7fc0  dynamic  ip,other   10.gabri03c3ecsw1/1:1
 1     0000.4716.8041  dynamic  ip,other   10.gabri03c3ecsw1/1:1
 1     0000.4716.a0ac  dynamic  ip,other   10.gabri03c3ecsw1/1:1
 1     0000.4716.a0ae  dynamic  ip,other   10.gabri03c3ecsw1/1:1
 1     0000.5a8a.24a2  dynamic  ip,other   10.gabri03c3ecsw1/1:1
 1     0000.5a8a.24a3  dynamic  ip,other   10.gabri03c3ecsw1/1:1
 1     0000.5f26.3ac2  dynamic  ip,other   10.gabri03c3ecsw1/1:1
 1     0000.5e5b.8e03  dynamic  ip,other   10.gabri03c3ecsw1/1:1
 1     0000.5e5b.8e04  dynamic  ip,other   10.gabri03c3ecsw1/1:1
 1     0000.5e5b.8e05  dynamic  ip,other   10.gabri03c3ecsw1/1:1
 1     0000.5e5f.0437  dynamic  ip,other   10.gabri03c3ecsw1/1:1
 1     0000.5e5f.0438  dynamic  ip,other   10.gabri03c3ecsw1/1:1
```

```
1    0014.5e54.0f09   dynamic  ip,other        GigabitEthernet3/1
1    0014.5e54.0f0a   dynamic  ip,other        GigabitEthernet3/1
1    0014.5e54.0f7f   dynamic  ip,other        GigabitEthernet3/1
1    0014.5e80.9042   dynamic  ip,other        GigabitEthernet3/1
1    0014.5e80.9043   dynamic  ip,other        GigabitEthernet3/1
1    0014.5e80.9073   dynamic  ip,other        GigabitEthernet3/1
1    0014.c0e6.3e40   dynamic  ip,other        GigabitEthernet3/1
1    0014.c0e6.3e41   dynamic  ip,other        GigabitEthernet3/1
1    0014.c1b0.b8b0   dynamic  ip,other        GigabitEthernet3/1
1    0015.6ba2.7c5a   dynamic  mcast,grmd      GigabitEthernet3/1
1    0017.a957.7e2d   dynamic  ip,other        GigabitEthernet3/1
1    0017.a957.7e54   dynamic  ip,other        GigabitEthernet3/1
1    0017.a9b9.0e0a   dynamic  ip,other        GigabitEthernet3/1
1    0017.a9c9.2ce4   dynamic  ip,other        GigabitEthernet3/1
1    0018.b9ba.f148   dynamic  ip,other        GigabitEthernet3/1
1    0018.b9ba.f149   dynamic  ip,other        GigabitEthernet3/1
1    0021.2f47.c7c7   dynamic  ip,other        GigabitEthernet3/1
1    0021.2f47.97e1   dynamic  ip,other        GigabitEthernet3/1
1    0021.2f47.97e2   dynamic  ip,other        GigabitEthernet3/1
1    0021.6a92.2b4e   dynamic  ip,other        GigabitEthernet3/1
1    0021.6a92.a47f   dynamic  ip,other        GigabitEthernet3/1
1    0021.6a92.a480   dynamic  ip,other        GigabitEthernet3/1
1    0240.1a24.2c4e   dynamic  mcast,grmd      GigabitEthernet3/1
1    0240.3c77.c6ba   dynamic  ip,other        GigabitEthernet3/1
1    0240.3c77.c6ba   dynamic  ip,other        GigabitEthernet3/1
1    0240.3c78.de1d   dynamic  ip,other        GigabitEthernet3/1
1    0240.3c78.de1d   dynamic  ip,other        GigabitEthernet3/1
1    0240.4c76.d7b1   dynamic  ip,other        GigabitEthernet3/1
1    0240.4c82.6b42   dynamic  ip,other        GigabitEthernet3/1
1    0240.4c82.6b42   dynamic  ip,other        GigabitEthernet3/1
1    0240.4c84.c9b1   dynamic  ip,other        GigabitEthernet3/1
1    0800.2085.b409   dynamic  ip,other        GigabitEthernet3/1
Switch#
```

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** *inv_value*]] | [**mac-move**] | [**threshold** [**limit** *percentage*] | **interval** *time*]] | [**learn-fail**[**interval** *time* | **limit** *num_fail*]]

no mac-address-table notification [**change** [**history-size** *hs_value* | **interval** *inv_value*] | | [**mac-move**] | [**threshold** [**limit** *percentage* | **interval** *time*] | [**learn-fail**[**interval** *time* | **limit** *num_fail*]]

Syntax Description

change	(Optional) Specifies enabling MAC change notification.
history-size *hs_value*	(Optional) Specifies a maximum number of entries in the MAC change notification history table. The range is 0 to 500 entries.
interval *inv_value*	(Optional) Specifies a notification trap interval the set interval time between two consecutive traps. The range is 0 to 2147483647 seconds.
mac-move	(Optional) Specifies enabling MAC move notification traps.
threshold	(Optional) Specifies enabling MAC threshold notification.
limit *percentage*	(Optional) Specifies the percentage of MAC utilization threshold; valid values are from 1 to 100 percent.
interval *time*	(Optional) Specifies the time between MAC threshold notifications; valid values are greater than or equal to 120 seconds.
learn-fail	(Optional) Specifies syslog (level 6) notification of failures to install MAC addresses learned in software into hardware. Disabled by default.
interval *time*	(Optional) Specifies the syslog interval between hardware MAC learning failure notifications. The default value is 150 seconds. The range is between 1 to 100000 seconds.
limit *num_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

Command History	Release	Modification
	12.2(25)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.2(52)SG	Support for this **mac-address-table notification** keyword, Supervisor Engine V-10, and Catalyst 4900M chassis added.

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 notification.
snmp trap mac-notification change	Enables SNMP MAC address notification.

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 configurations, 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

Command History

Release	Modification
12.1(12)EW	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

When a static MAC address is installed, it is associated with port.

The output interface specified must be a Layer 2 interface and not an SVI.

If you do not mess 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 addresses.

When removing a MAC address, entering **interface** *type* is optional. For unicast entries, the entry is removed automatically. For multicast entries, if you do not specify an interface, the entire entry is removed. You can specify the selected ports to be removed by specifying the interface.

Examples

This example shows how to add the static entries to the MAC address table:

```
Dak(config)# mac-address-table static 0001.0a81.c8d0 vlan 200 interface fastethernet1/7
Dak(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

Command History	Release	Modification
	12.2(31)SG	Support for this command was introduced on the Catalyst 4500 series switch.

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 the macro are as follows:

```
# Basic interface - Enable data VLAN only
# Recommended value for access vlan (VLAN) 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
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 bpdugard 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 SAVID *access_vlanid***DVID** *voice_vlanid*

Syntax Description	**SAVID** *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

Command History	Release	Modification
	12.2(18)EW	Support for this command was introduced on the Catalyst 2950 series switch.

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 fastethernet5/1
Switch(config-if)# macro apply cisco-phone SAVID 10 DVID 50
Switch(config-if)#
```

The contents of this macro are as follows:

```
# VoIP enabled interface - Enable data VLAN
# and voice VLAN (VVID)
# Change the port to access
switchport access vlan $SAVID [access_vlan_id]
switchport mode access
# Update the Voice VLAN(VVID) value which should be
# different from data VLAN
# Recommended value for voice vlan (VVID) should not be 1
switchport voice vlan $DVID [voice_vlan_id]
# Enable port security limiting port to a 3 MAC
# addresses -- One for desktop and two for phone
switchport port-security
switchport port-security maximum 3
# ensure port-security ages is greater than one minute
# and use inactivity timer
switchport port-security violation restrict
switchport port-security aging time 2
```

```
switchport port-security aging type inactivity
switchport port-security aging time 2 vlan 1-4094
macro phone voip vlan2-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_vlan id*

Syntax Description

SNVID *native_vlan id*	Specifies a native VLAN ID.

Defaults

This command has no default settings.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.2(31)SGW	Support for this command was introduced on the Catalyst 4500 series switch.

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 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
# To disable port security on trunk ports
# Recommended value for native vlan (VLAN) should not be 1
switchport trunk native vlan VLAN [native_vlan_id]
# Update the allowed VLAN range (VLANRL) such that it
# includes data, voice and native VLANs
# switchport trunk allowed vlan VLANRL [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
mls qos trip trust
qos trust dscp
```

```
8 Ethernet fast ethernet to the network when enabling the interface.
Ethernet fast ethernet to the access cannot become active on the interface.
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 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 SWVID *native_vlanid*

Syntax Description	**SWVID** *native_vlanid* Specifies a native VLAN ID.

Defaults

This command has no default settings.

Command Modes

Interface configuration mode

Command History	Release	Modification
	12.2(31)SGW	Support for this command was introduced on the Catalyst 4500 series switch.

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(config)# interface FastEthernet2/1
Switch(config-if)# macro apply cisco-switch SWVID 45
Switch(config-if)#

The contents of the macro are as follows:
# Access Uplink to Distribution
# Enable port security globally
# To disable port security on trunk ports
# Recommended value for native vlan (SWVID should not be 1
switchport trunk native vlan SWVID [native_vlan_id]
# Update the allowed VLAN range (VRANGE) such that it
# includes data, voice and native VLANS
# switchport trunk allowed vlan VRANGE
# Hardcode trunk and disable negotiation to
# speed up convergence
switchport mode trunk
switchport nonegotiate
# Port Fast and BPDU Guard this interface
spanning-tree portfast
# BDI:A defines the link as priority 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 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

Command History	Release	Modification
	12.2(20)EWA	Support for this command was introduced on the Catalyst 4500 series switch.

Examples These examples show how to apply the system-defined default to the switch:

```
Switch(config)# macro global apply cisco-global
Changing VTP domain name from qwq-vtp to [smartports] Device mode already VTP TRANSPARENT.
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

Command History	Release	Modification
	12.2(1)SG	Support for this command was introduced on the Catalyst 4500 series switch.

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

Command History

Release	Modification
12.2(25)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

This command associates comment text, or the macro name, with a switch. When multiple macros are applied on a switch, the description text will be from the last applied macro.

Examples

This example shows how to add a description to a switch:

```
Switch(config)# macro global description uplink 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 *cisco-global*	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

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.2(20)EW	Enhanced to enable automatic synchronization of the configuration files in NVRAM.

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 After you enter the main CPU submode, you can use the **auto-sync** command to automatically synchronize the configurations between the primary and secondary routes on a route-processor redundancy pair. In addition, you can use all of 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 commands in the startup-config and config-register configuration of the active supervisor engine with the standby supervisor engine. The updates for the boot variables are automatically generated.

```
Switch(config)#r m
Switch(config-r-m)#? main-cpu
Switch(config-r-m)#? auto-sync standard
Switch(config-r-m)#? auto-sync
Switch(config-r-m)# auto-sync standard-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

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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 yanyoo10 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.

Non-Supervisor Engine 6-E

match [**access-group** *acl-index-or-name* | **any** | **cos** *cos-list* | [**ip**] **dscp** *dscp-list* | [**ip**] **precedence** *ip-precedence-list*

no match [**access-group** *acl-index-or-name* | **any** | **cos** *cos-list* | [**ip**] **dscp** *dscp-list* | [**ip**] **precedence** *ip-precedence-list*

Supervisor Engine 6-E and Catalyst 6500M chassis

match [**access-group** *acl-index-or-name* | **any** | **cos** *cos-list* | [**ip**] **dscp** *dscp-list* | [**ip**] **precedence** *ip-precedence-list*| **qos-group** *value* | **protocol** [**ip** | **ipv6** | **arp**]

no match [**access-group** *acl-index-or-name* | **any** | **cos** *cos-list* | [**ip**] **dscp** *dscp-list* | [**ip**] **precedence** *ip-precedence-list*| **qos-group** *value* | **protocol** [**ip** | **ipv6** | **arp**]

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 ranges 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 a pre-defined qos-group value assigned to a packet on the input qos classification.
	protocol ip — Specifies IP for the Ethernet header. The match criteria are supported on the Supervisor Engine 6-E and Catalyst 6500M chassis. Though visible in the command-line help strings, the only protocol types supported are IP, IPv6, and ARP.

protocol ipv6	Specifies IPv6 in the Ethernet header. The match criteria are supported on the Supervisor Engine 6-E and Catalyst 6500M chassis. 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. The match criteria are supported on the Supervisor Engine 6-E and Catalyst 6500M chassis. 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

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 6500 series switches.
12.2(40)SG	Added support for the Supervisor Engine 6-E and Catalyst 6500M chassis.
12.2(18)SXD	Added support for the **match protocol arp** command on the Supervisor Engine 6-E and Catalyst 6500M chassis.

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 establish. 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** *dscp dscp-list* or the **match ip precedence** *ip-precedence-list* command, you can enter a numerous name for a commonly used value. For example, you can enter **match dscp af11** command, which is the same as entering **match dscp 10** command. You can enter the **match ip precedence critical** command, which is the same as entering the **match ip precedence 5** command. For a list of supported mnemonics, enter the **match dscp** *?* or the **match ip precedence** *?* command to see 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 use either the **ip** prefix or the protocol **ip** keyword.

To match only ARP packets, you must use the **match protocol arp** command.

You can configure the **match** *mac access-list*, **match** *vlan dscp dscp-list*, **match ip precedence** *ip-precedence-list* command in a class map within a policy map.

The **match** *cos* *cos-list* command applies only to Ethernet frames that carry a VLAN tag.

The **match qos-group** command is used by the class-map to uniquely 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 2-62.

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 match-any class1
Switch(config-cmap)#match ip precedence 5 6 7
Switch(config-cmap)#match ipv6 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#configure terminal
Switch(config)#class-map match-all ipv6 only
Switch(config-cmap)#match dscp ef1
Switch(config-cmap)#match ipv6 protocol tcpv6
Switch(config-cmap)#exit
Switch#
```

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 recent flows with a unique source or destination address as new flows, use the **match flow ip** command. To disable this feature, 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 L4 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

Command History	**Release**	**Modification**
	12.2(25)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.2(25)EW1	Support for the full flow option was added.

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 map is called a *flow-based policy map* when you configure the flow keywords on the class map that it uses. To attach 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 4500 series switch only when Supervisor Engine VI (WS-X4516-10GE-6) 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
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 c1
Switch(config-cmap)# match flow ip destination-address
Switch(config-cmap)# end
Switch#
Switch# show class-map c1
Class Map match-all c1 (id 2)
   Match flow ip destination-address
Switch#
```

Assume there are two active flows on the Fast Ethernet interface 6/1 with source addresses 192.168.10.20 and 192.168.10.21. The following example shows how to maintain each flow to 1 Mbps with an allowed burst value of 9000 bytes:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# class-map c1
Switch(config-cmap)# match flow ip source-address
Switch(config-cmap)# exit
Switch(config)# policy-map p1
Switch(config-pmap)# class c1
Switch(config-pmap-c1)# police 1000000 9000
Switch(config-pmap-c1)# 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: c1 (match-all)
      15412263 packets
      Match: flow ip source-address
      police: Per-interface:
        Conform: 24095634 bytes Exceed: 237095634 bytes

    Class-map: class-default (match-any)
      0 packets
      Match: any
      0 packets
Switch#
```

This example shows two entire flows on the Fast Ethernet interface 6/1 with destination addresses of 192.168.20.20 and 192.168.20.21. The following example shows how to mismatch one flow in 5 Mbps with an allowed burst value of 9000 bytes:

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#class-map c1
Switch(config-cmap)# match flow ip destination-address
Switch(config-cmap)# exit
Switch(config)# class-map c2
Switch(config-cmap)# match class c1
Switch(config-cmap)# police 5000000 9000
Switch(config-cmap)# exit
Switch(config)# exit
Switch(config)# interface fastethernet/1
Switch(config-if)# service-policy input p1
Switch(config-if)# exit
Switch# write memory

Switch# show policy-map interface
FastEthernet/1

  Service-policy input: p1

    Class-map: c1 (match-all)
      290237 packets
      match: class c1 (match-any)
      police Per-interface:
        Conform: 4245324 bytes Exceed: 4784574208 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 6/1:

Switch#sp          Switch#sp  Switch#show flowmask flowlabel
                   ecial      -d -i -v -f -p -s -t -l -m -n -o -r -u
192.168.10.10      192.168.20.20   20    6789    61
192.168.10.10      192.168.20.21   20    6789    21

With the following configuration, each flow is policed to a 5000000 bps with an allowed 9000-byte burst value.
```

Note If you use the **match flow ip source-address/protocol/destination-address** command, these two flows are consolidated into one flow because they have the same source and destination address.

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# class-map c1 match flow ip source-address ip destination-address ip protocol 16
source-port 16 destination-port
Switch(config-cmap)# exit
Switch(config)# policy-map p1
Switch(config-pmap)# class c1
Switch(config-pmap-c)# police 5000000 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)# exit
Switch# write memory
Switch# show policy-map interface
FastEthernet0/1

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 conform-action transmit exceed-action drop
!
interface FastEthernet 0/1
  service-policy input p1

Switch# show class-map c1
Class-map match-any 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 bytes conform-action transmit exceed-action drop

Switch# show policy-map interface
  FastEthernet0/1

    Service-policy input: p1

      Class-map: c1 (match-all)
        1542132 packets
        Match: flow ip source-address ip destination-address ip protocol 14 source-port 14
destination-port
        police: cbs,tbs,interface
          limiter 4289054 bytes Exceed: 1178891424 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 configurations 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

Command History

Release	Modification
12.2(33)SXI	Support for this command was introduced on the Catalyst 6500 series switch.
12.2(18)SXF	Added supported and unsupported linecard information to the usage guidelines.

Usage Guidelines The following linecards support Auto-MDIX through the CLI on their copper media ports: WS-X6124-RJ45, WS-X6148-RJ45 (hardware revision 3.0 or higher), and WS-X6224-GB-RJ45 (hardware revision 3.0, or higher), WS-X6824-GE-RJ45, and WS-6848-RJ45V-vl (Auto-MDIX support when inline power is disabled on the port).

Linecards that support auto-MDIX by default when port auto-negotiation enabled and cannot be tested off using **no mdix** CLI command include: WS-X6148-GE-RJ45, WS-X6148-GE-RJ45, WS-X6824-GE-RJ45, WS-X6824-GE-RJ45V, and WS-X6824-SFP.

Linecards that cannot support auto-MDIX functionality, either by default or CLI commands, include: WS-X6148-GE-RJ45V, WS-X6224-GB-RJ45V, WS-X6816-GBE-T, WS-X6148-45, WS-X6148-RJ21V, WS-X6248-RJ45V, WS-X6224-RJ45V, and WS-X6232-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 3/1
Switch(config-if)# speed auto 10 100 half-duplex|full
Switch(config-if)# duplex 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.
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

Command History	**Release**	**Modification**
	12.2(2)SXF6	Support for this command was introduced for the WS-X6704-10G-T module and the WS-X6848 chassis.

Usage Guidelines This command is supported on all ports on the WS-X6704-10G-T module and ports 1/45–48 on the WS-X6848 chassis.

Entering the **show interface capabilities** command provides the Multiple Media Types field, which displays the value **no** 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 5/45 on a WS-X6848 chassis to use the RJ-45 connector:

```
Switch(config)# interface gigabitethernet 5/45
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

For Catalyst 4500 series switches that are configured with Supervisor Engine III+, Supervisor Engine IV, and Supervisor Engine V, the defaults are as follows:

- SSO if the supervisor engine is using Cisco IOS Release 12.2(20)EWA.
- RPR if the supervisor engine is using Cisco IOS Release 12.2(20)EW through 12.2(50)SG as well as 12.1(19)EW.

Note If you are upgrading the current supervisor engine from Cisco IOS Release 12.2(20)EW or earlier releases to 12.2(20)EWA, and the RPR mode has been saved to the startup configuration, both supervisors reload continuously upon a switch-over. RPR mode after the software upgrade. To use SSO mode, you must manually change the redundancy mode to SSO.

Command Modes Redundancy configuration mode

Command History	**Release**	**Modification**
	12.2(20)EWA	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

RPR and SSO mode 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 modules 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 restarted.
- The FIB tables are cleared on a switchover. Routed traffic is interrupted until route tables reconverge.

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-r-ash)# mode sso
Switch(config-r-ash)#
```

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	Displays redundancy facility information.
show running-config	Displays the running configuration of a switch.

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 form of this command.

monitor session *session* {**destination interface** {**FastEthernet** *interface-number*} [**Ethernet**] **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_id*] [**rspan** [**space** *space_id*] | **sup** | **sup-tx** | **sup-rx** | **sup-ip** | **sup-ipx** | **sup-mac** | **sup-eigrp** | **sup-pim** | **sup-igmp** | **sup-arp** | **sup-bridge** | **sup-vtp** | **sup-dtp** | **sup-udld** | **sup-cdp** | **sup-pagp** | **sup-lacp** | **sup-dot1x** | **sup-sw** | **sup-all**} | **filter** {**vlan** *vlan_id*[,*vlan_id*[,*vlan_id*[,*vlan_id*]]] | {**ip-access-group** [*name*] [**ip**] | **mac-access-group** [*name*] [**ip**] | **packet-type** {**good** | **bad**} | **address-type** {**unicast** | **multicast** | **broadcast**} | **ipv** {**6** | **4**}}]

no monitor session *session* {**destination interface** {**FastEthernet** *interface-number*} [**Ethernet**] **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_id*] [**rspan** [**space** *space_id*] | **sup** | **sup-tx** | **sup-rx** | **sup-ip** | **sup-ipx** | **sup-mac** | **sup-eigrp** | **sup-pim** | **sup-igmp** | **sup-arp** | **sup-bridge** | **sup-vtp** | **sup-dtp** | **sup-udld** | **sup-cdp** | **sup-pagp** | **sup-lacp** | **sup-dot1x** | **sup-sw** | **sup-all**} | **filter** {**vlan** *vlan_id*[,*vlan_id*[,*vlan_id*[,*vlan_id*]]] | {**ip-access-group** [*name*] [**ip**] | **mac-access-group** [*name*] [**ip**] | **packet-type** {**good** | **bad**} | **address-type** {**unicast** | **multicast** | **broadcast**} | **ipv** {**6** | **4**}}]

Supervisor Engine 6 and Catalyst 6500 clients

monitor session *session* {**destination interface** {**FastEthernet** *interface-number*} [**Ethernet**] **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_id*] [**rspan** [**space** *space_id*] | **sup** | **sup-tx** | **sup-rx** | **sup-ip** | **sup-ipx** | **sup-mac** | **sup-eigrp** | **sup-pim** | **sup-igmp** | **sup-arp** | **sup-bridge** | **sup-vtp** | **sup-dtp** | **sup-udld** | **sup-cdp** | **sup-pagp** | **sup-lacp** | **sup-dot1x** | **sup-sw** | **sup-all**} | **filter** {**vlan** *vlan_id*[,*vlan_id*[,*vlan_id*[,*vlan_id*]]] | {**ip-access-group** [*name*] [**ip**] | **mac-access-group** [*name*] [**ip**] | **packet-type** {**good** | **bad**} | **address-type** {**unicast** | **multicast** | **broadcast**} | **ipv** {**6** | **4**}}

monitor session *session* {**destination interface** {**FastEthernet** *interface-number*} [**Ethernet**] **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_id*] [**rspan** [**space** *space_id*] | **sup** | **sup-tx** | **sup-rx** | **sup-ip** | **sup-ipx** | **sup-mac** | **sup-eigrp** | **sup-pim** | **sup-igmp** | **sup-arp** | **sup-bridge** | **sup-vtp** | **sup-dtp** | **sup-udld** | **sup-cdp** | **sup-pagp** | **sup-lacp** | **sup-dot1x** | **sup-sw** | **sup-all**} | **filter** {**vlan** *vlan_id*[,*vlan_id*[,*vlan_id*[,*vlan_id*]]] | {**ip-access-group** [*name*] [**ip**] | **mac-access-group** [*name*] [**ip**] | **packet-type** {**good** | **bad**} | **address-type** {**unicast** | **multicast** | **broadcast**} | **ipv** {**6** | **4**}}

monitor session *session* {**destination interface** {**FastEthernet** *interface-number*} [**Ethernet**] **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_id*] [**rspan** [**space** *space_id*] | **sup** | **sup-tx** | **sup-rx** | **sup-ip** | **sup-ipx** | **sup-mac** | **sup-eigrp** | **sup-pim** | **sup-igmp** | **sup-arp** | **sup-bridge** | **sup-vtp** | **sup-dtp** | **sup-udld** | **sup-cdp** | **sup-pagp** | **sup-lacp** | **sup-dot1x** | **sup-sw** | **sup-all**} | **filter** {**vlan** *vlan_id*[,*vlan_id*[,*vlan_id*[,*vlan_id*]]] | {**ip-access-group** [*name*] [**ip**] | **mac-access-group** [*name*] [**ip**] | **packet-type** {**good** | **bad**} | **address-type** {**unicast** | **multicast** | **broadcast**} | **ipv** {**6** | **4**}}

[**adj-same-if** [*ok*] | **bridge-cpu** [*ok*] | **ip-option** [*ok*] | **ipsk-scope-check-fail** [*ok*] | **l2-no-index-check-fail** [*ok*] | **mac-acl-fail** [*ok*] | **non-ospf** [*ok*] | **output-acl** [*ok*] | **tt-expired** [*ok*] | **uacc-if-fail** [*ok*] | **ttl-forward-forward** [*ok*] | **glean** [*ok*] | **receive** [*ok*] | **rpf-fail** [*ok*] | **acc-vio** [*ok*] | **mac-redirect** [*ok*] | **mac-table-miss** [*ok*] | **no-adj** [*ok*] | **no-route** [*ok*] | **fibre** [**ip access-group** [*name* | *idx*] | **class** [*cos*] | [*qos-tunnel-type* | **good** | **bad**]] | **address-type** [**unicast** | **multicast** | **broadcast**] | [**to** | **both**]

Syntax Description		
	session	Number of a SPAN session; valid values are from 1 to 6.
	destination	Specifies a SPAN destination.
	interface	Specifies an interface.
	FastEthernet *interface-number*	Specifies a Fast Ethernet module and port number; valid values are from 1 to 6.
	GigabitEthernet *interface-number*	Specifies a Gigabit Ethernet module and port number; valid values are from 1 to 16.
	encapsulation	(Optional) Specifies the encapsulation type of the destination port.
	isl	(Optional) Specifies ISL encapsulation.
	dot1q	(Optional) Specifies 802.1Q encapsulation.
	ingress	(Optional) Indicates whether the ingress option is enabled.
	vlan *vlan_id*	(Optional) Specifies the VLAN; valid values are from 1 to 4094.
	learning	(Optional) Enables host learning on ingress forwarding destination port.
	remote vlan *vlan_id*	Specifies an RSPAN source or destination session on a switch.
	source	Specifies a SPAN source.
	Port-channel interface-number	Specifies a port-channel interface; valid values are from 1 to 64.
	tcp	Causes traffic arrival on some form the CPU to be copied to the destination of the session.
	queue *queue_id*	(Optional) Specifies that only traffic received on the specified queue is copied to the destination of the session. Valid values are from 1 to 64, or by the following names: all, control-packet, error, mtu-exceeded, unknown-port-vlan-mapping, unknown-sa, rpf, input, acl input copy, acl input error, acl input forward, acl input punt, acl output, acl output copy, acl output error, acl output forward, acl output punt, l2-forward, adj-same-if, bridge-cpu, ip-option, ipsk-scope-check-fail, l2-no-index-check-fail, mac-acl-fail, non-ospf, output-acl, tt-expired, uacc-if-fail, l3-forward, glean, receive, acc-vio.
	acl	(Optional) Specifies input ACL; valid values are from 1 to 256.
	input	Specifies input ACLs; valid values are from 1 to 16.
	error	Specifies the ACL software errors.
	suppress	Specifies packets for ACL logging.
	punt	Specifies packets punted due to interface.
	rx	Specifies monitoring received traffic only.

output	Specifies output ACLs; valid values are from 17 to 20.
l2-forward	(Optional) Layer 2 or Layer 3 recognition packets.
lookup-cpu	Specifies packets lodged to CPU.
ip-options	Specifies packets with IP options.
ipv6-scope-check-fail	Specifies IPv6 packets with scope-check failures.
l2-src-index-check-fail	Specifies packets from mismatched SMC MAC and SRC IP addresses.
mcast-spt-fail	Specifies IPv4 PIM multicast RPF failures.
non-arpa	Specifies packets with non-ARPA encapsulation.
router-ipu	Specifies software-routed packets.
ttl-expired	Specifies IPv4 routed packets exceed TTL.
adj-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 low priority.
mcast-rpf fail	Specifies IPv4 IPv6 Unicast RPF failures.
all	(Optional) all causes.
l3-forward	(Optional) Layer 3 packets.
forward	Specifies special Layer 3 forwards tunnel encapsulation.
jbus	Specifies special Layer 3 forwards gleas.
recvlos	Specifies packets addressed to a port.
control-packet	(Optional) Layer 2 control packets.
esmp	(Optional) ESMP packets.
mtu-exceeded	(Optional) Outgoing Layer 3 interface MTU exceeded.
control	Specifies Layer 3 control packets.
unicast	Specifies packets addressed to a port.
rpf-failure	Specifies Multicast RPF failed packets.
unknown-port-vlan-mapping	(Optional) Packets with unknown port VLAN mapping.
unknown-vlan	(Optional) Packets with missing source-IP address.
-	(Optional) Symbol to specify another range of SPAN VLANs; valid values are from 1 to 4094.
,	(Optional) Symbol to specify a range of SPAN 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-ver-group	(Optional) Specifies an IP access group filter, either a name or a number.
name	(Optional) Specifies an IP access list name.

vlan *vlan_id*	(Optional) Specifies an IP access list number. Valid values are 1 to 199 for an IP access list and 1300 to 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.

Packets are transmitted untagged-that 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

Command History

Release	Modification
12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.1(13)EW	Support for differing directions within a single-user session and extended VLAN addressing was added.
12.1(19)EW	Support for ingress packets, encapsulation specification, packet and address type filtering, and CPU source traffic enhancements was added.
12.1(20)EW	Support for remote SPAN and best learning on ingress-enabled destination ports was added.
12.2(20)EW	Support for an IP access group filter was added.
12.2(40)SG	Support for Supervisor Engine 6-E and Catalyst 4500M chassis CPU queue options were added.

Usage Guidelines

Only one SPAN destination for a SPAN session is supported. If you attempt to add another destination interface to a 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 then configure a SPAN session with a source interface, and then try to add a source VLAN to the same SPAN session, you will receive an error. If you first configure a SPAN session with a source VLAN, and then try to add a source VLAN, and then try to add a source interface to that session, you receive the error message "Cannot mix source VLAN and source interface in a session." You can have two separate sessions for a SPAN session before switching to another proof source. CPU sources may 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 untagged (the default) or isl. If the encapsulation type is ISL, then no ingress VLAN specification is necessary.

By default, when you enable ingress, inbound learning is performed on destination ports. When you enter the **learning** keyword, host learning is performed on the destination port, and traffic is learned here is forwarded on the destination port.

If you enter the **filter** keyword on 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 them configured. VLAN interfaces are not supported. However, you can span a particular VLAN by entering the **source** and **session source vlan** clause of command.

The packet-type filters are supported only in the ffm direction. You can specify both Rx and Tx type filters and multiple type filters at the same time (for example, you can **no good** and **unicast**; only unif source unicast frames). As with VLAN filters, if you do not specify the type, the session will until all packet types.

The **queue** identifier allows telling the 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# conf ig t erminal
Switch(conf ig)# monitor session 1 filter ip access-group 100
Switch(conf ig)# end
Switch(conf ig)#
```

This example shows how to add a source interface to a SPAN session:

```
Switch# conf ig t erminal
Switch(conf ig)# monitor session 1 source interface fa5/1 b
Switch(conf ig)# end
Switch(conf ig)#
Switch(conf ig)#
```

This example shows how to configure the source in with different directions within a SPAN session:

```
Switch# conf ig t erminal
Switch(conf ig)# monitor session 1 source interface fa5/1 rx
Switch(conf ig)# monitor session 1 source interface fa5/2 tx
Switch(conf ig)# end
Switch(conf ig)#
```

This example shows how to remove a source interface from a SPAN session:

```
Switch(conf ig)# no monitor session 1 source interface fa5/1
Switch(conf ig)# end
Switch(conf ig)#
```

This example shows how to limit SPAN traffic to VLANs 100 through 300:

```
Switch(config)# monitor session 1 filter vlan 100 - 300
Switch(config)#
```

This example shows how to configure RSPAN VLAN 20 as the destination:

```
Switch(config)# monitor session 1 destination remote vlan 20
Switch(config)#
```

This example shows how to use queue number and queue number ranges for the CPU as a SPAN source on Supervisor Engine 6-E:

```
Switch(config)# monitor session 2 source cpu queue control-packet rx
Switch(config)# monitor session 2 source cpu queue 10 rx
Switch(config)#
```

Note For Supervisor Engine 6-E, 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

Command History	**Release**	**Modification**
	12.2(31)SGW	Support for this command was introduced on the Catalyst 4500 series switches.

Usage Guidelines

Jumbo frames are supported on nonblocking Gigabit Ethernet ports, switch virtual interfaces (SVI), and EtherChannels. Jumbo frames are not available for routed ports.

The baby giants feature uses the global **system mtu** *x* command to set the global baby giant MTU. It allows all routed-port interfaces to support an Ethernet payload size of up to 1552 bytes.

Both the **system mtu** *x* 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 1800 bytes:

```
Switch(config)# interface 4/1-2/1-2/8/1-2
Switch(config-if)# mtu 1800
```

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

Command History	**Release**	**Modification**
	12.1(11)EW	Support for this command was introduced on the Catalyst 6500 series switch.

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 features 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

Command History

Release	Modification
12.2(52)SG	Support for this command was introduced on the Catalyst 4500 series switch.

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

Command History	Release	Modification
	12.2(33)SXI	Support for this command was introduced on the Catalyst 6500 series switch.

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)# switch 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

Command History

Release	Modification
12.1(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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 to 255.
Defaults	Port priority is set to 128.
Command Modes	Interface configuration mode

Command History	**Release**	**Modification**
	12.1(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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 reenable 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 not on the interface.

Command Modes	Router configuration mode

Command History	**Release**	**Modification**
	12.2(18)SXF	Support for this command was introduced on the Catalyst 6500 series switch.

Usage Guidelines

You can use the **passive-interface range** command on the following interfaces: FastEthernet, GigabitEthernet, VLAN, Loopback, Port-channel, 10GigabitEthernet, 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 values 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 9/11-20, gigabitethernet 6/1-10
```

Use this format when entering the *port-range*:

- *interface-type* {*{mod}/{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 on SUP9, SUP10, RSP, and RSP720 modules.

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 the IP address for the specified interface without actually running IS-IS on that interface. The **no** form of this command for IS-IS disables advertising IP addresses for the specified address.

Note For IS-IS you must keep at least 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 (null interface on network 10.108.0.0 except Gigabitethernet interface 1/1:

```
Router(config)# interface gigabitethernet 1/1
Router(config-if)# router eigrp 100
Router(config-router)# network 10.108.0.0
Router(config-router)# passive-interface gigabitethernet 1/1
Router(config-router)#
```

The following configuration enables IS-IS on Ethernet interface 1 and serial interface 0 and advertises the IP addresses of Ethernet interface 0 in link-state protocol data units (PDUs):

```
Switch(config)#ipv6 router isis Finance
Switch(config-router)#interface ethernet 0
Switch(config-router)#interface Ethernet 1
Switch(config-router)#ip router isis Finance
Switch(config-router)#interface serial 0
Switch(config-router)#ip router isis Finance
Switch(config-router)#^Z
```

The following example sets all interfaces as passive, then activates Ethernet interface 0:

```
Switch(config)#ipv6 router ospf 10
Switch(config-router)#passive-interface default
Switch(config-router)#no passive-interface ethernet 0
Switch(config-router)#network 10.200.0.0 0.0.0.255 area 0
Switch(config-router)#^Z
```

The following configuration sets the Ethernet ports 3 through 6 on module 6 and Gigabit Ethernet ports 4 through 7 on module 1 as passive:

```
Switch(config)#ipv6 router ospf 100
Switch(config-router)#passive-interface range ethernet6/3-6,gigabitethernet1/4-7
Switch(config-router)#^Z
```

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** | **response**} [**ip** | **host** *sender-ip* | *sender-ip sender-ip-mask*] **mac** [**any** | **host** *sender-mac* | *sender-mac sender-mac-mask*] [**response ip** [**any** | **host** *target-ip* | *target-ip target-ip-mask*]] [**log**]
sender-ip-mask] [**any** | **host** *target-ip* | *target-ip target-ip-mask*] **mac** [**any** | **host** *target-mac* | *target-mac target-mac-mask*]]

no permit {**request** | **ip** [**any** | **host** *sender-ip* | *sender-ip sender-ip-mask*] **mac** [**any** | **host** *sender-mac* | *sender-mac sender-mac-mask*] **response ip** [**any** | **host** *sender-ip* | *sender-ip sender-ip-mask*] [**any** | **host** *target-ip* | *target-ip target-ip-mask*] **mac** [**any** | **host** *sender-mac* | *sender-mac sender-mac-mask*] [**log** | **host** *target-mac* | *target-mac target-mac-mask*]]

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 *any-mail configuration mode*

Command History	Release	Modification
	12.2(25)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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 acme-hosts
Switch(config-arp-nacl)# permit ip host 1.1.1.1 mac host 0000.0000.abcd
Switch(config-arp-nacl)# end
Switch# show arp access-list

ARP access list acme-hosts
    permit ip host 1.1.1.1 mac host 0000.0000.abcd
Switch#
```

Related Commands	Command	Description
	arp access-list	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 to define an ARP access list and apply 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 17,000,000,128. Burst 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 4,294,967,136. Burst value of upto 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 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.

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)

Command History	Release	Modification
	12.2(25)EW	This command was introduced on the Catalyst 4500 series switch using a Supervisor Engine 6E.

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 is ill 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 maximum of four actions at one time.
- You cannot specify contradictory action 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-token bucket algorithm and a two-token bucket algorithm. A single-token bucket system is used when the **violate-action** option is not specified, and a two-token bucket system is used when the **violate-action** option is specified.

Token Bucket Algorithm with One Token Bucket

The one-token bucket algorithm is used when the **violate-action** option is not specified in the **police** command of the command-line interface (CLI).

The conform 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 actions 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 * policer rate) B 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-rates bucket algorithm is used when the **exceed-action** keyword 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 actions occur:

- Tokens are updated in the conform bucket. If the previous arrival of the packet was at T1 and the current arrival of the packet is at T, the bucket is updated with T-T1 worth of tokens based on the token arrival rate. The refill tokens are placed in the conform bucket. If the tokens overflow the conform bucket, the overflow tokens are placed in the exceed bucket.

  The tokens arrival rate is calculated as follows:

  (time between packets * which is equal to 1/T) * * police amount bps

- If the number of bytes in the conform bucket - B is greater than or equal to 0, the packet conforms and the conform action is taken (the action of the packet conforms. If 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 0, and the number of bytes in the exceed bucket - B is greater than or equal to 0, the packet exceeds 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 traffic class (using the **class-map** command) and associate the match criteria from that 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 leaving Gigabit Ethernet interface 6/1.

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#class-map match
Router(config-cmap)#match access-group 1
Router(config-cmap)#exit
Router(config)#policy-map police-setting
Router(config-pmap)#class match
Router(config-pmap-c)#police 8000 1000 conform-action transmit exceed-action drop
Router(config-pmap-c)#exit
Router(config-pmap)#exit
Router(config)#interface gigabitethernet 6/1
Router(config-if)#service-policy output police-setting
Router(config-if)#exit
```

In this example, the initial token bucket starts full at 1000 bytes. If a 450-byte packet arrives, the packet conforms because enough tokens are available in the conform token bucket. The conform action (mark) 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, 250 bytes are added to the token bucket (0.25 * 1000 bytes), leaving 800 bytes in the token bucket. If the next packet is 800 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#conf t
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 policing-testing
Switch(config-pmap)# class access-match
Switch(config-pmap-c)# police 8000 1000 1000 conform-action transmit exceed-action set-qos-transmit 1
violate-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet 6/1
Switch(config-if)# service-policy output policing-testing
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 tokens are available in the conform token bucket. The conform action (mark) 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, 250 bytes are added to the conform token bucket (0.25 * 8000 bits), leaving 800 bytes in the conform token bucket. If the next packet is 800 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 excess burst size) is then checked. The packet is compared against the exceed token bucket. The packet exceeds and the exceed action (set IP QoS transmit value of 1) is taken and 800 bytes are taken from the exceed bucket (leaving 100 bytes in the exceed token bucket.

If the next packet arrives 0.50 seconds later, 400 bytes are added to the token bucket (0.50 * 8000 b/s). Therefore, the conform token bucket now has 1000 bytes (the maximum number of tokens available in the conform bucket) and 200 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 * 8000 b/s). 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 (two rates)	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 one or more 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* [**bc** *conform-burst-in-msec*] [**pir** **percent** *percent*] [**be** *peak-burst-in-msec*]}

no police {**cir** **percent** *percent* [**bc** *conform-burst-in-msec*] [**pir** **percent** *percentage*] [**be** *peak-burst-in-msec*]}

Syntax Description

cir	Committed information rate. Indicates that the CIR will be used for policing traffic.
percent	Specifies the 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 in bytes used by the first token bucket for policing.
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	Actions to take exceeds. 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 transmits 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

Command History	Release	Modification
	12.2(40)SG	This command was introduced on the Catalyst 4500 series switch using a Supervisor Engine III.

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 on the basis of the revised amount of bandwidth. If the CIR and PIR percentages are changed 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 size and the peak burst size in milliseconds. If you want bandwidth to be calculated as a percentage, the conform burst size and the peak burst size 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 4/2. In this example, a CIR of 20 percent and a PIR of 40 percent have been specified. Additionally, an optional bc value and be value (300 ms and 400 ms, respectively) have been specified.

```
Switch(config)#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)#police cbr percent 20 bc 300 pir percent 40 be 4 ms
Switch(config-pmap-c)#exit
Switch(config-pmap)#interface gigabitethernet 4/2
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 *units* **bps** [**burst** *burst-in-bytes bytes*] [**peak-rate** *peak-rate-in-bps bps*] [**pack-burst** *peak-burst-in-bytes bytes*]

no police rate *units* **bps** [**burst** *burst-in-bytes bytes*] [**peak-rate** *peak-rate-in-bps bps*] [**pack-burst** *peak-burst-in-bytes bytes*]

Syntax for Percent

police rate-percent *percentage* [**burst** *ms*] [**peak-rate percent** *percentage*] [**pack-burst** *ms ms*]

no police rate percent *percentage* [**burst** *ms*] [**peak-rate percent** *percentage*] [**pack-burst** *ms ms*]

Syntax Description		
	units	Specifies the traffic police rate in bits per second. Valid range is 32,000 to 32,000,000,000.
	bps	(Optional) Bits per second (bps) will be used to determine the rate at which traffic is policed.
		Note If a rate is not specified, traffic is policed via bps.
	burst *burst-in-bytes* **bytes**	(Optional) Specifies the burst rate, in bytes, will be used for policing traffic. Valid range is from 64 to 2,096,128,256.
	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 2,096,128,256.
	percent *percentage*	(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*	(Optional) Burst rate, in milliseconds, will be used for policing traffic. Valid range is a number from 1 to 2,000.
	peak-rate percent *percentage*	(Optional) A percentage of interface-bandwidth will be used to determine the peak-rate. Valid range is a number from 1 to 100.
	peak-burst *ms ms*	(Optional) Peak-burst rate, 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

Command History	Release	Modification
	12.2(40)SG	This command was introduced on the Catalyst 6500 series switch using a Supervisor Engine 6E.

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 bps 500000
Switch(config-pmap-c)# exit
```

Related Commands	Command	Description
	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.
	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* [**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. *cir* specifies the CIR in bits per second. The value is a number from 32,000 to 32,000,000,000.
bc *conform-burst*	(Optional) Conform burst (bc) your used by the first token bucket for policing. (Optional) Specifies the bc value in bytes. The value is a number from 64 to 2,000,000,128.
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 32,000,000,000.
be *peak-burst*	(Optional) Peak burst (be) you used by the second token bucket for policing. (Optional) Specifies the peak burst (be) size in bytes. The value is a number from 64 to 2,000,000,128.
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 service (CoS) value to a new value and send the packet. The range is 0 to 7. • **set-dscp-transmit** *new-dscp*—Sets the IP differentiated services code point (DSCP) value and sends the packet with the new IP DSCP value setting. • **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

Command History	Release	Modification
	12.2(18)SXD	This command was introduced on the Catalyst 6500 series switch using a Supervisor Engine 6E.

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 (Bp) value.

Updating Token Buckets

The following scenario illustrates how the token buckets are updated:

A packet of B bytes arrives at time t. The last packet arrived at time tl. The CIR and the PIR tokens in the token buckets are represented by Tc(t) and Tp(t), respectively. Using these values and in this scenario, the token buckets are updated at time t:

$$Tc(t) = min(CIR * (t-tl) + Tc(tl), Bc)$$

$$Tp(t) = min(PIR * (t-tl) + Tp(tl), Bp)$$

Marking Traffic

The two-rate policer marks packets as either conforming, exceeding, or violating a specified rate. The following points (using a packet of B bytes) determine how a packet is marked:

- If B > Tc(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:

$$Tc(t) = Tc(t) - B$$

$$Tp(t) = Tp(t) - B$$

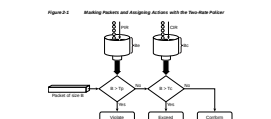
For example, if the CIR is 100 kbps, the PIR is 200 kbps, and a sales stream with a rate of 250 kbps arrives at the two-rate policer, the packet would be marked as follows:

- 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 Flowchart

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 Making Packets and Assigning Actions with the Two-Rate Policer



Examples

This example shows how to configure two-rate traffic policing on a class to limit traffic to an average committed rate of 500 kbps and a peak rate of 1 Mbps:

```
Switch(config)# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# class-map police
Switch(config-cmap)# match access-group 145
Switch(config-cmap)# policy-map policy1
Switch(config-pmap)# class police
Switch(config-pmap-c)# police 500000 bc 10000 pir 1000000 be 10000 conform-action
transmit exceed-action set-prec-transmit 2 violate-action drop
Switch(config-pmap-c)# interface gigabitethernet 4/1
Switch(config-if)# service-policy output policy1
Switch(config-if)# exit
Switch# show policy-map policy1

Policy Map policy1
  class police
    police cir 500000 conform-burst 10000 pir 1000000 peak-burst 10000 conform-action
transmit exceed-action set-prec-transmit 2 violate-action drop
Switch#
```

Traffic marked as conforming to the average committed rate (500 kbps) will be sent as is. Traffic marked as exceeding 500 kbps, but not exceeding 1 Mbps, will be marked with IP Precedence 2 and then sent. All traffic marked as exceeding 1 Mbps will be dropped. The burst parameters are set to 10000 bytes.

In the following example, 1.25 Mbps of traffic is sent ("offered") to a policer class:

```
Router# show policy-map interface gigabitethernet 4/1

GigabitEthernet4/1

  Service-policy output: policy1

    class-map: police (match all)
      148615 packets, 36629328 bytes
      30 second offered rate 1236000 bps, drop rate 247000 bps
      Match: access-group 150
      police:
        cir 500000 bps, conform-burst 10000, pir 1000000, peak-burst 100000
        conformed 59535 packets, 14682480 bytes; action: transmit
        exceeded 59535 packets, 14682480 bytes; action: set-prec-transmit 2
        violated 29543 packets, 7319024 bytes; action: drop
        conformed 495000 bps, exceed 500000 bps violate 247000 bps

    class-map: class-default (match-any)
      19 packets, 1292 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: any
Router#
```

The **police** command 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 or 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

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 6500 series switch.
	12.2(18)SXD	Added support for the Supervisor Engine 6-E and Catalyst 4500E chassis.

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 2-62.
- **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** less-than-global configuration commands.

Examples This example shows how to create a policy-map called policy1. When attached to the ingress direction, it 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 bursts at 20 KB. Traffic exceeding the profile is marked down to a DSCP value obtained from the policed-DSCP map and then sent. This policer action is applicable on all Catalyst 6500 supervisor engines except the Supervisor Engine 6-E and Catalyst 6500E chassis.

```
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# set ip dscp 10
Router(config-pmap-c)# police 200000 20000 exceed-action policed-dscp-transmit
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)#
```

This example shows how to configure multiple classes in a policy-map called policymap2 on a Supervisor Engine 6-E:

```
Router(config)# configure terminal
Router(config)# policy-map policymap2
Router(config-pmap)# class class1
Router(config-pmap-c)# police cir 10000 pir 20000 conform-action
Router(config-pmap-c)# exit-bandwidth-unit bit
Router(config-pmap-c)# exit-cos-transmit 3
Router(config-pmap-c)# exit
Router(config-pmap)# class class2
Router(config-pmap-c)# police cir 5000 pir 10000 conform-action transmit exceed-action
Router(config-pmap-c)# exit-bandwidth-unit violate-action drop
Router(config-pmap-c)# exit
Router(config-pmap)# class class3
Router(config-pmap-c)# set dscp cs4
Router(config-pmap-c)# exit
Router(config)#
```

This example shows how to delete the policy-map called policymap2:

```
Router(config)# configure terminal
Router(config)# no policy-map policymap2
Router(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.
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 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 or applies different QoS policies on VLANs that are transfer-forwarded.
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

Command History	**Release**	**Modification**
	12.1(3a)EW	Support for this command was introduced on the Catalyst 6500 series switch.

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-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

Command History	**Release**	**Modification**
	12.2(25)FWA	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines Layer 2 interfaces can be part of multiple VLANs (for example, a typical trunk port). In conjunction with the trunk 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 2-5:

```
Switch(config)# interface fastethernet
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 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

Command History	**Release**	**Modification**
	12.2(52)SG	Support for this command was introduced on the Catalyst 6500 series switch.

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 the **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 shows 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

Command History	Release	Modification
	12.2(25)EWA	Support for this command was introduced on the Catalyst 4500 series switch.

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 set the **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 is used for that VLAN. In this situation, the maximum number of addresses that can be secured on this VLAN is limited to the maximum value configured on the port.

Each VLAN can be configured with a maximum count that is greater than the value configured on the port. Also, the sum total of the maximum configured values for all the VLANs can exceed 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 GigabitEthernet 1/1 for VLANs 2–3:

```
Switch#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gi1/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# vlan 2-3
Switch(config-if-vlan-range)# port-security maximum 5
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 mac-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 300 to 8500.

Defaults DC power input is 2500 W.

Command Modes Global configuration mode

Command History	Release	Modification
	12.2(31)SGA	Support for this command was introduced on the Catalyst 4500 series switch.
	12.2(31)SGB	Support for **dc input** was added.

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 .idbin
```

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 inline

To set the inline-power state for the inline-power-capable interface, use the **power inline** command. To return to the default values, use the **no** form of this command.

power inline {**auto** | **max** *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-X6148-RJ45V-E, the maximum is 20000. For the WS-X6148-RJ45V+E, the maximum is 30000.
never	Disables both the detection and power for the inline-power-capable interface.
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 usage is set to 15400. For the WS-X6148-RJ45V-E, the maximum mW is set to 20000. For the WS-X6148-RJ45V+E, the maximum mW is set to 30000.
- Default allocation is set to 15400.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(11)b	Support for this command was introduced on the Catalyst 6500 series switch.
12.1(13)aE	Support added for static power allocation.
12.1(20)EW	Support added for Power over Ethernet.
12.2(14)SX1	Maximum supported wattage increased beyond 15400 for the WS-X6148-RJ45V-E and the WS-X6148-RJ45V+E.

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 FastEthernet 4/1
Switch(config-if)#power inline auto
Switch(config-if)#end
Switch#
```

This example shows how to disable 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 FastEthernet 4/1
Switch(config-if)#power inline never
Switch(config-if)#end
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)#end
Switch#
```

This example shows how to pre-allocate Power over Ethernet to 35000 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 35000
Switch(config-if)#end
Switch#
```

Related Commands

Command	Description
show power	Displays information about the power status.

power inline consumption

To set 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 15.400. Any non-default value disables automatic adjustment of power allocation.
Defaults	Milliwatt mode is set to 15400.
Command Modes	Global configuration mode

Command History	**Release**	**Modification**
	12.1(12)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(20)EW	Support added for Power over Ethernet.

Usage Guidelines The **inline power consumption** command overrides the power allocation by the port through IEEE/Cisco phase 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 xdmin
```

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 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**] [**evvidable** | **log**]

no power inline police [**action**] [**evvidable** | **log**]

Syntax Description		
	action	(Optional) Specifies the action to take on the port when a PoE policing fault occurs (the device consumes more power than it's allowed).
	evvidable	(Optional) Enables PoE policing on the interface and places the port in an evvidable 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

Command History		
	Release	**Modification**
	12.2(50)SG	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

If a port is in the evvidable 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 evvidable autorecovery so that an evvidable interface is automatically revived when the evvidable autorecovery timer expires.

Examples

This example shows how to enable PoE policing and configure a policing action:

```
Switch(config)# no gigabitethernet 2/1
Switch(config-if)# power inline police
Switch(config-if)# no power inline police gigabitethernet 2/1
Switch(config)# exit
Switch#show interfaces status
Port      Name               Status       Vlan       Duplex  Speed Type
Gi2/1                        evvidable    1          a-full  a-1.0 1.0
Switch(config-if)# power inline police action log
Switch(config)# exit
Switch#show power inline police
Interface Admin  Oper       Admin  Oper       Cutoff     Oper
          State  State       Police Police     Power      Power
---------- ------ ---------- ------ ---------- ---------- ----------
Gi2/1     auto   evvidable  log    evvidable  n/a        7.0
Switch(config-if)# power inline police action log
Switch(config)# exit
Switch#show power inline police
Interface Admin  Oper       Admin  Oper       Cutoff     Oper
          State  State       Police Police     Power      Power
---------- ------ ---------- ------ ---------- ---------- ----------
Gi2/1     auto   on         
```

```
Interface Admin Oper  Admin  Oper   Cutoff Oper
          State State Priority Police Power Power
--------- ----- ----- -------- ------ ----- -----
Gi2/1     auto  on    low      ok     17.4  9.6
```

Related Commands	Command	Description
	errdisable recovery	Enables errdisable autorecovery; the port automatically restarts 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

Command History	**Release**	**Modification**
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch (Catalyst 4506 series switches only: 4503, 4506, and 4507).

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 base 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 engine, 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

Command History	Release	Modification
	12.2(52)SG	Support for this command was introduced on the Catalyst 4500 series switch.

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 identifier 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

Command History	Release	Modification
	12.2(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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)# pppoe intermediate-agent
```

This example shows how to disable the PPPoE Intermediate Agent on an interface:

```
Switch(config)# 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.

Command	Description
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

Command History	Release	Modification
	12.2(50)SG	Support for this command was introduced on the Catalyst 4500 series switch.

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-if)# 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-if)# vlan-range 148
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*

pppoe intermediate-agent format-type generic-error-message *string*

pppoe intermediate-agent format-type identifier-string *string* **option** {**pppoe|pvc|spc**} **delimiter** {.|:|/|#}

no pppoe intermediate-agent format-type {**access-node identifier** | **generic-error-message** | **identifier-string**}

Syntax Description

access-node-identifier string	ASCII strong literal value for the access-node-identifier.
generic-error-message string	ASCII strong literal value for the generic error-message.
identifier-string string	ASCII strong literal value for the identifier-string.
option {**pppoe|pvc|spc**}	Options: **sp** = slot + port **sv** = slot + VLAN **pv** = port + VLAN **spv** = slot + port + VLAN
delimiter {.|:|/|#}	Delimiter between slot|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

Command History

Release	Modification
12.2(18)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

Use the **access-node-identifier** and **identifier-string** commands to enable the switch to generate the circuit-id parameter automatically.

The **no** form of **identifier-string** command resets the option and delimiter.

pppoe intermediate-agent format-type (global)

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-abc-123
```

This example shows how to unset 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 parameter, use the **no** form of this command.

pppoe intermediate-agent format-type {**circuit-id** | **remote-id**} *string*

no pppoe intermediate-agent format-type {**circuit-id** | **remote-id**} **string** *string*

Syntax Description	**circuit-id string** *string*	ASCII string (max) value for circuit-id.
	remote-id string *string*	ASCII string (max) value for remote-id.

Defaults No default values for circuit-id and remote-id.

Command Modes Interface configuration mode

Command History	Release	Modification
	12.2(52)SG	Support for this command was introduced on the Catalyst 4500 series switch.

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 automatically generates circuit-id value is used.

Examples This example shows how to set remote-id for an interface:

```
Switch(config-if)# pppoe intermediate-agent format-type remote-id string user001001
```

This example shows how to unset circuit-id for an interface:

```
Switch(config-if)# 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 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 to be set for circuit-id. **remote-id string** *string* — ASCII string literal value to be set for remote-id.
Defaults	No default values for circuit-id and remote-id.
Command Modes	Interface vlan-range configuration mode

Command History	Release	Modification
	12.2(25)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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 249
Switch(config-if-vlan-range)#
pppoe intermediate-agent format-type remote-id string name0101:0401:vsl4:ex
```

This example shows how to unset circuit-id on an interface vlan-range:

```
Switch(config)# int vlan-range 107-108
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

Command History

Release	Modification
12.2(33)SXH	Support for this command was introduced on the Catalyst 6500 series switch.

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, set 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

Command History	Release	Modification
	12.2(25)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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), set 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

Command History	Release	Modification
	12.2(18)SXF	Support for this command was introduced on the Catalyst 6500 series switch.

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 queuing [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

Command History	Release	Modification
	12.2(20)EW	This command was introduced on the Catalyst 4500 series switch using a Supervisor Engine 6E.

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 class-default.

This command configures LLQ and provides strict-priority queuing. Strict-priority queuing 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 is 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 strict-priority police-map class configuration command.

If the priority queuing 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)#policy-map policy1
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config-pmap)#class class1
Switch(config-pmap-c)#bandwidth 2000 remain
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 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.
	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 | primary}

private-vlan association *secondary-vlan-list* [**add** *secondary-vlan-list*] | [**remove** *secondary-vlan-list*]

no private-vlan {isolated | 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.
	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.
	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

Command History	Release	Modification
	12.1(2)EW	Support for this command was introduced on the Catalyst 6500 series switch.
	12.1(12c)EW	Support for extended addressing was added.
	12.2(1)EW	Support for community VLANs was added.

Usage Guidelines You cannot configure VLAN 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 contain only one 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 unidirectional VLANs and is used by isolated ports or by a community of ports to communicate with the switches.

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 by the isolated 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 or 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 associated to a VLAN.

The **private-vlan** commands do not take effect until you exit the config VLAN submode.

If you delete the primary or secondary VLAN, the ports that are associated with the VLAN become inactive.

Refer to the Catalyst 6500 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(config)#show private-vlan
Primary Secondary Type      Ports
------- --------- ----------- ------------------------------------------
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(config)#show vlan private-vlan
Primary Secondary Type      Ports
------- --------- ----------- ------------------------------------------
202     primary
303     community
```

This example shows how to configure VLAN 400 as an isolated VLAN and verify the configuration:

```
Switch(config)#vlan 400
Switch(config-vlan)#private-vlan isolated
Switch(config-vlan)# end
```

```
Switch#show vlan private-vlan
Primary Secondary Type              Interfaces
------- --------- ----------------- ------------------------------------------
  202     101     isolated
  202     102     community
  202     103     isolated
  202     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 19
Switch(config-vlan)# private-vlan isolated
Switch(config)# vlan 20
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# 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 associate community VLANs 303 through 307 and 309 and isolated VLAN 440 with primary VLAN 202 and verify the configuration

```
Switch(config)# configure terminal
Switch(config)# vlan 202
Switch(config-vlan)# private-vlan association 303-307,309,440
Switch(config-vlan)# exit
Switch(config)# show vlan private-vlan
Primary Secondary Type              Interfaces
------- --------- ----------------- ------------------------------------------
  202     101     community
  202     102     community
  202     103     community
  202     104     community
  202     105     community
  202     440     isolated
  202     106     community
```

The secondary VLAN 308 has no 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 18
Switch(config-vlan)#
```

This example shows how to configure interface FastEthernet 5/1 as a PVLAN host port and verify the configuration:

```
Switch(config)# configure 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
Administrative Trunking Encapsulation: dot1q
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
Operational Private-vlan:
  Host Association: 202 (VLAN0202) 440 (VLAN0440)
  Promiscuous Mapping: none
  Trunk encapsulation: dot1q
  Trunk vlans:
Operational private-vlan(s):
  Trunking VLANs Enabled: ALL
  Trunking VLANs Disabled: ALL
  Pruning VLANs Enabled: 2-1001
  Capture VLANs Enabled:
  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* [{{**add** *secondary-vlan-list*} | {**remove** *secondary-vlan-list*}}]

no private-vlan mapping

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

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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 at 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 PVLANs 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 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# configure terminal
Switch(config)# interface vlan 202
Switch(config-if)# private-vlan mapping add 303-307,309,440
Switch(config-if)# end
Switch# 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#
```

This example shows the displayed message that you will see if the VLAN that you are adding is already mapped on the SVI of VLAN 18. You must delete the mapping from the SVI of VLAN 18 first.

```
Switch(config)# interface vlan 18
Switch(config-if)# private-vlan mapping 19 add 21
  Command rejected: The secondary vlan 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 19:

```
Switch(config)# interface vlan 19
Switch(config-if)# no private-vlan mapping
Switch(config-if)#
```

```
Switch# configure terminal
Switch(config)# interface vlan 202
Switch(config-if)# private-vlan mapping add 303-307,309,440
Switch(config-if)# end
Switch# 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#
```

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

Command History

Release	Modification
12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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 VLAN 2, and that all VLANs are mapped to the MST instance 1. This example also shows the output if you try to change the mapping for the primary VLAN 2 and

```
Switch(config-mst)# exit from mst configuration
Switch(config-mst)# instance 1 vlan 2
Switch(config-mst)# exit
These secondary vlans are not mapped to the same instance as their primary:
  3 -> 1

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

Command History	**Release**	**Modification**
	12.2(52)SG	Support for this command was introduced on the Catalyst 4500 series switch.

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(config-call-home)# profile vlaru
Switch(cfg-call-home-profile)# transport-method http
Switch(cfg-call-home-profile)# destination address http
https://172.17.45.27/its/service/oddiservice/HttpService
Switch(cfg-call-home-profile)# subscribe-to-alert-group configuration
Switch(cfg-call-home-profile)# subscribe-to-alert-group diagnostic severity normal
Switch(cfg-call-home-profile)# subscribe-to-alert-group environment severity notification
Switch(cfg-call-home-profile)# subscribe-to-alert-group syslog severity notification
pattern "SYSMGM"
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.
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 (global configuration mode)

To globally enable QoS functionality on the switch, use the **qos** command. To globally disable QoS functionality, use the **no** form of this command.

qos

no qos

Syntax Description This command has no arguments or keywords.

Defaults QoS functionality is disabled.

Command Modes Global configuration mode

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines This command is not supported on the Supervisor Engine 6-E and the Catalyst 4500M chassis. On the Supervisor Engine 6-E and Catalyst 4500M chassis QoS is always enabled without being configured.

If QoS functionality is globally enabled, it is enabled on all interfaces, except on the interfaces where QoS has been disabled. If QoS functionality is globally disabled, all traffic is passed in QoS-pass-through mode.

Examples This example shows how to enable QoS functionality globally on the switch:

```
Switch(config)# qos
Switch(config)#
```

Related Commands

Command	Description
qos (interface configuration mode)	Enables QoS functionality on an interface.
show qos	Displays QoS information.

qos (interface configuration mode)

To enable QoS functionality on an interface, use the **qos** command. To disable QoS functionality on an interface, use the **no** form of this command.

qos

no qos

Syntax Description This command has no arguments or keywords.

Defaults QoS is enabled.

Command Modes Interface configuration mode

Command History	Release	Modification
	12.1(13)E9	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines This command is not supported on the Supervisor Engine 6-E and the Catalyst 4500M chassis. On the Supervisor Engine 6-E and Catalyst 4500M chassis, attaching a service policy implicitly enables QoS on the supervisor engine and detaching a service policy implicitly disables QoS on the supervisor engine.

If QoS functionality is globally disabled, it is also disabled on all interfaces.

Examples This example shows how to enable QoS functionality on an interface:

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

Related Commands

Command	Description
qos (global configuration mode)	Enables QoS functionality on the switch.
qos (interface configuration mode)	Enables QoS functionality on an interface.
show qos	Displays QoS information.

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** | **id** | **length** *inc*}

no qos account layer2 encapsulation {**arpa** | **dot1q** | **id** | **length** *inc*}

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).
id	Specifies the account length of the ISL encapsulated packet (48 bytes).
length *inc*	Specifies the additional packet length to account for (for valid range is from 0 to 64 bytes).

Defaults

On non-Supervisor Engine 6-E/6-L only the length that is specified in the IP header for the IP packets and the length that is specified in the Ethernet header for non-IP packets are included.

On the Supervisor Engine 6-E and the Catalyst 4900M chassis 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

Command History

Release	Modification
12.2(31)SGW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

This command is not supported on the Supervisor Engine 6-E and the Catalyst 4900M chassis.

In the Catalyst 4500 series switch, for non-Supervisor Engine 6-E supervisors the **qos account layer2 encapsulation** command indicates that the policing feature should consider the configured length in addition to the IP length of the packet when policing the IP packets.

Shaping and shaping always use the Ethernet ARPA length.

On Supervisor Engine 6-E and Catalyst 4900M chassis supervisors 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 VLANs 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 id** is configured, a fixed length of 48 bytes is included when policing all IP packets, not only those packets that are received with ISL encapsulation.

Shaping 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(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(config)#no qos account layer2 encapsulation
Switch(config)# end
Switch #
```

Related Commands

Command	Description
show interface	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 aggregate-policer

To define a named aggregate policer, use the **qos aggregate-policer** command. To delete a named aggregate policer, use the **no** form of this command.

qos aggregate-policer *name rate burst* [**conform-action** [**transmit** | **drop**] **exceed-action** [**transmit** | **drop**] **policed-dscp-transmit**]]

no qos aggregate-policer *name*

Syntax Description

name	Name of the aggregate policer.
rate	Max (mean) bits per second, valid values are from 32000 to 2000000000.
burst	Burst bytes, valid values are from 1000 to 512000000.
conform-action	(Optional) Specifies the action to be taken when the rate is not exceeded.
transmit	(Optional) Transmits the packet.
drop	(Optional) Drops the packet.
exceed-action	(Optional) Specifies action when the QoS values are exceeded.
policed-dscp-transmit	(Optional) Sends the DSCP per the policed-DSCP map.

Defaults

The default settings are as follows:

- Conform-action transmits.
- Exceed-action drops.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

This command is not supported on the Supervisor Engine 6-E and the Catalyst 4900M chassis.

This policer can be shared by different policy map classes and on different interfaces.

The Catalyst 4506 switch supports up to 1000 aggregate input policers and 1000 output policers.

The **qos aggregate-policer** command allows you to configure an aggregate flow and a policing rate for that aggregate. When you enter your rate and burst parameters, the range for the average rate is 32 Kbps to 32 Gbps, and the range for the burst size is 1 KB to 512 MB.

A rate can be entered in bits-per-second without a suffix. In addition, the suffixes described in Table 2-10 are allowed.

Table 2-22 Rate Suffix

Suffix	Description
k	1,000 bps
m	1,000,000 bps
g	1,000,000,000 bps

Burst can be entered in bytes without a suffix. In addition, the suffixes shown in Table 2-1 are allowed.

Table 2-22 Burst Suffix

Suffix	Description
k	1000 bytes
m	1,000,000 bytes
g	1,000,000,000 bytes

Note Due to hardware granularity, the rate value is limited, so the burst that you configure might not be the value that is used.

Modifying an existing aggregate rate limit modifies that entry in NVRAM and in the switch if it is currently being used.

When you enter the aggregate policer name, follow these naming conventions:

- Maximum of 31 characters long and may include a-z, A-Z, 0-9, the dash (-), the underscore (_), and the period (.).
- Must start with an alphabetic character and must be unique across all ACLs of all types.
- Aggregate policer names are case sensitive.
- Cannot be a number.
- Must not be a keyword; keywords to avoid are **all**, **default-action**, **map**, **help**, and **editbuffer**.

An aggregate policer can be applied to one or more interfaces. However, if you apply the same policer to the input direction on one interface and to the output direction on a different interface, then you have created the equivalent of two different aggregate policers in the switching engine. Each policer has the same policing parameters, with one policing the ingress traffic on one interface and the other policing the egress traffic on the other interface. If you apply the same policer to both input and output directions in the same direction, only one instance of the policer is created in the switching engine.

You can apply an aggregate policer to a physical interface or to a VLAN. If you apply the same aggregate policer to a physical interface and to a VLAN, then you have created the equivalent of two different aggregate policers in the switching engine. Each policer has the same policing parameters, with one policing the traffic on the configured physical interface and the other policing the traffic on the configured VLAN. If you apply an aggregate policer to only ports or only VLANs, then only one instance of the policer is created in the switching engine.

If you apply a single aggregate policer to the ports and the VLANs in different directions, then you have created the equivalent of four aggregate policers, one for all ports sharing the policer in the input direction, one for all ports sharing the policer in the output direction, one for all VLANs sharing the policer in the input direction, and one for all VLANs sharing the policer in the output direction.

Examples

This example shows how to configure a QoS aggregate policer to allow a maximum of 100,000 bits per second with a normal burst size of 10,000 bytes, in transmit when these rates are not exceeded, and to drop packets when these rates are exceeded:

```
qos aggregate policer micro-one 100000 10000 conform-action transmit exceed-action drop
```

Dual-mode (supervisor) (Dual-mode (supervisor)) (Dual-mode (supervisor))

Related Commands

Command	Description
show qos aggregate policer	Displays QoS aggregate policer information.

qos control-packets

To enable Layer 2 control packet QoS mode on control packets use the **qos control-packets** command. To disable Layer 2 control packet QoS mode on control packets, use the **no** form of this command.

qos control-packets {lipda-vsnap | cdp-vtp | setp | lldp}

no qos control-packets {lipda-vsnap | cdp-vtp | setp | lldp}

Syntax Description	**lipda-vsnap** Specifies enabling QoS on BPDU-snap packets. **cdp-vtp** Specifies enabling QoS on CDP and VTP packets. **setp** Specifies enabling QoS on SSTP packets. **lldp** Specifies enabling QoS on LLDP packets.
Defaults	This command has no default settings.
Command Modes	Global configuration mode

Command History

Release	Modification
12.2(40)SG	Support for this command was introduced on the Catalyst 4500 series switch.
12.2(46)SG	Support for the **lldp** keyword.

Usage Guidelines

This command is not supported on the Supervisor Engine 6-E and the Catalyst 4900M chassis.

The ranges of addresses that Layer 2 control packet QoS acts on when the relative command is entered are shown in Table 2-12.

Table 2-12 Packet Types and Actionable Address Range

Type of Packet on Which Feature Is Enabled	Range of address
BPDU-snap	0180.C200.0000 BPDU 0180.C200.0002 OAM, LACP 0180.C200.0003 Eapol
CDP-VTP	0100.0CCC.CCCC
SSTP	0100.0CCC.CCCD
LLDP	0180.C200.000E

Note If you enter **qos control-packet** without specifying any control packet type, the feature is enabled for all of them.

When Layer 2 control packet QoS is enabled, you need to configure policies to match the required Layer 2 packets and police them as desired. When the feature is enabled on a particular packet type, MACLs that match the desired control packets are automatically generated, if not already present. The generated MACLs are named in the form "system-control-packet-<protocol>". You can use these class maps in the policy maps in order to police the control packets, applying them a per port, per VLAN, or per port per VLAN just like any other policy map. In addition, you can define your own MACLs in class maps to match the control packets. The only limitation is that the user-defined class maps have to begin with the prefix "system-control-packet-".

Examples

This example shows how to enable QoS on BGPU packets:

```
Switch(config)#mode
Switch(config)#control-protocol
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#qos control-packets bgpu-range
Switch(config)#
```

This example shows how to enable QoS on CDP and VTP packets:

```
Switch(config)#mode
Switch(config)#control-protocol
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#qos control-packets cdp-vtp
Switch(config)#
```

This example shows how to enable QoS on SSTP packets:

```
Switch(config)#mode
Switch(config)#control-protocol
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#qos control-packets sstp
Switch(config)#
```

This example shows how to enable QoS on LLDP packets:

```
Switch(config)#mode
Switch(config)#control-protocol
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#qos control-packets lldp
Switch(config)#
```

Related Commands

Command	Description
show policy-map interface	Displays the statistics and configurations of the input and output policies that are attached to an interface.
show running-config	Displays the running configuration for a switch.

qos cos

To define the default CoS value for an interface, use the **qos cos** command. To remove a prior entry, use the **no** form of this command.

qos cos *cos_value*

no qos cos *cos_value*

Syntax Description	*cos_value* Default CoS value for the interface; valid values are from 0 to 7.
Defaults	On non-Supervisor Engines 6-E, the default CoS value is 0. On Supervisor Engine 6-E and Catalyst 4500M chassis, the default CoS is implicitly set to 1.
Note	CoS override is not configured.
Command Modes	Interface configuration mode

Command History	**Release**	**Modification**
	12.1(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines	CoS values are configurable on physical LAN ports only.

Examples	This example shows how to configure the default QoS CoS value as 6:
	`Switch(config-if)#qos cos 6`
	`Switch(config-if)#`

Related Commands	**Command**	**Description**
	show qos	Displays QoS information.

qos dbl

To enable Dynamic Buffer Limiting (DBL) globally on the switch, use the **qos dbl** command. To disable DBL, use the **no** form of this command.

qos dbl [**buffers** [*aggressive-flow buffers*] | **credits** [*aggressive-flow credits*] | **maximum** *max*] | **drop-based** [*value value range*] | **exceed-action** *(*{**ecn** | **probability** *percent*} [**flow** [**include** [*layer-4-ports* | *vlan*]]]*)*

no qos dbl [**buffers** [*aggressive-flow buffers*] | **credits** [*aggressive-flow credits*] | **maximum** *max*] | **drop-based** [*value value range*] | **exceed-action** *(*{**ecn** | **probability** *percent*} [**flow** [**include** [*layer-4-ports* | *vlan*]]]*)*

Syntax Description

buffers	(Optional) Specifies the buffer limit for aggressive flows.
aggressive-flow buffers	(Optional) Specifies the aggressive flow.
buffers	(Optional) Number of buffers for aggressive flows; valid values are from 0 to 255.
credits	(Optional) Specifies the credit limit for aggressive flows and all flows.
aggressive-flow credits	(Optional) Number of credits for aggressive flows; valid values are from 0 to 15.
maximum	(Optional) Specifies the maximum credit for all flows.
max	(Optional) Number of credits for all flows; valid values are from 0 to 15.
drop-based	(Optional) Specifies the packets that belong to the list of internal DSCPs.
value	(Optional) A single DSCP value; valid values are from 0 to 63.
value range	(Optional) A range of DSCP values; valid values are from 0 to63. Up to8 comma separated DSCP values can be specified.
exceed-action	(Optional) Specifies the packet marking when the limits are exceeded.
ecn	(Optional) Specifies the explicit congestion notification.
probability	(Optional) Specifies the probability of packet marking.
percent	(Optional) Probability number; valid values are from 0 to 100.
flow	(Optional) Specifies the flow-based limiting.
include	(Optional) Allows the Layer 4 ports and VLANs to be included in the flows.
layer4-ports	(Optional) Includes the Layer 4 ports in flows.
vlan	(Optional) Includes the VLANs in flows.

Defaults

On non-Supervisor Engine 6-E, the default settings are as follows:

- QoS DBL is disabled.
- Aggressive-flow buffers is set to 2.
- Aggressive-flow credits is set to 2, with a limit of 10.
- Layer 4 ports are included.
- VLANs are included.
- 15 maximum credits are allowed.
- 15%drop probability is set.
- DSCP values are inclusive.

On Supervisor Engines 6-E and Catalyst 4900M chassis, the default DBL values are implicitly set and cannot be changed. The settings are as follows:

- Seven maximum credits allowed.
- Aggressive-drop credits is set to 4.
- Aggressive-flow buffers is set to 4.
- Six percent drop probability is set.
- Hash function for layer 2 packets uses source and destination MAC addresses as well as transmit VLAN identifiers.
- Hash function for IPv4 and IPv6 packets uses source and destination IP addresses source and destination Layer 4 ports as well as transmit VLAN identifiers.

Command Modes Global configuration mode

QoS policy-map class configuration

Command History

Release	Modification
12.2(53)SG	Support for this command was introduced on the Catalyst 4500 series switch.
12.2(54)SG	Added support for DSCP-based flow management.

Usage Guidelines This command is not supported on the Supervisor Engine 6-E and Catalyst 4900M chassis.

Examples This example shows how to enable DBL globally on the switch:

```
Switch(config)# qos dbl
Global DBL enabled
Switch(config)#
```

This example shows how to enable DBL in the QoS policy-map class configuration mode:

```
Switch(config)# class-map c1
Switch(config-cmap)# policy-map p1
Switch(config-pmap)# class c1
Switch(config-pmap-c)# qos dbl
Switch(config-pmap-c)#
```

This example shows how to selectively enable DBL on DSCP values 1 through 10:

```
Switch# configure t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# qos dbl dscp-based 1-10
Switch(config)# end
Switch# show qos dbl
  DBL Flow Defaults vlan
  DBL Flow Defaults dscp-based
  DBL Enabled DSCP values 1-10
  DBL Aggressive-drop Credits: 4
  DBL Aggressive-flow Buffers: 4
  DBL Drop Probability: 6%
  DBL max-credits: 15
```

```
DBL aggressive credit limit:2
DBL aggressive buffer limit:2 packets
DBL drop with default drop probability
    1-10
```

This example shows how to selectively disable DBL on DSCP values 1 through 10:

```
Switch# configure t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# no qos dbl dscp-based 1-5, 7
Switch(config)# end
Switch# show qos dbl
DBL Slow includes vlan
DBL Slow includes layer2-ports
DBL Snoop not use arp to indicate congestion DBL ecn-mark-action probability: 10% DBL max
packet size:1500 DBL max packet rate: 50 DBL aggressive buffer limit: 2 packets DBL
DSCPs with default drop probability:
    5,6,8-63
```

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

Related Commands	Command	Description
	show qos dbl	Displays QoS Dynamic Buffer Limiting (DBL) information.

qos dscp

To define the default CoS value for an interface, use the **qos dscp** command. To remove a prior entry, use the **no** form of this command.

qos dscp *dscp_value*

no qos dscp *dscp_value*

Syntax Description	*dscp_value* Default DSCP value for the interface; valid values are from 0 to 63.

Defaults

On a non-Supervisor Engine 6-E, the default DSCP value is 0.
On a Supervisor Engine 6-E and Catalyst 4500M chassis, the port DSCP value is always set to 0.

Command Modes Interface configuration mode

Command History	**Release**	**Modification**
	12.1(8)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines This command is not supported on the Supervisor Engine 6-E and Catalyst 4500M chassis.

Examples This example shows how to configure the default QoS DSCP value as 6:

```
Switch(config)# int g1/2/4  qos dscp 6
Switch(config)# int g1/2/4
```

Related Commands

Command	Description
show qos interface	Displays QoS information for an interface.

qos map cos

To define the ingress CoS-to-DSCP mapping for the trusted interfaces, use the **qos map cos in dscp** command. To remove a prior entry, use the **no** form of this command.

Note You cannot remove a single entry from the table.

qos map cos *cos_values* **to dscp** *dscp*[ ]

no qos map cos to dscp

Syntax Description

cos_values	CoS values; list up to eight CoS values separated by spaces.
to dscp	Defines mapping and specifies DSCP value.
dscp	DSCP value to map to the CoS values; valid values are from 0 to 63.

Defaults

The default CoS-to-DSCP configuration settings are shown in the following table:

cos	0	1	2	3	4	5	6	7
DSCP	0	8	16	24	32	40	48	56

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

This command is not supported on the Supervisor Engine 6-E and Catalyst 4500M chassis. In place of this limited map capability, the Supervisor Engine 6-E and Catalyst 4500M chassis supports the setting of various marking fields in a packet within a policy map. Refer to the **set** command for more details.

The CoS-to-DSCP map is used to map the packet CoS (to the interfaces that are configured to trust CoS) to the internal DSCP value. This map is a table of eight CoS values (0 through 7) and their corresponding DSCP values. The switch has one map.

Examples

This example shows how to configure the ingress CoS-to-DSCP mapping for CoS 0:

```
Switch(config)# qos map cos 0 to dscp 20
Switch(config)#
```

This example shows how to clear the entire CoS-to-DSCP mapping table:

```
Switch(config)# no qos map cos 0 to dscp 20
Switch(config)#
```

Related Commands	Command	Description
	qos map dscp	Maps the DSCP values to selected transmit queues and to map the DSCP to Cos values.
	qos map dscp policed	Sets the mapping of the policed DSCP values to the marked-down DSCP values.
	show qos	Displays QoS information.
	sdbinsp (refer to Cisco IOS documentation)	Modifies metric and tag values when the IP routing table is updated with BGP learned routes.

qos map dscp

To map the DSCP values to selected transmit queues and to map the DSCP-to-CoS value, use the **qos map dscp** command. To return to the default value, use the **no** form of this command.

qos map dscp *dscp-list* **tx-queue** *queue-id*

no qos map dscp *dscp-list* **tx-queue** *queue-id*

qos map dscp *dscp-list* **to** *cos-value*

no qos map dscp *dscp-list* **to** *cos-value*

dscp-list	List of DSCP values to map to the queue ID, valid values are from 0 to 63.
tx	Defines mapping.
tx-queue	Sets class a transmit queue.
queue-id	Transmit queue, valid values are from 1 to 4.
to	Specifies the CoS value.
cos-value	Class of service, valid values are from 1 to 7.

Syntax Description

Defaults

The default DSCP-to-CoS configuration settings are shown in the following table:

DSCP	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
CoS	0	1	2	3	4	5	6	7

Command Modes

Global configuration mode

Command History	**Release**	**Modification**
	12.1(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Command History

Usage Guidelines

This command is not supported on the Supervisor Engine 6-E and Catalyst 4500M chassis. In place of this command the Supervisor Engine 6-E and Catalyst 4500M chassis uses the **table-map** command for QoS marking. Please refer to the **table-map** command for details.

You use the DSCP-to-CoS map to map the final DSCP classification to a final CoS. The CoS map is written into the ISL header or 802.1Q tag of the outgoing packet on trunk interfaces and contains a priority and a VLAN identifier. The switch uses the CoS to decide the switch fan-out map. You can mow up to eight DSCP values, separated by spaces, for a CoS value.

The DSCP-to-transmit-queue map is used to map the final DSCP classification to a transmit queue. You can mow up to eight DSCP values, separated by spaces, for a transmit queue.

Examples

This example shows how to configure the egress DSCP-to-CoS mapping:

```
Switch(config)# qos map dscp 20 25 to cos 3
Switch(config)#
```

This example shows how to configure the egress DSCP-to-transmit queue:

```
Switch(config)# qos map dscp 20 25 to tx-queue 1
Switch(config)#
```

Related Commands	Command	Description
	qos map cos	Defines the ingress CoS-to-DSCP mapping for the trusted interface.
	show qos interface	Displays queueing information.
	show qos	Displays QoS information.
	debug (refer to Cisco IOS documentation)	Modifies enable and log options when the IP routing table is updated with BGP-learned routes.
	tx-queue	Configures the transmit queue parameters for an interface.

qos map dscp policed

To set the mapping of the policed-DSCP values to the marked-down DSCP values, use the **qos map dscp policed** command. To restore a prior entry, use the **no** form of this command.

qos map dscp policed *dscp_list* **to** *dscp_policed_dscp*

no qos map dscp policed

Syntax Description

dscp_list	DSCP values; valid values are from 0 to 63.
to *dscp*	Defines mapping.
policed_dscp	Marked-down DSCP values; valid values are from 0 to 63.

Defaults

Mapping of DSCP values is disabled.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(8)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

This command is not supported on the Supervisor Engine 6-E and Catalyst 4500M chassis. Various policer types are supported on the Supervisor Engine 6-E and Catalyst 4500M chassis that supports *explicit* QoS marking of DSCP precedence, and CoS fields. Refer to the **police** command for details.

The DSCP-to-policed-DSCP map determines the marked-down DSCP value that is applied to the out-of-profile flows. The switch has one map.

You can enter up to eight DSCP values, separated by spaces.

You can enter only one policed DSCP value.

Note To avoid out-of-sequence packets, configure the DSCP-to-policed-DSCP map so that marked-down packets remain in the same queue as in-profile traffic.

Examples

This example chest how to map multiple DSCPs to a single policed-DSCP value:

```
Switch(config)# qos map dscp policed 20 25 43 to dscp 4
Switch(config)#
```

Related Commands

Command	Description
qos map cos	Defines the ingress CoS-to-DSCP mapping for the trusted interfaces.
qos map dscp	Maps the DSCP values to selected egress queues and to map the DSCP-to-CoS value.
show qos	Displays QoS information.

qos rewrite ip dscp

To enable DSCP rewrite for IP packets, use the **qos rewrite ip dscp** command. To disable IP DSCP rewrite, use the **no** form of this command.

qos rewrite ip dscp

no qos rewrite ip dscp

Syntax Description This command has no arguments or keywords.

Defaults IP DSCP rewrite is enabled.

Command Modes Global configuration mode

Command History	Release	Modification
	12.2(25)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines This command is not supported on the Supervisor Engine 6-E and Catalyst 4500M chassis.

If you disable IP DSCP rewrite and enable QoS globally, the following events occur:

- The ToS byte on the IP packet is not modified.
- Marked and marked-down DSCP values are used for queueing.
- The normally derived DSCP (as per the trust configuration on the interface or VLAN policy) is used for intserm queue and Layer 2 CoS determination. The DSCP is not rewritten on the IP packet header.

If you disable QoS, the CoS and DSCP of the incoming packet are preserved and are not rewritten.

Examples This example shows how to disable IP DSCP rewrite:

```
Switch(config)# no qos rewrite ip dscp
Switch(config)#
```

Related Commands

Command	Description
qos (global configuration mode)	Enables QoS functionality on the switch.
show qos	Displays QoS information.

qos trust

To set the trusted state of an interface (for example, whether the packets arriving at an interface are trusted or carry the correct CoS, ToS, and DSCP classification), 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 VLAN 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

Command History

Release	Modification
12.1(8)EW	Support for this command was introduced on the Catalyst 6500 series switch.
12.1(11)EW	Support for extending trust for voice was added.
12.1(20)EW	Support for trust device Cisco IP phone was added.

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 where 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 ingress CoS is always the incoming packet CoS (or the default CoS for the interface, if the packet is not tagged).

When the interface trust state is not **qos trust dscp**, the security and QoS ACL classification will always use the interface DSCP and not 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-if)# qos trust cos
Switch(config-if)#
```

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 IP/TCP 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	Defines the default CoS value for an interface.
qos vlan-based	Defines per-VLAN QoS for a Layer 2 interface.
show qos interface	Displays QoS information for an interface.

qos vlan-based

To enable per-VLAN QoS for a Layer 2 interface, use the **qos vlan-based** command. To disable per-VLAN QoS for a Layer 2 interface, use the **no** form of this command.

qos vlan-based

no qos vlan-based

Syntax Description This command has no arguments or keywords.

Defaults Per-VLAN QoS is disabled.

Command Modes Interface configuration mode

Command History

Release	Modification
12.1(8)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines This command is not supported on the Supervisor Engine 6-E and Catalyst 4500M chassis. On the Supervisor Engine 6-E and Catalyst 4500M chassis various QoS marking and policing actions at the interface and VLAN level are aggregately merged. For details, refer to the *Catalyst 4500 Series Switch Configuration Guide*.

In VLAN-based mode, the policy map that is attached to the Layer 2 interface is ignored, and QoS is driven by the policy map that is attached to the corresponding VLAN interface.

Per-VLAN QoS can be configured only on the Layer 2 interfaces.

If no input QoS policy is attached to a Layer 2 interface, then the input QoS policy that is attached to the VLAN (on which the packets received), if any, is used even if the port is not configured as VLAN-based.

If you do not want this default, attach a placeholder input QoS policy to the Layer 2 interface.

Similarly, if no output QoS policy is attached to a Layer 2 interface, then the output QoS policy that is attached to the VLAN (on which the packet is transmitted), if any, is used even if the port is not configured as VLAN-based.

If you do not want this default, attach a placeholder output QoS policy to the Layer 2 interface.

Layer 3 interfaces are always in interface-based mode. Layer 2 VLAN interfaces are always in VLAN-based mode.

Examples This example shows how to enable per-VLAN QoS for a Layer 2 interface:

```
Switch(config-if)# qos vlan-based
Switch(config-if)#
```

Related Commands	Command	Description
	qos cos	Defines the default CoS value for an 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 restore the queue packet limit from a class, use the **no** form of this command.

queue-limit *number-of-packets*

no queue-limit *no number-of-packets*

Syntax Description

number-of-packets	Number of packets that the queue for this class can accumulate; valid range is 16–16384. This number must be a multiple of 8.

Defaults

By default, each physical interface on a Catalyst 4500 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

Command History

Release	Modification
12.2(40)SG	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

This class-based queuing (CBQ) command applies only to the Supervisor Engine 6-E as part of the MQC support on the Catalyst 4500 Supervisor Engine.

By default, each physical interface on a Catalyst 4500 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 in each slot. The switch supports 31.2K queue-entries of which 100 K are set aside as a common shardbe pool. The remaining 412 K entries are equally distributed among the slots. Each slot further divides its allocated queue entries equally among its ports.

CBQ creates a queue for every class for which a class map is defined. Packets satisfying the match criteria 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 effect.

Note The queue-limit command is supported only after you first configure a scheduling action, such as bandwidth, shape, 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 class101. Policy for this class is set so that the queue reserved for it has a maximum packet limit of 40:

```
Switch(config)# configure terminal
Switch(config)# policy-map policy11
Switch(config-pmap)# class class101
Switch(config-pmap-c)# queue-limit 40
Switch(config-pmap-c)# queue-limit 40
Switch(config-pmap-c)# end
Switch#
```

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-default queueing)	Enables traffic shaping a class of traffic in 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

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch (Catalyst 4507R and 4510R only).

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 reenable redundancy, the switch returns to default redundancy settings.

Use the **exit** command to exit the redundancy configuration mode.

Examples This example shows how to enter redundancy mode:

```
Switch(config)# redundancy
Switch(config-red)#
```

This example shows how to enter the main CPU submode:

```
Switch(config)# redundancy
Switch(config-red)# main-cpu
Switch(config-r-mc)#
```

Related Commands

Command	Description
auto-sync	Enables automatic synchronization of the configuration files in NVRAM.
mode rpr	Enters the main CPU submode and manually synchronize the configurations on the two supervisor engines.

redundancy config-sync mismatched-commands

To move the active supervisor engine into the Mismatched Command List (MCL) and reset the standby supervisor engine, use the **redundancy config-sync mismatched-commands** command.

If your active and standby supervisors engines are running different version 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 system clock 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

Command History	**Release**	**Modification**
	12.2(31)SG-A	This command was introduced on the Catalyst 4500 series switch.
	12.2(52)SG	Updated command name from **issu config-sync** to **redundancy config-sync**.

Usage Guidelines The following is a log entry example for mismatched commands:

```
00:06:51: %redfp-3-psv: Bulk-sync failure due to Servicing Incompatibility. Please check
standby syslog for additional reason
00:06:51: %redfp-3-psv: Bulk-sync failure due to Servicing Incompatibility. Please check
standby syslog for additional reason
00:06:51: %redfp-3-psv: Starting lines from MCL file:
00:06:51: %redfp-3-psv: interface V11
00:06:51: %redfp-3-psv: ! no ip address
00:06:51: %redfp-3-psv: ip address 11.0.0.1 255.0.0.0
00:06:51: %redfp-3-psv: ! no shutdown
```

To display all minimal bed 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 reloading 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 still 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 establish SSO, after removing the offending configuration and rebooting the standby supervisor engine, fail because of a version mismatch. The CARD_REDUNDANCY-3-IOS_VERSION_CHECK_FAIL and ISSU-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 entries from the MCL:

```
Router#redundancy config-sync validate mismatched commands
Router#
```

Related Commands	Command	Description
	show redundancy config-sync	Displays an ISSU config-sync failure or the ignored mismatched 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

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch (Catalyst OS software).

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 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**}

peer	Reloads the peer unit.
shelf	Reboots both supervisor engines.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.2(52)SG	Support for this command was introduced on the Catalyst 4500 series switch (Catalyst 4507R only).

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:

```
Router(config)# redundancy reload shelf
Reload shelf
```

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

Command History

Release	Modification
12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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:

```
Switch> remote login module 5
Trying Gateway, 2002 ... Open
Type 'exit' at the Gateway 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

Command History	Release	Modification
	12.1(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to convert a VLAN into an RSPAN VLAN:

```
Switch(config-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 none** | **inet**]

Syntax Description	**validation none** (Optional) Specifies that the checksum associated with the content of the file specified by the URL is not verified.
	inet (Optional) Specifies the file from which the read is performed.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.1(20)EW	Support for this command was introduced on the Catalyst 6500 series switch.

Usage Guidelines If the URL is not provided, the switch tries to read the file from the cached memory.

Examples This example shows how to renew the DHCP binding database while bypassing the CRC checks:

```
Switch# renew ip dhcp snooping database validation none
Switch#
```

Related Commands	Command	Description
	ip dhcp snooping	Globally enables DHCP snooping.
	ip dhcp snooping binding	Sets up and gives axx a DHCP binding configuration to restore bindings across reboots.
	ip dhcp snooping info-option agent	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.

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

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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

Command History

Release	Modification
12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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

Command History

Release	Modification
12.1(8)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.2(25)EWA	Support for applying different QoS policies on VLANs was introduced.

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.

Non-Supervisor Engine 6-E

You cannot apply a policy map under an interface and a VLAN range at the same time.

To attach a service policy to a VLAN an SVI must be created for the VLAN and the policy must be applied to the SVI.

Supervisor Engine 6-E and Catalyst 4500E classic

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
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config-if)# interface fastethernet 5/20
Switch(config-if)# service-policy input pmap1
Switch(config-if)# exit
Switch(config)#
```

This example shows how to apply policy map p1 for traffic in VLAN 20 and 400, and policy map p2 for traffic in VLAN 300 through 301:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet 4/4
Switch(config-if)# autoqos trust acceptable delay
Switch(config-if)# autoqos mode trust
Switch(config-if)# exit
Switch(config)# interface range p1 p2
Switch(config-if-range)# service-policy input p1
Switch(config-if-range)# exit
Switch(config-if-range)# interface 301
Switch(config-if-range)# service-policy output p2
Switch(config-if-range)# end
Switch# show policy-map interface gigabitethernet 4/4 vlan 20
GigabitEthernet4/4 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 4/4
GigabitEthernet4/4 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

GigabitEthernet4/4 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

GigabitEthernet4/4 vlan 301

  Service-policy output: p2

    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets
```

```
        policy: Ber-interface
          Cmefced: 0 bytes Ormed: 0 bytes

Gigabitethernet4/1 vlan 400

  Service-policy input: pl

    Class-map: vlan-default (match-any)
      0 packets,
      Match: any
        0 packets
      policy: Ber-interface
        Cmefced: 0 bytes Ormed: 0 bytes
```

This example shows how to attach a policy map to a VLAN using an SVI on a non-Supervisor Engine 6-E:

```
Switch#conf configure terminal
Switch(config)#interface vlan 10
Switch(config-if)#service-policy ser policy-vlan
Switch(config-if)#end
Switch#
```

This example shows how to attach a policy map to a VLAN using a Supervisor Engine 6-E:

```
Switch#conf configure terminal
Switch(config)#vlan configuration 10
Switch(config-vlan-config)#service-policy ser policy-vlan
Switch(config-vlan-config)#end
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.
	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

Command History	**Release**	**Modification**
	7.0 (12.2)SY	Support for this command was introduced on the Catalyst 6500 series switch.
	12.2.18SXF	Added support for Supervisor Engine 6-E and Catalyst 4500E chassis.

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#configure terminal
Switch(config)#policy-map child
Switch(config-pmap)#class voice
Switch(config-pmap-c)#priority
Switch(config-pmap-c)#exit
Switch(config-pmap)#exit
Switch(config)#policy-map parent
Switch(config-pmap)#class class1
Switch(config-pmap-c)#police 32k
Switch(config-pmap-c)#service-policy child
Switch#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 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 queuing [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 queuing)**~~	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

Command History	**Release**	**Modification**
	12.2(18)SXD	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines In this release, the only policy-map accepted on the control-plane is system-cpp-policy. It is already set up by the system and cannot be changed. The system-cpp-policy is the recommended name for **global macro system-cpp** (internal 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 controlled, while allowing all remaining Telnet packets to be policed at the rate specified.

```
Router(config)# access-list 140 deny tcp host 10.1.1.1 any eq telnet
! Allow 10.1.1.2 unicast host traffic
Router(config)# access-list 140 deny tcp host 10.1.1.2 any eq telnet
! Rate limit all other Telnet traffic
Router(config)# access-list 140 permit tcp any any eq telnet
! Define class-map "telnet-class"
Router(config)# class-map match-all telnet-class
Router(config-cmap)# match access-group 140
Router(config-cmap)# exit
Router(config)# policy-map control-plane-policy
Router(config-pmap)# class telnet-class
Router(config-pmap-c)# police 8000 conform transmit exceed drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# control-plane service-for the entire Route Processor.
```

```
Switch(config)# control-plane
Switch(config-cp)# service-policy input control-plane-policy
Switch(config-cp)# end
```

Related Commands

Command	Description
control-plane	Enters control-plane configuration mode.
macro 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 attached a class or all classes for the policy map of a control plane.

session module

Note This command is only supported in SSO mode and does 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

Command History	Release	Modification
	12.2(25)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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 without requiring a physical connection to the standby console. It uses IPC over EOBC 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 onto 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-console#, 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 is also closed. However, the virtual console is also automatically terminated when the standby is rebooted. After the standby boots up, you need to enter another virtual console session.

The following limitations apply to the standby virtual console:

- Alt-commands on the virtual console run to completion. It does not provide the auto-more feature; it behaves as if the **terminal length 0** command has been executed. It is also 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 times-out 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 3
Trying 127.0.0.3, 2001 ... Open
Type "exit" or "quit" to end session

Switch-standby-console#ls unit
Switch#
```

If the standby console is not enabled, the following message appears:

```
Switch-standby-console#
Standby console disabled
Switch-standby-console#ls unit, 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*} | {**dscp** *new-dscp*} | **precedence** *new-precedence*} | **qos-group** *value*}

no set *cos new-cos* | {**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 can be any of service (ToS) traffic class byte in the IPv4 IPv6 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 classified packet on ingress to an interface.

Defaults

No marking is established packets.

Command Modes

Policy-map class configuration mode

Command History

Release	Modification
12.1(5)XW	Support for this command was introduced on the Catalyst 6500 series switch.
12.2(40)SG	Added support for Supervisor Engine 6-E and Catalyst 4500M chassis.

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, which is the same meaning as **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 pl with CoS values assigned to different traffic types. Class maps for voice and video-data have already been created.

```
Switch(config)#policy-map pl
Switch(config-pmap)# class voice
Switch(config-pmap-c)# set cos 5
Switch(config-pmap-c)# exit
Switch(config-pmap)# class video-data
Switch(config-pmap-c)# set cos 4
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

Command History	Release	Modification
	12.2(18)SXF	Support for this command was introduced on the Catalyst 4500 series switch using a Supervisor Engine 6-E and Catalyst 4900M chassis.

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 inline-name sequence, the default action will be to copy the value associated with the "from-field" category as the Cos value. For instance, if you configure the **set cos precedence** command, the precedence value will be copied and used as the Cos value.

You can do the same 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)#policy-map cos-set
Switch(config)#policy-map)#class voice
Switch(config)#policy-map)#set cos 5
Switch(config)#policy-map)#exit
Switch(config)#policy-map)#class video-data
Switch(config)#policy-map)#set cos 4
Switch(config)#policy-map)#exit
Switch#
```

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-match
Switch(config)#policy-map)#set cos precedence table table-map1
Switch(config)#policy-map)#end
Switch#show
```

Related Commands	Command	Description
	match (class-map)	Defines the match criteria for a class map.
	configure (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.

Command	Description
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	Specific 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

Command History

Release	Modification
12.2(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.2(18)EW	Added support for "from-field" for policy-map configuration on a Supervisor Engine 6-E.

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 in 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 "Type-field" packet-marking category to be used for mapping and setting the DSCP value. The "Type-field" packet-marking categories are as follows:

- Class of service (CoS)
- QoS group
- Precedence
- Differentiated services code point (DSCP)

If you specify a "Type-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 "Type-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 Values in IPv4 Packets only

When this command is used in IPv4 environments, the default match-any keyword is used. IPv4 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 Values 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 Values for IPv4 Packets Only

To set DSCP values for IPv4 packets only, use the **ipv4** keyword with 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 use 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#configure terminal
Switch(config)#policy-map policy1
Switch(config-pmap)#class class-default
Switch(config-pmap-c)#set dscp cos 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 state 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	Specifies 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

Command History

Release	Modification
12.2(18)EW	Support for this command was introduced on the Catalyst 4500 series switches.
12.2(40)SG	Added support for "from-field" for policy-map configured on a Supervisor Engine 6-E.

Usage Guidelines

Command Compatibility

The **set precedence** command cannot be used with the **set dscp** command to mark the same packet. The two values, DSCP and precedence, are mutually exclusive. A packet can be one value or the other, but not both.

qos precedence

You can use this command to specify the "from-field" packet-matching category to be used for mapping and setting the precedence value. The "from-field" packet-matching 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 argument, 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 value associated with CoS will be used as the precedence value.

You can do this based on the QoS group packet-matching 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 first two significant bits of qos-group are copied to precedence.

Precedence Values in IPv6 Environments

When this command is used in IPv6 environments it can set the value in both IPv4 and IPv6 packets. However, the actual packets 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 ipv4** command must also be used in the class-map that classified packets for this action. Without the **match protocol ipv4** command, the class-map may classify both IPv4 and IPv6 packets, (depending on other match criteria) and these **precedence** commands 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 similarly to the keyword like the **match ipv precedence** or **match ip dscp** command or include the **match protocol ip** command along with other criteria in the class-map. Without the additional keyword, the class-map may match both IPv4 and IPv6 packets (depending on the other match criteria) and the **set precedence** or **set dscp** command may act upon both types of packets.

Examples

In the following example, the policy-map named policy-vlan is created over the values defined in a table-map named tabletest-map1. The table-map named tabletest-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)# configure terminal
Switch(config)# policy-map policy-vlan
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set precedence cos table table-map1
Switch(config-pmap-c)# end
Switch#
```

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 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 (ID) 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 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 qos-group

To set a quality of service (QoS) group identifier (QI) 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

Command History	**Release**	**Modification**
	12.2(50)SG	Support for this command was introduced on the Catalyst 4500 series switch using a Supervisor Engine 6-E and Catalyst 4500M chassis.

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 to 5:

```
Switch(config)# configure terminal
Switch(config)# policy-map p1
Switch(config-pmap)# class c1
Switch(config-pmap-c)# set qos
Switch(config-pmap-c)# set qos-group 5
Switch(config-pmap-c)# end
Switch#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.
	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 {*mrtd* | **bps** | **kbps** | **mbps** | **gbps**}

shape average percent {*percent*_*value*}

no shape average

mrtd	Specifies an average rate for traffic shaping; the range is 16000 to 10000000000. Specify the value in bits per second. Only one 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

Command History	Release	Modification
	12.2(20)EWA	This command was introduced on the Catalyst 4500 series switch using a Supervisor Engine 6E.

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 distinct from policing. Policing drops packets that exceed a configured threshold, but shaping buffers packets so that 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# 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)# 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 1000000000. Peer-Rx 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

Command History	**Release**	**Modification**
	12.2(54)SG	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

This command is not supported on the Supervisor Engine 6-E and Catalyst 4900M chassis.

Traffic shaping is available on all the ports, and it sets an upper limit on the bandwidth.

When the high shape rates are configured on the Catalyst 4500 Supervisor Engine II-Plus-10GE (WS-X4515/10GE) and Catalyst 4500 Supervisor Engine V-10GE (WS-X4516/10GE), the Catalyst 4500 Supervisor Engine V-10GE (WS-X4516-10GE), the shaped traffic sometimes can be affected in situations that involve contention and unusual packet size distributions. On the ports that are multiplexed through a Stub ASIC and connected to the backplane gigaports, the shape rates above 7 Mbps may not be achieved under worst-case conditions. On ports that are connected directly to the backplane gigaports, or the supervisor engine gigaports, the shape rates above 50 Mbps may not be achieved under worst-case conditions.

Some examples of ports that are connected directly to the backplane are as follows:

- Uplink ports on Supervisor Engine II+, II+-10GE, III, IV, V, and V-10GE
- 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 20-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 line card
- 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)# tx-queue 3
Switch(config-if-tx-queue)# shape 70m
Switch(config-if-tx-queue)#
```

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

Command History	**Release**	**Modification**
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.2(25)EW	Support for the 10-Gigabit Ethernet interface was introduced on the Catalyst 4500 series switch.

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 FastEthernet interface 6/1:

```
Switch# show access-group mode interface fa6/1
interface fastethernet6/1
    access-group mode l4-merge
Switch#
```

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 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**, **pos**, **fddi**, 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

Command History	**Release**	**Modification**
	12.2(25)EW	Extended to include the 10 Gigabit Ethernet interface.

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 router.
- Time left before the adjacency rolls out of the adjacency table. After it rolls out, a packet must use the same next hop to the destination.

Examples

This example shows how to display adjacency information:

```
Router# show adjacency
Protocol Interface          Address
IP       Port-Channel1.3    172.20.52.1(10425)
IP       Port-Channel1.3    172.20.52.22(11)
Router#
```

This example shows how to display a summary of adjacency information:

```
Router# show adjacency summary
Adjacency table has 2 adjacencies
  Interface     Adjacency Count
  Port-Channel1.3  2
Router#
```

This example shows how to display protocol detail and timer information:

```
Router# show adjacency detail
Protocol Interface          Address
IP       Port-Channel1.3    172.20.52.1(10425)
                            0 packets, 0 bytes
                            00000000FF990000080000000800
                            AGE    00:04:12 RTR(0)
                            0000000A7A0C0000AC1434010800
IP       Port-Channel1.3    172.20.52.22(11)
                            0 packets, 0 bytes
                            00000000FF990000080000000800
                            00241C9C0C0000AC1434160800
                            AGE    00:04:06
Router#
```

This example shows how to display adjacency information for a specific interface:

```
Router# show adjacency Port-Channel1.3
Protocol Interface          Address
IP       Port-Channel1.3    172.20.52.1(10425)
IP       Port-Channel1.3    172.20.52.22(11)
Router#
```

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** *group-addr*] [**source** *source-addr*] | | **interface** *interfaceinfo*]

Syntax Description

group *group-addr*	(Optional) Specifies a multicast group address.
source *source-addr*	(Optional) Specifies a multicast source address.
interface *interfaceinfo*	(Optional) Specifies a multicast flowing on a specific interface.

Defaults

Displays all the multicast streams activated with ANCP.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(50)SG	Support for this command was introduced on the Catalyst 4500 series switch.

Examples

This example shows how to display multicast streams activated by ANCP:

```
ANCP-Client# show ancp mci
ANCP Multicast Streams
Interface: GigabitEthernet1/1.mcast vx
Group 225.1.1.1
0x0100000F000A0703 16 Pd/5 18:27:05 UTC Sat Sep 13 2008
0x0100000F000A0703 16 Pd/5 18:27:05 UTC Sat Sep 13 2008
0x0100000F000A0704 20 Pd/5 18:27:05 UTC Sat Sep 13 2008
0x0100000F000A0704 20 Pd/5 18:27:05 UTC Sat Sep 13 2008
0x0100000F000A0704 20 Pd/5 18:26:43 UTC Sat Sep 13 2008
Group 230.1.2.2
0x0100000F000A0703 16 Pd/5 18:27:07 UTC Sat Sep 13 2008
0x0100000F000A0703 16 Pd/5 18:27:07 UTC Sat Sep 13 2008
0x0100000F000A0704 20 Pd/5 18:26:43 UTC Sat Sep 13 2008
0x0100000F000A0704 20 Pd/5 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

Command History	Release	Modification
	12.1(13)E14	Support for this command was introduced on the Catalyst 6500 series switch.

Examples This example shows how to display the ARP ACL information for a switch:

```
Switch# show arp access-list
arp access-list ARP1
    permit ip 10.101.1.1 0.0.0.255 mac any
    permit ip 20.3.1.0 0.0.0.255 mac any
```

Related Commands

Command	Description
access-group mode	Specifies the override modes (for example, VACL-overridden 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*]

Syntax Description	**interface** *interface* — Displays all of the Auth Manager details associated with the specified interface. **registration** — 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 single or in combinations 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**
Command Default	This command has no default settings.
Command Modes	EXEC

Command History	**Release**	**Modification**
	12.2(54)SG	This command was introduced.

Usage Guidelines

Table 2–13 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, "Authz Success" or "Auths Failed" are displayed. "No methods" 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.
Authz 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 2-14 lists the possible values for the state of methods. For a session in terminal state, "Authc Success," "Authz 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 2-14 *State Method Values*

Method State	Status 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.
Authz 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 authentication registrations
Auth Methods registered with the Auth Manager:
Handle Priority Name
2 0 dot1x
3 1 mab
5 2 webauth
7 3 dot11
```

The following example shows how to display Auth Manager details for a specific interface.

```
Switch# show authentication interface gigabitethernet1/0/23
Client list:
MAC Address Domain Status Handle Interface
000e.84c5.99bd DATA Authz Success 0x4B000000 GigabitEthernet1/0/23
Available methods list:
Handle Priority Name
```

```
3 0 dot1x
Remotely authorm list:
Handle Security Name
3 0 dot1x
Switch#
```

The following example shows how to display all Auth Manager sessions on the switch:

```
Switch# show authorization session
Interface MAC Method Domain Status Session ID
Gi1/0/48 0015.63b0.f676 dot1x DATA Authz Success 0A030107000000C0090D9180
Gi1/0/2 0000.5000.0000 N/A DATA Authz Success 0A030107000000C0090D9180
```

The following example shows how to display all Auth Manager sessions on an interface:

```
Switch# show authorization session int g1/48
Interface: GigabitEthernet1/48
Mac Address: 0015.63b0.f676
IP Address: Unknown
Status: Authz Success
Domain: DATA
Oper Host Mode: multi-host
Oper control dir: both
Authorized By: Guest Vlan
Vlan Policy: 146
Session timeout: N/A
Idle timeout: N/A
Common Session ID: 0A030107000000C0090D9180
Acct Session ID: 0x00000006
Handle: 0xC0000008
Runnable methods list:
Method State
dot1x Failed over
```

The following example shows how to display Auth Manager session for a specified MAC address:

```
Switch# show authorization session mac 000e.84ad.0966
Interface: GigabitEthernet1/2
MAC Address: 000e.84ad.0966
Status: Authz Success
Domain: DATA
Oper host mode: single-host
Authorized By: Authentication Server
Vlan Policy: 10
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 authorization session method mab
No auth Manager Sessions match supplied criteria
Interface: GigabitEthernet1/23
MAC Address: 0000.0000.0000
Status: Authz Success
Domain: DATA
Oper Host Mode: single-host
Authorized By: Authentication Server
Vlan Policy: 10
Handle: 0x88000000
Runnable methods list:
Method State
dot1x Failed over
mab Authz Success
Switch#
```

The following example shows how to display all clients authorized via a specified auth method:

```
Switch# show authorization session method mab
No auth Manager Sessions match supplied criteria
Interface: GigabitEthernet1/23
MAC Address: 0000.0000.0000
Status: Authz Success
Domain: DATA
Oper Host Mode: single-host
Authorized By: Authentication Server
Vlan Policy: 10
Handle: 0x88000000 Gigabitethernet1/23
Switch#
```

Related Commands

Command	Description
authentication control-direction	Changes the port control to unidirectional 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.
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

Command History	Release	Modification
	12.2(25)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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             : 30.0.0.5
Config File Download    : Downloaded
```

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** 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 valid interface keywords, enter **?** after **interface**.
begin	(Optional) Begins output 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

Command History

Release	Modification
12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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 on a non-Supervisor Engine 6-E, 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* do not appear, 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
GigabitEthernet1/1
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 | 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 EXEC.

Command History	Release	Modification
	12.1(18)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to display file system status information:

```
Switch#: show bootflash: filesys
--------- F I L E  S Y S T E M  S T A T U S --------
  Device Number = 0
DEVICE INFO: bootflash
  Magic Number     = 4D4F5343  File System Vers = 10000   (1.0)
  Length           = 1000000   Sector Size     = 40000
  Programming Algorithm = 4    Erased State    = FFFFFFFF
  File System Offset    = 40000  Length = F40000
  MONLIB Offset         = 100    Length = C628
  Bytes Used Offset     = 800000 Length = 40008
  Squeezed Log Offset   = 880000 Length = 40000
  Squeezed Buffer Offset = 8C0000 Length = 40000
  Num Spare Sectors     = 0
  Spare Offset
STATUS INFO:
  Writable
  NO File Open for Write
  Complete Stat
  NO Squeeze in progress
SQUEEZE INFO:
  Bytes Used      = 917108  Bytes Available = 62892
  Sed Sectors     = 0       Spared Sectors  = 0
  Total Files     = 5       Total Bytes     = 917588
  Deleted Files   = 0       Bytes          = 0
  Files w/Errors  = 0       Bytes          = 0
Switch#:
```

This example shows how to display system image information:

```
Switch> show bootflash:
-# - ED --type- --crc--- --seed- --nlen -length- --date/time------ --name-
1  .. image  A0A2B3A1  2A7A0C  14  2303824 Aug 23 1999 16:18:45 c2955-ms
2  .. image  D8DEB8A2  9C5C8B  8   2470216 Aug 23 1999 13:48:48 sp.bin

62416896 bytes available (9514496 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     0A0A0A01  File System Vers = 10000   (1.0)
  Length           =  4194000  Sector Size   =  40000
  Programming Algorithm = 39   Erased State  = FFFFFFFF
  Pseudo Date Stamp = 0x0      Real Date Stamp = 0x0
  BUNDLE Offset     =  100     Length = 2A28
  Bad Sector Map Offset = 3FFFF  Length = 80
  Bytes Used Offset = 83000    Length = 40000
  Squeeze Log Offset = 81000   Length = 40000
  Squeeze Buffer Offset = 81000  Length = 40000
  Num Spare Sectors  = 0
  Spares:
STATUS INFO:
  Writable
  NO File Open for Write
  Complete Stats
  No Unclosed Files
  No Squeeze in progress
BLOCK INFO:
  Block Size  = 917508  Bytes Available = 62416896
  Bad Sectors = 0       Spared Sectors  = 0
  OK Files    = 2       Bytes = 917508
  Deleted Files = 0     Bytes = 0
  Files of Unknown = 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

Command History	Release	Modification
	12.1(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to display BOOT environment variable information:

```
Switch# show bootvar
BOOT variable = sup:1
CONFIG_FILE variable = disk0: mnt nmlat
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 Sunset Cisco IOS releases; use the **diagnostic start** command instead.

Syntax Description

interface *interface* *interface-number*	Interface type; valid values are **fastethernet** and **gigabitethernet**. Module and port number.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Command History

Release	Modification
12.2(25)SG	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines The TDR test is supported on Catalyst 4500 series switches running Cisco IOS Release 12.2(25)SG 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 distance to the fault is displayed in meters (m).

Examples This example shows how to display information about the TDR test:

```
Router# show cable-diagnostics tdr interface gi4/13
Interface Speed  Local pair  Pair  Cable  Length  Remote pair  Channel  Status
Gi4/13    10Mps  1-2        1-2   100 +- 30m    Unknown      Pair 1   
                 3-6        3-6   100 +- 30m    Unknown      Pair 2   
                 4-5        4-5   100 +- 30m    Unknown      Pair 3   
                 7-8        7-8   100 +- 30m    Unknown      Pair 4   

Router#
```

Table 2-15 describes the fields in the **show cable-diagnostics tdr** command output.

Table 2-15 show cable-diagnostics tdr Command Output Fields

Field	Description
Interface	Interface tested.
Speed	Current line speed.
Pair	Tested pair name.
Cable Length	Distance to the fault in meters (m).
Channel	Pair designation (A, B, C, or D).
Status	Pair status displayed is 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 conditions of copper cables on 48-port 10/100/1000 RJ45 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 (#)

Command History	Release	Modification
	12.2(52)SG	This command was introduced on the Catalyst 4500 series switch, Supervisor Engine 6-E, and Catalyst 4900M chassis.

Examples The following example displays the configured CallHome settings:

```
Cat4500 show call-home
Current call home settings:
    call home feature : disable
    call home message's from address: sw1@cha@cha.com
    call home message's reply-to address: support@cha@cha.com

    vrf for call home messages: Not yet set up

    contact person's email address: technical@cha@cha.com

    contact person's phone number: +1-408-555-1234
    street address: 1234 Picaboo Street, any city, any state, 12345
    customer ID: ExampleCorp
    site ID: SantaClara1234
    site ID: SantaClara
    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                          Disable configuration info
  diagnostic                             Disable diagnostic info
  environment                            Disable environmental info
  inventory                              Enable  inventory info
  syslog                                 Disable syslog info

Profiles:
  Profile Name: campus-noc
  Profile Name: CiscoTAC-1

Subscribed
```

Configured Callhome Information is Dumped

```
Subscribed show call-home detail
  Profile campus-noc (inactive)
    call home destsrc : disable
    call home message's from address: auth@domain.com
    call home message's reply-to address: support@domain.com

    url for call-home messages: Not yet set up

    contact person's email address: tac@tac@domain.com

    contact person's phone number: +1-408-555-1234
    street address: 1234 Broadon Street, Any city, Any state, 12345
    customer ID: SampleCorp
    site ID: SJ-Campus-1
    site ID: Identifier
    Mail-server[1]: Address: smtp.domain.com Priority: 1
    Mail-server[2]: Address: 192.168.2.1 Priority: 2
    Rate-limit: 20 messages per minute

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

Profiles:
  Profile Name: campus-noc
    Profile status: ACTIVE
    Preferred Message Format: long-text
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(s): noc@campus.com
    HTTP address(s): Not yet set up

    Alert-group             Severity
    ---------------------------------------------------------------
    inventory               minor

    Syslog-Pattern          Severity
    ---------------------------------------------------------------
    N/A                     N/A

  Profile Name: CiscoTAC-1
    Profile status: ACTIVE
    Preferred Message Format: xml
```

```
Message Size Limit: 3145728 Bytes
Email-addresses: cu@cisco.com
Email addresses: cu1@cisco1.com
HTTP addresses: https://tools.cisco.com/its/service/oddce/services/DDCEService

Periodic notification enabled sunday 1 day of the month at 09:27

Periodic inventory info message is scheduled every 1 day of the month at 09:32

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                        Disable 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
    Email-addresses: noc@example.com
    Email addresses: noc@example.com
    HTTP addresses: 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/DDCMService

    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 CiscoTAC-1
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/DDCMService

    Periodic configuration info message is scheduled every 11 day of the month at 11:26

    Periodic inventory info message is scheduled every 11 day of the month at 11:16

    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

Total Success   0               0               0
Total Failed    0               0               0
    Diagnostic  0               0               0
    Environment 0               0               0
    Inventory   0               0               0
    Syslog      0               0               0
    Direct      0               0               0
    Request     0               0               0
    Send-CLI    0               0               0
```

```
Total In-Queue: 0                    0                    0
  Configure: 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 Failed:                        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 Ratelimit
  dropped: 0
  Config: 0
  Diagnostic: 0
  Environment: 0
  Inventory: 0
  Syslog: 0
  Test: 0
  Request: 0
  Send-CLI: 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.
	service call-home (refer to Cisco IOS documentation)	Enables or disables call home.

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

Command History	Release	Modification
	12.2(25)EW	Extended to include the 10-Gigabit Ethernet interface.

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
lab-7206         Eth 0          143       R           7206      Eth 0/0
lab-ad5500-1     Eth 0          143       R           AS5500    Eth 0
lab-ad5500-2     Eth 0          143       R           AS5500    Eth 0
lab-ad5500-3     Eth 0          139       R           AS5500    Eth 0
lab-ad5500-4     Eth 0          132       R           AS5500    Eth 0/0
lab-5811         Eth 0          140       R S         WS-C5505  Eth 0/0
SONIA(FT08050    Eth 0          132       T           CS5500    1/2
Switch#
```

Table 2-16 describes the fields that are shown in the example.

Table 2-16 *show cdp neighbors Field Descriptions*

Field	Definition
Device ID	Configured ID (name), MAC address, or serial number of the neighbor device.
Local Interface	Local interface The protocol that is used by the connectivity media.
Holdtime	Remaining/Remaining amount of time, in seconds, that the current Cisco IOS device in 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 C—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: 172.19.169.83
Platform: cisco 7206, Capabilities: Router
Interface: Ethernet0,  Port ID (outgoing port): FastEthernet0/0/0
Holdtime : 123 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) 7200 Software (C7200-P-M), Version 12.1(2)
Copyright (c) 1986-2002 by Cisco Systems, Inc.

advertisement version: 2
Duplex: half

-------------------------
Device ID: lab-ad3500-1
Entry address(es):
  IP address: 172.19.169.87
-
-

Switch#
```

Table 2-17 describes the fields that are shown in the example.

Table 2-17 *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 information.
Platform	Product name and number of the neighbor device.
Capabilities	Device type of the neighbor. This device can be a router, a bridge, a transparent bridge, 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

Command History

Release	Modification
12.1(3a)E9	Support for this command was introduced on the Catalyst 6500 series switch.
12.2(25)SG	Display a crash from the full-flow option.

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 c1-simple (id 2)
    Match any
  Class Map match-all ipv6 (id 3)
    Match protocol ipv6
  Class Map match-all ugs-2 (id 3)
Switch#
```

This example shows how to display class map information for a specific class map:

```
Switch# show class-map ipv6
  Class Map match-all ipv6 (id 3)
    Match protocol ipv6
Switch#
```

Assume there are two active flows as shown below on Fast Ethernet interface 6/1:

```
SrcIp          DstIp          SPort SrcPort DstPort
---------------------------------------------------
192.168.10.10  192.168.20.20  26     8789   41
192.168.30.10  192.168.20.20  26     8789   21
```

With following configuration, each flow will be policed to a 1000000 bps with an allowed 9000-byte burst value.

Note If you set 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#show config terminal
Building configuration...Current configuration : 4096 bytes
!
Switch#config t class-map p4
Switch(config)#class-map match-any ip source-address ip destination-address ip protocol 14
Switch(config-cmap)#match ip dscp cs1 cs2 cs3 cs4
Switch(config-cmap)#match mac
Switch(config)#policy-map p2
Switch(config-pmap)#class c4
Switch(config-pmap-c)#police 1000000 9000
Switch(config-pmap-c)#exit
Switch(config-pmap)#exit
Switch(config)#interface FastEthernet 4/1
Switch(config-if)#service-policy input p2
Switch(config-if)#exit
Switch#show write memory
Switch#show policy-map interface
FastEthernet 4/1

class-map c4
  match ipv6 ip source-address ip destination-address ip protocol 14 source-port 14
destination-port
!
policy-map p2
  class c4
    police 1000000 bps 9000 bytes conform-action transmit exceed-action drop

interface FastEthernet 4/1
  service-policy input p2

Switch#show class-map c4
Class Map match-all c4 (id 2)
  Match ipv6 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 (who used enter class-map configuration mode.
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.

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.

Command History	**Release**	**Modification**
	12.2(33)SXH	Support for this command was introduced on the Catalyst 6500 series switch.

Examples This example shows how to display the test name, monitoring interval, and test attributes for all the modules of the chassis:

```
Router# show diagnostic content module all

module 1:

Diagnostic test suite attributes:
  B/* - Basic ondemand test / NA
  P/V/* - Performance test / Non-disruptive test / NA
  D/N/* - Disruptive test / Non-disruptive test / NA
  S/* - Only applicable to standby unit / NA
  X/* - Not a supported diagnostic test / NA
  F/* - Fixed monitoring interval test / NA
  E/* - Always enabled monitoring test / NA
  A/* - Administrative test / Non-administrative test / NA
  m/* - 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:Bootrom                      *B*N**A** not configured
 2) supervisor:Content Verification         *B*N**A** not configured
 3) packet memory:ongoing                   *P*N**O** not configured
```

```
module 4:

  Diagnostic test suite attributes:
    B/* - Basic ondemand test / NA
    P/* - Preset test only at bootup test / NA
    D/N/* - Disruptive test / Non-disruptive test / NA
    S/* - Only applicable to standby unit / NA
    X/* - Not a mandatory testing test / NA
    R/* - Run ondemand test / Run ondemand test / NA
    A/* - Always ondemand monitoring test / NA
    I/O - Monitoring in active / Monitoring in inactive
    */* - Mandatory bootup test, can't be bypassed / NA
    */+ - Ongoing test, always active / NA

                                                     Testing Interval
ID  Test Name                                Attributes  days:hh:mm:ss.ms
=== ============================================ ============ ==============
  1) linecard-online-diag ------------------- **D/N/*/I** not configured

Switch#
```

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**]

slot-num	(Optional) Specifies the slot on which diagnostics are displayed.
all	(Optional) Displays the diagnostics for all slots.
test	(Optional) Displays selected tests 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

Command History	Release	Modification
	12.2(18)SXF	Support for this command was introduced on the Catalyst 6500 series switch.

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) linecardconsole-dbg ------------------- .

module 6:

  Overall diagnostic result: PASS
  Diagnostic level at card bootup: minimal

  Test results: (. = Pass, F = Fail, U = Untested)

    1) linecardconsole-dbg ------------------- .
```

This example shows how to display the online diagnostic for module 1:

```
Sup6>#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-bootrom ------------------- .

        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/Test Status: (. = Pass F = Fail)
  Reset Reason: Soft/Sp Software/User

  Port Traffic: LZ Earliest Loopback :
    0: . . . . . 5: . . . . . 10: . . . . . 15: . . . . . 20: . . . . . 25: . . . . .
    30: . . . . . 35: . . . . . 40: . . . . . 45: . . . . . 50: . . . . . 55: . . . . .
    60: . . . . . 65: . . . . . 70: . . . . . 75: . . . . . 80: . . . . . 85: . . . . .

  Port Traffic: LZ Self Loopback :
    0: . . . . . 5: . . . . . 10: . . . . . 15: . . . . . 20: . . . . . 25: . . . . .
```

```
12c : 23: 14d : 35: 16d : 37: 18c : 39: 20c : 21: 22c : 23: .
34c : 36: 26c : 27: 28c : 29: 30c : 31: ae:

Port Traffic: L3 Lair Loopback ...
0: 1: 2: 3: 4: 5: 6: 7: 8: 9: 10: 11: .
12c : 23: 14d : 35: 16d : 37: 18c : 39: 20c : 21: 22c : 23: .
34c : 36: 26c : 27: 28c : 29: 30c : 31: ae:

Switch Subsystem Memory ...
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: 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) parker-memory-heavy.------------------- .

      Error code ------------------------ 0 (HEAL_SUCCESS)
      Total exe count ------------------- 0
      Last test execution time ---------- n/a
      Last test failure time ------------ n/a
      Last test failure count ----------- 0
      Last test pass time --------------- n/a
      Total failure count --------------- 0
      Consecutive failure count --------- 0
parker buffers on free list: 42857 bad: 0 used for ongoing tests: 979

Number of errors found: 0
Calls with hard errors (failed two or more tests): 0
Calls with soft errors (failed one test, retested bad): 0
Calls passed (passed on first or third retest bad): 0
Total buffers: 65536
Bad buffers: 0 (0.0%)
Free buffers: 42857 (65.4%)
Moving test results:0
No errors.
```

```
3) parker-memory-ongoing ------------------- 0

      Error code ------------------------ 0 (HEAL_SUCCESS)
      Total exe count ------------------- 0.
      Last test execution time ---------- n/a
      First test failure time ----------- n/a
      Last test failure time ------------ n/a
      Last test failure count ----------- 0
      Total failure count --------------- 0
      Consecutive failure count --------- 0
parker buffers on free list: 42857 bad: 0 used for ongoing tests: 979

Parker memory errors: 0 0
```

```
Current alarm level: green
Total Alarms to Green: 0
Current Alarms: 0 0 0 0
    0 0
Per5Minute 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
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
Per5Min 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
Short memory test 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
Packet memory failure/cell error:
    Ignored because of no access: 0 0
    Ignored because of mbe fifo overrun: 0 0
    Ignored because of ecc error: 0 0
    Ignored because id frames received: 0 0
    Ignored during boot: 0 0
    Ignored because of ecc error: 0 0
    Ignored at high pkbpscr: 0
Ongoing diag action mode: Normal
Last 1000 Memory Test Failures:
Last 1000 Packet Memory errors:
First 1000 Packet 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**]

Syntax Description	**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 analysis. This option is recommended.
Defaults	Non-detailed results.
Command Modes	EXEC mode

Command History	**Release**	**Modification**
	12.2(25)EZ	This command was introduced on the Catalyst 4500 series switch.

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:

```
Switch# show diagnostic result module 4 detail

module 4:

  Overall diagnostic result:OK

  Test results:( . Ports, P :, Fail, U :Untested)

  .

  1) linecard-online-diag -------------------- .

        Error code ------------------------------ 0 (DIAG_SUCCEED)
        Total run count ------------------------- 1
        Last test execution time ---------------- Jan 21 2001 19:48:50
        First test failure time ----------------- n/a
        Last test failure time ------------------ n/a
        Last test pass time --------------------- Jan 21 2001 19:48:50
        Total failure count --------------------- 0
        Consecutive failure count --------------- 0
```

```
Slot Ports Card Type                              Diag Status    Diag Details
---- ----- ---------------------------------------- ------------- ------------
  4   48   10/100/1000Base-T 3Com3C17171 Clarec/3SE  Passed        None

Detailed Status
---------------
. = Pass                    U = Unknown
F = Fastpath Failure        S = Scan Failure
I = Inline Power Failure    L = Loopback Failure
E = EEPROM Failure          C = CRC 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-diag-cdr:

Port  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
      ------------------------------------------------------------------------
      .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .

Port 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 (NULL_ERCODES)
        Total run count -------------------------> 1
        Total run duration ----------------------> 00 Jan 00 2000 00:01:54
        First test failure time -----------------> n/a
        Last test failure time ------------------> n/a
        Last test pass time ---------------------> Jan 02 2000 03:01:54
        TestLog buffer wraps --------------------> 0
        Consecutive failure count ---------------> 0

Detailed Status
---------------

TEST test is in progress on interface Gi2/1

Switch#
```

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 it was passed, failed, or was not run.

show diagnostic result module *N* **test** *2* **[detail]**

Syntax Description	*N* Specifies the module number.
	detail (Optional) Specifies the display of detailed information for analysis.
Defaults	Non-detailed results.
Command Modes	EXE C mode

Command History	**Release**	**Modification**
	12.2(52)SG	This command was introduced on the Catalyst 4500 series switch.

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:

```
Switch# show diagnostic result module 1 test 2

Test result: (. = Pass, F = Fail, U = Unexecuted)

  2) packet-memory-bootup :.............

This example shows how to display detailed results from the bootup packet memory test:

Switch# show diagnostic result module 2 test 2 detail

Test result: (. = Pass, F = Fail, U = Unexecuted)

.......................................................................

  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
parket buffers on from 11at: 62017 bad: 0 used for reqeing tests: 979
```

```
Number of errors found: 0
Cells with hard errors (failed two or more tests): 0
Cells with soft errors (failed one test, including hard): 0
Number of cells with a block that tested bad: 0
total buffers: 65536
bad buffers: 0 (0.0%)
good buffers: 65536 (100.0%)
Bootup test number:
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 3	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 *N* **test** [**detail**]

Syntax Description	*N*	Module number.
	detail	(Optional) Specifies the display of detailed information for analysis.

Defaults Non-detailed results.

Command Modes EXE C mode

Command History	**Release**	**Modification**
	12.2(18)SXF	This command was introduced on the Catalyst 6500 series switch.

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:

```
Router# show diagnostic result module 1 test 3

Test results: (. = Pass, F = Fail, U = Unexecuted)

  1 :  packet memory-ongoing  ----------- .
```

This example shows how to display the detailed results from the ongoing packet memory tests:

```
Router# show diagnostic result module 1 test 3 detail

Test results: (. = Pass, F = Fail, U = Unexecuted)

____________________________________________________________________________

  1) packet memory-ongoing  ----------- .

        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
parket buffers on from 21st: 62017 bad: 0 used for ongoing tests: 979
```

show diagnostic result module 2-217

```
Packet memory errors: 0 0
Current start level: green
Per 5 seconds in the last minute:
  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
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
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 0 0 0 0 0 0
Direct memory test 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
Potential false positives: 0 0
  Ignored because of port errors: 0 0
  Ignored because of cdb fifo overrun: 0 0
  Ignored because of crc: 0 0
  Ignored because of hdr/len mismatch: 0 0
  Ignored during boot: 0 0
  Ignored after setting by stats: 0 0
  Ignored on high gigaport: 0
Last Packet Memory Failure: 0
Last 1000 Memory Test Failures: 0
Last 1000 Packet Memory errors:
First 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 bootup packet memory test.

show dot1x

To display the 802.1X statistics and operational states 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.
	12.1(19)EW	Display enhanced to show the guest-VLAN value.
	12.2(25)EW	Support for the 10-Gigabit Ethernet interface was introduced on the Catalyst 4500 series switch.
	12.2(25)EWA	Support for currently assigned reauthentication timer (if the timer is configured or hence 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
Sysauthcontrol = Disabled
Dot1x Protocol Version = 2
Dot1x Info for GigabitEthernet0/1 = 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 fastethernet0/1
Dot1x Info for FastEthernet0/1
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
Port-Status               = AUTH[ DOMAIN]
ReAuthenticate            = Disabled
ReAuthPeriod              = 60
ExtraCredential           = 50
EapqTimeout               = 30
ReAuthMax                 = NONE (Locally configured)
MaxReq                    = 2
Mauthtmr                  = 36
ReAuthInterval            = 0

Dot1x Authenticator Client List
-------------------------------
Domain                    = DATA
Supplicant                = 0000.0000.a801
        Auth SM State     = AUTHENTICATED
        Auth BMSM SM State = IDLE

Port Status               = AUTHORIZED
Authentication Method     = Dot1x
Authorized By             = Authentication Server
Vlan Policy               = 10

Domain                    = VOICE
Supplicant                = 0011.2207.d007
        Auth SM State     = AUTHENTICATED
        Auth BMSM SM State = IDLE

Port Status               = AUTHORIZED
Authentication Method     = Dot1x
Authorized By             = Authentication Server

Switch#
```

Note Table 2-19 provides a partial list of the displayed fields. The remaining fields in the display show internal state information. For a detailed description of these state machines and their settings, refer to the 802.1X specification.

Table 2-28 *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.
MultiHost	Setting of the **dot1x multiple-hosts** interface configuration command (allowed or disallowed).

This is an example of output from the **show dot1x statistics interface gigabitethernet1/1** command. Table 2-29 describes the fields in the display.

```
Switch# show dot1x statistics interface gigabitethernet1/1

PortSamples/Sec Parameters for Dot1x
------------------------------------

TxRequest = 0     TxResp = 0     TxTotal = 0
RxStart = 0       RxLogoff = 0   RxRespID = 0   RxResp = 0
RxInvalid = 0     RxEpolLen = 0  RxTotal = 0
RxLastEpol = 0    LastSrcAddr 0000.0000.0000
Switch#
```

Table 2-29 *show dot1x statistics* Field Description

Field	Description
TxReqi/TxReqid	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 field is 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 port reinitialization.
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 authentication on a port.
mac address-table notification	Enables MAC address notification on a switch.

show energywise

Use the **show energywise** privileged-EXEC command to display the EnergyWise settings and status of the entity and the power over Ethernet (PoE) ports.

show energywise [**categories** | **children** | **domain** | **events** | **level** [**children** | **current** | **children**] | **delta children**] | **neighbors** | **resources** | **statistics** | **usage** [**children**] | **version**] | [**begin** | **exclude** | **include**] *expression*]

Syntax Description	**categories** (Optional) Displays the power levels.
	children (Optional) Displays the status of the entity and the PoE ports.
	domain (Optional) Displays the domain to which the entity belongs.
	events (Optional) Displays the last six events (messages) sent to other entities in the domain.
	level children current children delta children (Optional) Displays the available power level for the entity. • **children**—Available power levels for the entity and the PoE ports. • **current**—Current power level for the entity. (Optional) **children**—Current power levels for the entity and the PoE ports. • **delta**—Difference between the current and available power levels for the entity. (Optional) **children**—Difference between the current and available power levels for the entity and the PoE ports.
	neighbors (Optional) Displays the neighbor tables for the domains to which the entity belongs.
	resources (Optional) Displays the EnergyWise settings and status for resources.
	statistics (Optional) Displays the counters for events and errors.
	usage children (Optional) Displays the power for the entity. • **children**—Displays the power for the PoE ports.
	version (Optional) Displays the EnergyWise version.
Command Modes	Privileged EXEC

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

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

show energywise

Examples

```
Switch#show energywise
DomainName Role                 Name                    Usage     Lvl  Imp  Type
---------- ----                 ----                    -----     ---  ---  ----
           Switch               lobby.1                 SW.S (S)  10   10   parent

Switch#show energywise children
DomainName Name                 Role                    Usage     Lvl  Imp  Type
---------- ----                 ----                    -----     ---  ---  ----
           Switch               lobby.1                 SW.S (S)  10   10   parent
GI1/0/3    interface            GI1/0/3                 S.G (G)   10   10   child
GI1/0/5    interface            GI1/0/5                 S.G (G)   10   10   child
<output truncated>

Switch#show energywise domain
Name       : lobby.1
Domain     : ersr
Protocol   : udp
Port       : 43440
Port       : 43440

Switch#show energywise events
-----------------------------------------------------
Sequence:  240908  Reference:  0:1  Source:
Class:     SW_STATE_CHG
Action:    PS_ACTIVE_CHG,PS_INACTIVE_CHG
Reply To:  8.8.8.24:43440
-----------------------------------------------------
Sequence:  240909  Reference:  0:1  Source:
Class:     SW_CLASS_ACCESSORY
Action:    PS_ACTIVE_CHG,PS_INACTIVE_CHG,PS_ACCESSORY_STOPPED
Reply To:  8.8.8.24:43440
-----------------------------------------------------

Switch#show energywise level
                                        Levels (Watts)
DomainName Name                         0   1   2   3   4   5   6   7   8   9   10
---------- ----                         --  --  --  --  --  --  --  --  --  --  --
           lobby.1                      0.0 50.0 50.0 50.0 50.0 50.0 50.0 50.0 50.0 50.0 50.0

Switch#show energywise level children
                                        Levels (Watts)
DomainName Name                         0   1   2   3   4   5   6   7   8   9   10
---------- ----                         --  --  --  --  --  --  --  --  --  --  --
           lobby.1                      0.0 50.0 50.0 50.0 50.0 50.0 50.0 50.0 50.0 50.0 50.0
GI1/0/1    GI1.0.1                      0.0 15.4 15.4 15.4 15.4 15.4 15.4 15.4 15.4 15.4 15.4
GI1/0/2    GI1.0.2                      0.0 15.4 15.4 15.4 15.4 15.4 15.4 15.4 15.4 15.4 15.4
GI1/0/3    GI1.0.3                      0.0 15.4 15.4 15.4 15.4 15.4 15.4 15.4 15.4 15.4 15.4
GI1/0/4    GI1.0.4                      0.0 15.4 15.4 15.4 15.4 15.4 15.4 15.4 15.4 15.4 15.4
GI1/0/5    GI1.0.5                      0.0 15.4 15.4 15.4 15.4 15.4 15.4 15.4 15.4 15.4 15.4
<output truncated>

Switch#show energywise level current
DomainName Name                         Level Value
---------- ----                         ----- -----
           lobby.1                      10    50.0 (S)

Switch#show energywise level current children
DomainName Name                         Level Value
---------- ----                         ----- -----
           lobby.1                      10    50.0 (S)
GI1/0/1    GI1.0.1                      10    15.4 (G)
```

```
G11/0/2   G11.0.2              1    15.4  (6)
G11/0/3   G11.0.3              1    15.4  (6)
G11/0/4   G11.0.4              1    15.4  (6)
G11/0/5   G11.0.5              1    15.4  (6)
<output truncated>
```

Switch# **show energywise level delta**

```
Interface   Name                 Levels (Watts)
                                 0    1    2    3    4    5    6    7    8    9    10
----------  ----------------     ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----
            Lobby.1              <SH:0.0 0.0  0.0  0.0  0.0  0.0  0.0  0.0  0.0  0.0  0.0
```

Switch# **show energywise level delta child**

```
Interface   Name                 Levels (Watts)
                                 0    1    2    3    4    5    6    7    8    9    10
----------  ----------------     ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----
            Lobby.1              <SH:0.0 0.0  0.0  0.0  0.0  0.0  0.0  0.0  0.0  0.0  0.0
G11/0/1     G11.0.1              0.0  15.4 15.4 15.4 15.4 15.4 15.4 15.4 15.4 15.4 15.4
G11/0/2     G11.0.2              0.0  15.4 15.4 15.4 15.4 15.4 15.4 15.4 15.4 15.4 15.4
G11/0/3     G11.0.3              0.0  15.4 15.4 15.4 15.4 15.4 15.4 15.4 15.4 15.4 15.4
G11/0/4     G11.0.4              0.0  15.4 15.4 15.4 15.4 15.4 15.4 15.4 15.4 15.4 15.4
G11/0/5     G11.0.5              0.0  15.4 15.4 15.4 15.4 15.4 15.4 15.4 15.4 15.4 15.4
<output truncated>
```

Switch# **show energywise neighbors**

```
Capability Codes: S - Source, D - Domain Bridge, B - Source Bridge
                  S - Switch, R - Router, I - IGMP, r - Repeater, P - Phone
ID  Neighbor Name/                                   Capability
    Ipv4Addr                                         Port
1   Switch.A                                         Gi1/0/1
    2.2.2.20:24443                                   Gi1/0/1
2   Switch.B                                         Gi1/0/2
    2.2.2.20:24443                                   Gi1/0/2
<output truncated>
```

Switch# **show energywise recurrences**

```
Id  Name                                             Interval
-   ----------------------------------               --------
1   G11/0/17 QUERY GET                               1 minutes
2   G11/0/18 QUERY GET                               1 minutes
<output truncated>
```

Switch# **show energywise statistics**

```
Children: AP Devices: 2 Groups: 2 Domains: 14
```

Switch# **show energywise usage**

```
Interface Name                                       Usage      Caliber
-------------------------------------------------    ---------  -------
          Lobby.1                                    <SH:0.0>   max
```

Switch# **show energywise usage child**

```
Interface Name                                       Usage      Caliber
-------------------------------------------------    ---------  -------
          Lobby.1                                    <SH:0.0>   max
G11/0/1   G11.0.1                                    0.0 (W)    promoted
G11/0/2   G11.0.2                                    0.0 (W)    promoted
G11/0/3   G11.0.3                                    0.0 (W)    promoted
G11/0/4   G11.0.4                                    0.0 (W)    promoted
G11/0/5   G11.0.5                                    0.0 (W)    promoted
<output truncated>
```

```
Switch# show energywise version
Cisco Systems, Inc.
IOS Version: 12.2(52)SG(0.35)
EnergyWise Specification: in_ovgyn_v122_52_sg_showversion1.0.34
```

Related Commands	Command	Description
	energywise (global configuration)	Enables and configures EnergyWise on the entity.
	energywise (interface configuration)	Configures EnergyWise on the PoE port.

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** | **powersupply** | **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.
powersupply	(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

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 6500 series switch.
12.2(18)SXF	Support for the ability to display generic environment information with the **show environment** command was added.

Examples

This example shows how to display information about the environment alarms, operational status, and current temperature readings for the chassis:

```
Catalyst 6500 series Switch Cisco IOS Command Reference—Release 12.2(33)SXH
```

```
Power supplies needed by system : 1

Chassis Type : WS-C4507R

Supervisor Led Color : Green

Fantray : good

Fantray removal timeout: 240

Power consumed by Fantray : 50 Watts
```

This example shows how to display information about the environment alarms:

```
Switch#show environment alarm
no alarm
Switch#
```

This example shows how to display information about the power supplies, chassis type, and fan trays:

```
Switch#show environment status
Power
Supply  Model No.          Type        Status      Fan
                                                   Sensor
------  ---------------    ----------  ----------  ------
PS1     PWR-C45-1400AC     AC 1400W    good        good
PS2     none               --          --          --

Power Supply    Max    Min    Max    Min    Absolute
(Nos in Watts)  Inline Inline System System Maximum
--------------  ------ ------ ------ ------ -------
PS1             0      0      1360   1360   1400
PS2             0      0      0      0      0

Power supplies needed by system : 1

Chassis Type : WS-C4507R

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-C4507R
Switch#
```

This example shows how to display information about the fantray:

```
Switch#show environment status fantray
Fantray : good
Power consumed by Fantray : 50 Watts
Switch#
```

This example shows how to display information about the power supply:

```
Switch# show environment status powersupply
Power                                                    Fan
Supply  Model No.          Type       Status            Sensor
------- ------------------ ---------- ----------------- ------
PS1     WS-CAC-2500        AC 2500    good              good
PS2     WS-CAC-2500        AC 2500    good              good
PS3
PS4
Switch#
```

This example shows how to display information about the supervisor engine:

```
Switch# show environment status supervisor
Supervisor Card Slot: Current
Switch#
```

This example shows how to display information about the temperature of the chassis:

```
Switch# show environment temperature
Chassis Inlet Temperature Threshold = 51 degrees Celsius
Chassis Over Temperature Threshold  = 75 degrees Celsius
Chassis Critical Temperature Threshold = 85 degrees Celsius
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

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.2(37)SG	Display includes the status of storm control.

Examples This example shows how to display the error disable detection status:

```
Switch#show errdisable detect
Errdisable Reason    Detection status
-----------------    ----------------
udld                 Enabled
bpduguard            Enabled
security-violatio    Enabled
bindings             Enabled
psecure-violation    Enabled
mcast                Enabled
dhcp-rate-lim        Enabled
dtp-flap             Enabled
link-flap            Enabled
l2protocol           Enabled
pagp-flap            Enabled
dhcp-snoop-limit     Enabled
storm-control        Enabled
arcon-control        Enabled
inlinepower          Enabled
arp-inspection       Enabled
Switch#
```

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 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

Command History

Release	Modification
12.1(8)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.1(12)EW	Display includes the status of storm control.

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
security-violation   Disabled
channel-misconfig    Disabled
vmps                 Disabled
pagp-flap            Disabled
dtp-flap             Disabled
link-flap            Disabled
l2ptguard            Disabled
gbic-invalid         Disabled
dhcp-rate-limit      Disabled
dhcp-rate-limit      Disabled
storm-control        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)
---------    -----------------   --------------
Gi7/12       arp-inspect         13
```

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

Command History	Release	Modification
	12.2(18)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW	Support for LACP was added to this command.

Usage Guidelines If you do not specify a channel group, all channel groups are displayed.

In the output below, the Receive port list field is displayed for Layer 3 port channels only. This field means that the physical interface, which is still not up, is configured to be in the channel group (and indirectly is the 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   = 12h:17m:26s
Logical slot/port   = 14/1          Number of ports in agport = 0
GC                  = 0x00080001    HotStandby port = null
Port-channel Ptr    = 0x8189fa00
Port-channel Ipc    = 0x8189fa20
Port status         = Po1u4mu4u5u6u7u8u9u10u11u12u13u14u15u16u17u18u19u20u21u22u23u24
```

```
Port=1e Port-channel:
Index---- ----- Port
-----     -----
Switch#
```

This example shows how to display load-balancing information:

```
Switch#show etherchannel load-balance
Source XOR Destination mac address
Switch#
```

This example shows how to display a summary of information for a specific group:

```
Switch#show etherchannel 1 brief
Group state = L2
Ports: 2  Maxports = 8
port-channel 1: Fwd port-channel e 1
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-channel 1: Fwd port-channel e 1
                ------------
                Ports in the group:
                -------------------

Port: Fa5/4
-----------

Port state    = EC-Enbld Down Bndl Ec-Ewrl Dup-Config
Channel group = 1          Mode = Desirable      Gcchange = 0
Port-channel  = null       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.
        W - Hello timer is running.        Q - Quit timer is running.
        I - Info timer is running.         S - Interface timer is running.

Local information:
                                Hello  Partner  PAgP     Learning  Group
Port      Flags State  Timers  Interval Count  Priority  Method    Ifindex
Fa5/4     A    U1/S1           1s     0        128       Any       0

Age of the port in the current state: 03d:19h:14m
Port: Fa5/5
-----------

Port state    = EC-Enbld Down Bndl Ec-Ewrl Dup-Config
Channel group = 1          Mode = Desirable      Gcchange = 0
Port-channel  = null       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.
        W - Hello timer is running.        Q - Quit timer is running.
        I - Info timer is running.         S - Interface timer is running.

Local information:
                                Hello  Partner  PAgP     Learning  Group
Port      Flags State  Timers  Interval Count  Priority  Method    Ifindex
Fa5/5     A    U1/S1           1s     0        128       Any       0
```

```
Age of the port in the current state: 22h:19m:27s
                  Port-channel is the group
---------------
Port-channel: Po1
---------------
Age of the Port-channel  - 22h:19m:45s
Logical slot/port   - 16/1          Number of ports in agport - 0
GC                  - 0x00000000    Port-channel prev - null
Smallest port Idx   - 0x8c1d 0x870
Port array          - Port-channel idx dg-No: Gcmem

Ports in the Port-channel:

Index   Load  Port
-----+------+------+
0x8c1d  ---   +
0x870   ---   +
```

This example shows how to display a one-line summary per channel group:

```
Switch# show etherchannel summary
Flags:  D - down        P - bundled     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 of #ports in agg not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

Group Port-channel  Ports
------+-------------+-----------------------------------------
1     Po1(SU)       Fa5/4(I)  Fa5/5(I)
2     Po2(SU)       Fa5/6(I)  Fa5/7(I)
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-channel: Po1
                -----------------

Port-channel   : NO-Shutdown Non-Protocol Non-Gvrp
Channel group : 1            Mode : Desirable     Gcchange : 0
Port-channel   : 0x8c1d      GC   : 0x00000000    Pseudo agport : Po1
Port index     : 0           Load : 0x55

Ports in the group:
-------------------
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.
Timers: H - Hello timer is running.        Q - Quit timer is running.
        S - Switching timer is running.    I - Interface timer is running.

Local information:
                                     Hello  Partner  PAgP     Learning  Group
Port      Flags State   Timers Interval Count  Priority  Method  Ifindex
Fa5/4     d     U1/S1                1s     0        128       Any     0

Age of the port in the current state: 22h:19m:27s
Port: Fa5/5
-----------

Port-channel   : NO-Shutdown Non-Protocol Non-Gvrp
Channel group : 1            Mode : Desirable     Gcchange : 0
Port-channel   : 0x8c1d      GC   : 0x00000000    Pseudo agport : Po1
Port index     : 0           Load : 0x55

Ports in the group:
-------------------
```

```
Flags:  d - Down        s - Suspended       A - Agg        C - Down in Port-channel state.
        A - Active in auto mode.            P - Active Learns on physical port.
Timers: H - Hello timer is running.         Q - Quit timer is running.
        S - Switching timer is running.     I - Interface timer is running.

r...output truncated...r

Exit=0d
```

This example shows how to display the protocol enabled:

```
Exit=0d show etherchannel protocol
                Channel-group listing:
                ----------------------

Group: 12
---------
Protocol:  PAgP

Group: 24
---------
Protocol:  -  (Mode ON)
Exit=0d
```

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

Command History

Release	Modification
12.1(11)EW	Support for this command was introduced on the Catalyst 6500 series switch.
12.2(18)EW	Support for the 10-Gigabit Ethernet interface was introduced on the Catalyst 6500 series switch.

Usage Guidelines

Table 2-20 describes the fields in the **show flowcontrol** command output.

Table 2-20 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 by default; **disagree** 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.
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:

```
Switch#show flowcontrol
Port      Send FlowControl  Receive FlowControl  RxPause TxPause
          admin    oper     admin    oper
--------  -------  -------  -------  -------  -------  -------
Te1/1     off      off      on       off      0        0
Te1/2     off      off      on       off      0        0
Gi1/1     off      off      desired  on       0        0
Gi1/2     off      off      desired  on       0        0
Gi1/3     off      off      desired  on       0        0
Gi1/4     off      off      desired  on       0        0
Gi1/5     off      off      desired  on       0        0
Gi1/6     off      off      desired  on       0        0
Gi1/7     off      off      desired  on       0        0
Gi1/8     off      off      desired  on       0        0
Gi1/9     off      off      desired  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     desired  off      off      off      0        0
Gi1/2     on       disagree on       on       0        0
Switch#
```

This example shows how to display the flow control status on Gigabit Ethernet interface 3/6:

```
Switch#show flowcontrol interface gigabitethernet3/6
Port      Send FlowControl  Receive FlowControl  RxPause TxPause
          admin    oper     admin    oper
--------  -------  -------  -------  -------  -------  -------
Gi3/6     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	Configure a Gigabit Ethernet interface to send or receive pause frames.
show interfaces status	Displays the interface status or a list of interfaces in error-disabled state.

show hw-module port-group

To display how the X2 Inter-Lots module are grouped, set the **show hw-module port-group** command.

show hw-module module *number* **port-group**

Syntax Description	**module** Specifies a line module.
	number Specifies a slot or module number.
	port-group Specifies a port-group on a switch.
Defaults	X2 mode.
Command Modes	Global configuration mode

Command History	Release	Modification
	12.2(18)SXF	Support for WS-X6704-10GE-E Twin Gigabit converter introduced.

Usage Guidelines When a TwinGig converter is enabled or disabled, the number and type of ports on the line card change dynamically. The terminology must reflect this behavior. In Cisco IOS, 10G gigabit ports are named TenGigabit and 1-Gigabit ports are named GigabitE. Starting with Cisco IOS Release 12.2(18)SXF6, to avoid ambiguity (named TenGigabitE1 and GigabitE1), the 10-Gigabit and 1-Gigabit port numbers are independent. The WS-X6704-10GE-E module with its X2 ports are named TenGigabitEthernet<1-4>, and the SFP ports are named Gigabit<slot-num>/7-10>.

In the Supervisor Engine 6-E and Catalyst 6500M chassis, the ports are connected to the switching fabric through a 40-Gigabit ASIC. The 40-Gigabit ASIC provides four 10-Gigabit ports and four 10-Gigabit ports cannot be mixed on a single 40-Gigabit ASIC; they must either be all 10-Gigabit (X2), or all Gigabit (TwinGig converter and SFP). The Interplane of X2 modules show this side-port grouping, either with an actual physical grouping, or a box drawn around a grouping.

Examples This example shows to determine how the X2 Inter-Lots a module are grouped on a WS-X6704-10GE-E:

```
Switch# show hw-module module 1 port-group
Module  Port-group   Active      Inactive
------  ----------   ------      --------
1       1            Gi1/1-3     gi1/1-12
        2            Te1/4-6     gi1/13-18
Switch#
```

Related Commands	**Command**	**Description**
	hw-module port-group	Selects either Gigabit Ethernet or Ten Gigabit Ethernet interfaces on your module.

show hw-module uplink

To display the current uplink mode, use the **show hw-module uplink** command.

show hw-module uplink

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.2(25)SW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines If the active uplink mode is different than configured mode, the output displays the change.

By default, the current (operational) uplink selection is displayed.

Examples This example shows the output displaying the current (active) uplinks:

```
Switch# show hw-module uplink
Active uplink configuration is TenGigabitEthernet
```

This example shows the output for redundant systems in SSO mode if the 10-Gigabit Ethernet uplinks are active, and the Gigabit Ethernet uplinks are selected:

```
Switch# show hw-module uplink
Active uplink configuration is TenGigabitEthernet
(will be GigabitEthernet after next reload)
To switch uplinks, either a power-cycle of chassis is required to
apply the new configuration.
```

This example shows the output for redundant systems in RPR mode if the 10-Gigabit Ethernet uplinks are active, and the Gigabit Ethernet uplinks are selected:

```
Switch# show hw-module uplink
Active uplink configuration is TenGigabitEthernet
(will be GigabitEthernet after next reload)
A reload of active supervisor is required to apply the new configuration.
```

Related Commands	Command	Description
	hw-module uplink select	Selects the 10-Gigabit Ethernet or Gigabit Ethernet uplinks on the Supervisor Engine V-10GE within the WS-C6510R chassis.

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**[*num*] | **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.
num	(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 IDPROM.
fan-tray	Displays information for the fan tray IDPROMs.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.1(12c)EW	Support for the **power-supply fan-tray**, **clock module**, and **mux-buffer** keywords was added.
12.1(13)EW	Support for the **interface** keyword was added.
12.2(18)EW	Enhanced the **show idprom interface** output to include the hexadecimal display of the GBIC/SFP EEPROM contents.
12.2(25)EW	Support for the 10-Gigabit Ethernet interface was introduced on the Catalyst 4500 series switch.

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 EEPROM information for module 4:

```
Switch> show idprom module 4
Module 4 IDprom:
  Common Block Signature = 0xABAB
  Common Block Version = 1
  Common Block Length = 144
  Common Block Checksum = 4199
  IDprom Size = 256
  Block Count = 2
  FRU Major Type = 0x4201
  FRU Minor Type = 363
  Optional Footer Present = Cisco Systems, Inc.
  Product Number = WS-X4148
  Serial Number = SCD10135
  Manufacture Issue = 9
  Hardware Revision = 0.2
  Manufacturing Bits = 0x0000
  Engineering Bits = 0x0000
  Snmp OID = 0.0.0.0.0.0.0.0
  Power Consumption = 0
  RMA Failure Code = 0 0 0 0
  Lineartool Block Signature = 0xAIAI
  Lineartool Block Length = 112
  Lineartool Block Version = 4
  Lineartool Block Checksum = 458
  Lineartool Block Data 0000000000000000
  Last Factory Data = 50
  MAC Base = 0013.7ba6.9f40
  MAC Blks = 48
  Extended
```

This example shows how to display EEPROM information for the GBICs on the Gigabit Ethernet interface 1/2:

```
Switch> show idprom interface gigabitethernet1/2
Gigabit Ethernet GBIC(2) Contents:
  Common Block:
  Identifier             = GBIC [0x1]
  Extended Id            = Not specified/not recognized with defined MOD_DEF [0x0]
  Connector              = SC connector [0x1]
  Transceiver:
    Speed                = Not available [0x0]
    Comments             = Not available [0x0]
    Technology           = Not available [0x0]
    1.6G Length          = Not available [0x0]
    Media                = Not available [0x0]
    SONET Comp Codes     = Not available [0x0]
  Encoding               = 8B10B [0x4]
  BR, Nominal            = 1.3000GHz MHz
  Length(9u) in km       = GBIC does not support single mode fiber, or the length may be determined from the transceiver technology.
  Length(9u)             = 0 (0.1 km
  Length(50u)            = GBIC does not support 50 micron multi-mode fiber, or the length may be determined from the transceiver technology.
  Length(62.5u)          = GBIC does not support 62.5 micron multi-mode fiber, or the length may be determined from the transceiver technology.
  Length(Copper)         = GBIC does not support copper cable, or the length may be determined from the transceiver technology.
  Vendor name            = CISCO-FINISAR
  Vendor OUI             = [0x00]
  Vendor Part No.        = FTLX-1119-C3C
  Vendor Part Rev.       = B
  Wavelength             = Not available
```

```
                    Gbit
  GC_BAND           = 0x04

Extended IS Fields:
  Options           = Loss of Signal implemented,TX_FAULT signal implemented,TX_DISABLE is
implemented and disabled,RATE select not except [0x1a]
  BR_min            = Unspecified
  BR_max            = Unspecified
  Link Length Del Sm. = 0x12[0]
  Link Length Del Lg. = 0x12[0]
  Diag monitoring   = Implemented
  Calibration type  = Internal
  Ex per measurement = Optical Modulation Amplitude (OMA)
  Enhanced Diag     = Implemented
  GC_BAND           = 0x04

Vendor Specific IS Fields:
20:A200  20 20 32 32 30 38 30 37 47 8B 88 ED 69 AA  |..'SFGBP'G..m'j*|
20:A240  1A 80 00 00 00 00 00 00 00 00 00 00 33 32  |.P..........8K..|

                    SERDOES contents (hex) size 128:
0x0000  51 18 00 00 46 42 00 00 00 00 01 00 00 00  |Q...FB..........|
0x0010  00 00 00 00 46 42 31 47 42 42 42 48 55 41  |....FB1GBBBHUA|
0x0020  52 20 20 20 20 20 20 20 41 48 52 32 30 30 31 31 30  |R   GAFTR-8119
0x0030  2d 47 41 20 20 20 20 20 41 20 20 20 20 20  |-GA    A     |
0x0040  00 4a 00 00 46 31 32 37 33 4d 4d 20 20 20 30 32  |..J..FCGM   |
0x0050  30 30 38 30 37 32 30 30 30 30 30 30 00 00  |000807200000..|
0x0060  00 00 00 00 00 00 00 00 00 00 00 00 47 45 4d 47 47 41 4c 4f  |..GEMGGALO
0x0070  1a 80 00 00 00 00 00 00 00 00 00 00 33 32 3b  |.Ma.........8K;|
Gbit

This example shows how to display EDROM information for the 10-Gigabit Ethernet interface 3/1:
Switch# show gigbit interface tenGigabitEthernet3/1
10 Gbit EDROM Contents:
Base Ethernet Descriptor (0x00) Fields
  ID EDR Structure supported          =0x4
  EDR Size in bytes                   =0x200
  Number of Extended Bytes            =0x0
  Base Ethernet Descriptor            =0x0
  Customer Field Address              =0x77
  Vendor Field Address                =0x87
  Extended Vendor Field Address       =0x200
  Connector                           =0x7
  Transceiver type                    =0x2 -x2
  Optical transceiver type            =0x1 -SC
  Cable assembly                      =0x0 -Unspecified
  Normal Bitrate in multiple of 100 Mb/s =0x28[40]
  Protocol Type                       =0x1 -10GigE

  Standards Compliance Codes :
  10GbE Code Byte 0                   =0x1 -10GBASE-LR
  SONET Code Byte 1                   =0x0
  SONET Code Byte 2                   =0x0
  SONET/SDH Code Byte 3               =0x0
  SONET/SDH Code Byte 4               =0x0
  SONET/SDH Code Byte 5               =0x0
  SONET/SDH Code Byte 6               =0x0
  10GFC Code Byte 7                   =0x0
  10GFC Code Byte 8                   =0x0
  10GFC Code Byte 9                   =0x0
  Transmission range in 10m           =0x1E8
Fibre Type :
  Fibre Type Byte 0                   =0x40 -SMF only

  Fibre Type Byte 1                   =0x0
  Link Length Supported for EMF type in 10m units :
  Link Length Supported for EMF type =0x0
  Link Length Supported for copper in 1m units :
  Link Length Supported for copper =0x0
  Link Length Supported for OM1 in 10m units :
  Link Length Supported for OM1 =0x0
  Link Length Supported for OM2 in 10m units :
  Link Length Supported for OM2 =0x0
  Link Length Supported for OM3 in 10m units :
  Link Length Supported for OM3 =0x0
  Vendor name [ASCII] ="FTLX8571D3BCV-IT"
  Vendor OUI [IEEE] =0x000000
  Vendor PN [ASCII] ="      "
  Vendor rev [ASCII] ="  "
  Wavelength =0x0
  Diagnostic Monitoring Type =0x68
  Enhanced Options =0xFA0
  Sonet Compliance =0x0
  Checksum of extended EEPROM =0xD3
  Checksum of base EEPROM =0x51
  Vendor specific [ASCII] ="      "
  Diagnostic Monitoring Implemented
  Internally calibrated
  Externally calibrated
  Digital diagnostic monitoring implemented
  Diagnostic Monitoring Type =0x68
  Enhanced Options =0xFA0
  Sonet Compliance =0x0
  Checksum of extended EEPROM =0xD3
  Checksum of base EEPROM =0x51
  Vendor specific [ASCII] ="      "
  Diagnostic Monitoring Implemented
  Internally calibrated
  Externally calibrated
  Digital diagnostic monitoring implemented
```

```
Fiber Type Byte 1                        (0x0 )Unspecified

Centre Optical Wavelength in 0.05nm steps (Channel 1 (0x0 0x0F 0x88
Centre Optical Wavelength in 0.05nm steps (Channel 2 (0x0 0x0 0x0
Centre Optical Wavelength in 0.05nm steps (Channel 3 (0x0 0x0 0x0
Centre Optical Wavelength in 0.05nm steps (Channel 4 (0x0 0x0 0x0
Package Identifier OUI  (0x00000
Connector type (SC,LC,MT-RJ,MU) (0x23
Transceiver vendor name (CISCO-OPNEXT,)0
Part number provided by transceiver vendor  (VSFP31128-GM3-V
Revision level of part number provided by vendor (02
Vendor serial number                    (AGX0P200541
Vendor manufacturing date code (2004/07/20)

Reserved1: (00 02 02 20 00 00
Basic Field(Hex,Dec) (0x0

Customer Writable(Hex )
0x00: 46 49 42 45 52 4C 41 42 20 20 20 20 20 20
0x10: 20 20 20 20 4F 4E 44 50 56 31 38 32 31 34 31
0x20: 31 30 20 20 30 35 30 32 00 31 20 20 45 30 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: 54 34 34 2A 00 00 00 00 00 00 00 00 00 00 00 BF
0x40: F4 A2 1D 37 11 98 01 54 00
Switch#
```

This example shows how to display EEPROM information for the supervisor engine:

```
Switch#show idprom supervisor
Supervisor IDprom:
Product Number = WS-X4515
Common Block Version = 1
Common Block Length = 144
Common Block Checksum = 4193
Number Hexes = 2
Block Count = 2
FRU Major Type = 0x4101
FRU Minor Type = 353
Manufacture Date = Wednesday, Inc.
Product Number = WS-X4515
Serial Number = JAB0512201C
Hardware Revision = 0.3.0.0
Part Number = 00
Manufacturing Deviation String = 0
Hardware Change = 0
Manufacturing Bits = 0x0000
Engineering Bits = 0x0000
Snmp OID = 0.0.0.0.0.0.0.0
Power Consumption = 0
RMA Failure Code = 0 0 0 0
Supervisor Block Signature = 0x4101
Supervisor Block Version = 1
Supervisor Block Length = 144
Supervisor Block Checksum = 148
Feature Bits = 0x00000000000000
Mac Base = 0007.0e0f.3a40
Mac Amount = 1024
Mac Count = 2
Switch#
```

This example shows how to display IDPROM information for the chassis:

```
Switch# show idprom chassis
IDPROM for chassis:
Common Block Signature = 0xABAB
Common Block Version = 1
Common Block Length = 144
Common Block Checksum = 4245
Idprom Size = 256
Block Count = 2
FRU Major Type = 0x0101
FRU Minor Type = 24
OEM String = Cisco Systems, Inc.
Product Number = WS-C6513E
Serial Number = SAD0831 0EDD
Part Number = 73-4189-02
Part Revision = 02
Manufacturing Date = Manufacturing Date = 0x60
Hardware Revision = 0.3
Manufacturing Date = 0x0000
Snmp OID = 0.0.0.0.0.0.0.0
Snmp OID = 0.0.0.0.0.0.0.0
Chassis Block Signature = 0xAD01
Chassis Block Length = 32
Chassis Block Version = 1
Chassis Block Checksum = 425
Feature Bits = 0x00000000000000000000
MAC Base = 0004.9862.2800
MAC Block Size = 1024
Switch#
```

This example shows how to display IDPROM information for power supply 1:

```
Switch# show idprom power-supply 1
IDPROM for power-supply 1:
Common Block Signature = 0xABAB
Common Block Version = 1
Common Block Length = 144
Common Block Checksum = 12247
Idprom Size = 256
Block Count = 2
FRU Major Type = 0x4001
FRU Minor Type = 8224
OEM String = Cisco Systems, Inc.
Product Number = WS-CAC-1440W
Serial Number = ACP0918G2AG
Part Number = 34-2232-01
Part Revision = A0
Manufacturing Date = Manufacturing Date = 0x60
Hardware Revision = 1.1
Manufacturing Date = 0x0000
Snmp OID = 0.0.0.0.0.0.0.0
Snmp OID = 0.12.2.65534.65534.65534.65534.65534
Power Consumption = 14
RMA Failure Code = 255 255 255 255
Power Supply Block Signature = 0xFF99
Power Supply Block Version = 255
Power Supply Block Length = 255
Power Supply Block Checksum = 65534
Feature Bits = 0xFFFFFFFFFFFFFFFF
Current A [12V] = 11
Current B [20V] = 13
Max=MCB [12V] = 65535
```

```
Switch#
```

This example shows how to display IDPROM information for the fan tray:

```
Switch# show idprom fan-tray
Fan Tray IDprom :
  Common Block Signature = 0xABAB
  Common Block Version = 1
  Common Block Length = 144
  Common Block Checksum = 18781
  Eeprom Size = 256
  Block Count = 2
  FRU Major Type = 0x4002
  FRU Minor Type = 0
  OEM String = "Cisco Systems"
  Product Number = WS-C4503-Fan
  Serial Number =
  Part Number =
  Hardware Revision =
  Manufacturing Variation String =
  Hardware Revision = 0.1
  Manufacture Bits = 0x0000
  Engineering Bits = 0x0000
  Comp SOL = 65535,65535,65535,65535,65535,65535,65535,65535
  Power Consumption = 15
  OBL 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

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW	Support for extended VLAN addresses was added.
	12.2(25)EW	Support for extended VLAN addresses was introduced on the Catalyst 4500 series switch.
	12.2(31)SG-X	Support for nonMIBs affected in command output.
	12.2(52)SG	Added support for per-VLAN error-disable detection.

Usage Guidelines The statistics are collected per VLAN for Layer 2 switched packets and Layer 3 routed packets. The statistics are available for both unicast and multicast. The Layer 3 switched packet counts are available for both the ingress and egress 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 that the interface is running. The **show interfaces** command shows the operating 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 an MDIX configuration on their copper media ports include: WS-X6124-RJ45, WS-X6148-RJ45 with hardware revision 10 or later, and WS-X6232-GB-RJ with hardware revision 3.0 or later.

Examples This example shows how to display traffic for Gigabit Ethernet interface 2/5:

```
Switch# show interfaces gigabitethernet2/5
GigabitEthernet2/5 is up, line protocol is up (connected) (vlan1ce-dis)
  Hardware is C6k 1000Mb 802.3, address is 0030.6498.1ba6 (bia 0030.6498.1ba6)
  Internet address is 172.20.26.218
  MTU 9600 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)
  Half-duplex, 100Mb/s
  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 1000 bits/sec, 2 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     1 packets input, 64 bytes, 0 no buffer, 0 broadcasts, 0 dribble, 0 multicast
     12 in-ds(ucast) unicast 0 pkts, 0 bytes - mcast 1 pkts, 0 bytes mcast
     12 out-ds(ucast) unicast 0 pkts, 0 bytes - mcast 0 pkts, 0 bytes
     0 runts, 0 giants, 0 throttles, 0 input errors, 0 CRC, 0 frame,
     Received 24438 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
     15245 packets output, 1980404 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
Switch Port: Tenth Gigabit Ethernet 1/1
Dot1Qtunnel: Enabled
Administrative Mode: private-vlan promiscuous trunk
Operational Mode: private-vlan promiscuous trunk (operational mode of bundle Po1)
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: none
Trunking Native Mode VLAN: none
Administrative Private VLAN trunking: enabled
Trunking VLANs:
Administrative private-vlan host-association: none
Administrative private-vlan mapping: 300 (VLAN0300) 305 (VLAN0305) 306 (VLAN0306)
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation:
Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Administrative private-vlan mapping trunk: 300 (VLAN0300) 305 (VLAN0305) 306
(VLAN0306) 307 (VLAN0307) 308 (VLAN0308) 309 (VLAN0309)
```

```
Operational protocol:stat: 200 (%LAN200) 303 (%LAN303) 304 (%LAN304)
Ethernet Protocol: Ethernet2
Routing Table Enabled: 2-1000
Capture Mode Disabled
Capture Buffer Allocated: ALL
Delay:10
```

This example shows how to verify the status of auto-MDIX on an RJ-45 port:

Note You can verify the configuration setting and the operational state of auto-MDIX on the interface by entering the **show interfaces** EXE command. This field is applicable and appears only on the **show interfaces** command output for 10/100/1000BaseT RJ-45 copper ports on supported line cards (WS-X6148-RJ45, WS-X6148-RJ-45V and other modules revision 3 for later, and WS-X6248-TX and WS-X6248-RJ-45V line cards) or later.

```
FastEthernet2/1 is up, line protocol is up (connected)
  Hardware is Fast Ethernet Port, address is 0015.2bac.ad49 (bia 0015.2bac.ad49)
  MTU 2500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 1000Mb, link type is auto, media type is 10/100/BaseTX
  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
  Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     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    1          a-full  a-1000 1000-SXLHW-MSEMOD
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
Gi1/1                        connected    1          full    1000 1000base-LH
Gi1/2                        connected    1          full    1000 1000base-LH
Switch#
```

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

Command History

Release	Modification
12.2(18)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.2(25)EW	Support for the 10-Gigabit Ethernet interface was introduced on the Catalyst 4500 series switch.
12.2(31)SGA	Support for auto-MDIX reflected in command output.

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-RJ and WS-X4148-RJ with hardware version 3.0 or higher, and WS-X4232-GB-RJ with hardware version 3.0 or higher.

Examples This example shows how to display the interface capabilities for a module:

```
Switch> show interfaces capabilities module 1
GigabitEthernet1/1
  Model:                 WS-X6748-GE-TX
  Type:                  Unsupported GBIC
  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
  QoS scheduling:        rx-(1q),tx-(1p1q, 2q1q,1p2q1q)
  CoS rewrite:           yes
  ToS rewrite:           yes
  UDLD:                  yes
  SPAN:                  source,destination
  SVLAN:                 yes
  Link Debounce:         no
  Link Debounce Time:    no
  Port Security:         yes
  Dot1x:                 yes
GigabitEthernet1/2
  Model:                 WS-X6748-GE-TX
  Type:                  Unsupported GBIC
  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
  QoS scheduling:        rx-(1q),tx-(1p1q, 2q1q,1p2q1q)
  CoS rewrite:           yes
  ToS rewrite:           yes
  UDLD:                  yes
  SPAN:                  source,destination
  SVLAN:                 yes
  Link Debounce:         no
  Link Debounce Time:    no
  Port Security:         yes
  Dot1x:                 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-X6707-10G
  Type:                  10GBase-LR
  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:(1p2q2t, Sharing/Shaping)
Flow-control:      yes
Jumbo frames:      yes
Internal power:    yes
Online power:      no
Sensor:            source/destination
EEE:               yes
Link Debounce:     no
Link Debounce Time: no
Port-channel:      yes
Duplex:            full
Hardware MTU:      9198 Bytes (Jumbo Frames)
Multicast Hardware Types: no
Hardware Multicast Entry: N/A
Switch#
```

This example shows how to display the interface capabilities for Gigabit Ethernet interface 3/1:

```
Switch#show interfaces gigabitethernet3/1 capabilities
GigabitEthernet3/1
  Model:             WS-X4516-10G
  Type:              No.10G
  Speed:             1000
  Duplex:            full
  Trunk encap. type: 802.1Q,ISL
  Trunk mode:        on,off,desirable,nonegotiate
  Channel:           yes
  Broadcast suppression:percentage(0-100), nw
  Flowcontrol:       rx-(off,on,desired),tx-(off,on,desired)
  VLAN Membership:   static, dynamic
  Fast Start:        yes
  Queueing:          rx-(N/A), tx-(4q2t, Sharing/Shaping)
  CoS rewrite:       yes
  ToS rewrite:       yes
  Inline power:      no
  SPAN:              source/destination
  UDLD:              yes
  Link Debounce:     no
  Link Debounce Time: no
  Port-channel:      yes
  Jumbo frames:      yes
  MTU Supported:     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
Fast Ethernet3/1
  Model:             WS-X4148-RJ-RJ-45
  Type:              10/100BaseTX
  Speed:             10,100,auto
  Duplex:            half,full,auto
  Trunk encap. type: 802.1Q,ISL
  Trunk mode:        on,off,desirable,nonegotiate
  Channel:           yes
  Broadcast suppression:percentage(0-100), nw
  Flowcontrol:       rx-(off,on),tx-(off,on)
  VLAN Membership:   static, dynamic
  Fast Start:        yes
  Queueing:          rx-(N/A), tx-(4q1t, Sharing)
  CoS rewrite:       yes
  ToS rewrite:       yes
  Inline power:      no
  SPAN:              source/destination
  UDLD:              yes
```

```
  Link Debounce:        no
  Link Debounce Time:   no
  Port Security:        yes
  Dot1x:                yes
  Internal Tag:         no (only frames, baby giants)
Router#
```

This example shows how to verify that the auto-MDIX configuration is supported on a port:

```
Router#show interfaces fastethernet3/2 capabilities
FastEthernet3/2
  Model:                WS-X6148-GE-TX-SP
  Type:                 10/100BaseTX
  Speed:                10,100,auto
  Duplex:               half,full,auto
  Trunk encap:          dot1q
  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)
  Fast Ethernet:        yes, Uplink, Dynamic
  Fast Uplink:          yes
  Queueing:             rx-(8q2t), tx-(1p2q2t, Sharing/Shaping)
  CoS rewrite:          yes
  ToS rewrite:          yes
  Inline power:         yes
  SPAN:                 source/destination
  UDLD:                 yes
  Link Debounce:        yes
  Link Debounce Time:   no
  Port Security:        yes
  Dot1x:                yes
  Maximum MTU:          1552 bytes (Baby Giants)
  Multicast Hwfwd Types: no
  Diagnostic Monitoring: N/A
Router#
```

Related Commands:	Command	Description
	show interface 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

Command History	Release	Modification
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(19)EW	Support for trunk counter.
	12.2(18)EW	Support for the storm-control keyword to display the storm-control discards.

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     0            0         0           0         0
Gi1/2     0            0         0           0         0

Port      Single-Col   Multi-Col Late-Col    Excess-Col Carri-Sen    Runts     Giants
Gi1/1     0            0         0           0          0            0         0
Gi1/2     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          InOctets    InUcastPkts   InMcastPkts   InBcastPkts
Gi1/1            0            0             0             0
Gi1/2            0            0             0             0

Port          OutOctets   OutUcastPkts  OutMcastPkts  OutBcastPkts
Gi1/1            0            0             0             0
Gi1/2            0            0             0             0
Switch#
```

This example shows how to display the trunk counters for a specific module:

```
Switch# show interfaces counters trunk module 1

Port          TrunkFrameIn  TrunkFrameOut  GroupBandwidth
Gi1/1            0             0              0
Gi1/2            0             0              0
Switch#
```

This example shows how to display the number of packets that are discarded due to suppression:

```
Switch# show interfaces counters storm-control

Multicast Suppression : Enabled

Port      BroadcastSupp:1   PerformerSupp:2  UnicastSupp:3
Fa6/36        10,024            4,234,932
Switch#
```

Related Commands	Command	Description
	show interface 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

Command History	Release	Modification
	12.1(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples

This example shows how to display information for all interfaces:

```
Switch# show interfaces description
Interface Status         Protocol Description
Fa0/1     admin down     down     First interface
Fa0/2     admin down     down
Gi1/1     up             up       Gig0/1 to server farm
Switch#
```

Related Commands	Command	Description
	description (refer to Cisco IOS documentation)	Includes a specific description about 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

Command History	**Release**	**Modification**
	12.2(18)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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
Gi1/4                            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
Gi1/6                            1 minutes 28 secs
Gi1/7                            1 minutes 28 secs
Gi1/8                            1 minutes 28 secs
Gi1/9                            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

Command History

Release	Modification
12.2(12)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples

This example shows how to display the MTU size for all interfaces on module 1:

```
Switch> show interfaces mtu module 1
Port      Name               MTU
Gi1/1/1                      1500
Gi1/1/2                      1500
Switch>
```

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

Command History	**Release**	**Modification**
	12.1(8)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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
---------- --------------- ----------
vlan10    301             isolated
vlan10    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
12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.2(18)EW	Support for WS-X4506-10GE-E 10-port Gigabit connect modules.
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          a-full  a-100 10/100BaseTX
Fa1/2                        connected    vl-err-dis a-full  a-10  10BaseT-LR
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  5-6
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 TwinGig Converter:

```
Router# show interfaces status module 1
Port      Name               Status       Vlan       Duplex  Speed Type
Gi1/1     inactive 1 full 100 Ex SX
Gi1/2     inactive 1 full 100 Ex SX
Gi1/3     inactive 1 full 100 Ex SX
Gi1/4     inactive 1 full 100 Ex SX
Gi1/5     notconnect 1 full 100 Ex SX
Gi1/6     notconnect 1 full 100 Ex SX
Gi1/7     notconnect 1 full 100 Ex SX
Gi1/8     notconnect 1 full 1000 No GBIC
Gi1/9     notconnect 1 full 1000 No GBIC
Gi1/10    notconnect 1 full 1000 No GBIC
Gi1/11    notconnect 1 full 1000 No GBIC
Gi1/12    notconnect 1 full 1000 No GBIC
Gi1/13    inactive 1 full 1000 No GBIC
Gi1/14    inactive 1 full 1000 No GBIC
Gi1/15    inactive 1 full 1000 No GBIC
Gi1/16    inactive 1 full 1000 No GBIC
Gi1/17    inactive 1 full 1000 No GBIC
Gi1/18    inactive 1 full 1000 No GBIC
Router#
```

Related Commands

Command	Description
errdisable detect	Enables error-disable detection.
for-module port-group	Selects either Gigabit Ethernet or Ten Gigabit Ethernet interfaces on one module.
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

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 6500 series switch.
12.1(11)EW	Support for pse interface display.
12.2(18)EW	Support for displaying the status of native VLAN tagging in the command output.

Examples

This example shows how to display switch-port information using the **begin** output modifier:

```
Switch# show interfaces switchport | include VlanE
Name: Fa5/6
Access Mode VLAN: 200 (VlanE200)
Trunking Native Mode VLAN: 1 (default)
Trunking VlanEs Enabled: ALL
Pruning VlanEs 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
Operational Trunking Encapsulation:
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 VlanEs Enabled:ALL
Pruning VlanEs Enabled:2-1001

Name:Gi1/2
Switchport:Disabled
```

```
Administrative Mode:dynamic auto
Operational Mode:trunk
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
Administrative private-vlan trunk native VLAN:none
Trunking VLANs Enabled:ALL
Pruning VLANs Enabled:2-1001
Priority for untagged frames:0
Override vlan tag priority:FALSE
Voice VLAN:none
Administrative private-vlan trunk encapsulation:dot1q
Administrative private-vlan trunk normal VLANs:none
Administrative private-vlan trunk mapping:none
  10 (VLAN0010) 100 (VLAN0100)
Operational private-vlan:
Trunking VLANs Enabled:ALL
Pruning VLANs Enabled:2-1001
Capture VLANs Allowed:ALL

Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Protected: false
Assigned bundle:none
```

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 {[*int_name*] **transceiver** {**detail** } } | {**transceiver** {**module** *mod*} | **detail** [**module** *mod*] }

Syntax Description

int_name	(Optional) Interface name.
detail	(Optional) Displays the calibrated values and the A/D readouts if the module values differ from the calibrated values. Also displays the high-alarm, high-warning, low-warning, and low-alarm thresholds.
module *mod*	(Optional) Limits the display to interfaces on a specific module.

Defaults

The noninterface-specific versions of the **show interfaces transceiver** command are enabled by default.

The interface-specific versions 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

Command History

Release	Modification
12.1(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.2(20)EW	Support for the **calibration** keyword was withdrawn.

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
  If device is externally calibrated, only calibrated values are printed.
  ++ high alarm, +  high warning, -  low warning, -- low warning.
  N/A or N/A means extended digital monitoring not implemented.
  mA: milliAmperes, dBm: dBmilliWatt (milliwatts)

                                                        Optical   Optical
                                                        Tx Power  Rx Power
Port      Temperature   Voltage   Current   Tx Bias     (dBm)     (dBm)
          (Celsius)     (Volts)   (mA)      (mA)
--------  ----------    -------   -------   -------   --------  --------
Gi1/1/1   48.0          3.30      0.00      0.00      -8.1 ++   N/A
Gi1/1/2   33.0          3.30      1.8       1.8       -10.0     -16.8
Gi1/1/3   45.7          5.03      50.6      50.6      -4.7 ++   N/A
Gi1/1/4   39.5          5.02      25.7      0.8       N/A       N/A
Switch#
```

Note The value for the Optical Tx Power (reading) equals ten times log10 (Tx Power in mW). If the Tx Power value is 1 mW, then the Optical Tx Power value equals 10 * log (1), which equals 10 * 0 or 4.77 dBm. The Optical Rx Power value behaves similarly. If the Tx Power or the Rx Power is zero, then its value is displayed as zero or shown as N/A (not applicable).

This example shows how to display detailed diagnostic monitoring data, including calibrated values, alarm and warning thresholds, A/D values, and alarm and warning flags. The A/D readouts are reported separately in parameters only if they differ from the calibrated values:

```
Switch# show interfaces transceiver detail
mac address-range, dbm/dBmilliWatt (milliwatts), N/A or N/A not applicable.
++ high alarm, +  high warning, -  low warning, -- low alarm.
A/D readouts (if they differ), are reported in parentheses.
The threshold values are calibrated.

                                  High Alarm  High Warn  Low Warn   Low Alarm
                                  Threshold   Threshold   Threshold  Threshold
Port      Temperature             (Celsius)   (Celsius)   (Celsius)  (Celsius)
          (Celsius)               --------    --------    --------   --------
--------  ----------              100.0       90.0        0.0        0.0
Gi1/1/1   48.0                    100.0       90.0        0.0        0.0
Gi1/1/2   33.0                    70.0        60.0        0.0        0.0
Gi1/1/3   45.5                    70.0        60.0        0.0        0.0
Gi1/1/4   39.1                    70.0        60.0        0.0        0.0

                                  High Alarm  High Warn   Low Warn   Low Alarm
Port      Voltage                 Threshold   Threshold   Threshold  Threshold
          (Volts)                 (Volts)     (Volts)     (Volts)    (Volts)
--------  -------                 --------    --------    --------   --------
Gi1/1/1   3.30                    6.50        6.50        N/A        N/A
Gi1/1/2   3.30                    6.50        6.50        N/A        N/A
Gi1/1/3   5.03                    6.50        6.50        4.75       4.50
Gi1/1/4   5.02                    6.50        6.50        4.75       4.50

                                  High Alarm  High Warn   Low Warn   Low Alarm
Port      Current                 Threshold   Threshold   Threshold  Threshold
          (milliAmperes)          (mA)        (mA)        (mA)       (mA)
--------  --------                --------    --------    --------   --------
Gi1/1/1   0.0                     150.0       150.0       N/A        N/A
Gi1/1/2   1.8                     150.0       150.0       N/A        N/A
Gi1/1/3   50.6                    80.0        80.0        10.0       5.0
Gi1/1/4   25.8                    80.0        80.0        10.0       5.0
```

Port	Optical Transmit Power (dBm)	Optical Receive Power (dBm)	High alarm threshold (dBm)	High warn threshold (dBm)	Low warn threshold (dBm)	Low alarm threshold (dBm)
Gi1/1	0.1	--	8.1	6.1	N/A	N/A
Gi1/2	0.0	0.1	8.1	6.1	-1.0	-5.0
Gi2/1	-26.7	-13.01	--	1.2	-0.1	-5.5
Gi2/2	0.0	0.1	3.4	1.2	-0.1	-5.5

Port	Optical Transmit Power (dBm)	Optical Receive Power (dBm)	High alarm threshold (dBm)	High warn threshold (dBm)	Low warn threshold (dBm)	Low alarm threshold (dBm)
Gi1/1	N/A	8.1	8.1	N/A	N/A	N/A
Gi1/2	N/A	8.1	8.1	N/A	N/A	N/A
Gi2/1	-26.7	-28.01	3.4	1.2	-0.1	-5.5
Gi2/2	N/A	-28.01	3.4	1.2	-28.0	-28.0

Switch#

This example shows how to display the monitoring data for the interfaces that have transceivers installed extended 2:

```
Switch#show interfaces transceiver module 2
If device is externally calibrated, only calibrated values are printed.
++ = high alarm, + = high warning, - = low warning, -- = low alarm.
N/A or N/Ca= not applicable, Tr = transmit, Rx= receive.
mA= milliamperes, dBm= decibels (milliwatts).

                                                    Optical   Optical
                                                    Tx Power  Rx Power
Port    Temperature  Voltage  Current  dBm
        (Celsius)    (Volts)  (mA)     (Tx)        (Rx)
--------- ---------- -------- -------- ----------- -----------
Gi2/1    45.7         5.00     70.4     -14.0       N/A
Gi2/2    39.2         5.00     29.7     0.0         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
mA= milliamperes, dBm= decibels (milliwatts), N/A or N/Ca= not applicable.
++ = high alarm, + = high warning, - = low warning, -- = low alarm.
Gi2 readings (if they differ), are reported in parentheses.
The threshold values are calibrated.

                                        High alarm  High warn  Low warn  Low alarm
Port    Temperature  High alarm  Low alarm threshold  threshold  threshold  threshold
        (Celsius)    threshold   threshold (Celsius)  (Celsius)  (Celsius)  (Celsius)
--------- ---------- ----------- ---------- ---------- ---------- ---------- ----------
Gi2/1    45.5         70.0        0.0        80.0       70.0       0.0        0.0
Gi2/2    39.1         70.0        0.0        80.0       70.0       0.0        0.0

                                                        High alarm  High warn  Low warn  Low alarm
Port    Voltage      High alarm  Low alarm  Current     threshold  threshold  threshold  threshold
        (Volts)      threshold   threshold  (mA)        (Volts)    (Volts)    (Volts)    (Volts)
--------- ---------- ----------- ---------- ----------- ---------- ---------- ---------- ----------
Gi2/1    5.25         5.50        5.25       70.4        4.75       4.50
Gi2/2    5.25         5.50        5.25       29.7        4.75       4.50
```

Port	Current (mA)	High Alarm Threshold (mA)	High Warn Threshold (mA)	Low Warn Threshold (mA)	Low Alarm Threshold (mA)
Gi2/1	58.8	60.0	57.0	10.0	8.0
Gi2/2	58.8	60.0	60.0	10.0	8.0

Port	Optical Transmit Power (dBm)	High Alarm Threshold (dBm)	High Warn Threshold (dBm)	Low Warn Threshold (dBm)	Low Alarm Threshold (dBm)
Gi2/1	-14.7 (-12.0)	3.4	1.2	-2.3	-5.5
Gi2/2	0.6 (5.1)	3.4	1.2	-2.3	-5.5

Port	Optical Receiver Power (dBm)	High Alarm Threshold (dBm)	High Warn Threshold (dBm)	Low Warn Threshold (dBm)	Low Alarm Threshold (dBm)
Gi2/1	N/A (-28.5)	5.9	4.7	-26.0	-29.5
Gi2/2	N/A (-28.5)	5.9	4.7	-26.0	-29.5

Switch>

This example shows how to display the monitoring data for the transceivers on interface Gi1/2:

```
Switch# show interface gi1/2 transceiver
Name : GigabitEthernet1/2
Transceiver is internally calibrated.
If device is externally calibrated, only calibrated values are printed.
++ : high alarm, + : high warning, - : low warning, -- : low alarm.
A2D readings are not calibrated and represent uncorrected.
mA: milliamperes, dBm: decibels (milliwatts)

                    Temperature  Voltage  Current   Optical  Optical
Port                (Celsius)    (Volts)  (mA)      Tx Power Rx Power
                                                     (dBm)    (dBm)
---------           -----------  -------  --------  -------  -------
Gi1/2                 45.5       5.00     50.4      -14.7    N/A
Switch>
```

This example shows how to display detailed the monitoring data for the transceivers on interface Gi1/2:

```
Switch# show interface gi1/2 transceiver detail
ITU Channel not known
Transceiver is internally calibrated.
mA: milliamperes, dBm: decibels (milliwatts), N/A or N/A: not applicable.
++ : high alarm, + : high warning, - : low warning, -- : low alarm.
A2D readings are not calibrated and represent uncorrected.
The thresholds values are calibrated.

                    High Alarm  High Warn  Low Warn  Low Alarm
Temperature         Threshold   Threshold  Threshold Threshold
Port (Celsius)      (Celsius)   (Celsius)  (Celsius) (Celsius)
---------- -------- ----------- ---------- --------- ---------
Gi1/2      45.5     75.0        60.0       5.0       0.0

                    High Alarm  High Warn  Low Warn  Low Alarm
Voltage             Threshold   Threshold  Threshold Threshold
Port       (Volts)  (Volts)     (Volts)    (Volts)   (Volts)
---------- -------- ----------- ---------- --------- ---------
Gi1/2      5.00     6.50        6.25       4.75      4.75
```

```
                  Current                High alarm  High warn  Low warn   Low alarm
Port      Temp    (milliamperes)         threshold   threshold  threshold  threshold
                                         (mA)        (mA)       (mA)       (mA)
---------+-------+----------------------+-----------+----------+----------+----------
Gi2/1     50.0    7                      65.0        60.0       10.0       5.0

                  Optical                High alarm  High warn  Low warn   Low alarm
                  Transmit Power         Threshold   Threshold  Threshold  Threshold
Port      Bias    (dBm)                  (dBm)       (dBm)      (dBm)      (dBm)
---------+-------+----------------------+-----------+----------+----------+----------
Gi2/1     38.7    (-13.0)                3.4         3.2        -9.5       -9.9

                  Optical                High alarm  High warn  Low warn   Low alarm
                  Receive Power          Threshold   Threshold  Threshold  Threshold
Port      Bias    (dBm)                  (dBm)       (dBm)      (dBm)      (dBm)
---------+-------+----------------------+-----------+----------+----------+----------
Gi2/1     N/A     (-28.5)                0.4         -0.7       -28.5      -28.5

Delta-48
```

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

Command History

Release	Modification
12.1(8)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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     on           negotiate      trunking      1
Fa5/2     on           negotiate      trunking      1
Fa5/3     on           negotiate      trunking      1
Fa5/4     on           negotiate      trunking      1
Fa5/5     on           negotiate      trunking      1
Fa5/6     on           negotiate      not-trunking  10
Fa5/7     on           negotiate      not-trunking  10
Fa5/8     off          negotiate      not-trunking  1
Fa5/9     desirable    n-isl          trunking      1
Fa5/10    desirable    negotiate      trunking      1
Fa5/11    desirable    negotiate      trunking      1
Fa5/12    on           negotiate      trunking      1

Fa5/48    on           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     200
Fa5/10    1-1005
```

```
Fa5/20    none
Fa5/21    none
Fa5/22    none

Fa5/48    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     200
Fa5/9     1-2,10,20,50,100,152,200,300,303-305,349-351,400,500,521,524,570,801-8
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     200
Fa5/9     1-2,10,20,50,100,152,200,300,303-305,349-351,400,500,521,524,570,801-8
02,850,917,999,1002-1005
Fa5/10    none
Fa5/11    none

Fa5/48    none
Router#
```

This example shows how to display trunking information for active trunking ports:

```
Router#show interfaces trunk

Port      Mode         Encapsulation  Status        Native vlan
Fa5/9     desirable    n-isl          trunking      1

Port      Vlans allowed on trunk
Fa5/9     1-4094

Port      Vlans allowed and active in management domain
Fa5/9     1-2,10,20,50,100,152,200,300,303-305,349-351,400,500,521,524,570,801-8
02,850,917,999,1002-1005

Port      Vlans in spanning tree forwarding state and not pruned
Fa5/9     1-2,10,20,50,100,152,200,300,303-305,349-351,400,500,521,524,570,801-8
02,850,917,999,1002-1005
Router#
```

show ip arp inspection

To show the status of dynamic ARP inspection for a specific 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

Command History

Release	Modification
12.2(18)SXF	Support for this command was introduced on the Catalyst 6500 series switch.

Examples

This example shows how to display the statistics of packets that have been processed by DAI for VLAN 3:

```
Switch# show ip arp inspection statistics vlan 3

Vlan     Forwarded           Dropped     DHCP Drops    ACL Drops
----     ---------           -------     ----------    ---------
   3          11753            10247            0            0

Vlan     DHCP Permits     ACL Permits    Source Mac Failures
----     ------------     -----------    -------------------
   3            11753               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 IM for all active VLANs:

```
Switch#show arp inspection statistics

Vlans      Forwarded        Dropped      DHCP Drops      ACL Drops
----       ---------        -------      ----------      ---------
   1            0              0              0              0
   2            0              0              0              0
   3        28532          220358         220358              0
 100            0              0              0              0
 200            0              0              0              0
 201            0              0              0              0
1004            0              0              0              0
1007            0              0              0              0

Vlans  DHCP Permits   ACL Permits   Source MAC Failures
----   ------------   -----------   -------------------
   1            0              0                     0
   2            0              0                     0
   3        28532              0                     0
 100            0              0                     0
 200            0              0                     0
 201            0              0                     0
1004            0              0                     0
1007            0              0                     0

Vlans  Dest MAC Failures   IP Validation Failures
----   ----------------   ----------------------
   1                  0                        0
   2                  0                        0
   3                  0                        0
 100                  0                        0
 200                  0                        0
 201                  0                        0
1004                  0                        0
1007                  0                        0
Switch#
```

This example shows how to display the configuration and operating state of DAI for VLAN 1:

```
Switch#show 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 arp inspection interfaces FastEthernet 6/1
Interfaces        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
Po1:1        Trusted            None
Fa6/1        Untrusted          15
Fa6/5        Untrusted          15
Fa6/6        Untrusted          15
Fa6/7        Untrusted          15
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.

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

Command History	Release	Modification
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows how to display the current contents of the log buffer before and after the buffer is cleared:

```
Switch#show arp inspection log
Total\ Buffer\ Size\ 32
Syslog rate:5 entries per 10 seconds.

 Interfaces        Vlan   Sender MAC        Sender IP        Num of Pkts
 ----------        ----   ----------        ---------        -----------
 Fa6/3             1      0002.0002.0002    1.1.1.2          1(12:02:02 UTC Fri Apr 25 2003)
 Fa6/3             1      0002.0002.0002    1.1.1.3          1(12:02:02 UTC Fri Apr 25 2003)
 Fa6/3             1      0002.0002.0002    1.1.1.4          1(12:02:02 UTC Fri Apr 25 2003)
 Fa6/3             1      0002.0002.0002    1.1.1.5          1(12:02:02 UTC Fri Apr 25 2003)
 Fa6/3             1      0002.0002.0002    1.1.1.6          1(12:02:02 UTC Fri Apr 25 2003)
 Fa6/3             1      0002.0002.0002    1.1.1.7          1(12:02:02 UTC Fri Apr 25 2003)
 Fa6/3             1      0002.0002.0002    1.1.1.8          1(12:02:02 UTC Fri Apr 25 2003)
 Fa6/3             1      0002.0002.0002    1.1.1.9          1(12:02:02 UTC Fri Apr 25 2003)
 Fa6/3             1      0002.0002.0002    1.1.1.10         1(12:02:02 UTC Fri Apr 25 2003)
 Fa6/3             1      0002.0002.0002    1.1.1.11         1(12:02:02 UTC Fri Apr 25 2003)
                                                             9(12:02:02 UTC Fri 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\ Buffer\ Size\ 32
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 states 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

Command History	**Release**	**Modification**
	12.2(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples

This example shows how to display the prefixes for a specific VLAN:

```
Switch# show ip cef vlan 1403
Prefix      Next Hop        Interface
0.0.0.0/32  receive         FastEthernet3/3
0.0.0.0/32  receive
10.7.0.36   172.26.92.1     FastEthernet3/3
10.16.16.0/23   172.26.92.1     FastEthernet3/3
Switch#
```

This example shows how to display detailed IP CEF information for a specific VLAN:

```
Switch# show ip cef vlan 1403 detail
IP Distributed CEF with switching (Table Version 2364), flags=0x0
  2382 routes, 0 reresolve, 0 unresolved (0 old, 0 new)
  2382 leaves, 1191 nodes, 1430 KBytes, 2382 inserts, 999 invalidations
  0 load sharing elements, 0 bytes, 0 references
  universal per-destination load sharing algorithm, id 9B4CF421
  3564 CEF resets, 182 revalidations, 0 unresolved
  refcounts: 5635 leaf, 5732 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

Command History

Release	Modification
12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.2(52)SG	Support for option 82 on untrusted ports was added.

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
DHCP snooping is operational on following VLANs:
500,505
DHCP snooping is configured on the following L2 Interfaces:
Insertion of option 82 is enabled
circuit-id default format: vlan-mod-port
remote-id: 00d0c0a8bc00 (cisco)
Option 82 on untrusted port is not allowed Verification of hwaddr field is enabled DHCP
snooping trust/rate is configured on the following Interfaces:
Interface Trusted Rate limit (pps)
-----------------------------------------
FastEthernet3/1 yes 100
Gigabit ethernet:1/2n
VLAN 500: rate-limit 100
Gigabit ethernet:1/2n untrusted
Gigabit ethernet:1/2n
VLAN 500: rate-limit 100
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.

Command	Description
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_no*] [**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

Command History	**Release**	**Modification**
	12.2(18)SXF	Support for this command was introduced on the Catalyst 6500 series switch.

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
------------------  --------------  -------------    -------------  ----  --------------------
00:00:01:00:02:03   10.0.0.1        1400             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 172.20.101.102
MacAddress          IP Address      Lease (seconds)  Type           VLAN  Interface
------------------  --------------  -------------    -------------  ----  --------------------
00:00:01:00:02:03   172.20.101.102  1400             dhcp-snooping  100   FastEthernet3/1
Switch#
```

This example shows how to display the MAC address for the DHCP snooping binding entries:

```
Switch#show ip dhcp snooping binding 00.01.02.03.04.05
Switch#
MacAddress          IpAddress       Lease(sec)  Type           VLAN  Interface
------------------  --------------  ----------  -------------  ----  --------------------
00:02:B8:3E:3B:50   10.1.1.2        492         dhcp-snooping  99    FastEthernet6/36
Switch#
```

This example shows how to display the DHCP snooping binding entries' MAC address for a specific VLAN:

```
Switch#show ip dhcp snooping binding 00.01.02.03.04.05vlan 99
Switch#
MacAddress          IpAddress       Lease(sec)  Type           VLAN  Interface
------------------  --------------  ----------  -------------  ----  --------------------
00:02:B8:3E:3B:50   10.1.1.2        478         dhcp-snooping  99    FastEthernet6/36
Switch#
```

This example shows how to display the dynamic DHCP snooping binding entries:

```
Switch#show ip dhcp snooping binding dynamic
Switch#
MacAddress          IP Address      Lease (seconds)  Type           VLAN  Interface
------------------  --------------  ---------------  -------------  ----  --------------------
00:00:0300.0301.0302  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
Switch#
MacAddress          IP Address      Lease (seconds)  Type           VLAN  Interface
------------------  --------------  ---------------  -------------  ----  --------------------
0000.0300.0301.0302  10.0.0.1       1600             dhcp-snooping  100   FastEthernet3/1
Switch#
```

This example show how to display the DHCP snooping binding entries on Ethernet interface 0/1:

```
Switch#show ip dhcp snooping binding interface fastethernet3/1
Switch#
MacAddress          IP Address      Lease (seconds)  Type           VLAN  Interface
------------------  --------------  ---------------  -------------  ----  --------------------
0000.0300.0301.0302  10.0.0.1       1600             dhcp-snooping  100   FastEthernet3/1
Switch#
```

Table 2-21 describes the fields in the **show ip dhcp snooping** command output.

Table 2-21 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.
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

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(19)EW	Added support of state and statistics information.

Examples

This example shows how to display the DHCP snooping database:

```
Switch# show ip dhcp snooping database
Agent URL:
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : Not Running
Abort Timer Expiry : Not Running

Last Succeeded Time : None
Last Failed Time : None
Last Failed Reason : No Failure recorded.

Total attempts      :    0   Startup Failures :    0
Successful Transfers :    0   Failed Transfers :    0
Successful Reads    :    0   Failed Reads     :    0
Successful Writes   :    0   Failed Writes    :    0
Media Failures      :    0

Switch#
```

This example shows how to view additional operating statistics:

```
Switch# show ip dhcp snooping database detail
Agent URL : nfsp://10.1.1.2/directory/file
Write delay Interval : 300 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : 7 (00:00:07)
Abort Timer Expiry : Not Running

Last Succeeded Time : None
Last Failed Time : 17:14:25 UTC Sat Jul 7 2001
Last Failed Reason : Unable to access URL

Total attempts      :   21   Startup Failures :    0
Successful Transfers :    0   Failed Transfers :   21
Successful Reads    :    0   Failed Reads     :    0
Successful Writes   :    0   Failed Writes    :   21
Media Failures      :    0

First successful access: Read

Last ignored bindings counters :
Binding Collisions  :    0   Expired Leases   :    0
Invalid Interfaces  :    0   Unsupported vlans :    0
Parse Failures      :    0
Last Ignored Time : None

Total ignored bindings counters:
Binding Collisions  :    0   Expired Leases   :    0
Invalid Interfaces  :    0   Unsupported vlans :    0
Parse Failures      :    0

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* | **null** *interface-number* | **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.
	null *interface-number*	(Optional) Specifies the null interface and the number of the interface; the only valid value is **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

Command History	Release	Modification
	12.1(15)SW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW	Added support for extended VLAN addresses.
	12.2(25)EW	Added support for the 10-Gigabit Ethernet interface.

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
vlan200 is administrative up, line protocol is up
IGMP enabling on admin.net on this Vlan
IGMP accepting Immediate-leaves is disabled on this Vlan
IGMP accepting Immediate-leaves is disabled on this Vlan
IGMP accepting is running in IGMP-SNOP mode on this Vlan
Switch#
```

Related Commands	Command	Description
	clear ip igmp group	Deletes the IGMP group cache entries.
	show ip igmp snooping mrouter	Displays information on the dynamically learned and manually configured multicast router interfaces.

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 4294967295.
Defaults	This command has no default settings.
Command Modes	Privileged EXEC mode

Command History	**Release**	**Modification**
	12.1(12)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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 19
      range 230.9.9.0 230.9.9.0
IGMP Profile 4
      permit
      range 229.9.9.0 229.255.255.255
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** | **vlan** *vlan_id a.b.c.d*[*summary* | *sources* | *hosts*] [*count*]

Syntax Description	**querier** (Optional) Specifies that the display will contain IP address and version information. **groups** (Optional) Specifies that the display will list VLAN numbers noticed by group IP addresses. **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 v2 or v3 group. **sources** (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. **count** (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

Command History

Release	Modification
12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.1(20)EW	Support for extended addressing was added.
12.1(20)EW	Added support to display configuration state for IGMPv3 explicit host tracking.

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
CGMP interoperability     : Enabled
Multicast router learning mode : pim-dvmrp
IGMP interoperability mode : IGMP_ONLY

Vlan 2:
--------
IGMP snooping             : Enabled
IGMPv2 immediate leave    : Disabled
CGMP interoperability     : 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
IGMPv2 immediate leave    : Disabled
CGMP interoperability     : 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    v2              Router
3      172.20.50.22  v3              Fa3/15
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    Ports
----------------------------------------------------------
2         224.0.1.40      v3         Router
            239.0.2.2     v3         Fa6/10
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         239.0.2.4       v3         Gi2/1,Fa3/3
          239.0.2.2       v3         Fa6/10
Switch>
```

This example shows how to display the group's host types and ports in VLAN 1:

```
Switch# show ip igmp snooping group vlan 22 224.0.4.7
Vlan      Group           Version    Ports
----------------------------------------------------------
22        224.0.4.7       v3         Fa7/13, 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 10 226.6.6.7 sources
Source information for group 226.6.6.7:
Timers: Expired sources are deleted on next IGMP General Query
SourceIP         Expires   Uptime  Inc Hosts Exc Hosts
----------------------------------------------------------
2.2.2.1          00:03:44  00:43:48  2    0
2.2.2.2          00:03:44  00:02:07  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 10 224.4.4.5 hosts
IGMPv3 host information for group 224.4.4.5
Timers: Expired hosts are deleted on next IGMP General Query

Host (MAC/IP)  Filter mode  Expires  Uptime  # Sources
---------------------------------------------------------
175.1.2.29     INCLUDE      stopped  00:16:14  2
175.2.0.50     INCLUDE      stopped  00:16:14  2
Switch#
```

This example shows how to display summary information for a v3 group:

```
Switch# show ip igmp snooping group vlan 10 224.4.4.7 summary
Group Address (Vlan 10)  : 224.4.4.7
Host types               : 2
Number Hosts             : 0x7110, 0x7114
Filter mode              : INCLUDE
Expires                  : stopped
Uptime                   : 00:16:14
Sources(Inclusion/Exclusion) : 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         Gi1/1,Gi1/2,Po1,Po128,Router
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: 55
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: 55
Switch#
```

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping.
ip igmp snooping tcn 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*]
[**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 VLAN number and multicast IP address of a VLAN. Valid values are from 1 to 1001 and from 1006 to 4094.
source *a.b.c.d*	(Optional) Displays a 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

Command History

Release	Modification
12.1(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.2(25)EW	Added support for the 10 Gigabit Ethernet interface.

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
Switch#
Hosts: 1 , 1
Snooping Group Interface Reporter Uptime Last /Join Last /Leave

40.40.40.2/224.10.10.10 (224/1 20.20.20.20 00:03:17 00:00:56 00:20:30
40.40.40.4/224.10.10.10(224/1 20.20.20.20 00:04:30 00:00:27
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
Switch#
Hosts: 1 , 1
Snooping Group Interface Reporter Uptime Last /Join Last /Leave

40.40.40.2/224.10.10.10 (224/1 20.20.20.20 00:03:17 00:00:56 00:20:30
Switch#
```

show ip igmp snooping membership

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 20
----------------------------------------------
Total number of channels:5
Total number of hosts   :4

Source/Group            Interface       Reporter        Uptime  Last/Left
                                                                Last/Leave
----------------------------------------------------------------------------
40.0.0.1/224.1.1.1      Fa5/37          0002.4baf.a480  00:00:44 00:00:04 /
                                                                          v
40.0.0.2/224.1.1.1      Fa5/37          0002.4b86.8730  00:00:07 00:00:17 /
                                                                          v
40.0.0.3/224.1.1.1      Fa5/36          20.20.20.20     00:00:04 00:00:04 /
                                                                          v
40.0.0.4/224.1.1.1      Fa5/35          20.20.20.200    00:00:07 00:00:17 /
                                                                          v
40.0.0.5/224.1.1.1      Fa5/37          0002.4b86.8730  00:00:07 00:00:17 /
                                                                          v
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 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

Command History

Release	Modification
12.1(12c)EW	Support for this command was introduction the Catalyst 4500 series switch.
12.1(20)EW	Added support for extended VLAN addresses.

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 interface 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,Po1:5,Fa6:60
Switch#
```

Related Commands

Command	Description
ip igmp snooping vlan mrouter	Statically 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

Command History

Release	Modification
12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.2(31)SG3	Support for extended addressing was added.

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 Fast leaving is globally enabled
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 router 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

Command History	**Release**	**Modification**
	12.2(25)EW	Extended to include the 10-Gigabit Ethernet interface.

Usage Guidelines The Cisco IOS software automatically enters a directly connected route in the routing table if the interface is usable. A usable interface is one through which the software can send and receive packets. If the software determines that an interface is not usable, 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 up, line protocol is up
  Internet address is 172.20.226.96/24
  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 access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
```

```
Local Proxy ARP is disabled
security level is unset
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 fast switching on the same interface is disabled
IP Flow switching is disabled
IP CEF switching is enabled
IP Fast switching turbo vector
IP Normal CEF switching turbo vector
IP multicast fast switching is enabled
IP multicast distributed fast switching is disabled
IP route-cache flags are Fast, CEF
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Probe proxy name replies are disabled
Policy routing is enabled,
local policy routing is enabled
WCCP Redirect outbound is disabled
WCCP Redirect inbound is disabled
WCCP Redirect exclude is disabled
BGP Policy Mapping is disabled
Sampled Netflow is disabled
IP multicast multilayer switching is disabled
Hardware Switch Feature(s) handled by
hardwa
```

Table 2-22 describes the fields that are shown in the example.

Table 2-22 *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 value 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.

Table 2-22 show ip interface Field Descriptions (continued)

Field	Description
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.
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 targeted for an interface are excluded from being redirected to a cache engine.
Netflow Data Export (hardware) is enabled	TOS hardware flow status on the interface.

show ip mfib

To display active Multicast Forwarding Information Base (MFIB) routes, use the **show ip mfib** command.

show ip mfib [**all** | **counters** | **log** [*n*]]

Syntax Description

all	(Optional) Specifies all routes in the MFIB, including those routes that are used to generate fast-switching flags but are not necessarily in the supervisor routing protocol table.
counters	(Optional) Specifies the counts of MFIB related events. Only nonzero counters are shown.
log	(Optional) Specifies a log of the most recent number of MFIB related events. The most recent event is first.
n	(Optional) Number of events.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 6500 series switch.
12.2(18)SXD	Support for command introduced on the Supervisor Engine 6-E and Catalyst 6500E chassis.

Usage Guidelines

In the Supervisor Engine 6-E and Catalyst 6500E chassis, the output of the **show ip mfib** command does not display any hardware counters.

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 an 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 process needs notification that 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 on 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 router 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 can contain 1 indicating that the ingress packets should be tested and whether packets matching the route should be forwarded onto interface 1. These per-interface flags are associated with MFIB states:

- 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)—Used on the A flags packets that arrive on the Forwarding interfaces together from a multicast slot or output interface list.
- Signaling (S)—Set when interface when multicast routing protocol process in Cisco IOS needs to be notified of ingress packets on that interface.
- Not Platform (NP)—Set switched—Used with the F flag. A forwarding interface is also marked as Not Platform (set-switched whenever that output interface cannot be fast-switched by the platform hardware and requires software forwarding.

  For example, the Catalyst 6506 switch with Supervisor Engine III cannot switch tunnel interfaces in hardware so these interfaces are marked with the NP flag. When an NP interface is associated with a mroute, a copy of every ingress packet arriving on an Accepting interface is sent to the switch software forwarding path for software replication and then forwarded to the NP interface.

Examples

This example shows how to display all active MFIB routes:

```
Router# show ip mfib
IP Multicast Forwarding Information Base
Entry Flags: C - Directly Connected, S - Signal,
             IN - Internal Copy
Interface Flags: A - Accept, F - Forward, NS - Signal,
             ID - Set platform switched
Router#show ipmulticast Vlan Syrac Fast/Partial/Slow
(171.69.10.13, 224.0.1.40), Flags IKS
  Vlan2 (2/65/0/0/0), Rpkts/ 42492/0/0/52803
  Vlan7 (s)
  Vlan100 (F NS)
  Vlan101 (F NS)
  Vlan 2: (*, Flags I)
  Partner: 32/0/0/0, Rpkts/ 53492/0/0
  Vlan 7: (s)
(*, 224.0.1.75), Flags I)
  Vlan 2: (s)
(171.69.10.13, 239.192.128.80), Flags I)
  Vlan 2: (2/65/0/0/0, 2112/0/0/0/0/0/0 bytes
  Vlan7 (F NS)
  Vlan100 (s)
(*, 239.192.128.70), Flags I)
  Vlan 2: (0/0/0/0, 0/0/0/0 bytes
  Vlan7 (s)
Router#
```

Related Commands	Command	Description
	clear ip mfib counters	Clears the global MFIB counter and the counters for all active MFIB routes.

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

Command History	Release	Modification
	12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples This example shows 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 ) 00:01:32
(10.1.0.2, 224.1.2.3, Vlan9 ) 00:02:00
(10.1.0.3, 224.0.1.4, Vlan9) 00:00:05
Switch#
```

Related Commands	Command	Description
	show 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*] | *interface_type slot/port* | **count** | **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

Command History

Release	Modification
12.1(18a)SW	Support for this command was introduced on the Catalyst 6500 series switch.
12.2(2)XN	Added support for the 10-Gigabit Ethernet interface.

Usage Guidelines

If you omit 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 creating source, group (S,G) entries from star, group (*,G) entries. The star refers to all source addresses, the "*" refers to a single source address, and the "G" refers to the destination multicast group address. In creating (S,G) entries, the software uses the best path to that destination group found in the unicast routing table (through Reverse Path Forwarding (RPF).

Examples This example shows how to display all the entries in the IP multicast routing table:

```
Switch# show ip mcache
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - BGP 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: Ambrosia.Interface, Ext-Ethernet 0/0, Statistics
(*, 224.0.1.40), 00:04:45/00:00:00, RP 26.15.1.250, Flags:SJC
  Incoming Interface:Gigabit0/0Ethernet4/8, RPF nbr 15.15.1.250
  Outgoing Interface List:Null

(26.15.1.2, 224.0.1.40), 00:04:45/00:00:00, RP 26.15.1.250, Flags:SJCT

  Incoming Interface:Gigabit0/0Ethernet4/8, RPF nbr 15.15.1.250, RPF NBR:
  15.15.1.250
  Gigabit0/0Ethernet4/8, Forward/Sparse-Dense, 00:04:45/00:00:00, H

(26.15.1.15, 224.0.1.40), 00:04:45/00:00:00, RP 26.15.1.250, Flags:SJT

  Incoming Interface:Gigabit0/0Ethernet4/8, RPF nbr 15.15.1.250, RPF NBR:
  15.15.1.250
  Gigabit0/0Ethernet4/8, Forward/Sparse-Dense, 00:04:45/00:00:00, H

(*, 239.192.128.128), 00:04:45/00:00:00, Flags:SCJ
  Incoming Interface:Gigabit0/0Ethernet4/8, RPF nbr 15.15.1.250, RPF NBR:
  15.15.1.250
  Outgoing Interface List:Null
Switch#
```

This example shows how to display the rate that the active sources are sending to the multicast groups and to display only the active sources that are sending at greater than the default rate:

```
Switch# show ip mcache active

Active IP Multicast Sources - sending >= 4 kbps

Group: 224.2.127.254, (sdr.cisco.com)
     Source: 146.137.28.69 (mbone.ipd.anl.gov)
       Rate: 9 pps/5 kbps(last) 4 kbps(last 5 secs), 4 kbps(life avg)

Group: 224.2.201.241, ADM ST
     Source: 192.168.52.160 (mankoont5-vlan447.telscap.net)
       Rate: 9 pps/5 kbps(last), 145 kbps(last 30 secs), 85 kbps(life avg)

Group: 224.2.207.215, ADM ST
     Source: 192.168.52.160 (mankoont5-vlan447.telscap.net)
       Rate: 7 pps/5 kbps(last), 63 kbps(last 30 secs), 85 kbps(life avg)
Switch#
```

This example shows how to display route and packet count information:

```
Router#show ip mroute,#route
IP Multicast Statistics
7 routes using 4184 bytes of memory
15 groups, 0.13 group sources per group
Forwarding Counts:Pkts (Pkts per second),Kbs (Kbs/sec),Bytes (Bytes per second)

Other counts:Total/RPF failed/OIF-Null;Uptime:hh:mm:ss (mm:ss)

Group:232.2.154.89, Source count:1, Group pkt count:1
   Source:192.168.70.28/32, Forwarding:2905/2/278/5.56/0, Other:8572/6/0/0(00:
Route:

This example shows how to display summary information:

Router#show ip mroute,#summary
IP Multicast Route Summary
  (*,G) = Number of (*,Group) x = SSM 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, S = Proxy Join Timer Running,
    A = Advertised via MSDP, U = URD, I = Received Source Specific Host
    Report
Outgoing Interface Flags: H = Hardware switched
  A = Assert winner
  Interface state: Interface, Next-Hop or VCD, State/Mode

Route:
```

Table 2-23 describes the fields shown in the output.

Table 2-23 *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.
x - SSM Group	Entry is a member of an SSM group.
C - Connected	Member of the multicast group is present on the directly connected interface.
L - Local	Router 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 or the (S,G) entry pointing toward the RP. The R - Rp-bit set is typically a prune 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 2-23 show ip mcast Field Descriptions (continued)

Field	Description
J - Join SPT	(*,G) entries, indicates that the rate of traffic flowing down the shared tree is exceeding the SPT-Threshold set for the group. (The SPT-Threshold setting is shown by the ip pim spt-threshold CLI command). For (S,G) entries, indicates that the source data stream triggers an (S,G) join 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 unconditionally switches back to the shared tree if a threshold is never exceeded. 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 set on (*, 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 installed in hardware switched.
Timer:	Expiration/Expires.
Interface state:	Interface, Next-Hop or VCD, State/Mode.
(*, 224.0.255.1) (198.92.37.100/12, 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 2-23 show ip mroute Field Descriptions (continued)

Field	Description
RP	Address of the RP router. 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 hexadecimal number in parentheses indicates which RP is tunneling. Each bit indicates a different RP if multiple RPs are configured.
DVMRP or Mroute	Status of whether RPF information is obtained from the DVMRP routing table or the static mroute configuration.
Outgoing interface list	Interfaces through which packets are forwarded. When the **ip pim mroute-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 forwarded on the interface or if a prune message has sent over this interface. For PIM, Forwarding, following the slash (/), mode (a, which the interface is operating (dense or sparse). Sparse mode interface is in forward mode.
Forward/Sparse	Sparse mode interface is in forward mode.
time/time (optional on pim-sm interfaces)	Per interface, how long (seconds, 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

Command History

Release	Modification
12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

The optional parameters filter the display output result.

Examples

This example shows how to display the IP source bindings:

```
Router# show ip source binding
Bindings for all interfaces:
IP address      MAC address     Lease(sec)  Type        VLAN  Interface
-----------     -----------     ----------  ----        ----  ---------
00:00:00:ab:cd:ef 11.0.0.1      infinite    static      10    FastEthernet4/10
Total 1 bindings
```

This example shows how to display the static IP binding entry of IP address 11.0.01:

```
Router# show ip source binding 11.0.0.1 0000.0000.0000 static vlan 10 interface fa4/10
Bindings for all interfaces:
IP address      MAC address     Lease(sec)  Type        VLAN  Interface
-----------     -----------     ----------  ----        ----  ---------
00:00:00:ab:cd:ef 11.0.0.1      infinite    static      10    FastEthernet4/10
Total 1 bindings
```

Related Commands

Command	
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

Command History

Release	Modification
12.2(52)SG	Support for this command was introduced on the Catalyst 4500 series switch.

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 snooping-enabled VLANs that do not have a valid IP source binding.

- This output appears when you enter the **show ip verify source interface fa6/1** 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
---------------------------------------------------------------------
fa6/1     ip          active      10.0.0.1       ---            10
fa6/1     ip          inactive-trunk-port
```

- This output appears when you enter the **show ip verify source interface fa6/1** command and the interface fa6/1 does not have a VLAN enabled for DHCP snooping:

```
Interface Filter-type Filter-mode IP-address     Mac-address    Vlan
---------------------------------------------------------------------
fa6/1     ip          inactive-no-snooping-vlan
```

- This *output* appears when you enter the **show ip verify source interface fa4/4** command and the interface fa4/4 has an IP source filter mode that is configured as IP MAC and the existing IP MAC the binds 10.0.0.2 ieee3888.cccc on VLAN 10 and 11.0.0.3 ieee3888.cccd on VLAN 11:

```
Interface Filter-type Filter-mode IP-address       Mac-address     Vlan
---------------------------------------------------------------------------
fa4/4     ip-mac      active      10.0.0.2         aaaa.bbbb.cccc  10
fa4/4     ip-mac      active      11.0.0.1         aaaa.bbbb.cccd  11
fa4/4     ip-mac      active      deny-all         deny-all        10-20
```

- This *output* appears when you enter the **show ip verify source interface fa4/4** command and the interface fa4/4 has IP source filter mode that is configured as IP MAC and existing IP MAC binds 10.0.0.2aaaa.bbbb.cccc on VLAN 10, but port security is not enabled on fa4/4:

```
Interface Filter-type Filter-mode IP-address       Mac-address     Vlan
---------------------------------------------------------------------------
fa4/4     ip-mac      active      10.0.0.2         permit-all      10
fa4/4     ip-mac      active      deny-all         permit-all      11-20
```

Note Enable port security first because the DHCP security MAC filter cannot apply mode port or VLAN.

- This *output* appears when you enter the **show ip verify source interface fa4/4** command and the interface fa4/4 does not have IP source filter mode that is configured:

```
IPSG security is not configured on the interface fa4/4.
```

This example shows how to display all the interfaces on the switch that have DHCP snooping security and IP Port Security tracking 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
-----------------------------------------------------------------------------
fa6/1      ip          active       10.5.5.1         ----------      10
fa6/1      ip          active       deny-all         ----------      11-20
fa6/2      ip          inactive-trust-port
fa6/3      ip vlan     active       40.1.1.24                        10
fa6/3      ip vlan     active       40.1.1.25                        20
fa6/3      ip vlan     active       40.1.1.23                        30
fa6/4      ip          active       10.5.5.2         aaaa.bbbb.cccc  10
fa6/4      ip          active       10.5.5.3         aaaa.bbbb.cccd  11
fa6/4      ip          active       deny-all         deny-all        20-30
fa6/5      ip-mac      active       10.5.5.5         permit-all      10
fa6/5      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 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

Command History	Release	Modification
	12.1(11)EW	Support for this command was introduced on the Catalyst 6500 series switch.

Examples This example shows how to display the participating nodes:

```
Switch# show ipc nodes
There are 3 nodes in this IPC realm.
  ID   Type                                          Last  Last
                                                     Sent  Heard
  10000 Local   IPC Master                           0     0
  20100001 Local   QALIGN IPC-Card 1                 0     0
  20200001 Remote  IPC Slave-Card 2                  12    26
Switch#
```

This example shows how to display the local IPC port:

```
Switch# show ipc ports
There are 11 ports defined.

Port ID      Type        Name                    (current/peak/total)
  10000.1    ved-conn    IPC Master/Echo
  10000.2    ved-conn    IPC Master/Echo
  10000.3    ved-conn    IPC Master/Control
  10000.4    ved-conn    Remote TCP Server Port
  20100001.1 ved-conn    QALIGN IPC Master
    inbox 0 max_id 0x00200001 last sent 0      Sent0 0 (4/0)    0/1/4(4)

  20100001.8 ved-conn    QALIGN RED-Active
    inbox 0 max_id 0x00200001 last sent 0      Sent0 0 2        0/1/2

  20200001.7 ved-conn    QALIGN IPC-Card 2-Control
  20200001.8 ved-conn    QALIGN RED-Active
  20200001.9 ved-conn    Slave Remote IPC Client Port
  20200001.a ved-conn    QALIGN RF -Standby
  20200001.b ved-conn    QALIGN RED-Standby
Switch#
```

```
IPC packets: 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 0 IPC messages waiting for acknowledgment in the transmit queue.
There are 0 IPC messages waiting for a response.
There are 0 IPC messages waiting for additional fragments.
There are 0 IPC messages received on the IPC inbound Q.
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.

4000 IPC message headers in cache
3140 messages in, 3140 rec, 3140 delivered to local port,
0 messages out, 0 sent, 0 confirmed, 1875 sent,
0 NACKS received, 0 sent,
0 messages dropped on input, 0 messages dropped on output
0 no port, 0 duplicate port, 0 port conflicts, 0 ports
0 aliasing callback in queue, 0 duplicate ACKs, 0 retries,
0 message timeouts,
0 "get_buffer failures, 0 sav failures,
0 "get_buffer" failures, 0 xmsr msg alloc failed, 0 no cntxp for ERC replies
0 pak alloc failed, 0 msmsr alloc failed
0 no msg, 1 failed cpuss, 0 hardware errors
No regular dropping of IPC output packets for test purposes
Switch#
```

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

Command History

Release	Modification
12.2(50)SG	This command was introduced on the Catalyst 4500.

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              : Disabled
MLDv2 snooping (minimal)  : Disabled
Listener message suppression : Disabled
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
Multicast router learning           : pim-dvmrp
Listener message suppression        : Enabled
TCN solicit query                   : Disabled
Tcn flood query count               : 2
Robustness variable                 : 2
Last listener query count           : 2
Last listener query interval        : 1000

Vlan 1:
--------
MLD snooping                        : Disabled
Multicast router learning           : pim-dvmrp
Explicit host tracking              : Enabled
Multicast router learning mode      : pim-dvmrp
Robustness variable                 : 2
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                 : 2
Last listener query count           : 2
Last listener query interval        : 1000
```

Related Commands

Command	Description
ipv6 mld snooping	Enables IP version6 (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

Command History	Release	Modification
	12.2(18)SXD	This command was introduced on Catalyst 6500.

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.

```
Router#show ipv6 mld snooping mrouter
Vlan    ports
----    -----
   2    Gi3/5(fixed)
  200   Gi3/5(fixed)
  201   Gi3/5(fixed)
```

This is an example of output from the **show ipv6 mld snooping mrouter vlan** command. It shows multicast switch ports for a specific VLAN.

```
Router#show ipv6 mld snooping mrouter vlan 100
Vlan    ports
----    -----
   2    Gi3/5(fixed)
```

Related Commands

Command	Description
ipv6 mld snooping	Enables IP version 6 (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 VLANs. the range is 1 to 1001 and 1006 to 4094.

Command Modes | User EXEC mode

Command History	Release	Modification
	12.2(40)SG	This command was introduced on the Catalyst 4500.

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 routers 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 user-configured VLANs that are shutdown. If no information is available in the specified VLAN, or if the VLAN information is stored only on the MLSQ (message-this is sent by the switch. It does not exercise the user-configured robustness variable that is used for aging out a member that does not respond to query messages.

VLANs number 1002 through 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in MLSD 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
-----------------------------------------------------------
2       FE80::201:C9FF:FE40:8200 v2         Gi3/3
```

This is an example of output from the **show ipv6 mld snooping querier vlan** command:

```
Switch> show ipv6 mld snooping querier vlan 2
IP address: FE80::201:C9FF:FE40:8200
MLD version: v2
Port: Gi3/3/1
Max response time: 10sec
```

Related Commands

Command	Description
ipv6 mld snooping	Enables IP version 6 (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 version 6 (IPv6) MLD snooping last-listener query interval on the switch or on a VLAN.
ipv6 mld snooping robustness-variable	Configures the number of IP version 6 (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 Notifications (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 can also be independent.
	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.
	client_id (Optional) Identifies the client registered in 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

Command History	Release	Modification
	12.2(31)SGA	This command was introduced on the Catalyst 4500 series switch.

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 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 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 = 5
Switch#
```

The following example shows how to display the ISSU capability entries for the IP host ISSU client (client#=2002):

```
Switch#show issu capability entries 2002
Client_ID = 2002, Entry_ID = 1 :
        Cap_Entry = 1,          Cap_Type = 5
Switch#
```

The following example shows how to display the ISSU capabilities groups for the IP host ISSU client (client=20):

```
Switch# show issu capability groups 2042
Client=20 Client_Name= Session_id = 0
  Group_Id=0 ,
        Cap_Entry = 1,
                Cap_Type = 0

Switch#
```

Related Commands:	Command	Description
	show issu clients	Displays the ISSU clients.

show issu clients

To display the ISSU clients, use the **show issu clients** command.

show issu clients [*peer_uid*]

Syntax Description *peer_uid* (Optional) Displays a list of clients registered to ISSU infrastructure at the peer supervisor engine.

Defaults Displays a list of clients registered to the ISSU infrastructure at the supervisor engine where the command is entered.

Command Modes User EXEC mode

Command History	Release	Modification
	12.2(25)EWA	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines To implement ISSU versioning functionality, a client must first register itself, client capability, and client message information with the ISSU infrastructure during the system initialization.

Examples The following example shows how to display the ISSU clients:

```
Switch# show issu clients
Client_id = 1, Client_Name = ISSU Trans client,  Reding_Quant = 1
Client_id = 2, Client_Name = ISSU RF,  Reding_Quant = 1
Client_id = 3, Client_Name = ISSU Network RF client,  Reding_Quant = 1
Client_id = 4, Client_Name = ISSU Network RF client,  Reding_Quant = 1
Client_id = 5, Client_Name = ISSU CF client,  Reding_Quant = 1
Client_id = 6, Client_Name = ISSU iPrefixes sync,  Reding_Quant = 1
Client_id = 8, Client_Name = ISSU IPC client,  Reding_Quant = 1
Client_id = 10, Client_Name = ISSU Port Manager client,  Reding_Quant = 1
Client_id = 11, Client_Name = ISSU Hwd Mode client,  Reding_Quant = 1
Client_id = 100, Client_Name = ISSU vlr client,  Reding_Quant = 1
Client_id = 101, Client_Name = ISSU Mac client,  Reding_Quant = 1
Client_id = 102, Client_Name = ISSU Boses Manager client,  Reding_Quant = 1
Client_id = 200, Client_Name = CEF Sush ISSU client,  Reding_Quant = 1
Client_id = 201, Client_Name = IGMPS ISSU client,  Reding_Quant = 1
Client_id = 202, Client_Name = IGMPS ISSU client,  Reding_Quant = 1
Client_id = 203, Client_Name = ARP NSL,  Reding_Quant = 1
Client_id = 204, Client_Name = IGMPS ESSU client,  Reding_Quant = 1
Client_id = 205, Client_Name = ESM Svc Delivery ISSU client,  Reding_Quant = 1
Client_id = 206, Client_Name = PIM ESM ISSU client,  Reding_Quant = 1
Client_id = 207, Client_Name = PIM MSDSA ISSU client,  Reding_Quant = 1
Client_id = 208, Client_Name = PIM ESM ISSU client,  Reding_Quant = 1
Client_id = 209, Client_Name = PIM MSDSA ISSU client,  Reding_Quant = 1
Client_id = 210, Client_Name = PIM MC ADMIN ISSU client,  Reding_Quant = 1
Client_id = 227, Client_Name = AdjacenCy ISSU client,  Reding_Quant = 1
Client_id = 228, Client_Name = PIM ESM ISSU client,  Reding_Quant = 1
```

```
Client_ID = 2054, Client_Name = IEEE process client, Entry_Count = 1
Client_ID = 2055, Client_Name = IEEE Test client, Entry_Count = 1
Client_ID = 2056, Client_Name = IEEE LED OM client, Entry_Count = 1
Client_ID = 2047, Client_Name = IEEE PM Client, Entry_Count = 1
Client_ID = 2048, Client_Name = IEEE Port Manager Client, Entry_Count = 1
Client_ID = 2049, Client_Name = IEEE Port Security client, Entry_Count = 1
Client_ID = 2071, Client_Name = IEEE Switch VLAN client, Entry_Count = 1
Client_ID = 2072, Client_Name = IEEE DTP client, Entry_Count = 1
Client_ID = 2073, Client_Name = IEEE CDL client, Entry_Count = 1
Client_ID = 2077, Client_Name = IEEE MFS MGR, Entry_Count = 1
Client_ID = 2078, Client_Name = IEEE SNMP, Entry_Count = 1
Client_ID = 2079, Client_Name = IEEE SPS MGR, Entry_Count = 1
Client_ID = 2080, Client_Name = IEEE Port Manager Client, Entry_Count = 1
Client_ID = 2081, Client_Name = IEEE Ifl Port client, Entry_Count = 1
Client_ID = 2083, Client_Name = IEEE Inline Power client, Entry_Count = 1
Client_ID = 2084, Client_Name = IEEE Port Manager Client, Entry_Count = 1
Client_ID = 4001, Client_Name = IEEE QM Channel client, Entry_Count = 1
Client_ID = 4002, Client_Name = IEEE QM Port client, Entry_Count = 1
Client_ID = 4003, Client_Name = IEEE QM Vlan Mapping client, Entry_Count = 1
Client_ID = 4004, Client_Name = IEEE QM Stackwise client, Entry_Count = 1
Client_ID = 4005, Client_Name = IEEE QM CallHomeSecondary client, Entry_Count = 1

Name Filters:
Client_Name = IEEE Proto client
Client_Name = IEEE NP
Client_Name = IEEE CP client
Client_Name = IEEE Proto_CP client
Client_Name = IEEE GSMTIL SNMC
Client_Name = IEEE ifIndex sync
Client_Name = IEEE Sensor
Client_Name = IEEE Sensor client
Client_Name = IEEE Red Mode Client
Client_Name = IEEE Test
Client_Name = IEEE ifm client
Client_Name = IEEE Smart Manager client
Client_Name = IEEE Test IEEE client
Client_Name = IEEE Test client
Client_Name = IEEE Ldc
Client_Name = IEEE Inc Polarity IEEE client
Client_Name = IEEE Pcor Polarity IEEE client
Client_Name = IEEE Pcor IEEE client
Client_Name = FIB IEEE client
Client_Name = FIB PM subblock IEEE client
Client_Name = IEEE Adjacency client
Client_Name = IEEE Adjacency IEEE client
Client_Name = FIB IPX IEEE client
Client_Name = IEEE Adjacency client
Client_Name = IEEE MM client
Client_Name = IEEE QM Channel client
Client_Name = IEEE QM Port client
Client_Name = IEEE QM Event client
Client_Name = IEEE QM Stackwise client
Client_Name = IEEE QM CallHomeSecondary client
```

Related Commands	Command	Description
	show ieee capability	Displays the IEEE capability for a client.
	show ieee entries	Displays the IEEE entry information.

show issu comp-matrix

To display information regarding the In Service Software Upgrade (ISSU) compatibility matrix, use the **show issu comp-matrix** command.

show issu comp-matrix {**negotiated** | **stored**} **unit** |

Syntax Description

negotiated	Displays negotiated compatibility matrix information.
stored	Displays stored compatibility matrix information.
unit	Displays negotiated compatibility matrix information in XML format.

Defaults

This command has no default settings.

Command Modes

User EXEC mode

Command History

Release	Modification
12.2(31)SGA	This command was introduced on the Catalyst 4500 series switch.

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 can be performed with the ISSU process. The compatibility matrix during the ISSU process and later by entering the **show issu comp-matrix** command. To display information on the negotiation of the compatibility matrix data between two software versions on a given system, use the **show issu 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 issu comp-matrix stored** command.

The compatibility matrix information are built-in any Cisco IOS ISSU image. The ISSU infrastructure performs a matrix lookup as soon as the communication 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 disruption.
- 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 an operation and service of the switchover be considered carefully.

- Incompatible—A set of core system infrastructure must be able to execute in a stateful manner for SSO redundancy switchover. 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". In this case, stateful redundancy switchover operation between these versions is not possible. The systems operate in RPR mode during the period when the versions of Cisco IOS or the active and standby supervisor engines differ.

Examples

This example displays negotiated compatibility matrix information:

```
Switch# show hw-module-compatible negotiated

CardType: WS-X6708-10G, Slot 2, Image Ver: 12.2(18)SXA
Image Name: rsv2600-ipbase-mz

Slot  Slot4  Slot5  pSlot  pSlot5  Compatibility
-----------------------------------------------------
1     1      12.2(18)  1      -       COMPATIBLE
2     1      12.2(18)  5      1       COMPATIBLE
3     1      12.2(18)  -      -       COMPATIBLE
4     1      12.2(18)  105    1       COMPATIBLE
5     1      12.2(18)  10     1       COMPATIBLE
6     1      12.2(18)  7      1       COMPATIBLE
8     1      12.2(18)  1      1       COMPATIBLE
9     1      12.2(18)  1      1       COMPATIBLE
10    1      12.2(18)  1      1       COMPATIBLE
11    1      12.2(18)  6      1       COMPATIBLE
100   1      12.2(18)  13     1       COMPATIBLE
200   1      12.2(18)  13     1       COMPATIBLE
300   1      12.2(18)  24     1       COMPATIBLE
400   1      -         -      -       UNCHECKED
1000  1      12.2(18)  2.0    1       UNCHECKED
1001  1      12.2(18)  1.0    1       COMPATIBLE
2000  1      12.2(18)  2.0    1       COMPATIBLE
2001  1      12.2(18)  1.0    1       COMPATIBLE
3000  1      12.2(18)  2.0    1       COMPATIBLE
3001  1      12.2(18)  1.0    1       COMPATIBLE
3002  1      12.2(18)  3.1    1       COMPATIBLE
3003  1      12.2(18)  4.1    1       COMPATIBLE
3004  1      12.2(18)  4.2    1       COMPATIBLE
1000  2      -         -      -       UNCHECKED
1001  2      -         -      -       UNCHECKED
2000  2      -         -      -       UNCHECKED
2001  2      -         -      -       UNCHECKED
3000  2      -         -      -       UNCHECKED
3001  2      -         -      -       UNCHECKED
3002  2      -         -      -       UNCHECKED
3003  2      -         -      -       UNCHECKED
3004  2      -         -      -       UNCHECKED
2000  1      12.2(18)  8      1       COMPATIBLE
2001  1      12.2(18)  2.0    1       COMPATIBLE
2002  1      12.2(18)  2.0    1       COMPATIBLE
2003  1      12.2(18)  2.0    1       COMPATIBLE
2004  1      1944.0    4.0    1       COMPATIBLE
2005  1      12.2(18)  2.1    1       COMPATIBLE
2006  1      12.2(18)  1.1    1       COMPATIBLE
2007  1      12.2(18)  2.0    1       COMPATIBLE
2008  1      12.2(18)  2.0    1       COMPATIBLE
2009  1      1944.0    3.0    1       COMPATIBLE
2010  1      1944.0    3.1    1       COMPATIBLE
2011  1      12.2(18)  1.0    1       COMPATIBLE
2012  1      12.2(18)  2.0    1       COMPATIBLE
2013  1      12.2(18)  1.0    1       COMPATIBLE
4001  1      12.2(18)  1.7    1       COMPATIBLE
4002  1      12.2(18)  1.8    1       COMPATIBLE
```

show lacp neighbor

```
4005   5G   24224:80  19     1        CONDUCTABLE
4006   5G   24224:80  20     1        CONDUCTABLE
4007   5G   24224:80   6     1        CONDUCTABLE

Message group summary:
Port   Port   LagId    Port    Port    Port    Nbrs Pseudo
=======================================================================
1      1      1        24224:0   1     1       1
2      1      1        24224:0   2     1       1
4      1      1        24224:0   9     1       1
5      1      1        24224:0  25     1       1
7      1      1        24224:0  16     1       1
8      1      1        24224:0   1     1       1
9      1      1        24224:0   3     1       1
10     1      1        24224:0   2     1       1
11     1      1        24224:0   4     1       1
110    1      1        24224:0  13     1       1
110    113    135      24224:0  14     1       1
111    1      1        24224:0  24     1       1
2000   1      1                 -     -       -       0  Port not negotiate
2001   1      1        24224:0  23     1       1
2002   1      1        24224:0  15     1       1
2006   1      1        24224:0  26     1       1
2008   1      1        24224:0  27     1       1
2010   1      1        24224:0  32     1       1
2012   1      1        24224:0  31     1       1
2014   1      1        24224:0  30     1       1
2020   1      1        24224:0  42     1       1
2021   1      1                 -     -       -       0  Port not negotiate
2022   1      1                 -     -       -       0  Port not negotiate
2024   1      1                 -     -       -       0  Port not negotiate
2026   1      1                 -     -       -       0  Port not negotiate
2028   1      1                 -     -       -       0  Port not negotiate
2030   1      1                 -     -       -       0  Port not negotiate
2054   1      1        24224:0   8     1       1
2055   1      1        24224:0  11     1       1
2056   1      1        24224:0  28     1       1
2067   1      1        24224:0  12     1       1
2068   1      1        24224:0  40     1       1
2070   1      1        24224:0  21     1       1
2071   1      1        24224:0  20     1       1
2072   1      1        24224:0  18     1       1
2073   1      1        24224:0  33     1       1
2074   1      1        24224:0  34     1       1
2076   1      1        24224:0  44     1       1
2078   1      1        24224:0  36     1       1
2079   1      1        24224:0  35     1       1
2080   1      1        24224:0  39     1       1
2081   1      1        24224:0  38     1       1
4000   10G    1        24224:0  37     1       1
4001   10G    1        24224:0   1     1       1
4002   10G    1        24224:0   1     1       1
4003   10G    1        24224:0  19     1       1
4004   40G    1        24224:0  22     1       1
4005   1      1        24224:0   4     1       1

List of Clients:
Client Name                     Resend/Non-Resend
=======================================================================
2    DOSD Proto-client          Resend
3    LACP                       Resend
4    DOSD PF-client             Resend
5    DOSD Network PF-client     Resend
6    DOSD CONFIG-DOSD           Resend
```

```
8      DEC LPDaemon myer          Same
9      DEC SNMP myer              Same
10     DEC DR factory client      Same
11     DEC Sad Node Client        Same
12     DEC Mirror client          Same
130    DEC LSA client             Same
200    DEC Boot Manager client    Same
201    DEC MOP client             Same
202    DEC LAT client             Same
204    DEC DNS client             Same
2008   DEC Testcoll client        Same
2010   ARP NL                     Same
2011   DEC Ethernet Client        Same
2021   ARP Int Priority DEC client
2022   ARP Port Priority DEC client
2023   PIB LSA DEC client         Same
2024   PIB LSR DEC client         Same
2025   PIB NW subblock DEC client
2026   PIB Port subblock DEC client
2027   ARP priority DEC client    Same
2028   PIB IPX DEC client         Same
2029   DEC Ethernet Client        Same
2056   DEC DSRP NNL               Same
2058   DEC DSRP DNL client        Same
2067   DEC PM client              Same
2068   DEC PAGP_NETCON Client     Not-Same
2069   DEC Port Agg client        Not-Same
2071   DEC Switch Vlan client     Not-Same
2072   DEC Ser-Vlan               Not-Same
2073   DEC Ser-Port               Not-Same
2074   DEC STP MST                Not-Same
2079   DEC PTP DEC                Not-Same
2080   DEC PTP client             Not-Same
2081   DEC SNMP Managing client   Not-Same
2082   DEC IP Host client         Not-Same
2083   DEC Ethernet Frame client  Not-Same
2084   DEC Ethernet Frame client  Not-Same
4001   DEC VAC Channel client     Same
4002   DEC VAC Port client        Same
4003   DEC VAC Xbrcm client       Same
4004   DEC VAC Xbrcm client       Same
4005   DEC VAC LatCollectServ     Same
```

This example displays stored compatibility matrix information:

```
Switch# show hw-module-slot-compatible-matrix

Number of Entries = 2

        (1) Matrix for ver(DEC-NETSERVICES-M-012) - ver(DEC-NETSERVICES-M-012)
        ==========================================================================
        Start Flag (0x00LEA2AB)

                  Hw Image Ver:   12.2-(1)(6)A
                  Sw Image Ver:   Compatibility
                  Sw Version
                  12.2-(1)(6)A    Comp(3)
```

show ieee-lldp events

Related Commands	Command	Description
	show ieee-lldp events	Displays the IEEE LLDP events.
	show ieee-lldp neighbors	Displays IEEE neighbor 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

Command History

Release	Modification
12.2(31)SG1A	This command was introduced on the Catalyst 4500 series switch.

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 session and to perform session negotiation for ISSU clients.

Examples The following example shows how to display the ISSU endpoints:

```
Switch# show issu endpoints
Eg_Unique_ID = 1(Local), 2(Peer_Source = 4)

This endpoint communication with 1 peer endpoints :
  Peer_Unique_ID      CLP     VSN   LOCAL   REG      Compatibility
       2(Peer)         1       1       1     1            Same

Shared Negotiation Session Info :
  Session_Id = 0x00000000
  Nego_Function_Mask = shared nego session
  Transport_Mtu = 4096
  Nego_Op_Mem = 0
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

Command History	**Release**	**Modification**
	12.2(31)SGA	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

Entity is a logical group of sessions with some 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 2172
Client_id = 2172 :
Client_name = ISSU , Entity_Name = ISSU device entity ;
   HwPlan HwApply SwPlan SwApply CapEntry
   Count  Count   Count  Count   Count
     28     5      5      5       5

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

Command History

Release	Modification
12.2(18)SXA	This command was introduced on the Catalyst 6500 series switch.

Examples

The following example displays and verifies the ISSU state after LOA DIVERSION:

```
Switch#> show issu fsm 24
Session_id = 24
FSM_ID          Sess_State      CCB_State       Error_Reason
FSM_C1          IDLE(0)         A_CCB           none
FSM_C2_SHLLO    ESTP            ESTD            none
FSM_C2_A_CLAP   A_ESTP          A_ESTP          none
FSM_C2_A_CCBS   A_ESTP          A_ESTP          none
FSM_C2_A_CRM    A_ESTP          A_SND_ESTP      none
FSM_C2_A_VRM    P_ESTP          unknown         none
FSM_C2_A_CCBR   A_ESTP          A_ESTP          none
Current FSM is SNA_C2_SNDSND
Session is complete
Negotiation started at 00:01:07.688, duration is 0.148 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 type information for all clients registered to the ISSU infrastructure.

Command Modes User EXEC mode

Command History	**Release**	**Modification**
	12.2(31)SGA	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines Messages are type-data (plus known as checksum 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 messages for Client_id 2002:

```
Switch>show issu message groups 2002
Client_Id = 2002, Entry_Ptr = 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, Entry_Ptr = 1
  Message_Type = 1,  Version_Range = 1 - 2
                Message_Dir = 0,   Message_Len = 12
                Message_Ver = 1,   Message_Len = 0
  Message_Type = 2,  Version_Range = 1 - 2
                Message_Dir = 0,   Message_Len = 12
                Message_Ver = 2,   Message_Len = 0

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

Command History	**Release**	**Modification**
	12.2(50)SG	This command was introduced on the Catalyst 4500 series switch.

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 cap value assigned

Switch#show issu negotiated version 24
Session_ID = 24 :
    Message_Type = 1,  Negotiated_Version = 1,  Message_MTU = 44
    Message_Type = 2,  Negotiated_Version = 1,  Message_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

Command History	Release	Modification
	12.2(31)SG-A	This command was introduced on the Catalyst 4500 series switch.

Examples The following example shows how to display the rollback-timer status:

```
Switch#show issu rollback-timer
        Rollback Process State = Rbk 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 commitversion	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 info mation for all clients registered to the ISSU infrastructure.

Command Modes User EXEC mode

Command History	Release	Modification
	12.2(31)SGA	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines Session is bidirectional and a reliable connection is established between two endpoints. Syn- ckn and negotiation messages are sent to the peer endpoint through a session. On a Catalyst 4500 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 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 rollback-timer status:

```
Switch#show issu sessions 2672
Client_ID = 2672, Entity_ID = 1

*** Session_ID = 26, Session_Name = delta :

Peer  Peer  Negotiated Negotiated  Cap   Msg   Session
Unique ID  Role  Peer   Version  GroupID Group ID Flags
2     26   PRIMARY    COMPATIBLE  3     1     0
                      no policy)

Negotiation Session Info for This Message Session:
    Msg_Session_ID = 26
    Msg_Session_Name = delta
    Transport_Flow = 17004
Switch#
```

Related Commands	Command	Description
	show issu clients	Displays the ISSU clients.

show issu state

To display the ISSU state and current boot 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 if ISSU is active.
	detail (Optional) Provides detailed information about the state of the active and standby supervisor engines.
Defaults	The command displays the ISSU state and current boot image name of both the active and standby supervisor engines.
Command Modes	Privileged EXEC mode

Command History	Release	Modification
	12.2(18)SXA	This command was introduced on the Catalyst 6500 series switch.

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 transition 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 LOAD INVERSION:

```
Switch# show issu state detail
                        Slot = 5
                   RG State = Active
                   Sub State = Load Version
              Boot Variable = boot flash:c6k_image.12
           Operating Mode = Stateful Switchover
         Primary Version = boot flash:c6k_image
       Secondary Version = boot flash:new_image
          Current Version = boot flash:new_image

                        Slot = 9
                   RG State = Standby
                   ISSU State = Load Version
              Boot Variable = boot flash:new_image,12;boot flash:c6k_image,12
         Primary Version = boot flash:c6k_image
       Secondary Version = boot flash:new_image
          Current Version = boot flash: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 summary information.
begin	(Optional) Displays information beginning with the line that matches the *expression*.
exclude	(Optional) Displays information that excludes 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

Command History

Release	Modification
12.2(18)SXF	This command was first introduced on the Catalyst 6500 series switch.
12.2(33)SXH	Added support for the 10-Gigabit Ethernet interface.

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 tfpm-rt-if-tunnel** command:

```
Switch> show tfpm-rt-if-tunnel
OOS for Responsiveness Factor: 5

Port      Protocol  Shortfall  Drop      Responsiveness Dropsqualified Drop
                    Threshold  Threshold Counter        Counter       Counter
========  ========  =========  ========  ============   ============  ======
Fa0/12    udp       ****       ****      ****           ****          ****
          vtp       ****       ****      5847           1486          0
          vtp       ****       ****      72             12            0
          pagp      ****       ****      899            582           0
          pagp      ****       ****      1              1             0
          udld      ****       ****      229            211           0
Fa0/12    udp       1100       ****      2354           2350          0
          vtp       1100       ****      12768          12            0
          vtp       1100       ****      1              17            0
          pagp      ****       ****      902 854        5848          0
          pagp      ****       ****      905 0          0             0
          udld      ****       ****      229            0             0
Fa0/12    udp       ****       ****      2354           0             0
          vtp       ****       ****      12767          0             0
          vtp       ****       ****      81             0             0
          pagp      ****       ****      0              0             0
          pagp      ****       ****      848            0             0
          udld      ****       ****      0              0             0
Fa0/13    udp       ****       ****      2354           0             0
          vtp       ****       ****      12768          0             0
          vtp       ****       ****      81             0             0
          pagp      ****       ****      0              0             0
          pagp      ****       ****      848            0             0
          udld      ****       ****      0              0             0
Switch>
```

This is an example of output from the **show tfpm-rt-if-tunnel summary** command:

```
Switch> show tfpm-rt-if-tunnel summary
OOS for Responsiveness Factor: 5

Port      Protocol  Shortfall  Shortfall  Drop      Drop      Status
                    Threshold  Threshold  Threshold Threshold
                    (udp/sctp/tcp)        (udp/sctp/tcp)
                    (pagp/Lacp/udld)      (pagp/Lacp/udld)
========  ========  ==========================================
Fa0/10    udp/sctp/tcp ****/****/****     ****/****/****    up
          pagp/Lacp/udld ****/****/****   ****/****/****
Fa0/11    udp/sctp/tcp ****/****/****     ****/****/****    up
          pagp/Lacp/udld ****/****/****   ****/****/****
Fa0/12    udp/sctp/tcp ****/****/****     ****/****/****    up
          pagp/Lacp/udld ****/****/****   ****/****/****
Fa0/13    udp/sctp/tcp ****/****/****     ****/****/****    up
          pagp/Lacp/udld ****/****/****   ****/****/****
Fa0/14    udp/sctp/tcp ****/****/****     ****/****/****    down
          pagp/Lacp/udld ****/****/****   ****/****/****
Fa0/15    udp/sctp/tcp ****/****/****     ****/****/****    down
          pagp/Lacp/udld ****/****/****   ****/****/****
Fa0/16    udp/sctp/tcp ****/****/****     ****/****/****    down
          pagp/Lacp/udld ****/****/****   ****/****/****
Fa0/17    udp/sctp/tcp ****/****/****     ****/****/****    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

Command History	Release	Modification
	12.2(11)EW	Support for this command was introduced on the Catalyst 4500 series switches.

Usage Guidelines This command is not supported on systems that are configured with a Supervisor Engine I.

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    LACPDUs
Port        Sent   Recv   Sent   Recv  Errors Pkts Err
---------------------------------------------------------
Channel group: 1
  Fa1/1     15     15     0      0     0      0
  Fa1/2     16     16     0      0     0      0
  Fa1/3     14     16     0      0     0      0
  Fa1/4     15     16     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   Port Id   Interval   Priority  Key     Key     Number  State
Fa6/1   saf     bndl    31e       32768      255       100     100     0x41    0x76
Fa6/2   saf     bndl    31e       32768      255       100     100     0x42    0x76
Fa6/3   saf     bndl    31e       32768      255       100     100     0x43    0x76
Fa6/4   saf     bndl    31e       32768      255       100     100     0x44    0x76
Switch#
```

Table 2-24 lists the output field definitions.

Table 2-24 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 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	Operative 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]: • **bit0**: *LACP_Activity* • **bit1**: *LACP_Timeout* • **bit2**: *Aggregation* • **bit3**: *Synchronization* • **bit4**: *Collecting* • **bit5**: *Distributing* • **bit6**: *Defaulted* • **bit7**: *Expired*

This example shows how to display LACP neighbors information for a specific port channel:

```
Switch#show lacp 1 neighbors
Flags:  S - Device sends PDUs at slow rate. F - Device sends PDUs at fast rate.
        A - Device is in active mode.       P - Device is in passive mode.

Channel group 1 neighbors

                                    Partner
Port      System ID                 Port Number     Age    Flags
Fa4/1     8000,0060.c3ac.d84a       0x0001          29s    P
Fa4/2     8000,0060.c3ac.d84a       0x0002          0s     P
Fa4/3     8000,0060.c3ac.d84a       0x0003          2s     P
Fa4/4     8000,0060.c3ac.d84a       0x0004          0s     P

          Port      Admin     Oper      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 bracks.

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 mab

To display MAC authentication bypass (MAB) information, use the **show mab** command in EXEC mode.

show mab [**interface** *interface interface-number* | **all**] [**detail**]

Syntax Description

interface *interface*	Interface type; possible valid values are **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

Command History

Release	Modification
12.2(33)SXI	This command was introduced.

Usage Guidelines Table 2-35 lists the fields in the **show mab** command.

Table 2-35 *show mab 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 2-36 lists the possible values for the state of the MAB state machine.

Table 2-36 *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.

Table 2-26 *MAB State Machine Values (continued)*

Authorizing	Intermediate	The state of the session during MAC-based authentication.
Terminate	Terminal	The state of the session once a result has been reached. The session is in a terminal state. "TERMINATE" displays.

Table 2-27 lists the possible displayed values for the MAB authentication status.

Table 2-27 *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 GigabitEthernet1/1
-----------------------------------------
Mac-auth-Bypass: Enabled
Inactivity Timeout: None
Switch#
```

The following example shows how to display detailed MAB information:

```
Switch# show mab all detail
MAB details for GigabitEthernet1/1
-----------------------------------------
Mac-auth-Bypass: Enabled
Inactivity Timeout: None
MAB Client List
---------------
Client MAC - 0000.2222.4401
Client Mac Address - 00000222401
Auth Status: AUTHORIZED
```

The following example shows how to display MAB information for a specific interface:

```
Switch# show mab interface gigabitethernet1/1
MAB details for GigabitEthernet1/1
-----------------------------------------
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 gigabitethernet1/1 detail
MAB details for Gigabitethernet1/1
--------------------------------------
Mac Auth-Bypass = Enabled
Inactivity Timeout = None
MAB Client List
---------------
Client MAC = 0000.2104.a420
MAB IM state = THROUGHPUT
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**, **po**, **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

Command History

Release	Modification
12.2(25)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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 4/1:

```
Switch# show mac access-group interface fast 4/1
Interface fast4/1mac4/1:1:
    Inbound access-list is ip-simple-mac-acl
    Outbound access-list is mac acc
```

Related Commands

Command	Description
access-group mode	Specifies the override modes (for example, VACL-overridePACL) 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 more information.
vlan *vlan_id*	(Optional) Displays entries for the specific VLAN; valid values are from 1 to 4094.

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.
12.1(13)EW	Added support for extended VLAN addresses.
12.2(20)EW	Added support for the 10 Gigabit Ethernet interface.

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.

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 0030.94c4.a809
Destinat Source
 vlan  mac address     type        protocols          port
-------+---------------+--------+---------------------+--------
   1    0030.94c.b809  static ip,ipx,assigned,other  Swlo0b
Fa4/1   0030.94c.b809  static ip,ipx,assigned,other  Swlo0b
Fa5/2   0030.94c.b809  static ip,ipx,assigned,other  Swlo0b
Swlo0b
```

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

Command History	Release	Modification
	12.1(3a)EW	Support for this command was introduced on the Catalyst 6500 series switch.
	12.1(11b)EW	Support for extended addressing was added.

Examples This example shows how to display the currently configured aging time for all VLANs:

```
Router# show mac-address-table aging-time
Vlan   Aging Time
----   ----------
100    300
200    1000
Router#
```

This example shows how to display the currently configured aging time for a specific VLAN:

```
Router# show mac-address-table aging-time vlan 100
Vlan   Aging Time
----   ----------
100    300
Router#
```

Related Commands

Command	Description
show 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.

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 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

Command History

Release	Modification
12.1(8)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.1(12c)EW	Added support for extended VLAN addresses.

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: 1
Dynamic Unicast Address (System-defined) Count: 1
Unicast Mac Address Table Size:         8192
Total Unicast MAC Addresses In Use:     131068
Multicast MAC Address Count:            0
Total Multicast MAC Addresses Available: 131068
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.

Command	Description
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

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 6500 series switch.
12.1(12c)EW	Added support for extended VLAN addresses.
12.2(52)SG	Added support for the 10 Gigabit Ethernet interface.

Usage Guidelines

The keyword definitions for the *protocol* argument are as follows:

- **assigned** specifies assigned protocol entries.
- **ip** specifies IP protocol.
- **ipx** specifies IPX protocol.
- **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, *Po86*).

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 all the dynamic MAC address entries:

```
Switch#show mac-address-table dynamic
Destinat Source
 Vlan    Mac Address       Type        Protocols          Port
-------+----------------+--------+-----------+--------------------------------
   1    0002.0000.0001    dynamic*    ip        Fast-Ethernet4/15
   1    0002.0000.0002    dynamic*    ip        Fast-Ethernet4/15
   1    0002.0000.0003    dynamic*    ip,ipx,vines Fast-Ethernet4/15
   1    0002.0000.0004    dynamic*    ip,ipx,vines Fast-Ethernet4/15
   2    0002.0000.0101    dynamic*    ip,ipx,vines Fast-Ethernet4/14
   2    0002.0000.0102    dynamic*    ip        Fast-Ethernet4/14
   2    0002.0000.0103    dynamic*    ip        Fast-Ethernet4/14
   2    0002.0000.0104    dynamic*    ip,ipx,vines Fast-Ethernet4/14
   2    0002.0000.0105    dynamic*    ip,ipx,vines Fast-Ethernet4/14
   2    0002.0000.0106    dynamic*    ip,ipx,vines Fast-Ethernet4/14
Switch#
```

This example shows how to display the dynamic MAC address entries with a specific protocol type (in this case, assigned):

```
Switch#show mac-address-table dynamic protocol assigned
Destinat Source
 Vlan    Mac Address       Type        Protocols          Port
-------+----------------+--------+-----------+--------------------------------
   1    0002.0000.0003    dynamic*    ip,ipx,vines Fast-Ethernet4/15
   1    0002.0000.0004    dynamic*    ip,ipx,vines Fast-Ethernet4/15
   2    0002.0000.0101    dynamic*    ip,ipx,vines Fast-Ethernet4/14
   2    0002.0000.0104    dynamic*    ip,ipx,vines Fast-Ethernet4/14
   2    0002.0000.0105    dynamic*    ip,ipx,vines Fast-Ethernet4/14
   2    0002.0000.0106    dynamic*    ip,ipx,vines Fast-Ethernet4/14
Switch#
```

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

Command History	**Release**	**Modification**
	12.1(8)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.2(25)EW	Added support for the 10 Gigabit Ethernet interface.

Usage Guidelines For the MAC address table entries that are seed by the control-port, the control-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 fastethernet4/16
Dynamic Entries
 vlan   mac address     type        protocols       port
-------+---------------+--------+---------+--------------------
   2    0000.0000.0101 dynamic  ip,ipx      FastEthernet4/16
   2    0000.0000.0102 dynamic  ip,ipx      FastEthernet4/16
   2    0000.0000.0103 dynamic  ip,ipx      FastEthernet4/16
   2    0000.0000.0104 dynamic  ip,ipx      FastEthernet4/16
   2    0000.0000.0105 dynamic  ip,ipx      FastEthernet4/16
   2    0000.0000.0106 dynamic  ip,ipx      FastEthernet4/16

Multicast Entries
 vlan   mac address     type        ports
-------+---------------+--------+---------+--------------------
   2    0100.0100.0100 system  Fa4/16
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 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 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-entered static address.
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

Command History

Release	Modification
12.1(3a)EW	Support for this command was introduced on the Catalyst 6500 series switch.
12.1(12c)EW	Added support for extended VLAN addresses.

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:

```
Switch# show mac-address-table multicast vlan 1
Multicast Entries
vlan   mac address     type    ports
------+----------------+--------+-----------------------------------
  1    0100.0cdd.dddd  system  GigabitEth.6/46,Fa6/15
Switch#
```

This example shows how to display the number of multicast MAC entries for all VLANs:

```
Switch# show mac-address-table multicast count
MAC Entries for all vlans:
Multicast MAC Addresses (Count):                    141
Total Non-CPU MAC Addresses Installed:              14184
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 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**] | [**trans-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 threshold notification status.
	trans-fail (Optional) Displays general information of hardware MAC learning failure notifications.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Command History	**Release**	**Modification**
	12.2(18)ZG	Support for this command was introduced on the Catalyst 4500 series switch.
	12.2(52)SG	Support for **trans-fail** keyword, Supervisor Engine 6-E, and Catalyst 4500M chassis added.

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 this switch
Interval between Notifications is 1 seconds
Number of MAC Addresses Added 5
Number of MAC Addresses Removed 1
Number of MAC Address Entries Flushed 3
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 476171, Dequeued Timestamp 476173
MAC Changed Messages :
Operation: Added Vlan: 1  MAC addr: 1234.5678.5a40 DstIntfAddr: 525
History Index 2, Entry Timestamp 481854, Dequeued Timestamp 481854
MAC Changed Messages :
Operation: Added Vlan: 1  MAC addr: 1234.5678.5a41 DstIntfAddr: 525
Operation: Added Vlan: 1  MAC addr: 1234.5678.5a42 DstIntfAddr: 525
Operation: Added Vlan: 1  MAC addr: 1234.5678.5a43 DstIntfAddr: 525
Operation: Added Vlan: 1  MAC addr: 1234.5678.5a44 DstIntfAddr: 525
History Index 3, Entry Timestamp 484534, Dequeued Timestamp 484534
MAC Changed Messages :
Operation: Added Vlan: 1  MAC addr: 1234.5678.5a45 DstIntfAddr: 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        Enabled        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 notification traps or informs.
	snmp trap mac-notification change	Enables SNMP MAC address notifications.

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

Command History	**Release**	**Modification**
	12.1(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines For the MAC address table entries that are used by the router-port, the router-port name is displayed in the "vlan" column not 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  qos         ports
------+----------------+--------+---------+-----+----------------------------------
  200  0030.94fb.6bb2 static  assigned  --  Gw1/0/5
  200  0030.94fb.6bb3 static  assigned  --  Gw1/0/5
  200  0030.94fb.6bb4 static  assigned  --  Gw1/0/5
 1000  0000.0000.0000 static  assigned  --  Drop
    1  0030.94fb.6bb0 static  assigned  --  Gw1/0/5
    1  0030.94fb.6bb1 static  assigned  --  Gw1/0/5
    4  0030.94fb.6bb2 static  assigned  --  Gw1/0/5
 4094  0100.0ccc.cccc static  assigned  --  CPU
 4092  0100.0ccc.ccd0 dynamic assigned  --  Po1/0
    1  0010.7b3b.0978 dynamic assigned  --  Po1/0
Switch#
```

This example shows the other output for the previous example:

```
Switch#show mac-address-table protocol ipx
Unicast Entries
 vlan  mac address     type        protocols          port
-------+---------------+--------+---------------------+--------------------
   1    0002.0000.0001  dynamic*  other               Fast0/6,Gi4/1/1
   1    0002.0000.0002  dynamic*  other               Fast0/6,Gi4/1/1
   1    0002.0000.0003  dynamic*  other               Fast0/6,Gi4/1/1
   1    0002.0000.0004  dynamic*  other               Fast0/6,Gi4/1/1
   1    0002.0000.0005  dynamic*  other               Fast0/6,Gi4/1/1
   2    0002.0000.0006  dynamic*  ip,ipx,assigned,other Fast0/6
   2    0002.0000.0007  dynamic*  other               Fast0/6,Gi4/1/1
   2    0002.0000.0008  dynamic*  other               Fast0/6,Gi4/1/1
   2    0002.0000.0009  dynamic*  other               Fast0/6,Gi4/1/1
   2    0002.0000.000a  dynamic*  other               Fast0/6,Gi4/1/1
   2    0002.0000.000b  static    ip,ipx,assigned,other Gi4/1/1
Fa0/1   0001.96ff.0d00  static    ip,ipx,assigned,other Swlo0
Multicast Entries
 vlan  mac address     type        protocols
-------+---------------+--------+---------------------+--------------------
   1    ffff.ffff.ffff  system    Swlo0,Fa0/16
   2    ffff.ffff.ffff  system    Fa0/16
1002    ffff.ffff.ffff  system
1003    ffff.ffff.ffff  system
1004    ffff.ffff.ffff  system
1005    ffff.ffff.ffff  system
Fa0/1   ffff.ffff.ffff  system    Swlo0,Fa0/1
Fa0/2   ffff.ffff.ffff  system    Swlo0,Fa0/2
Total Mac Addresses: 1
```

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 **tenGigabitethernet**.
	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

Command History

Release	Modification
12.1(11)EW	Support for this command was introduced on the Catalyst 6500 series switch.
12.1(12c)EW	Added support for extended VLAN addresses.
12.2(52)SE	Added support for the 10 Gigabit Ethernet interface.

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.

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 protocol.
- **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
Destinat Source
 Vlan  mac address     type    protocols                  port
-------+----------------+-------+---------------------------------------
   1    0030.94fc.0800  static  ip,ipx,assigned,other  Swlo0
   1    0030.94fc.0801  static  ip,ipx,assigned,other  Swlo0
Fa5/2   0030.94fc.0804  static  ip,ipx,assigned,other  Swlo0

Multicast Entries
 Vlan  mac address     type    ports
-------+----------------+-------+---------------------------------------
   2    0101.0101.0101  system  Swlo0,Fa5/15
   2    0101.0101.0102  system  Fa5/15
1002    ffff.ffff.ffff  system
1003    ffff.ffff.ffff  system
1004    ffff.ffff.ffff  system
1005    ffff.ffff.ffff  system
Fa5/1   0101.0101.0101  system  Swlo0,Fa5/1
Fa5/2   0101.0101.0102  system  Swlo0,Fa5/2

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
Destinat Source
 Vlan  mac address     type    protocols                  port
-------+----------------+-------+---------------------------------------
   1    0030.94fc.0800  static  ip,ipx,assigned,other  Swlo0
   1    0030.94fc.0801  static  ip,ipx,assigned,other  Swlo0
Fa5/2   0030.94fc.0804  static  ip,ipx,assigned,other  Swlo0

Multicast Entries
 Vlan  mac address     type    ports
-------+----------------+-------+---------------------------------------
   2    0101.0101.0101  system  Swlo0,Fa5/15
   2    0101.0101.0102  system  Fa5/15
1002    ffff.ffff.ffff  system
1003    ffff.ffff.ffff  system
1004    ffff.ffff.ffff  system
1005    ffff.ffff.ffff  system
Fa5/1   0101.0101.0101  system  Swlo0,Fa5/1
Fa5/2   0101.0101.0102  system  Swlo0,Fa5/2

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.

Command	Description
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

Command History	**Release**	**Modification**
	12.1(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW	Support for extended addressing was added.

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 protocols.
- **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    0000.0000.0141  dynamic  ip      Fast Ethernet 6/15
   1    0000.0000.0142  dynamic  ip      Fast Ethernet 6/15
   1    0000.0000.0240  dynamic  ortho   Fast Ethernet 6/15
   1    0010.7b7c.b400  static   ipx,appletlk,other  Fast Ethernet 6/15
   1    0010.7b7c.b400  static   ip,ipx,appletlk,other  fastcdp
Multicast Entries
 vlan  mac address     type        ports
-------+---------------+--------+---------+-------+----------------------------
   1    ffff.ffff.ffff  system   fastcdp,Fa6/15
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    0000.0000.0240  dynamic  ortho   Fast Ethernet 6/15
   1    0010.7b7c.b400  static   ipx,appletlk,other  Fast Ethernet 6/15
   1    0010.7b7c.b400  static   ip,ipx,appletlk,other  fastcdp
Multicast Entries
 vlan  mac address     type        ports
-------+---------------+--------+---------+-------+----------------------------
   1    ffff.ffff.ffff  system   fastcdp,Fa6/15
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 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 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

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.2(25)EW	Enhanced the output of the **show tdpneighbor command** to include the 10-Gigabit Ethernet interface.

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 consumed by the module is more than 50 W, above the administratively allocated PoE, the "Status" displays as "PwrOver." If the PoE consumed 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 "Pwr(deny)".

```
Cat6506 show module all
Mod Ports Card Type                              Model              Serial No.
--- ----- -------------------------------------  ------------------ -----------
  1     2  10GBaseX (X2G2) Supervisor(active)    WS-X6704           JAE07041P4J8
  2     8  1000BaseX (X2G2)                      WS-X6708           SAD0631
  3    16  1000BaseX (X2G2)                      WS-X6416           JAE0351A6HB
  4    48  10/100/1000BaseT(RJ45) for module     WS-X6148-FX-MT     SAD0631
  5    48  10/100BaseTX (RJ45)                   WS-X6148           JAE0351A2DP

M MAC addresses                  Hw  Fw  Sw              Status
--- ---------------------------------------------------------------------------
1 00bc.8d1ac.f940 to 00bc.8d1ac.f943 0.5 12.1(12abc)EW 12.2(20SXD3)13-06  Ok
2 0005.5d4a.a930 to 0005.5d4a.a937  1.0  8.4(0.0)    8.5(0.0)RP1         Ok
3 0005.5d4a.a940 to 0005.5d4a.a95f  1.0  8.4(0.0)    8.5(0.0)RP1         Ok
4 0005.5d4a.a970 to 0005.5d4a.a97f  2.0  8.4(0.0)    8.5(0.0)RP1         Ok

5 0030.9231.2f80 to 0030.9231.2f87  1.0                                  On
Cat6506>
```

This example shows how to display information for a specific module:

```
Cat6506 show module 5
Mod Ports Card Type                              Model              Serial No.
--- ----- -------------------------------------  ------------------ -----------
  5     2  Catalyst 4000 supervisor I (active)   WS-X4014           JAB0440Y2QD

Mod MAC addresses                Hw  Fw  Sw              Status
--- ---------------------------------------------------------------------------
5 0001.4a41.9bc0 to 0001.4a41.9bc1  1.1  5.4(3)    6.2(0.97)         On
Mod Sub-Module                   Model              Serial No.  Hw     Status
--- ------------------------------ ------------------ ----------- ------ ------
2 Policy Feature Card 3          WS-F6K-PFC3        SAD0440E0YU 1.1    On
2 Cards MSFC 3 daughtercard      WS-F6K-MSFC3       SAD0441QP8K 1.1    On
Cat6506>
```

This example shows how to display information for all the modules on the switch:

```
Cat6506 show module
Chassis Type : WS-C6506

Power consumed by backplane : 0 Watts

Mod Ports Card Type                              Model              Serial No.
--- ----- -------------------------------------  ------------------ -----------
  1     2  8G (X2), 1GEBaseX (GBIC) Supervisor   WS-X6K-S2U-MSFC2   SAD0810YJ1J
  2     8  1000BaseX (GBIC)                      WS-X6408A          SAD0810111V

M MAC addresses                  Hw  Fw  Sw              Status
--- ---------------------------------------------------------------------------
1 0004.4844.7700 to 0004.4844.7709 0.3  6.3(19b)8(0.2)  12.2(20SXD3)13-06  Ok
2 0010.7bab.8620 to 0010.7bab.8629 0.2                                  Ok
Cat6506>
```

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 from1 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

Command History	**Release**	**Modification**
	12.1(20)EW	Support for this command was introduced on the Catalyst 6500 series switch.
	12.1(11)EW	Added support for defining destination within a single user session.
	12.1(13)EW	Output enhanced to display configuration status of SPAN enhancements.
	12.2(18)EW	Added support to display configuration state for remote SPAN and learning.
	12.2(25)EW	Added support to display ACLs that are applied to SPAN session.

Examples

This example shows how to display whether ACLs are applied to a given SPAN session on a Catalyst 6500 series switch:

```
Switch# show monitor

Session 1
---------
Type              : local Session
Source Ports      :
    Both          : Fa6/2
Destination Ports : Fa6/10
    Encapsulation : Native
          Ingress : Disabled
    Learning      : Disabled
Filter VLANs      : 1-2
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:        Fa(1/1-3)
    TX Only:        Fa(1/1-3)
Dest Ports:        Gi(4/1)
    Encapsulation: Replicate
    Ingressing: Disabled
    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          : gi(1/1), CPU
Source VLANs:
    RX Only       : None
    TX Only       : None
    Both          : None
Source RSPAN VLAN : None
Destination Ports : Fa(1/1)
    Encapsulation : dot1q
    Ingressing    : Dot1q(x), dot1q(1 VLAN + 2
Filter VLANs      : All
    Filter Types Rx : Good
    Filter Types Tx : None
Dest Rspan Vlan : 901
Ingressing packets: disabled VLAN0
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
Filter VLANs: None
Switch#
Switch#
```

Related Commands:	Command	Description
	monitor session	Enables the SPAN sessions on interfaces or VLANs.

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 connections.
	subscription detail | **summary** — Displays the subscription information on 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

Command History	**Release**	**Modification**
	12.2(52)SG	Support for this command was introduced on the Catalyst 4500 series switch.

Examples

This is an example of output from the **show nmsp attachment suppress interface** command:

```
Switch#sh show nmsp attachment suppress interface
NMSP Attachment Suppression Interfaces

Gi1/46(10.56.0.56)vlan(1/2)
Gi1/48(10.56.0.56)vlan(1/2)
Switch#sh
```

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

```
Switch# show snmp capability
SNMP Switch Capability

 Description                    Submenuine
 ------------------------------ ----------
 Entmib                         Entmib
 Entsensormib                   Entsensor
 Ciscomemorypoolmib             Ciscomemorypool
 Interface                      Interface
 Ciscoflashmib                  Ciscoflash
 Ciscoipprotocolmib             Ciscoipprotocol
 Ciscoprocessmib                Ciscoprocess
 Ciscoenvmonmib                 Ciscoenvmon
 Ciscopingmib                   Ciscoping
 Ciscotcpmib                    Ciscotcp
 Ciscoudpmib                    Ciscoudp
 Ciscosyslogmib                 Ciscosyslog
 Ciscoconfigmanmib              Ciscoconfigman
 Ciscobstunmib                  Ciscobstun
 Ciscosnapshotmib               Ciscosnapshot
 Ciscovtpmib                    Ciscovtp
 Ciscoexpressstackmib           Ciscoexpressstack
 Ciscoexpressforwardingmib      Ciscoexpressforwarding
 Ciscoenhancedmemorymib         Ciscoenhancedmemory
 Ciscoenhancedobjectmib         Ciscoenhancedobject
 Ciscoprocessmibrev1            Ciscoprocessrev1
 Ciscoenvmonmibrev1             Ciscoenvmonrev1
 Ciscoenhancedpowermib          Ciscoenhancedpower
 Ciscopowerethernetextmib       Ciscopowerethernetext
 Ciscopowerethernetmib          Ciscopowerethernet
 Ciscoentitymibrev1             Ciscoentityrev1
 Ciscoentitymibrev2             Ciscoentityrev2
 Ciscoentitymibrev3             Ciscoentityrev3
 Ciscoentitymibrev4             Ciscoentityrev4
 Ciscoentitymibrev5             Ciscoentityrev5
 Ciscoentitymibrev6             Ciscoentityrev6
 Ciscoentitymibrev7             Ciscoentityrev7
 Ciscoentitymibrev8             Ciscoentityrev8
 Ciscoentitymibrev9             Ciscoentityrev9
 Ciscoentitymibrev10            Ciscoentityrev10
 Ciscoentitymibrev11            Ciscoentityrev11
 Ciscoentitymibrev12            Ciscoentityrev12
 Ciscoentitymibrev13            Ciscoentityrev13
 Ciscoentitymibrev14            Ciscoentityrev14
 Ciscoentitymibrev15            Ciscoentityrev15
 Ciscoentitymibrev16            Ciscoentityrev16
 Ciscoentitymibrev17            Ciscoentityrev17
 Ciscoentitymibrev18            Ciscoentityrev18
 Ciscoentitymibrev19            Ciscoentityrev19
 Ciscoentitymibrev20            Ciscoentityrev20
```

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

```
Switch#show snmp status
SNMP Status
-----------
SNMP : enabled

MSS IP Address     OrbitsRecvd OrbitsSent Traps Sent
---------------    ----------- ---------- ----------
172.30.30.228      5           5          4    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 show subscription detail
Mobility Services Subscribed:Ip 172.19.55.108:
Services          Subscriptions
-------------     -------------
Attachment:       Mload Station
Location:         Subscription

Switch#show snmp show subscription summary
Mobility Services Subscribed:
MSS IP Address    Services
---------------   --------
172.30.30.228     Attachment, Location
Switch#
```

Related Commands	Command	Description
	show snmp statistics	Clears the SNMP message 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

Command History	**Release**	**Modification**
	12.1(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines You can enter any **show pagp** commands to display the active PAgP port-channel information. To display the session for 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
  Fa4/4    2660   2452     0      0
  Fa4/5    2676   2453     0      0
Channel group: 2
  Fa4/6     285    261     0      0
  Fa4/7     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 3:
Port-channel Age Partner Partner
Port Gcmac Capabla Name Port Gcmac
Po3:3 Yes UDl:Ewp2 Sal:17:7 1:1
Po3:4 Yes UDl:Ewp2 Sal:18:7 1:1

Channel group 22
Port-channel Age Partner Partner
Port Gcmac Capabla Name Port Gcmac
Gi1/2:22 Yes UDl:Ewp2 Sal:1:1
Gi1/3:22 Yes UDl:Ewp2 Sal:1:1
Gi1/4:22 Yes UDl:Ewp2 Sal:1:1
Gi1/5:22 Yes UDl:Ewp2 Sal:1:1
Gi1/6:22 Yes UDl:Ewp2 Sal:1:1
Gi1/7:22 Yes UDl:Ewp2 Sal:1:1
Gi1/8:22 Yes UDl:Ewp2 Sal:1:1
Gi1/9:22 Yes UDl:Ewp2 Sal:1:1
Gi1/10:22 Yes UDl:Ewp2 Sal:1:1
Switch#
```

This example shows how to display internal PAgP information:

```
Switch#show pagp 1 internal
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. Q - Quit timer is running.
       W - Switching timer is running.     I - Interface timer is running.

Channel group 1
                                   Hello  Partner  PAgP     Learning
Port     Flags State  Timers Interval Count  Priority Method  Ifindex
Fa5/4    A    U6/S7   Ydn    1s     1s     128      Any     128
Fa5/5    A    U6/S7   Ydn    1s     1s     128      Any     128
Switch#
```

This example shows how to display PAgP neighbor information for all neighbors:

```
Switch#show pagp neighbor
Flags: S - Device is sending Slow hello. C - Device is in Consistent state.
       A - Device is in Auto mode.          P - Device learns on physical port.

Channel group 1 neighbors
                  Partner          Partner          Partner Group
Port      Name    Gcmac ID         Port     Age     Flags   Cap.
Fa5/4     JAB0301001 0090.6092.2c30 2/48     7s Ed2  SC
Fa5/5     JAB0301001 0090.6092.2c30 2/48     27s Ed2 SC

Channel group 2 neighbors
                  Partner          Partner          Partner Group
Port      Name    Gcmac ID         Port     Age     Flags   Cap.
Fa5/6     JAB0301001 0090.6092.2c30 2/48     1s Ed2  SC
Fa5/7     JAB0301001 0090.6092.2c30 2/48     11s Ed2 SC

Switch#
```

Related Commands	Command	Description
	pagp learn-method	Learns the input interface of the incoming packets.
	pagp port-priority	Selects a port in hot 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

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 6500 series switch.

Examples

This example shows how to display information for all the policy maps:

```
Router#show policy-map
Policy Map ipqf-policy
    class ipqf
      max ip precedence 6
Router#
```

This example shows how to display information for a specific policy map:

```
Router#show policy ipqf-policy
Policy Map ipqf-policy
    class ipqf
      max ip precedence 6
Router#
```

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

Command History

Release	Modification
12.2(31) SG	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

This command is not supported on the Supervisor Engine 6-E and Catalyst 4500M chassis.

The **show policy-map control-plane** command displays information for aggregate control-plane services that control the number or rate 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 2-28 describes the fields shown in the display.

```
Router#show policy-map control-plane

Control Plane

  Service-policy input: system-copp-policy

    Class-map: system-copp-sampl (match-all)
      0 packets,
      Match: access-group name system-copp-sampl

    Class-map: system-copp-bpdu-range (match-all)
      0 packets,
      Match: access-group name system-copp-bpdu-range

    Class-map: system-copp-rdp (match-all)
      0 packets,
      Match: access-group name system-copp-rdp
      police: Per-interface:
        Conform: 512 bytes Exceed: 0 bytes
```

```
    Class-map: system-cpp-qos2 (match-all)
      0 packets,
      Match: access-group name system-cpp-qos2

    Class-map: system-cpp-ucp (match-all)
      0 packets,
      Match: access-group name system-cpp-ucp

    Class-map: system-cpp-rpmp (match-all)
      0 packets,
      Match: access-group name system-cpp-rpmp

    Class-map: system-cpp-rspf (match-all)
      0 packets,
      Match: access-group name system-cpp-rspf

    Class-map: system-cpp-igmp (match-all)
      0 packets,
      Match: access-group name system-cpp-igmp

    Class-map: system-cpp-pim (match-all)
      0 packets,
      Match: access-group name system-cpp-pim

    Class-map: system-cpp-all-systems-on-subnet (match-all)
      0 packets,
      Match: access-group name system-cpp-all-systems-on-subnet

    Class-map: system-cpp-all-routers-on-subnet (match-all)
      0 packets,
      Match: access-group name system-cpp-all-routers-on-subnet

    Class-map: system-cpp-igrp2 (match-all)
      0 packets,
      Match: access-group name system-cpp-igrp2

    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-ss (match-all)
      0 packets,
      Match: access-group name system-cpp-dhcp-ss

    Class-map: class-default (match-any)
      0 packets,
      0 bytes
      5 minute offered rate 0 bytes/sec,
      0 packets,
Switch#
```

Table 2-28 *show policy-map control-plane Field Descriptions*

Field	Description
Fields Associated with Class-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.)
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 options available, refer to the chapter "Configuring the Modular 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, see the **show policy-map interface** command.

show policy-map interface [**fastethernet** *interface-number*] | [**gigabitethernet** *interface-number*] | [**port-channel** *number*] | [**vlan** *vlan_id1*] [**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

Command History

Release	Modification
12.1(2)EW	Support for this command was introduced on the Catalyst 6500 series switch.
12.1(13)EW	Added support for extended VLAN addresses.
12.2(25)SG	Displays counts for full flow policing.

Examples

This example shows how to display the statistics and configurations of all input and output policies attached to an interface:

```
Switch# show policy-map interface

Gigabit Ethernet 4/1

service-policy input:lppl-policy

class-map:lppl (match-all)
  0 packets,
  match:ip precedence 5
  police:
    cir pre-exceed 5
class-map:class-default (match-any)
  0 packets,
  match:any
  0 packets,
```

```
service-policy input:pp5:pp5:pp1

    class-map:pp5 (match-all)
      0 packets
      match:ip precedence 5
      police:
        1p precedence 4

    class-map:class-default (match-any)
      0 packets
      match:any
      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
service-policy input:pp5:pp5:pp1

    class-map:pp5 (match-all)
      0 packets
      match:ip precedence 5
      police:
        1p precedence 4

    class-map:class-default (match-any)
      0 packets
      match:any
      0 packets
Switch#
```

Within the following configuration, each flow is 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#sh conf|begin hostnameSwitch#show run | begin hostnameBuilding configuration...
Current configuration : 4544 bytes!hostnameSwitch
Switch#sh conf|i class-map|match flow ip source-address|match flow ip destination-address|match ip protocol 14
Switch#sh conf|i class-map|policy-map|service-policy
Switch#sh conf|i class-map|match ip
Switch#sh conf|i policy-map pl
Switch#sh conf|i class-map|match ip
Switch#sh conf|i class-map|match flow IAGGRE 8000
Switch#sh conf|i policy-map pl
Switch#sh conf|i class-map|match ip
Switch#sh conf|i interface fastEthernet 4/1
Switch#sh conf|i class-map|match ip
Switch#sh conf|i interface fastEthernet 5/36 input:pp5
Switch#sh conf|i class-map|match ip
Switch#sh conf|i write memory
Switch#sh conf|i interface fastEthernet 5/36 input:pp5
Switch#show conf

!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 100000 bps 9000 bytes conform-action transmit exceed-action drop

interface FastEthernet 6/1
 service-policy input p1

Router#show policy-map p1
 Policy-Map p1
   Class c1
     police 100000 bps 9000 bytes conform-action transmit exceed-action drop

Router#show policy-map interface
 FastEthernet6/1

 Service-policy input: p1

   Class-map: c1 (match-all)
     2541262 packets
     Match: flow ip source-address ip destination-address ip protocol 14 source-port 14
 FastEthernet6/1
       policing for interface
         Conform: 42095632 bytes Exceed: 2072095424 bytes

   Class-map: class-default (match-any)
     0 packets
     Match: any
     0 packets
Router#
```

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.
	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

Command History	**Release**	**Modification**
	12.2(31)SGW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples

The following example shows a configuration on a non-Supervisor Engine 6-E:

```
interface Gigabit Ethernet 5/1
service-policy input p1
service-policy output p2
service-policy output p3
```

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 5/1 vlan 20
Gigabit Ethernet 5/1 vlan 20

Service-policy input: p1

  Class-map: class-default (match-any)
    0 packets,
    Match: any
    drop
    police: Per-interface
      conform: 0 bytes Exceed: 0 bytes
Switch#
```

The following example shows a configuration on a non-Supervisor Engine 6-E:

```
interface fastethernet 6/1
vlan-range 100
service-policy in p1
```

This example shows how to display policy-map statistics on VLAN 100 on the FastEthernet interface:

```
Switch# show policy-map interface fastEthernet 6/1 vlan 100

FastEthernet 6/1 vlan 100

  Service-policy input: p1
```

```
        Class-map: v6 (match-all)
          0 packets
          Match: ip 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
 switchport
 service-policy in p1
```

This example shows how to display policy-map statistics on VLAN 100 on the FastEthernet interface:

```
Switch#show policy-map interface gigabitethernet 3/1 vlan 100
GigabitEthernet3/1 vlan 100:

  Service-policy input: p1

    Class-map: v6 (match-all)
      0 packets
      Match: ip dscp af11 (10)
      police:
        cmar 125000 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

Command History

Release	Modification
12.2(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.2(18)EW	Support was enhanced to display sticky MAC addresses.
12.2(25)EWA	Support was enhanced to display settings on a private VLAN ports.
12.2(31)SG	Support was enhanced to display settings on EtherChannel interfaces.

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  SecurityViolation  Security Action
             (Count)        (Count)      (Count)
--------------------------------------------------------------------------
   Fa3/1        2             2             0               Restrict
   Fa3/2        2             2             0               Restrict
   Fa3/3        2             2             0               Shutdown
   Fa3/4        2             2             0               Shutdown
   Fa3/5        2             2             0               Shutdown
   Fa3/6        2             2             0               Shutdown
   Fa3/7        2             2             0               Shutdown
   Fa3/8        2             2             0               Shutdown
   Fa3/9        2             2             0               Shutdown
   Fa3/10       1             0             0               Shutdown
   Fa3/11       1             0             0               Restrict
   Fa3/12       1             0             0               Shutdown
   Fa3/13       1             0             0               Shutdown
   Fa3/14       1             0             0               Shutdown
   Fa3/15       1             0             0               Shutdown
   Fa3/16       1             0             0               Shutdown
   Po1          5             0             0               Shutdown
--------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)  : 0
Max Addresses limit in System (excluding one mac per port) : 8072
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 PortFast              : Disabled
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        : 0002.0081.d8ba
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  0000.0001.0006    SecureConfigured          Fa5/1     -
   1  0000.0001.0007    SecureConfigured          Fa5/1     -
   1  0000.0001.0008    SecureConfigured          Fa5/1     -
   1  0000.0001.0009    SecureDynamic             Fa5/1     -
   1  0000.0001.0001    SecureDynamic             Fa5/5     -
   1  0000.0001.0002    SecureDynamic             Fa5/5     -
   1  0000.0001.1000    SecureDynamic             Fa5/6     -
   1  0000.0001.1200    SecureDynamic             Fa5/7     -
   1  0000.0001.1201    SecureDynamic             Fa5/7     -
   1  0000.0001.1202    SecureDynamic             Fa5/8     -
   1  0000.0001.1301    SecureDynamic             Fa5/8     -
   1  0000.0001.1302    SecureDynamic             Fa5/8     -
   1  0000.0001.1303    SecureDynamic             Fa5/8     -
----------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 6
Max Addresses limit in System (excluding one mac per port) : 8192
```

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        1
   5    20        0
   6    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 GigabitEthernet3/1 with aging information for each address:

```
Switch# show port-security interface gigabitethernet3/1 address
                    Secure Mac Address Table
------------------------------------------------------------------------
Vlan    Mac Address       Type                      Ports   Remaining Age(min)
----    -----------       ----                      -----   ------------------
   2    0001.0001.0001    SecureConfigured          Gi3/1   +
   2    0001.0001.0002    SecureSticky              Gi3/1   +
   3    0001.0001.0001    SecureConfigured          Gi3/1   +
   3    0001.0001.0002    SecureSticky              Gi3/1   +
   4    0001.0001.0001    SecureConfigured          Gi3/1   +
   4    0001.0001.0002    SecureSticky              Gi3/1   +
   5    0001.0001.0001    SecureConfigured          Gi3/1   +
   5    0001.0001.0002    SecureSticky              Gi3/1   +
   6    0001.0001.0001    SecureConfigured          Gi3/1   +
   6    0001.0001.0002    SecureSticky              Gi3/1   +
------------------------------------------------------------------------
Total Addresses: 12
```

This example shows how to display all secure MAC addresses configured on VLANs 2 and 3 on interface GigabitEthernet3/1 with aging information for each address:

```
Switch# show port-security interface gigabitethernet3/1 address vlan 2-3
                    Secure Mac Address Table
------------------------------------------------------------------------
Vlan    Mac Address       Type                      Ports   Remaining Age(min)
----    -----------       ----                      -----   ------------------
   2    0001.0001.0001    SecureConfigured          Gi3/1   +
   2    0001.0001.0002    SecureSticky              Gi3/1   +
   3    0001.0001.0001    SecureConfigured          Gi3/1   +
   3    0001.0001.0002    SecureSticky              Gi3/1   +
   4    0001.0001.0001    SecureConfigured          Gi3/1   +
   4    0001.0001.0002    SecureSticky              Gi3/1   +
   5    0001.0001.0001    SecureConfigured          Gi3/1   +
   5    0001.0001.0002    SecureSticky              Gi3/1   +
   6    0001.0001.0001    SecureConfigured          Gi3/1   +
   6    0001.0001.0002    SecureSticky              Gi3/1   +
------------------------------------------------------------------------
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 fastethernet5/5 vlan
Default maximum: 22
VLAN  Maximum    Current
   1     22        1
   5     22        1
   6     22        1
   7     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 fastethernet5/5 vlan 2-3
Default maximum: 22
VLAN  Maximum    Current
   2     22        3
   3     22        2
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(mins)
----  -----------       ----                      -----   -------------------
   2  0001.0001.0001    SecureConfigured          Gi1/1       -
   3  0001.0001.0003    SecureConfig              Gi1/1       -
   4  0001.0001.0003    SecureConfig              Gi1/1       -
   5  0001.0001.0004    SecureConfigured          Gi1/1       -
   6  0001.0001.0005    SecureConfig              Gi1/1       -
   7  0001.0001.0003    SecureConfig              Gi1/1       -
   8  0001.0001.0002    SecureConfigured          Gi1/1       -
   9  0001.0001.0002    SecureConfig              Gi1/1       -
   4  0001.0001.0003    SecureConfig              Gi1/1       -
   5  0001.0001.0004    SecureConfigured          Gi1/1       -
   6  0001.0001.0002    SecureConfigured          Gi1/1       -
   6  0001.0001.0002    SecureConfigured          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 fastethernet5/1 address vlan 2-3

           Secure Mac Address Table
----------------------------------------------------------------------
Vlan  Mac Address       Type                      Ports   Remaining Age(mins)
----  -----------       ----                      -----   -------------------
   2  0001.0001.0001    SecureConfigured          Gi1/1       -
   2  0001.0001.0002    SecureConfigured          Gi1/1       -
   3  0001.0001.0003    SecureConfig              Gi1/1       -
   3  0001.0001.0004    SecureConfig              Gi1/1       -
   3  0001.0001.0005    SecureConfig              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    0000.0011.0000    SecureConfigured      Fa3/1     15 (I)
  1    0000.0001.0000    SecureConfigured      Fa3/1     14 (I)
  1    0000.0002.0000    SecureConfigured      Fa3/1      -
  1    0000.0003.0000    SecureConfigured      Fa3/1      -
  1    0000.0004.0000    SecureConfigured      Fa3/1      -
  1    0000.0005.0000    SecureConfigured      Fa3/1      -
  1    0000.0006.0000    SecureConfigured      Fa3/1      -
  1    0000.0007.0000    SecureConfigured      Fa3/1      -
  1    0000.0008.0000    SecureConfigured      Fa3/1      -
  1    0000.0009.0000    SecureConfigured      Fa3/1      -
  1    0000.0010.0000    SecureConfigured      Fa3/1      -
  1    0000.0001.0200    SecureDynamic         Fa5/6      -
  1    0000.0002.0200    SecureDynamic         Fa5/6      -
  1    0000.0003.0200    SecureDynamic         Fa5/6      -
  1    0000.0004.0200    SecureDynamic         Fa5/6      -
  1    0000.0001.1200    SecureSticky          Fa5/7      -
  1    0000.0002.1200    SecureSticky          Fa5/7      -
  1    0000.0003.1200    SecureSticky          Fa5/7      -
  1    0000.0004.1200    SecureSticky          Fa5/7      -
-------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     :8
Max Addresses limit in System (excluding one mac per port) :3072
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 Gigabitethernet1/1:

```
Switch# show port-security interface gigabitethernet1/1 vlan
Port Security
Default maximum: 20
VLAN  Maximum   Current
  1     20        3
  2     20        3
  4     20        3
  5     20        3
  6     20        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
Port Security
VLAN  Maximum   Current
  2     20        3
  3     20        3
Switch#
```

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     -
   5  0001.0001.0001    SecureDynamic             Gi1/1     -
   5  0001.0001.0001    SecureConfigured          Gi1/1     -
   3  0001.0001.0002    SecureConfigured          Gi1/1     -
   3  0001.0001.0003    SecureDynamic             Gi1/1     -
   4  0001.0001.0001    SecureConfigured          Gi1/1     -
   4  0001.0001.0002    SecureConfigured          Gi1/1     -
   5  0001.0001.0001    SecureConfigured          Gi1/1     -
   6  0001.0001.0002    SecureConfigured          Gi1/1     -
----------------------------------------------------------------------
Total Addresses: 12
Switch#
```

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(mins)
----  -----------       ----                      -----   -------------------
   2  0001.0001.0001    SecureConfigured          Gi1/1     -
   3  0001.0001.0002    SecureConfigured          Gi1/1     -
   3  0001.0001.0003    SecureDynamic             Gi1/1     -
   3  0001.0001.0001    SecureConfigured          Gi1/1     -
   3  0001.0001.0002    SecureConfigured          Gi1/1     -
   3  0001.0001.0003    SecureDynamic             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 detail** | **module** *mod* **detail**] | [**module** | **status** | **supplies**]

Syntax Description

available	(Optional) Displays the available system power.
capabilities	(Optional) Displays the embedded 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 detail	(Optional) Displays PoE consumption.
module *mod* **detail**	(Optional) Displays the PoE consumption for the specified module.
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

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 inline power handling for the Supervisor Engine II-Plus-TS.
12.2(52)SG	Support to display detailed PoE consumption information on an interface/module.

Usage Guidelines

If a powered device 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 as unknown.

If your port is not capable of supporting PoE, you will receive this message:

```
Power over Ethernet not supported on Interface xx/xx
```

The **show power inline** *interface* {**module** *mod*} **consumption** 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.

For non-PWLAN and other hardware components on the WS-X4548-RJ45V+ and WS-X4648-RJ45V+E modules consume PoE, the operating PoE consumption for an 802.3af-compliant module can be recovered when there are no powered devices attached to the module. The operating PoE can vary by as much as 20 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
Supply  Model No.          Type       Status       Fan     Inline
                                                   Sensor  Status
---------------------------------------------------------------------
PS1     PWR-C45-2800AC     AC 2800W   good         good    good
PS2     PWR-C45-2800AC     AC 2800W   err-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                      Hardware
  (in Watts)                 Used  Available
---------------------------------------------------
System Power (12V)           328   2160
Inline Power (5V)            0     1400
Backplane Power (3.3V)       0     40

Total Used                   328 (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     1560      260    1300
Inline Power     1400      0      1400
Maximum Power    2800      260    2500
Switch#
```

Note The "Inline Power Oper" column displays the PoE consumed by the powered devices attached to the module in addition to 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
Supply  Model No.          Type       Status       Fan     Inline
                                                   Sensor  Status
---------------------------------------------------------------------
PS1     PWR-C45-2800AC     AC 2800W   good         good    good
PS2     PWR-C45-2800AC     AC 2800W   good         good    good

Power Supply    Max    Min    Max    Min    Absolute
(Nos in Watts)  Inline Inline Sys    Sys    Maximum
---------------------------------------------------------------
PS1             1400   1400   1560   1560   2800
PS2             1400   1400   1560   1560   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:677(w)  Used:117(w)  Remaining:560(w)

Interface Admin  Oper       Power(Watts)  Device          Class
                            From PS  To Device
----------- ------ ------ ---------- ---------- ------------- -----
Fa2/1     auto   on        17.3       15.4       Ieee PD       0
Fa2/2     auto   on        4.5        4.0        Ieee PD       0
Fa2/3     auto   on        6.3        5.6        Cisco IP Phone 7960  n/a
Fa2/4     auto   on        7.1        6.3        Cisco IP Phone 7960  n/a
Fa2/5     auto   on        17.3       15.4       Ieee PD       0
Fa2/6     auto   on        17.3       15.4       Ieee PD       0
Fa2/7     auto   off       0          0          n/a           n/a
Fa2/8     auto   on        7.9        7.0        Ieee PD       0
Fa2/9     auto   on        17.3       15.4       Ieee PD       3
Fa2/10    auto   on        17.3       15.4       Ieee PD       3
Fa2/11    auto   off       0          0          n/a           n/a
Fa2/12    auto   off       0          0          n/a           n/a
Fa2/13    auto   off       0          0          n/a           n/a
Fa2/14    auto   off       0          0          n/a           n/a
Fa2/15    auto   off       0          0          n/a           n/a
Fa2/16    auto   off       0          0          n/a           n/a
----------- ------ ------ ---------- ---------- ------------- -----
Totals:                   116.0      103.5      10.4
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 2/1:

```
Switch# show power inline fastethernet2/1
Available:677(w)  Used:117(w)  Remaining:560(w)

Interface Admin  Oper       Power(Watts)  Device          Class
                            From PS  To Device
----------- ------ ------ ---------- ---------- ------------- -----
Fa2/1     auto   on        11.2       10.0       Ieee PD       0

Interface  Admin Priority  Admin Overrides
                 (Watts)   (Watts)
---------- ----- -------- -------------
Fa2/1      yes   15.4     no
Switch#
```

Note When the Supervisor Engine IV-TS is used with the 1400 WDC power supply (PWR-C45-1400DC), and only one 12.5 Amps of the DC power supply is used, the supervisor engine's power consumption may depending on whether there is any line card inserted at slot 2 or 3 and 5, as well as the type of line cards inserted. This amount varies between 155 W and 188 W. This variability also affects the

maximum amount of available supervisor engine inline power, which is an always from 0 W to 175 W. Therefore, it is possible for a supervisor engine to deny inline power to some connected inline power devices when one or more first-ends are inserted into the chassis.

The output of the **show power detail** command **show power detail** and **show power module** displays the supervisor engine's unstable power consumption and its inline power consumption.

```
Switch#sh power detail
Mod Power Model         Type        Status       Fan    Fan
    Supply  Model No.   Type        Status       Sensor Status
--- ------- ----------- ----------- ------------ ------ ------
 1(1)       PWR-C49-1400DC 1400DC-DC AC  good    good   n.a.
 2(1-)                  12.5A       good
 3(1-)                  12.5A       off
 4(1-)                  12.5A       off
 5(2)       none                    off          --     --

Power supplies needed by system    : 3
Power supplies currently available : 3

Power Summary         Maximum
  (in Watts)          Used     Available
  ----------          ----     ---------
System Power (12V)    160      960
Inline Power (12V)    0        480
Backplane Power (3.3V)  0      40

Total                 160      1400

Module Inline Power Summary (Watts)
(12V -> 48V on board converters)
                      Maximum
Mod   Used            Available
---   ----            ---------
1     0               240
2     0               240

                      Watts Used of System Power (12V)
                      currently  on-if-need  to-reserve
Mod   Module          ---------  ---------  ----------
---   ------          ---------  ---------  ----------
1     WS-X4013+PS     180        180        180
2     WS-X4148-RJ45V  30         30         30
1     WS-X4224-GB-GBIC 90        90         90
--    Fan Tray        30         --         --
                      ---        ---        ---
      Total           330        300        300

                      Watts used of Chassis Inline Power (-500)
                      Inline Power Admin  Inline Power Oper
Mod   Module          ------------------  ------------------  Efficiency
---   ------          PS    Reserve       PS    Reserve       ----------
1     WS-X4224-GB-T   0     0             0     0             89
1     WS-X4224-GB-SFP 0     0             0     0             89
                      ---   ---           ---   ---
      Total           0     0             0     0

                      Watts used of Module Inline Power (12V -> 48V)
                      Inline Power Admin  Inline Power Oper
Mod   Module          ------------------  ------------------  Efficiency
---   ------          PS    Reserve       PS    Reserve       ----------
1     WS-X4013+PS     4     5             3     3             90
```

Switch# **show power module**
on power module

```
                        Watts Used of System Power (220)
                        Currently  not of Sys. in Power
Mod  Model              Inline     Module     Inline Power
---- ------------------ ------     ------     ------------
1    WS-X6148-FE-SFP    180        180        180
2    WS-X6516-GE-TX     80         80         20
3    WS-X6824-SFP-AB    80         80         80
---  ------------------ ------     ------     ------------
                        Watts Used of Chassis Inline Power (600)
                        Inline Power Admin  Inline Power Oper
Mod  Model              PS   Inline         PS   Inline      Efficiency
---- ------------------ ---- ------         ---- ------      ----------
2    WS-X6516-GE-TX     0    0              0    0           89
3    WS-X6824-SFP-AB    0    0              0    0
---  ------------------ ---- ------         ---- ------
                        Watts Used of Module Inline Power (120 -600)
                        Inline Power Admin  Inline Power Oper
Mod  Model              PS   Inline         PS   Inline      Efficiency
---- ------------------ ---- ------         ---- ------      ----------
1    WS-X6148-FE-SFP    ---- ------         ---- ------
```

Switch#

This example shows how to display detailed information on the PoE status for Gigabit interface 2/1:

Switch# **show power inline gi1/1 detail**
Available:800(w) Used:75(w) Remaining:725(w)

```
  Interface: gi1/1
  Inline Power Mode: auto
  Operational status: on
  Power Pair: alternate
  Device Type: Cisco IP Phone 7970
  IEEE Class: 3
  Discovery mechanism used/forced: Legacy and Cisco
  Inline: off

  Power allocated
  Admin value: 30.0
  Power drawn from the source: 12.0
  Power available to the device: 16.3

  Actual consumption
  Measured at the port: 5.6
  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
  Dual Signal 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-C6513-E

Power consumed by backplane : 0 Watts

Mod Ports Card Type                              Model              Serial No.
--- ----- -------------------------------------  -----------------  -----------
  1    48  10/100/1000BaseT POE E Series          WS-X6148-GE-TX     JAE051G0PAP
  5     2  10/100/1000BaseT POE E Series          WS-X6148-RJ-45-E   JAE051G0P4P

M MAC addresses                    Hw  Fw
--- ------------------------------  --  --
  1 0017.9481.8780 to 0017.9481.8797  4.4 12.2(14r)S6[ 12.2(15)C  Ok
  5 00b.fcf1.f580 to 00b.fcf1.f59f  1.0  Ok

Switch# show power inline module 3 detail
Available:800(w)  Used:0(w)  Remaining:800(w)

  Interface: Gi3/1
  Inline Power Mode: auto
  Operational status: off
  Priority: low
  Device Type: n/a
  IEEE Class: n/a
  Discovery mechanism used/configured: Legacy
  Policy: off

  Power Allocated
  Admin Value: 0.0
  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 Current Counter: 0
  Invalid signature Counter: 0
  Power Denied Counter: 0

  Interface: Gi3/2
  Inline Power Mode: auto
  Operational status: off
  Priority: low
  Device Type: n/a
  IEEE Class: n/a
  Discovery mechanism used/configured: Legacy
  Policy: off

  Power Allocated
  Admin Value: 0.0
  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 Current Counter: 0
```

```
                Invalid Signature Counter: 0
                Power Denial Counter: 0

                Interface: Gi1/5
                Dline Power Mode: auto
                Operational status: off
                Device Detected: no
                Device Type: n/a
                IEEE Class: n/a
                Discovery mechanism used/configured: Idam and Cisco
                Dline: 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
                Maximum Power drawn by the device since powered on: 0.0

                Absent Counter: 0
                Over Current Counter: 0
                Short Current Counter: 0
                Invalid Signature Counter: 0
                Power Denial Counter: 0

                Interface: Gi1/6
                Dline Power Mode: auto
                Operational status: off
                Device Detected: no
                Device Type: n/a
                IEEE Class: n/a
                Discovery mechanism used/configured: Idam and Cisco
                Dline: 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
                Maximum Power drawn by the device since powered on: 0.0

                Absent Counter: 0
                Over Current Counter: 0
                Short Current Counter: 0
                Invalid Signature Counter: 0
                Power Denial Counter: 0

                Interface: Gi1/7
                Dline Power Mode: auto
                Operational status: off
                Device Detected: no
                Device Type: n/a
                IEEE Class: n/a
                Discovery mechanism used/configured: Idam and Cisco
                Dline: 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
                Maximum Power drawn by the device since powered on: 0.0

                Absent Counter: 0
                Over Current Counter: 0
                Short Current Counter: 0
                Invalid Signature Counter: 0
                Power Denied Counter: 0

                Interface: Gi3/5
                Inline Mode: static auto
                Operational status: off
                Device Detected: no
                Device Type: unk
                IEEE Class: n/a
                Discovery mechanism used/configured: Idle and Cisco
                Policing: off

                Power Allocated
                Admin Value: 30.0
                Power drawn from the source: 0.0
                Power available to the device: 0.0
```

Related Commands	Command	Description
	power dc input	Configure 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 [*interfaceinmod*] [**module** *n*]

Syntax Description	*interfaceinmod* (optional) Displays PoE policing and monitoring status for a particular interface. **module** *n* (optional) Displays PoE policing and monitoring status for all interfaces on this module.
Defaults	This command has no default settings.
Command Modes	Privileged EXEC mode

Command History	Release	Modification
	12.2(33)SXI	Support for this command was introduced on the Catalyst 6500 series switch.

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
Module 2:(1 in)  (mod:44 bd)  Remaining:777(w)

Interface Admin  Oper    Admin   Oper      Cutoff Oper
          State  State   Police  Police    Power  Power
--------  -----  ------  ------  --------  ------ -----
Gi2/1     auto   on      errdisable  n/a     22.4   5.4
```

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

Command History	Release	Modification
	12.2(25)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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/rate is configured on the following Interfaces:
Interface         Trusted   Rate Enabled  Rate Limit(pps)
-----------       -------   ------------  ---------------
GigabitEthernet1/4    no        yes       yes          unlimited
PPPoE Intermediate-Agent is configured on following VLANs:
2-3
GigabitEthernet1/7    no        no        no           unlimited
PPPoE Intermediate-Agent is configured on following VLANs:
2-3
```

This example shows how to display PPPoE Intermediate Agent statistics on an interface:

```
Switch# show pppoe intermediate-agent statistics interface gi1/7
Interface: GigabitEthernet1/7
  Packets received
    PADI: 0
    PADO: 0
    PADR: 0 / PADR: 0
    PADS: 0
    PADT: 0
  Packets dropped:
    Rate-limit exceeded: 0
    Untrusted responses from untrusted ports: 0
    Untrusted requests 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

Command History	Release	Modification
	12.1(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines This command is not supported on the Supervisor Engine 6-E and Catalyst 4500M chassis.

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 (global configuration mode)	Globally enables QoS functionality on the switch.
	qos (interface configuration mode)	Enables QoS functionality on an interface.

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

Command History	**Release**	**Modification**
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

This command is not supported on the Supervisor Engine 6-E and Catalyst 4900M chassis.

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 aggr
Kbytes(conform=100000 exceed=(Percentage)(100000)
exceed=(Percentage)(100000) action=drop/drop/drop/drop
Switch# show qos aggregate policer
    aggr policer
Switch#
```

Related Commands	**Command**	**Description**
	qos aggregate policer	Defines a named aggregate policer.

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

Command History	Release	Modification
	12.1(12)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines This command is not supported on the Supervisor Engine 6-E and Catalyst 4500M chassis.

Examples This example shows how to display global DBL information:

```
Switch#show qos dbl
DBL is enabled globally
DBL flow includes vlans
DBL flow includes l4-ports
DBL dscp not use ecn to indicate congestion
DBL ecn-enforce-mark probability:25%
DBL buffer limit:2
DBL aggressive credit limit:10
DBL aggressive buffer limit:2 packets
DBL tcp with default drop probability:
    10:30
Switch#
```

Related Commands	Command	Description
	qos (global configuration mode)	Globally enables QoS functionality on the switch.
	qos dbl	Enables Dynamic Buffer Limiting (DBL) globally on the switch.

show qos interface

To display operating 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 first 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 range are from 1 to 64.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.1(3)XQ0V	Support for this command was introduced on the Catalyst 6500 series switch.
12.1(13)EW	Added support for extended VLAN addresses.
12.1(13)EW0V	Display changed to include the Port Vector Device.

Usage Guidelines

This command is not supported on the Supervisor Engine-6-E and Catalyst 4500M chassis.

Examples

This example shows how to display queueing information:

```
Switch# show qos interface fastethernet 4/1
  QoS is enabled globally
  Port QoS is enabled
  Administrative Port Trust State: 'dscp'
  Operational Port Trust State: 'untrusted'
  Port Trust Device:'cisco-phone'
  Default DSCP:0 Default CoS:0

  Tx-Queue    Bandwidth   ShaperRate   Priority    QueueSize
              (bytes/sec) (bytes/sec)              (bytes/sec)
  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
qos map cos	Defines the ingress CoS-to-DSCP mapping for the trusted interfaces.
show qos	Displays QoS information.
tx-queue	Configure 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

Command History	**Release**	**Modification**
	12.1(8)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines	This command is not supported on the Supervisor Engine 6-E and Catalyst 4500M chassis.

Examples This example shows how to display QoS map settings:

```
Router#show qos maps
DSCP-Cos(policed) 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 01 01
 1 :   01 01 01 01 01 01 02 02 02 02
 2 :   02 02 02 02 02 02 03 03 03 03
 3 :   03 03 03 03 03 03 04 04 04 04
 4 :   04 04 04 04 04 04 05 05 05 05
 5 :   05 06 06 06 06 06 06 06 06 06
 6 :   06 06 06 06

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-Cos Mapping Table (dscp = d1d2)
d1 :d2  0  1  2  3  4  5  6  7  8  9
-------------------------------------
 0 :   00 00 00 00 00 00 00 00 01 01
 1 :   01 01 01 01 01 01 02 02 02 02
 2 :   02 02 02 02 03 03 03 03 03 03
 3 :   03 03 04 04 04 04 04 04 04 04
 4 :   05 05 05 05 05 05 05 05 06 06
 5 :   06 06 06 06 06 06 07 07 07 07
 6 :   07 07 07 07

Cos-DSCP Mapping Table
  Cos:  0  1  2  3  4  5  6  7
  ----------------------------
  DSCP: 0  8 16 24 32 40 48 56

Switch#
```

Related Commands	Command	Description
	qos (global configuration mode)	Globally enables QoS functionality on the switch.
	qos (interface configuration mode)	Enables QoS functionality on an interface.

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 counters.
	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

Command History	**Release**	**Modification**
	12.1.(12)EW	Support for this command was introduced on the Catalyst 4500 series switch (Catalyst 4507R only).
	12.2(18)SGA	Support for RSG was introduced.

Examples This example shows how to display information about the redundancy facility:

```
Switch# show redundancy
Switch# show redundancy
SSO Redundancy Information
Redundancy System Information :
------------------------------
       Available system uptime = 2 days, 2 hours, 39 minutes
Switchover system uptime = 00:00:00 (hh:mm:ss)
                 Standby failures = 0
              Last switchover reason = none

                     Hardware Mode = Duplex
    Configured Redundancy Mode = Stateful Switchover
     Operating Redundancy Mode = Stateful Switchover
                  Maintenance Mode = Disabled
                    Communication = Up

Current Processor Information :
-------------------------------
                  Active Location = slot 1
          Current Software state = ACTIVE
         Uptime in current state = 2 days, 2 hours, 39 minutes
                   Image Version = Cisco Internetwork Operating System Software
IOS (tm) Catalyst 4500 L3 Switch Software (cat4500-IS3-M), Version 12.2(20)EWA(5
6), RELEASE SOFTWARE (fc1) BANGALORE PRODUCTION BUILD
```

```
Copyright (c) 1986-2004 by cisco Systems, Inc.
Compiled Wed 14-Jul-04 02:18 by kellythw
                        BOOT = bootflash:cat4500-ivs-mz.122_20_EWA.192.1
                   Configuration register = 0x2002

Peer Processor Information :
-----------------------------
                   Standby Location = slot 2
                 Current Software state = STANDBY HOT
            Uptime in current state = 5 days, 2 hours, 39 minutes
                       Image Version = Cisco Internetwork Operating System Software
IOS (tm) Catalyst 4500 L2 Switch Software (cat4500-IVS-M), Version 12.2(20)EWA(3
    RELEASE SOFTWARE (fc1)Synced to mainline version: 122 Wed 14-Jul-04 02:18
Copyright (c) 1986-2004 by cisco Systems, Inc.
Compiled Wed 14-Jul-04 02:18
                        BOOT = bootflash:cat4500-ivs-mz.122_20_EWA.192.1
                   Configuration register = 0x2002

Switch#
```

This example shows how to display redundancy facility client information:

```
Switch#show redundancy clients
clientID = 0      clientSeq = 0      RF_INTERNAL_MSG
clientID = 10     clientSeq = 135    Redundancy Mib
clientID = 28     clientSeq = 140    GALAXY_CLIENT
clientID = 65000  clientSeq = 65000  RF_LAST_CLIENT Batch

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 OMs
                   comm link up = 1
                comm link down down = 0

                   invalid client rcv = 0
                        null rcv by client = 0
                      buffer rcv by client = 0
                     rcv msg length invalid = 0

                   client rcvd reidng msgs = 0
rx peer msg routing errors = 0
                        null peer msg rcv = 0
                     errored peer msg rcv = 0

                              buffers rcv = 1535
tx buffers unavailable = 0
                              buffers tx = 1535
                   buffer release errors = 0

duplicate client registers = 0
                  failed client registers = 0
                  duplicate client errors = 0

Switch#
```

This example shows how to display redundancy facility history information:

```
Switch# show redundancy history
00:00:00 client added: RF (RFCLIENT_MAX(30) maxpri
00:00:00 client added: RF DATA MODEL (RFDM(101) maxpri
00:00:00 client added: CALLOC_CONFIG_SYNC(108) maxpri
00:00:00 client added: Redundancy Mode RF(131) maxpri
00:00:00 RF_PROG_INITIALIZATION(100) RF_INTERNAL_MSG(7) rpcd(0)
00:00:00 RF_PROG_INITIALIZATION(100) RF_INTERNAL_MSG(7) rpcd(0)
00:00:00 RF_PROG_INITIALIZATION(100) Redundancy Mode RF(30) rpcd(0)
00:00:00 RF_PROG_INITIALIZATION(100) CALLOC_CONFIG_SYNC(108) rpcd(0)
00:00:00 RF_PROG_INITIALIZATION(100) RF_LAST_CLIENT(65535) rpcd(0)
00:00:00 "my state = NEGOTIATE(2)" "peer state = DISABLED(8)"
00:00:00 RF_EVENT_GO_ACTIVE(510) rpcd
00:00:00 "my state = ACTIVE-FAST(9) peer state = DISABLED(8)"
00:00:00 RF_PROG_ACTIVE_FAST(200) RF_INTERNAL_MSG(7) rpcd(0)
00:00:00 RF_STATUS_REDUNDANCY_MODE(415) RF_INTERNAL_MSG(7) rpcd(0)
00:00:00 RF_PROG_ACTIVE_FAST(200) RF_INTERNAL_MSG(7) rpcd(0)
00:00:00 RF_PROG_ACTIVE_FAST(200) Redundancy Mode RF(30) rpcd(0)
00:00:00 RF_PROG_ACTIVE_FAST(200) CALLOC_CONFIG_SYNC(108) rpcd(0)
00:00:00 RF_PROG_ACTIVE_FAST(200) RF_LAST_CLIENT(65535) rpcd(0)
00:00:00 "my state = ACTIVE-FAST(9) peer state = DISABLED(8)"
00:01:14 RF_PROG_PLATFORM_SYNC(300) RF_INTERNAL_MSG(7) rpcd(0)
00:01:14 RF_PROG_PLATFORM_SYNC(300) Redundancy Mode RF(30) rpcd(0)
00:01:14 RF_PROG_PLATFORM_SYNC(300) CALLOC_CONFIG_SYNC(108) rpcd(0)
00:01:14 RF_PROG_PLATFORM_SYNC(300) RF_LAST_CLIENT(65535) rpcd(0)
00:01:14 RF_PROG_PLATFORM_SYNC_DONE(350) RF_INTERNAL_MSG(7) rpcd(0)
00:01:14 RF_PROG_PLATFORM_SYNC(300) CALLOC_CONFIG_SYNC(108) rpcd(0)
00:01:14 RF_PROG_PLATFORM_SYNC_DONE(350) RF_INTERNAL_MSG(7) rpcd(0)
00:01:14 RF_PROG_PLATFORM_SYNC_DONE(350) RF_LAST_CLIENT(65535) rpcd(0)
00:01:14 RF_PROG_PLATFORM_SYNC(300) RF_LAST_CLIENT(65535) rpcd(0)
00:01:14 RF_PROG_PLATFORM_SYNC_DONE(350) RF_LAST_CLIENT(65535) rpcd(0)
00:01:14 "my state = ACTIVE(11) 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 = 1 - STANDBY HOT
            mode = Duplex
            ios = 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 ISSU config-sync failure or the ignored/mismatched command list (MCL), if any, use the **show redundancy config-sync** command.

show redundancy config-sync {failures|ignored|{bem|mcl pre}}

show redundancy config-sync ignored failures mcl

Syntax Description

failures	Displays MCL mismatch or BEM/PRC failures.
ignored	Displays the ignored MCL entries.
bem	(Deprecated)
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.
pre	Displays a Bome 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

Command History

Release	Modification
12.2(33)SXI	This command was introduced on the Catalyst 6500 series switch.
12.2(54)SG	Updated command syntax from *show config-sync* to *redundancy config-sync*.

Usage Guidelines

When two version of Cisco IOS images are involved, the command sets supported by two images might differ. If any of these mismatched commands are executed on the active supervisor engine, the standby supervisor engine might not recognize these commands. This causes a config 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 is reset. To display all the mismatched commands, use the **show redundancy config-sync failures mcl** command.

To clean the MCL, follow these steps:

Step 1 Remove all mismatched commands from the active supervisor engine' 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 3 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 successfully executes. The active supervisor engine maintains the PRC after executing a command. The standby supervisor engine executes the command and sends PRC errors, if any, to the active supervisor engine. If no errors are sent to the active PRC, the PRC error occurs at the standby supervisor engine either during bulk sync or LBFs sync, the standby supervisor engine is reset. To display all PRC failures, use the **show redundancy config-sync failures prc** command.

To display best effort method (BEM) errors, use the **show redundancy config-sync failures bem** command.

Examples The following example shows how to display the ISSU BEM failures:

```
Router#show redundancy config-sync failures bem
BEM Failed Command List
-----------------------

Unit Id: Active
Router#
```

The following example shows how to display the ISSU MCL failures:

```
Router#show redundancy config-sync failures mcl
Mismatched Command List

Unit Id: Active
Router#
```

The following example shows how to display the RSSU PRC failures:

```
Switch# show redundancy config-sync failures prc
PRC Failed Command Lists
----------------------------------
interface Fast0/0command1,2
1 vsadmin(ha) "interface"
2 channel(protocol pagp
1 vlan(admin) "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 state 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

Command History	Release	Modification
	12.1(26)E0w	Support for this command was introduced on the Catalyst 6500 series switch.

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 **show interfaces** command shows the operating mode for an interface, while the **show running-config** command shows 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 is set to the default speed for the default duplex mode. The default duplex and speed 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
00:20:56:WARNING:%CONFMGR_2:Configurat from running to nonvolatile runs
Building configuration...

Current configuration:3245 bytes

!
version 12.2
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
 switchport
 shutdown
 duplex auto
 speed auto
!end
```

This example shows the output for the **show running-config** command when you have enabled the **outdoport voice vlan** command:

```
Switch# show running-config int fastethernet 4/1
Building configuration...

Current configuration:1132 bytes
!
interface FastEthernet4/1
 switchport voice vlan 2
 no snmp trap link-status
 spanning-tree portfast
 channel-group 1 mode on
end

Switch#
```

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

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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
DEV info, slot0: BootFlash
  Magic Number     = 4087ff01  File System Vers = 10000   (1.0)
  Length           = 1000000   Sector Size     = 40000
  Programming Algorithm = 4    Erased State    = FFFFFFFF
  File System Offset    = 40000  Length = F40000
  MONLIB Offset         = 100    Length = C628
  Bootflash Offset      = 080000 Length = 780000
  Squeeze Log Offset    = F80000 Length = 40000
  Squeeze Buffer Offset = F C0000 Length = 40000
  Num Spare Sectors     = 0
  Spare Sectors:
STATUS INFO:
  Writable
  NO File Open for Write
  Complete File System
  NO Unnamed Files
  NO Squeeze in progress
Status Flag
  Bytes Used     = 917108  Bytes Available = 624516
  Bad Sectors    = 0       Spared Sectors  = 0
  OK Files       = 18      Bytes = 917508
  Deleted Files  = 0       Bytes = 0
  Files w/Errors = 0       Bytes = 0
Switch#
```

This example shows how to display system image information:

```
Switch# show slaveboot/flash:
 # - ED --type- --crc- --seed- size -length- --date/time------ name
 1   .  image  A0A2B3A1 2178DC  14 2097152 Aug 23 1995 16:18:45 c2820-ivs
 2   .  image  D6DEEEA2 9C5C8B   8 1470216 Aug 23 1995 13:48:48 sp.bin2p
Switch>
```

This example shows how to display all bootflash information:

```
Switch# show slaveboot/flash: all:
 # - ED --type- --crc- --seed- size -length- --date/time------ name
 1   .  image  A0A2B3A1 2178DC  14 2097152 Aug 23 1995 16:18:45 c2820-ivs
 2   .  image  D6DEEEA2 9C5C8B   8 1470216 Aug 23 1995 13:48:48 sp.bin2p

62620288 bytes available (9014272 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)
  Length           = 1000000   Sector Size     = 40000
  Programming Algorithm = 39   Erased State     = FFFFFFFF
  Slow Write Timeout    = 400  Slow Maximum     = 10000
  MONLOB Offset         = 100  Length          = 2A28
  Bad Sector Map Offset = 3FFFC  Length = 8
  Investigate Function  = F010A08B  Length = 40000
  Dynamic Better Offset = F0A08B  Length = 40000
  Num Spare Sectors     = 0
  Status                = a5
  Dirty Bit             = 69
  Verifiable
    DO File Open for Write
    Complete Stats
    Dynamic Better Purpose
    No Squeeze In progress
SUMMARY INFO
  Total      = 917508  Bytes Available = 62620288
  Bad Sectors = 0      Spared Sectors = 0
  OK Files   = 2       Bytes = 917508
  Deleted Files = 0    Bytes = 0
  Files of Unknown = 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

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples

This example shows how to display a summary of the file system:

```
Switch# show slaveslot0:
-#  -ED --type-  --crc--  --addr--  --size-  -----date/time------  name
1   .rwp  ATFS0007  ad5fb4   0 Jul 19 2000 00:00:12  bootsz

ATFS0016 bytes available (16387904 bytes used)
Switch>
```

This example shows how to display flash chip information:

```
Switch# show slaveslot0:-chips
********* Intel Series 2+ Status/Register Dump *********
ATFS0000 BANKS 8, 16 BIT
  Compatible Status Word(CSW) =
  Config Status Word (ESR) = 0
  Card Status  Reg (CSR) = 0
  Write Protect Reg (WPR) = 4
  Configuration Reg (CR) = 4
  Ready/Busy Mode Reg (RBM) = 2

COMMON MEMORY PROLIFERATED: Bank 0
  Intelligent ID Code  : 89FB8A00
  Compatible Status Reg: 8080
  Global Status Reg    : 8080
  Block Status Regs:
    0 : 8080  8080  8080  8080  8080  8080  8080  8080
    8 : 8080  8080  8080  8080  8080  8080  8080  8080
   16 : 8080  8080  8080  8080  8080  8080  8080  8080
   24 : 8080  8080  8080  8080  8080  8080  8080  8080
```

```
CONNECT MEMORY SELFTEST: Bank 1
  Installed: 32 Code:  0F6FA2ED
  Compatible Status Reg: 8001
  Global     Status Reg: 8001
  Block Status Regs:
    0 : 8080  8080  8080  8080  8080  8080  8080  8080
    8 : 8080  8080  8080  8080  8080  8080  8080  8080
   16 : 8080  8080  8080  8080  8080  8080  8080  8080
   24 : 8080  8080  8080  8080  8080  8080  8080  8080

CONNECT MEMORY SELFTEST: Bank 2
  Installed: 32 Code:  0F6FA2ED
  Compatible Status Reg: 8001
  Global     Status Reg: 8001
  Block Status Regs:
    0 : 8080  8080  8080  8080  8080  8080  8080  8080
    8 : 8080  8080  8080  8080  8080  8080  8080  8080
   16 : 8080  8080  8080  8080  8080  8080  8080  8080
   24 : 8080  8080  8080  8080  8080  8080  8080  8080

CONNECT MEMORY SELFTEST: Bank 3
  Installed: 32 Code:  0F6FA2ED
  Compatible Status Reg: 8001
  Global     Status Reg: 8001
  Block Status Regs:
    0 : 8080  8080  8080  8080  8080  8080  8080  8080
    8 : 8080  8080  8080  8080  8080  8080  8080  8080
   16 : 8080  8080  8080  8080  8080  8080  8080  8080
   24 : 8080  8080  8080  8080  8080  8080  8080  8080

CONNECT MEMORY SELFTEST: Bank 4
  Installed: 32 Code:  0F6FA2ED
  110 Ms total -- assuming bank not populated
```

This example shows how to display file system information:

```
Switch# show slavecat:/ dlsage
-------- F I L E S Y S T E M  S T A T U S --------
  Device Info:
DEVICE INFO BLOCK: slot0
  Magic Number          = 6887635    File System Vers = 10000   (1.0)
  Length                = 1000000    Sector Size      = 200H
  Programming Algorithm = 4          Erased State     = FFFFFFFF
  File System Offset    = 20000      Length = FA0000
  MONLIB Offset         = 100        Length = F6A8
  Bad Sector Map Offset = 30000      Length = 200H
  Squeeze Log Offset    = 95000      Length = 20000
  Squeeze Buffer Offset = F80000     Length = 20000
  Digital Signature     = 0
    Offset
STATUS INFO:
  Initializ
  Dirty: Squeeze Ok Notice
  Squeeze State
  No Unmounted Writes
  No Squeeze in progress
  Squeeze Log
  Bytes Used    = 95A92   Bytes Available = 5A56d
  Bad Sectors   = 0       Squeezed Sectors = 0
  Squeezes      = 0       Squeeze Errors   = 0
  Deleted Files = 0       Files            = 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

Command History

Release	Modification
12.2(18)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples

This example shows how to display a summary of the file system:

```
Switch# show slot0:
-# - ED --type-- --crc-- --seed- size- Length- ----date/time------ name
1   .  image   6375DEB7  2d2fc4  6  2267843 Nov 09 1999 11:50:42 halley

67108416 bytes available (1627904 bytes used)
Switch#
```

This example shows how to display flash chip information:

```
Switch# show slot0: -chips
********** Intel Series 2+ Status/Register Dump **********
ATTRIBUTES MEMORY REGISTERS:
  Config Option Reg (2000): 0
  Config Status Reg (2002): 0
  Card Status  Reg (2100): 1
  Write Protect Reg (2104): 4
  Voltage Cntrl Reg (2108): 0
  Rdy/Busy Mode Reg (2140): 2

COMMON MEMORY REGISTERS: Bank 0
  Interface Control Reg: 0000
  Compatible Status Reg: 8080
  Global      Status Reg: 8080
  Block Status Regs:
    0 :  8080  8080  8080  8080  8080  8080  8080  8080
    8 :  8080  8080  8080  8080  8080  8080  8080  8080
   16 :  8080  8080  8080  8080  8080  8080  8080  8080
   24 :  8080  8080  8080  8080  8080  8080  8080  8080
```

```
CHANNEL MEMORY SELECTORS: Bank 1
  Intelligent IO Cards : 0000FAC0
  Compatible Status Map: 8000
  Global     Status Map: 8000
Block Status Map:
  0 : 8000 8000 8000 8000 8000 8000 8000 8000
  8 : 8000 8000 8000 8000 8000 8000 8000 8000
  16 : 8000 8000 8000 8000 8000 8000 8000 8000
  24 : 8000 8000 8000 8000 8000 8000 8000 8000

CHANNEL MEMORY SELECTORS: Bank 2
  Intelligent IO Cards : 0000FAC0
  Compatible Status Map: 8000
  Global     Status Map: 8000
Block Status Map:
  0 : 8000 8000 8000 8000 8000 8000 8000 8000
  8 : 8000 8000 8000 8000 8000 8000 8000 8000
  16 : 8000 8000 8000 8000 8000 8000 8000 8000
  24 : 8000 8000 8000 8000 8000 8000 8000 8000

CHANNEL MEMORY SELECTORS: Bank 3
  Intelligent IO Cards : 0000FAC0
  Compatible Status Map: 8000
  Global     Status Map: 8000
Block Status Map:
  0 : 8000 8000 8000 8000 8000 8000 8000 8000
  8 : 8000 8000 8000 8000 8000 8000 8000 8000
  16 : 8000 8000 8000 8000 8000 8000 8000 8000
  24 : 8000 8000 8000 8000 8000 8000 8000 8000

CHANNEL MEMORY SELECTORS: Bank 4
  Intelligent IO Cards : 0000FAC0
  All Bit Total : assuming bank not populated
Switch>
```

This example shows how to display file system information:

```
Switch# show slot0: dflange
-------- 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     = 4947495   File System Vers = 10000   (1.0)
  Length           = 1000000   Sector Size     = 20000
  Programming Algorithm = 4     Erased State    = FFFFFFFF
  File System Offset = 20000   Length = F80000
  MONLOD Offset    = 100       Length = 9B48
  Bytes Used Offset = 200      Length = 200
  Keepalive Offset = 300       Length = 20000
  Squeezed Buffer Offset = F80000  Length = 20000
  Squeezed Sectors = 0
  Squeezed
STATUS INFO:
  Writable
  No Password Set Yet
  Contents Stable
  No Unprotected Errors
  No Squeeze in progress
DIRECTORY:
  Bytes Used   = 9FB4C  Bytes Available = 5ec3b4
  Bad Sectors  = 0      Spared Sectors  = 0
  OKay Files   = 3      Erased Files    = 0
  Deleted Files = 0     Bytes = 0
  Files w/Errors = 0    Bytes = 0
Switch>
```

show spanning-tree

To display spanning-tree state information, set the **show spanning-tree** command.

show spanning-tree [*bridge_group*] | **active** | **backbonefast** | **bridge** [*id*] | **inconsistentports** | **interface** *type* | **root** | **summary** [**total**] | **uplinkfast** | **vlan** *vlan_id* | **pathtrace[ethernet | 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 the 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).
	root	(Optional) Displays the root 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.
	pathcostmethod	(Optional) Displays the default path cost calculation method used.
	detail	(Optional) Displays a summary of interface information.
Defaults	Interface information summary is displayed.	
Command Modes	Privileged EXEC mode	

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW	Support for extended addressing was added.
	12.2(25)EW	Added support for the 10-Gigabit Ethernet interface.

Examples This example shows how to display spanning-tree information on the active interfaces only:

```
Switch# show spanning-tree active
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32768
             Address     0030.94fb.6401
             Cost        19
             Port        1 (FastEthernet0/1)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32768  (priority 32768 sys-id-ext 1)
             Address     0030.94fb.6401
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300

Interfaces
   Name   Port ID Prio Cost Sts Cost Bridge ID            PortID
   ------ ------- ---- ---- --- ---- -------------------- -------
   Fa0/1  128.1   128   19 FWD   19 32768 0030.94fb.6400 128.1
   Fa0/2  128.2   128   19 FWD   19 32768 0030.94fb.6400 128.2
   Fa0/3  128.3   128   19 FWD   19 32768 0030.94fb.6400 128.3
   Fa0/4  128.4   128   19 FWD   19 32768 0030.94fb.6400 128.4
   Fa0/5  128.5   128   19 FWD   19 32768 0030.94fb.6400 128.5
   Fa0/6  128.6   128   19 FWD   19 32768 0030.94fb.6400 128.6
   Fa0/7  128.7   128   19 FWD   19 32768 0030.94fb.6400 128.7
   Fa0/8  128.8   128   19 FWD   19 32768 0030.94fb.6400 128.8
   Fa0/9  128.9   128   19 FWD   19 32768 0030.94fb.6400 128.9
   Fa0/10 128.10  128   19 FWD   19 32768 0030.94fb.6400 128.10
   Fa0/11 128.11  128   19 FWD   19 32768 0030.94fb.6400 128.11
   Fa0/12 128.12  128   19 FWD   19 32768 0030.94fb.6400 128.12
   Fa0/13 128.13  128   19 FWD   19 32768 0030.94fb.6400 128.13
   Fa0/14 128.14  128   19 FWD   19 32768 0030.94fb.6400 128.14
   Fa0/15 128.15  128   19 FWD   19 32768 0030.94fb.6400 128.15
   Fa0/16 128.16  128   19 FWD   19 32768 0030.94fb.6400 128.16
   Fa0/17 128.17  128   19 FWD   19 32768 0030.94fb.6400 128.17
   Fa0/18 128.18  128   19 FWD   19 32768 0030.94fb.6400 128.18
   Fa0/19 128.19  128   19 FWD   19 32768 0030.94fb.6400 128.19
   Fa0/20 128.20  128   19 FWD   19 32768 0030.94fb.6400 128.20
   Fa0/21 128.21  128   19 FWD   19 32768 0030.94fb.6400 128.21
   Fa0/22 128.22  128   19 FWD   19 32768 0030.94fb.6400 128.22
   Fa0/23 128.23  128   19 FWD   19 32768 0030.94fb.6400 128.23
   Fa0/24 128.24  128   19 FWD   19 32768 0030.94fb.6400 128.24
   Gi0/1  129.1   128    4 FWD    4 32768 0030.94fb.6400 129.1
   Gi0/2  129.2   128    4 FWD    4 32768 0030.94fb.6400 129.2
Switch#
```

This example shows how to display spanning-tree information on the active interfaces only:

```
Switch# show spanning-tree active
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32768
             Address     0030.94fb.6401
             Cost        19
             Port        1 (FastEthernet0/1)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32768  (priority 32768 sys-id-ext 1)
             Address     0030.94fb.6401
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300

Interfaces
   Name   Port ID Prio Cost Sts Cost Bridge ID            PortID
   ------ ------- ---- ---- --- ---- -------------------- -------
   Fa0/1  128.1   128   19 FWD   19 32768 0030.94fb.6400 128.1
   Fa0/2  128.2   128   19 FWD   19 32768 0030.94fb.6400 128.2
   Fa0/3  128.3   128   19 FWD   19 32768 0030.94fb.6400 128.3
   Fa0/4  128.4   128   19 FWD   19 32768 0030.94fb.6400 128.4
   Fa0/5  128.5   128   19 FWD   19 32768 0030.94fb.6400 128.5
   Fa0/6  128.6   128   19 FWD   19 32768 0030.94fb.6400 128.6
   Fa0/7  128.7   128   19 FWD   19 32768 0030.94fb.6400 128.7
   Fa0/8  128.8   128   19 FWD   19 32768 0030.94fb.6400 128.8
   Fa0/9  128.9   128   19 FWD   19 32768 0030.94fb.6400 128.9
   Fa0/10 128.10  128   19 FWD   19 32768 0030.94fb.6400 128.10
   Fa0/11 128.11  128   19 FWD   19 32768 0030.94fb.6400 128.11
   Fa0/12 128.12  128   19 FWD   19 32768 0030.94fb.6400 128.12
   Fa0/13 128.13  128   19 FWD   19 32768 0030.94fb.6400 128.13
   Fa0/14 128.14  128   19 FWD   19 32768 0030.94fb.6400 128.14
   Fa0/15 128.15  128   19 FWD   19 32768 0030.94fb.6400 128.15
   Fa0/16 128.16  128   19 FWD   19 32768 0030.94fb.6400 128.16
   Fa0/17 128.17  128   19 FWD   19 32768 0030.94fb.6400 128.17
   Fa0/18 128.18  128   19 FWD   19 32768 0030.94fb.6400 128.18
   Fa0/19 128.19  128   19 FWD   19 32768 0030.94fb.6400 128.19
   Fa0/20 128.20  128   19 FWD   19 32768 0030.94fb.6400 128.20
   Fa0/21 128.21  128   19 FWD   19 32768 0030.94fb.6400 128.21
   Fa0/22 128.22  128   19 FWD   19 32768 0030.94fb.6400 128.22
   Fa0/23 128.23  128   19 FWD   19 32768 0030.94fb.6400 128.23
   Fa0/24 128.24  128   19 FWD   19 32768 0030.94fb.6400 128.24
   Gi0/1  129.1   128    4 FWD    4 32768 0030.94fb.6400 129.1
   Gi0/2  129.2   128    4 FWD    4 32768 0030.94fb.6400 129.2
Switch#
```

This example shows how to display spanning-tree information for the bridge:

```
Switch# show spanning-tree bridge
VLAN1
  Bridge ID  Priority    32768
             Address     0002.4a86.4401
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
VLAN2
  Bridge ID  Priority    32768
             Address     0002.4a86.4402
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
VLAN3
  Bridge ID  Priority    32768
             Address     0002.4a86.4403
             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     0030.96fc.6a00
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32768
             Address     0030.96fc.6a00
             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
---------------- -------- ---- ---- --- ---- -------------------- --------
FastEthernet2/31    129.79  128   19 FWD   0 32768 0030.96fc.6a00 129.79

VLAN2
  Spanning-tree enabled protocol ieee
  Root ID    Priority    32768
             Address     0030.96fc.6a01
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32768
             Address     0030.96fc.6a01
             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
---------------- -------- ---- ---- --- ---- -------------------- --------
FastEthernet2/31    129.80  128   19 FWD   0 32768 0030.96fc.6a00 129.80
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 EnabledCONNECTIVITY
Port 25 (FastEthernet5/9) of VLAN1 is forwarding
Designated port has priority 8192, address 0090.0c71.a400
Designated bridge has priority 32768, address 00e0.1e9f.8940
Designated port is 25, path cost 19
Timers: message age 0, forward delay 0, hold 0
BPDU: sent 0, received 0
The port is in the portfast mode
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 0030.96fc.6a00
  Configured hello time 2, max age 20, forward delay 15
  We are the root of the spanning tree
  Topology change flag not set, detected flag not set
  Number of topology changes 7 last change occurred 01:50:27 ago
          from FastEthernet2/16
  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 (FastEthernet2/31) of VLAN1 is forwarding
```

```
Port path cost 19, Port priority 128, Port Identifier 128.79.
Designated root has priority 32768, address 0030.94fc.0a00
Designated bridge has priority 32768, address 0030.94fc.0a00
Designated port id is 129.79, designated path cost 0
Timers: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state:1
BPDU:sent 6127, received 0
Switch#
```

This example shows how to display spanning-tree information for a specific bridge group:

```
Switch show spanning-tree vlan 1
QinQtoPort is disabled
BackbonePort 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
Etherchannel misconfiguration guard is enabled
QinQtoPort is disabled
BackbonePort is disabled
Default pathcost method used is short

Name              Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN1                  0        0         0        1          1
VLAN2                  0        0         0        1          1
---------------------- -------- --------- -------- ---------- ----------
               2 VLANs 0        0         0        2          2
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
QinQtoPort is disabled
BackbonePort is disabled
Default pathcost method used is short

Name              Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
               2 VLANs 0        0         0        2          2
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/Gigabit0/1       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

Command History	**Release**	**Modification**
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.2(25)EW	Added support for the 10-Gigabit Ethernet interface.

Usage Guidelines This command is not supported on systems that are configured with a Supervisor Engine 1.

In the output display of the **show spanning-tree mst configuration** command, a warning message might display. This message appears if you do not map secondary VLANs to the same instance as the associated primary VLANs. The display includes a list of the secondary VLANs that are not mapped to the same instance as the associated primary VLANs. The warning message is as follows:

```
These 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      [lab]
Revision  1792
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
### MST03  vlan mapped: 3070-3079,3181-3188
Bridge address 0002.172c.f400 priority 32771 (32768 sysid 3)
Root this switch for MST03

GigabitEthernet1/1 of MST03 is boundary forwarding
Port info port id 128.1 priority 128
cost 20000
Designated root address 0002.172c.f400 priority 32771
cost 0
Designated bridge address 0002.172c.f400 priority 32771 port
128.1
Timers: message expires in 0 sec, forward delay 0, forward transitions 1
Bpdus (MRecords) sent 3, received 0

FastEthernet2/2 of MST03 is backup blocking
Port info port id 128.196 priority 128 cost
200000
Designated root address 0002.172c.f400 priority 32771
cost 0
Designated bridge address 0002.172c.f400 priority 32771 port 4
128.196
Timers: message expires in 2 sec, forward delay 0, forward transitions 1
Bpdus (MRecords) sent 3, received 242
Switch#
```

This example shows how to display MST information for a specific interface:

```
Switch# show spanning-tree mst 3 interface FastEthernet4/5 detail
Edge port: no  guard: gbpdu (default)
(default)
Link type: point-to-point (point-to-point) bpdu filter: disable
(default)
Boundary: internal bpdu guard : disable
(default)
FastEthernet4/5 of MST03 is designated forwarding
Vlans mapped to MST03 1-2,3888,4000-4094
Port info port id 128.195 priority 128 cost
20000
Designated root address 0002.5a08.8000 priority 8193
cost 20004
Designated int master address 0002.172c.8400 priority 49152
cost 0
Designated bridge address 0002.172c.f400 priority 49152 port 16
128.195
Timers: message expires in 0 sec, forward delay 0, forward transitions 1
Bpdus (MRecords) sent 3, received 3
Switch#
```

Related Commands	Command	Description
	spanning-tree mst	Sets the path-cost and port-priority parameters for any MST 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 4500E chassis

show storm-control [*interface-id*] [**broadcast** | **multicast**]

Syntax 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

Command History	Release	Modification
	12.2(18)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.2(25)SW	Added support for the 10-Gigabit Ethernet interface.
	12.2(40)SG	Added support for the Supervisor Engine 6-E and Catalyst 4500E chassis.

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 on the switch.

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#sh show storm-control
Interface  Filter State   Upper    Lower    Current
---------  ------------  -------  -------  -------
Gi2/1      Forwarding    30.00%   30.00%   N/A
Gi2/2      Forwarding    30.00%   30.00%   N/A
Gi4/5      Forwarding    30.00%   30.00%   N/A
Switch#sh
```

This is an example of output from the **show storm-control multicast** command on a Supervisor Engine 6-E:

```
Switch# show storm-control multicast //Supervisor Engine 6-E
Interface Filter State  Broadcast Multicast Level
---------  ------------ --------- --------- -----
Fa1/1     Blocking     Enabled   Enabled   83%
Fa1/2     Blocking     Enabled   Enabled   83%
```

This is an example of output from the **show storm-control** command on a Supervisor Engine 6-E when no keywords are entered:

```
Switch# show storm-control
Interface Filter State  Broadcast Multicast Level
---------  ------------ --------- --------- -----
Fa1/1     Blocking     Enabled   Enabled   83%
Fa1/2     Blocking     Enabled   Enabled   83%
Switch#
```

This is an example of output from the **show storm-control** command for a specified interface:

```
Switch# show storm-control fastethernet1/1
Interface Filter State  Broadcast Multicast Level
---------  ------------ --------- --------- -----
Fa1/1     Forwarding   Disabled  Disabled  100%
Switch#
```

This is an example of output from the **show storm-control** command for a specified interface on a Supervisor Engine 6-E:

```
Switch# show storm-control interface fastethernet1/1
Interface Filter State  Broadcast Multicast Level
---------  ------------ --------- --------- -----
Fa1/1     Forwarding   Disabled  Disabled  83%
Switch#
```

Table 2-29 describes the fields in the **show storm-control** display.

Table 2-29 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

Command History

Release	Modification
12.1(13)E3	Support for this command was introduced on the Catalyst 6500 series switch.

Examples This example shows how to display the global MTU setting:

```
Switch# show system mtu
Global Ethernet MTU is 1500 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** | **ntc** | **password** [**page**] | **page**]

Syntax Description

bridging	(Optional) Specifies bridging-related information.
cef	(Optional) Specifies Cisco Express Forwarding-related information.
ipmulticast	(Optional) Specifies IP multicast-related information.
ntc	(Optional) Specifies CLSS and ISIS-related information.
password	(Optional) Includes password 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 informations are removed from the output.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 6500 series switch.

Usage Guidelines

Output from the **show tech-support** command may be terminated in midstream with the key combination Ctrl-shift-6. The command output is buffered so that the command terminates a few output of the current subcommand running under this command completes.

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 encrypt-port 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** commands 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 three **show** commands :

- **show version**
- **show running-config**
- **show stacks**

- **show interfaces**
- **show interfaces**
- **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 **ipmulticast** 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 mcroute count**
- **show ip mcroute**
- **show ip mcache**
- **show ip dvmrp route**

Examples For a sample display 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** command.

show udld *interface-id*

Syntax Description

interface-id	Name of the interface.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.1(3)EW	Support for this command was introduced on the Catalyst 6500 series switch.
12.2(2)EW	Added support for the 10-Gigabit Ethernet interface.

Usage Guidelines

If you do not enter an interface ID value, the administrative and operational UDLD status for all interfaces is displayed.

Examples

This example shows how to display the UDLD state for Gigabit Ethernet interface 2/2:

```
Switch# show udld gigabitethernet2/2
Interface 2/2:
---------------
Port enable administrative configuration setting: Follows device default
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement
Message interval: 60
Time out interval: 5
No neighbor cache
    Device 1
    -------
        Application time: 146
        Device ID: 1
        Current neighbor state: Bidirectional
        Device name: SSI24250D30
        Port ID: 2/2
        Neighbor echo 1 device: SAD03160954
        Neighbor echo 1 port: Gi1/1
        Message interval: 5
        Time-out interval: 5
        Device name: SAD03127T9L
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

Command History

Release	Modification
12.1(8)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.1(12c)EW	Added support for extended VLAN addresses.

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    VLAN0002                         active    Fa5/9
3    VLAN0003                         active    Fa5/9
4    VLAN0004                         active    Fa5/9
5    VLAN0005                         active    Fa5/9
6    VLAN0006                         active    Fa5/9
10   VLAN0010                         active    Fa5/9
20   VLAN0020                         active    Fa5/9
...Output truncated...
```

```
950  VLAN0950                         active    Fa5/9
917  VLAN0917                         active    Fa5/9
999  VLAN0999                         active    Fa5/9
1003 fddi-default                     act/unsup
1002 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID  MTU   Parent RingNo BridgeNo Stp  BridgeMode Trans1 Trans2
---- ----- ----- ----- ------ ------ -------- ---- ---------- ------ ------
1    enet  100001  1500  -      -      -        -    -          0      0
950  enet  100950  1500  -      -      -        -    -          0      0
917  enet  100917  1500  -      -      -        -    -        324      0
999  enet  100999  1500  -      -      -        -    -        324      0
1003 fddi  101003  1500  -      -      -        -    -          0      0
4    enet  100004  1500  -      -      -        -    -          0      0
10   enet  100010  1500  -      -      -        -    -          0      0
20   enet  100020  1500  -      -      -        -    -          0      0
50   enet  100050  1500  -      -      -        -    -          0      0

<...output truncated...>

950  enet  100950  1500  -      -      -        -    -          0      0
917  enet  100917  1500  -      -      -        -    -          0      0
999  enet  100999  1500  -      -      -        -    -          0      0
1003 fddi  101003  1500  -      -      -        -    -          0      0
1003 trcrf 101003  4472  1005   3274   -        srb  -          0      0
1004 fdnet 101004  1500  -      -      -        ieee -          0      0
1005 trbrf 101005  4472  -      15     ibm      -    -          0      0

VLAN ASLBRaps STGRaps Backup CRF
---- ------- ------- ------ ---
950  -       -       off    -
1003 7       -       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
950  VLAN0950                         active    Fa5/9
917  VLAN0917                         active    Fa5/9
4    VLAN0004                         active    Fa5/9
10   VLAN0010                         active    Fa5/9
20   VLAN0020                         active    Fa5/9
50   VLAN0050                         active    Fa5/9
.
.
.
999  VLAN0999                         active    Fa5/9
1003 fddi-default                     act/unsup
1002 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
Switch#
```

This example shows how to display the VLAN parameters for VLAN 3 only:

```
Switch#show vlan id 3

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
3    VLAN0003                         active    Fa5/9

VLAN Type  SAID  MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ----- ----- ------ ------ -------- ---- -------- ------ ------
3    enet  100003  1500  -      -      -        -    -        0      0
Switch#
```

Table 2-30 describes the fields in the **show vlan** command output.

Table 2-30 *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 vlan private-vlan

Primary Secondary Type         Ports
------- --------- ---------------  ------------------------------------------
10      100       community      Fa5/1, Fa5/2

Switch#
```

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-vlan
Primary Secondary Type         Ports
------- --------- ---------------  ------------------------------------------
10      -         primary
        100       community
```

This example show how to verify PVLAN configuration on the interface:

```
Switch# show interface fa1/2 status
Port      Name               Status       Vlan       Duplex  Speed Type
Fa1/2                        connected    pvlan serv a-full  a-100 10/100BaseTX

Switch# show interface fa1/2 status
Port      Name               Status       Vlan       Duplex  Speed Type
Fa1/2                        connected    pvlan prom a-full  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

Command History	Release	Modification
	12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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 drop
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) Display the software-cached counter values for a specific VLAN.
Defaults	This command has no default settings.
Command Modes	Privileged EXEC mode

Command History	**Release**	**Modification**
	12.1(12)E1	Support for this command was introduced on the Catalyst 6500 series switches.

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 10                                   : 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                      : 1
L2 Multicast Octets                       : 94
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 Use EXEC mode

Command History	Release	Modification
	12.1(20)EW	This command was introduced on the Catalyst 4500 series switch.

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
----------------------------------------------------------------
----------------------------------------------------------------

Fl/1/1  trunk           enabled
Fl/1/2  trunk           enabled
Fl/1/3  trunk           enabled
```

Related Commands

Command	Description
switchport mode	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 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

Command History	**Release**	**Modification**
	12.1(13)E14	Support for this command was introduced on the Catalyst 6500 series switch.

Examples

This example shows how to display information about the current internal VLAN allocation:

```
Switch# show vlan internal usage

VLAN Usage
----------
1025 -
1026 -
1027 -
1028 -
1029 Port-channel16
1030 GigabitEthernet1/2
1031 FastEthernet1/20
1032 FastEthernet1/21
1033 -
```

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 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

Command History	Release	Modification
	12.1(12)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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 ports with different MTUs, and packets might be dropped that are switched from a port with a larger 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 name 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, "Routing" 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  MismMTU(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, non-operational, and normal).
Defaults	This command has no default settings.
Command Modes	Privileged EXEC mode

Command History	**Release**	**Modification**
	12.1(8)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.2(20)EW	Support for community VLANs was added.

Usage Guidelines When the **show vlan 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       301       community         Fa5/3, Fa5/25
2       302       community
2       303       community
100     101       isolated
150     151       non-operational
        152       community
        153       community
401     402       non-operational
Switch#
```

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

Vlan Type
----  -----------
202  primary
203  isolated
204  community
305  community
306  community
307  isolated
308  normal
309  community
440  isolated
Switch#
```

Table 2-21 describes the fields in the **show vlan private-vlan** command output.

Table 2-21 *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 (**isolated** or **community**).
Ports	Indicates the ports within a VLAN.
Type	Type of VLAN: possible values are **primary**, **isolated**, community, nonoperational, 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

Command History	Release	Modification
	12.1(13)E W	This command was introduced on the Catalyst 6500 series switches.

Examples This example shows how to display a list of RSPAN VLANs:

```
Switch# 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

Command History	**Release**	**Modification**
	12.1(12)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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

```
Switch# show vmps
VQP Client Status:
-------------------
VMPS VQP Version:  1
Reconfirm Interval: 60 min
Server retry count: 3
VMPS domain server: 172.20.50.120 (primary, current)

Reconfirmation status
---------------------
VMPS Action:       No Dynamic Port
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
VMPS Changes:              0
VQP Shutdowns:             0
VQP Errors:                0
VQP Wrong Domain:          0
VQP Wrong Version:         0
VQP Insufficient Resource: 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

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 6500 series switch.

Examples This example shows how to display the VTP statistics:

```
Switch# show vtp counters
VTP statistics:
Summary advts/summary received    : 1
Subset advts received             : 2
Request advts/summary received    : 1
Summary advts/summary transmitted : 51
Subset advts transmitted          : 6
Request advts/summary 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                  15555            15614                    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        : 53
VTP Operating Mode              : Server
VTP Domain Name                 : Lab_Network
VTP Pruning Mode                : Enabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
```

```
MDS digest              : 0x8A6 0x8F 0x6D 0x6D 0xA4 0xF5 0x7C 0xE0
Configured from console by console 2d18h in 10 days 2 weeks
Local updatee is 172.20.52.3[ on interface V1 (lowest numbered VLAN interfac
e 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    : 3
Summary advertisements transmitted : 32
                   .Join Transmitted  .Join Received   Summary adrts received from
Switch#
```

Table 2-32 describes the fields in the **show vtp** command output.

Table 2-32 *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 Join transmitted.
Join Received	Number of VTP-Pruning Joins received.
Summary advrts received from non-pruning-capable device	Number of Summary advertisements received from nonpruning-capable devices.
Number of existing VLANs	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 (global 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.
	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

Command History	Release	Modification
	12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switches.

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 the 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) on 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 Interface 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

Command History	Release	Modification
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switches.

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 ifIndex 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 notification.
	removal	(Optional) Controls the SNMP flash removal trap notification.
	fru-ctrl	(Optional) Controls the SNMP entity FRU control trap notification.
	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 notification.
	threshold	(Optional) Controls the SNMP MAC threshold trap notification.

Defaults SNMP notifications are disabled.

Command Modes Global configuration mode

Command History	Release	Modification
	12.1(12)E	Support for this command was introduced on the Catalyst 4500 series switch.
	12.2(17d)SX	Support for MAC notification was added.

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 inform 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 FlashInsertion trap notifications.
  - **removal**—Controls the SNMP FlashRemoval trap notifications.
- **frame-relay**—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.
- **stpx**—Controls all the traps from the CISCO-STP-EXTENSIONS-MIB.
- **vlancore**—Controls SNMP VLAN control trap notifications.
- **vlanlistin**—Controls SNMP VLAN deleted trap notifications.
- **vtp**—Controls the VTP traps from the CISCO-VTP-MIB.

Examples

This example shows 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 shows 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(s) or direct port-security violations due to restrict mode. The following example shows how to enable traps for port-security on port 5/1:

```
Switch(config)# snmp-server enable traps port-security trap-rate 5
Switch(config)#
```

Related Commands

Command	Description
clear 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 notifications.
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

Command History	Release	Modification
	12.1(12b)W	Support for this command was introduced on the Catalyst 4500 series switches.

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 commandoes 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 running device using ifIndex 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 Interface MIB (IF-MIB) that persist across reboots (ifIndex persistence) 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 decompressed 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.

Command History	Release	Modification
	12.2(54)SG	Support for this command was introduced on the Catalyst 4500 series switches.

Usage Guidelines This command is hidden on Supervisor Engine V and later supervisor engines because the ifIndex table is always in a compressed format on those supervisor engines.

At boosing, if the mount-ifindex-table.gz file (the ifIndex table ina compressed format) is present on a Supervisor Engine II+, Supervisor Engine III, or Supervisor Engine IV, the **snmp-server ifindex persist compress** command is automatically run even if the startup-config file does not have this configuration.

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 to be interfaces MIB (IF-MIB) that persist 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

Command History

Release	Modification
12.2(13)SG	Support for this command was introduced on the Catalyst 4500 series switch.

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
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.
show mac address-table notification	Displays the MAC address table notification status and history.
snmp-server enable traps	Enables SNMP notifications.

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

Command History	Release	Modification
	12.1(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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

Command History	**Release**	**Modification**
	12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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 correctly used.

When configuring a port (trunk or 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 in 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)# spanning-tree bpdufilter enable
Switch(config)#
```

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 errDisable 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 **no** 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—1

Command Modes Interface configuration mode

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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 that interface:

```
Switch(config)# interface fastethernet 3/1
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

Command History	Release	Modification
	12.1(8)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines When an EtherChannel guard misconfiguration is detected, this message is displayed:

```
%PAGP/SPAN-2-CHNL_MISCFG:Channel loop due to etherchannel misconfig of interface
Po<n> 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 the **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

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines Releases 12.1(12)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

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.1(12c)EW	Loop guard support was added.

Examples

This example shows how to enable root guard:

```
Switch(config-if)# spanning-tree guard root
Switch(config-if)#
```

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

Command History

Release	Modification
12.2(25)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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)# interface fastethernet 6/1
Switch(config-if)# spanning-tree link-type shared
Switch(config-if)#
```

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

Command History

Release	Modification
12.1(11b)E	Support for this command was introduced on the Catalyst 4500 series switch.

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.

Inconsistent 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

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(19)EW	Support for the **rapid-pvst** keyword.

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 MST instance (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

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

The higher **cost** port 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

Command History	Release	Modification
	12.1(11)EW	Support for this command was introduced on the Catalyst 6500 series switch.

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 and lists the secondary VL AN s 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:
->5
```

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 can apply the new configuration to the switch by exiting from the MST configuration submode without committing any changes to the switch position by using **abort** keyword.

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 CFG: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 time is set for 15 seconds.
Command Modes	Global configuration mode

Command History	**Release**	**Modification**
	12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples

This example shows how to set the forward-delay time:

```
spanning-tree mst forward-time 20
```

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 timer is set for 2 seconds.

Command Modes

Global configuration mode

Command History

Release	Modification
12.2(31)SGW	Support for this command was introduced on the Catalyst 4500 series switch.

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 5
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 time 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

Command History	**Release**	**Modification**
	12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples

This example shows how to set the max-age timer:

```
spanning-tree mst max-age 40
```

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 *hopcount*

no spanning-tree mst max-hops

Syntax Description

hopcount	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

Command History

Release	Modification
12.2(25)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples

This example shows how to set the number of possible hops in the region before a BPDU is discarded to 25:

```
Switch(config)# spanning-tree mst max-hops 25
Switch(config)#
```

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 inter-value 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

Command History

Release	Modification
12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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 mst 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 0 root primary
Switch(config)#
```

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

Command History

Release	Modification
12.1(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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:

```
Switch(config)# spanning-tree pathcost method long
Switch(config)#
```

This example shows how to set the path cost calculation method to short:

```
Switch(config)# spanning-tree pathcost method short
Switch(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 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

Command History

Release	**Modification**
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.1(12c)EW	The **disable** and **trunk** options were added.

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 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.

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 set 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

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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 versus globally. 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

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

Caution Be careful when using this command. You should 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 on 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

Command History	Release	Modification
	12.1(1)a EW	Support for this command was introduced on the Catalyst 6500 series switch.

Usage Guidelines

Caution Be careful when using this command. You should 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 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.

You can set 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

Command History	**Release**	**Modification**
	12.1(19)xEW	Support for this command was introduced on the Catalyst 4500 series switch.

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)# interface fastethernet 2/1
Switch(config-if)# spanning-tree port-priority 0
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 (in packets per second) at which update packets are sent; valid values are from 0 to 65536.

Defaults

The default settings are as follows:

- Disabled.
- Maximum update rate is 150.

Command Modes Global configuration mode

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 6500 series switch.

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 instance are also increased by 3000.

When spanning tree detects that the root interface has failed, the UplinkFast feature causes an immediate switch over to an alternate root interface, transitioning the new root interface directly to the forwarding state. During this time, a topology change notification is sent. To minimize the disruption caused by the topology change, a station address update packet (dummy CD-CP-CP-CP) for each station address in the forwarding table is sent 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.
	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 root

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(2)EW	Support for this command was introduced on the Catalyst 6500 series switch.
12.1(3)XW	Support for extended addressing was added.

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, the 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 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 only.

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 specify the max 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

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.2(20)EW	Support for auto negotiating specific speeds added.

Usage Guidelines

Table 2-33 lists the supported command options by interface.

Table 2-33 *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.	Is only applicable to Gigabit Ethernet ports.
10/100/1000	**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 (ports with no subset numbering, 1000 [e.g. **speed auto 10 1000** or **speed auto** on 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, 10or 100 Mbps), make sure that you configure the connecting interface speed command to a matching speed but do not set 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 4500s switches 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 reconfigure the interface during the reconfiguration.

Table 2-34 describes the system's performance for different combinations of the duplex and speed modes. The **speed duplex** command that is configured with the specified **speed** command produces the resulting system action.

Table 2-34 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 full	**speed 10**	Forces 10 Mbps and full duplex
duplex half	**speed 100**	Forces 100 Mbps and half 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 set the interface speed to 100 Mbps on the Fast Ethernet interface 5/4:

```
Switch>enable | interface fastethernet 5/4
Switch>enable | speed 100
```

This example shows how to allow Fast Ethernet interface 5/4 to autonegotiate the speed and duplex mode:

```
Switch>enable | interface fastethernet 5/4
Switch>enable | 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>enable | interface gigabitethernet 1/1
Switch>enable | speed auto 10 100
```

This example shows how to limit the speed negotiation to 100 Mbps on the Gigabit Ethernet interface 1/1:

```
Switch>enable | interface gigabitethernet 1/1
Switch>enable | 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 controllers (refer to Cisco IOS documentation)	Displays controller information.
show interfaces	Displays traffic on a specific interface.

storm-control

To enable broadcast storm control on a port and to specify what traffic modes (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*] **|** **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* [*lower 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. Blocks 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 level.
	action Directs the switch to take action when a storm occurs on a port. **shutdown** 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

Command History	Release	Modification
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	7.1.2(2.0)SG	Support for the Supervisor Engine 6-E and Catalyst 4900M chassis is introduced.

Usage Guidelines Enter **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 Catalyst4500 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 to 100 percent for the specified traffic type.
- Use the **no** form of this command.

The lower level is signaled for the interfaces that perform storm control in the hardware.

Note The **lower level** keyword does not apply to the Supervisor Engine 6-E and Catalyst 4500E chassis implementations.

Examples

This example shows how to enable broadcast storm control on a port with a 75.67 percent rising suppression level:

```
Switch(config)#interface gigabitethernet 3/1
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 Global configuration mode
Interface configuration mode on a Supervisor Engine 6-E and Catalyst 4500E chassis

Command History	Release	Modification
	12.2(25)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.2(40)SG	Support for the Supervisor Engine 6-E and Catalyst 4500E chassis is introduced.

Usage Guidelines This command prompts the hardware to filter multicast packets if it is already filtering broadcast packets.

The Supervisor Engine 6-E and Catalyst 4500E chassis supports per-interface 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(config)#storm-control
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#storm-control broadcast include multicast
Switch(config)#end
```

This example shows how to enable per-port Multicast storm control on a Supervisor Engine 6-E:

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface fastethernet3/4
Switch(config-if)#storm-control broadcast include multicast
Switch(config)#end
```

Related Commands

Command	Description
show storm-control	Enables 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

Command History	Release	Modification
	12.2(52)SG	Support was introduced on the Catalyst 4500 series switches.

Usage Guidelines To enter profile call-home configuration submode, use the **profile** command in call-home configuration mode.

Examples This example shows 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.

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 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

Command History	**Release**	**Modification**
	12.2(52)SG	Support was introduced on the Catalyst 4500 series switches.

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 cisco
Switch(cfg-call-home-profile)# subscribe-to-alert-group configuration periodic weekly
Tuesday 21:16
```

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.

Command	Description
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 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 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

Command History

Release	Modification
12.2(52)SG	Support was introduced on the Catalyst 4500 series switches.

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(config)# call-home
Switch(cfg-call-home)# profile alert
Switch(cfg-call-home-profile)# subscribe-to-alert-group diagnostic severity normal
```

Related Commands

Command	Description
destination address	Configure the destination e-mail address or URL to which Call Home messages will be sent.
destination message-size-limit bytes	Configure a maximum destination message size for the destination profile.
destination preferred-msg-format	Configure 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 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 and 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

Command History

Release	Modification
12.2(52)SG	Support was introduced on the Catalyst 4500 series switches.

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 cisco
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	Configure the destination e-mail address or URL to which Call Home messages will be sent.
destination message-size-limit bytes	Configure a maximum destination message size for the destination profile.
destination preferred-msg-format	Configure 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 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 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

Command History

Release	Modification
12.2(52)SG	Support was introduced on the Catalyst 4500 series switches.

Usage Guidelines

To error 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 cisco
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.

Command	Description
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 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 files 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 (Syslog log level 5).
normal	(Optional) Specifies returning to a normal state (Syslog log level 6).
debugging	(Optional) Specifies a debugging message (Loglevel severity).

Defaults

normal

Command Modes

cfg-call-home-profile

Command History

Release	Modification
12.2(52)SG	Support was introduced on the Catalyst 4500 series switches.

Usage Guidelines

To enter 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 contains 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 state
Switch(cfg-call-home-profile)# subscribe-to-alert-group syslog severity notification
pattern "SYSTEM"
```

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 profile	Enables the message transport method.
show call-home	Displays the current Call Home configuration submode settings.
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 where the interface is in access mode; valid values are from 1 to 1005.
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 1005.
dot1p	(Optional) Specifies that the PVID packets are tagged as priority.
none	(Optional) Specifies that the telephone and voice VLAN do not communicate.
untagged	(Optional) Specifies the untagged PVID 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

Command History

Release	Modification
12.1(11)EW	Support for this command was introduced on the Catalyst 6500 series switch.
12.1(11)EW	Support for voice VLAN was added.

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.

When you set the **of-noticlient access** command over 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 set 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 it 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 nonegotiate
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 when an 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 correspond to the platform or the interface hardware.
- All VLAN lists include all VLANs.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(11)b EW	Support for this command was introduced on the Catalyst 6500 series switch.
12.1(12)E W	Support for VPWS was added.

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 entered the **no switchport** command for the interface.

Entering the **no switchport** command shuts down the port and then enables 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.

If your system is configured with a Supervisor Engine I, valid values for *vlan-id* are from 1 to 1005. If your system is configured with a Supervisor Engine II, valid values for *vlan-id* are from 1 to 4094. Extended-range VLANs are not supported on systems configured with a Supervisor Engine I.

Examples

This example shows how to cause the port interface to stop operating as a Cisco-routed port and convert to a Layer 2-switched interface:

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

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-if)# switchport access vlan 2
Switch(config-if)#
```

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

Command History	**Release**	**Modification**
	12.2(17d)SXB	Support for this command was introduced on the Catalyst 6500 series switches.

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 2-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* **switchport** 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 gi1/1/4 switchport autostate exclude
Switch(config)#int gi1/1/4
```

This example shows how to include a port in the VLAN interface link-up calculation:

```
Switch(config)#int gi1/1/4 no switchport autostate exclude
Switch(config)#int gi1/1/4
```

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

■ Switchport access vlan

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

Command History

Release	Modification
12.1(12B)W	Support for this command was introduced on the Catalyst 4500 series switch.

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-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 reset 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 port with a valid PVLAN trunk association become active host private VLAN trunk port.
private-vlan promiscuous	Specifies that the ports with a valid PVLAN mapping become active promiscuous port.
private-vlan trunk promiscuous	Specifies that the ports with valid PVLAN trunk mapping become active promiscuous trunk port.
private-vlan trunk secondary	Specifies that the ports with a valid PVLAN trunk association become active host private VLAN trunk port.

Defaults

Link converts to a trunk link.
dot1q-tunnel port.is disabled.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.2(18)EW	Support was added for configuring dot1q-tunnel ports.
12.2(31)SG	Support was added for trunk promiscuous ports.

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**, **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>enable | Switch#enable
Switch>(enable) | Switch#(enable) set/clear mode dynamic desirable
```

This example shows how to set a port to PVLAN host mode:

```
Switch>enable | Switch#enable
Switch>(enable) | Switch#(enable) set/clear mode private-vlan host
```

This example shows how to set a port to private VLAN trunk:

```
Switch>enable | Switch#enable
Switch>(enable) | Switch#(enable) set/clear mode private-vlan trunk
```

This example shows how to configure a port for an 802.1Q tunnel port:

```
Switch>enable | Switch#enable
Switch>(enable) | Switch#(enable) set/clear mode dot1q-tunnel
```

This example shows how to configure a promiscuous trunk port:

```
Switch>enable | Switch#enable
Switch>(enable) | Switch#(enable) set/clear mode private-vlan trunk promiscuous
```

This example shows how to configure an isolated trunk port:

```
Switch>enable | Switch#enable
Switch>(enable) | Switch#(enable) set/clear mode private-vlan trunk
```

```
Switch>enable | Switch#enable
Switch>(enable) | Switch#(enable) set/clear mode private-vlan trunk secondary
```

You can verify your settings by entering the **show interfaces switchport** command and examining information in the Administrative 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#conf terminal
Enter configuration commands.
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: Off
Access Mode VLAN:1 (default)
Trunking Native Mode VLAN:1 (default)
Administrative Private-vlan
Administrative Private-vlan Host-association:none
Administrative Private-vlan Promiscuous-mapping:200 (VLAN0200) 2 (VLAN0002)
Administrative Private-vlan trunk native VLAN:none
Administrative Private-vlan trunk Encapsulation:dot1q
Administrative Private-vlan trunk Normal VLANs:none
Administrative Private-vlan trunk Private VLANs:none
Operational Private-vlan:
Trunking VLANs Enabled:ALL(1-4094)
Pruning VLANs Enabled:2-1001
Capture Mode Disabled
Capture VLANs Allowed:ALL
```

This example shows how to configure interface FastEthernet 5/3 as a PVLAN host port and verify the configuration:

```
Switch#conf terminal
Enter configuration commands.
Switch(config)# interface fastethernet 5/3
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 5/3 switchport
Name: Fa5/3
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
Administrative Private-vlan
Administrative Private-vlan
  Host Association: 202 (VLAN0202) 440 (VLAN0440)
  Promiscuous Mapping: none
  Trunk encapsulation : dot1q
  Trunk mapping:none
Operational private-vlan:(
  202 (VLAN0202) 440 (VLAN0440)
Administrative Pruning VLANs:
Pruning VLANs Enabled: 2-1001
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# 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 0
  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 (VLAN0002) 501 (VLAN0501)
  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(config-if)#
```

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: 5-6,10
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings:
  10 (VLAN0010) 101 (VLAN0101)  301 (VLAN0301)
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
Appliance trust: none
Switch(config)#
```

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 mode status 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 parameters to their default state, use the **no** form of this command.

switchport port-security [aging | static | time time | type | absolute | inactivity] | [limit rate | maximum value | mac-address mac-address | vlan [access | voice] | mac-address sticky [mac-address] | jam mac-address | jam access | vlan access | vlan [access | voice] | violation {protect | restrict | shutdown | shutdown vlan}]

no switchport port-security [aging | static | time time | type | absolute | inactivity] | [limit rate | maximum value | mac-address | mac-address mac-address | vlan [access | voice] | mac-address sticky [mac-address] | jam mac-address | jam access | vlan access | vlan [access | voice] | violation {protect | restrict | shutdown | shutdown vlan}]

Syntax Description		
	aging	(Optional) Specifies aging for port security.
	static	(Optional) Enables 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*	(Optional) Specifies the rate limit for bad packets. This rate limit an update to the port's *Bad packets DROP accepting security* mode is enabled as filtering on the BP and MAC address.
	N *rate*	(Optional) Supplies a rate limit (N) or indefinite (**none**) *rate*.
	mac-address *mac-address*	(Optional) Specifies a secure MAC address for the interface; a 48-bit MAC address. You can add additional secure MAC addresses up to the maximum value for is configured.
	sticky	(Optional) Configures the dynamic addresses as sticky on the interface.
	vlan access	(Optional) Identifies the access VLAN. Specifies the access VLANs.
	vlan voice	(Optional) Defines the secure MAC addresses for voice VLANs.
	maximum *value*	(Optional) Sets the maximum number of secure MAC addresses for the interface. Valid values are from 1 to 3072. The default setting is 1.
	violation	(Optional) Sets the security violation mode and enables the selected port security violation.
	restrict	(Optional) Sets the security violation restrict mode. In this mode, a port security violation restricts data and causes the security violation counter to increment.

switchport port-security

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 time is 0 minutes.
- All secure addresses on this port age out immediately after they are removed from the secure address list.

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.
12.1(19)EW	Extended to include DHCP snooping security enhancement.
12.2(18)EW	Added support for sticky interfaces.
12.2(31)SG	Added support for sticky port security.
12.2(52)SG	Added support for per-VLAN error-disable detection.

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 first EtherChannel or Gigabit EtherChannel port group.

When a secure ports in the enter-disabled state, you can remove it from this state by entering the **errdisable recovery** [**cause** *pseudo-reason*] global configuration command, or you can manually re-enable it by entering the **shutdown** and **no shut** **down** interface configuration command. 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 time lapses, the secure addresses are deleted.

To allow continuous access to a limited number of secure addresses, set the aging type as **inactivity**. This 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 sticky. You can also specify a specific MAC address to be a sticky address by entering the **sticky** keyword next to it.

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 **no** form 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)# switchport port-security aging type inactivity
Switch(config-if)#
```

The following example shows how to configure size 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 size 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 2/12
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 2/12
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address 1000.2000.3000
Switch(config-if)#
```

This example shows how to make all MAC addresses learned on Fast Ethernet port 12 sticky:

```
Switch(config)# interface fastethernet 2/12
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)#
```

This example shows how to make MAC address 1000.2000.3000 sticky on Fast Ethernet port 12:

```
Switch(config)# interface fastethernet 2/12
Switch(config-if)# switchport port-security mac-address sticky 1000.2000.3000
Switch(config-if)#
```

This example shows how to disable the sticky feature on Fast Ethernet port 12:

```
Switch(config)# interface fastethernet 2/12
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 **vlan [access | voice]** keywords are not supported.

This example shows how to configure sticky MAC address on for voice and data VLANs on Fast Ethernet interface 5/1 and to verify the configuration:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fa5/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport voice vlan 10
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.abcd vlan voice
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.0065 vlan access
Switch(config-if)# end
```

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 5/1 and to verify the configuration:

```
Switch# end
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fa5/1
```

```
Switch(config)#int switchport mode access
Switch(config)#int switchport port-security
Switch(config)#int switchport port-security mac-address sticky
Switch(config)#int switchport port-security maximum 1 vlan voice
Switch(config)#int switchport port-security maximum 1 vlan access
Switch(config)#int end
```

This example shows how to configure a port to shut down only the VLAN if a violation occurs:

```
Switch(config)# interface gigabitethernet 5/1
Switch(config)# switchport port-security violation shutdown vlan
```

Note Sending traffic to the port 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

Command History

Release	Modification
12.1(11)EW	Support for this command was introduced on the Catalyst 6500 series switch.
12.2(18)EW	Support for community VLANs was added.

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-if)# switchport private-vlan association trunk 18 20
Switch(config-if)#
```

This example shows how to remove the private VLAN association from the port:

```
Switch(config-if)# no switchport private-vlan association trunk 18
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 10
Switch(config-if)# switchport private-vlan trunk allowed vlan 10, 5-4
Switch(config-if)# switchport private-vlan association trunk 3 301
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 5
  Administrative private-vlan mapping: none
  Administrative private-vlan trunk native VLAN: 10
  Operational 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 (VLAN0003) 301 (VLAN0301)
  Administrative private-vlan trunk mappings: none
  Operational private-vlan: none
  Trunking VLANs Enabled: ALL
  Trunking VLANs Enabled: 2-1001
  Capture Mode Disabled Capture VLANs Allowed: ALL

  Unknown unicast blocked: disabled
  Unknown multicast blocked: disabled
  Appliance trust: none
Switch#show(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 in 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 this 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

Command History

Release	Modification
12.1(8)EW	Support for this command was introduced on the Catalyst 4500 series switch.
12.1(12c)EW	Support for extended addressing was added.

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 made 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 a PVLAN host port and verify the configuration:

```
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)#exit
Switch(config)#interface fastethernet 5/1 switchport
Name: 5/1
Switchport: Enabled
Administrative Mode: private-vlan host
Operational Mode: private-vlan host
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
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: 202 (VLAN0202) 440 (VLAN0440)
  Promiscuous Mapping: none
  Trunk encapsulation: dot1q
  Trunk vlans:
Operational private-vlan(s):
  202 (VLAN0202) 440 (VLAN0440)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
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 mapping from the primary VLAN, use the form of the command.

switchport private-vlan mapping {*primary-vlan-id*} {*secondary-vlan-list*} | {**add** *secondary-vlan-list*} | {**remove** *secondary-vlan-list*}

switchport private-vlan mapping {*primary-vlan-id*} | {**add**} | {**remove**} *secondary-vlan-list*

no switchport private-vlan mapping {**trunk**}

primary-vlan-id	Number of the primary VLAN of the private VLAN relationship; valid values are from 2 to 1001 and from 1006 to 4094.
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 VLANs.
trunk	Maps the trunks secondary VLANs to the primary VLAN.

Syntax Description

Defaults

Private VLAN mapping is disabled.

Command Modes

Interface configuration mode

Command History	Release	Modification
	12.1(19)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.1(20)EW	Support for extended addressing was added.
	12.2(20)EW	Support for community VLAN was added.
	12.2(25)EW	Support for trunk VLAN was added.

Command History

Usage Guidelines

There is no runtime 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 *does* or *will*, for example, one thousand secondary VLANs could map to one primary VLAN, or one thousand secondary VLANs could map 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 as a pair:

```
Switch(config)#int switchport private-vlan mapping 10 20
Switch(config)#int
```

This example shows how to add a VLAN to the mapping:

```
Switch(config)#int switchport private-vlan mapping 10 add 21
Switch(config)#int
```

This example shows how to add a range of secondary VLANs to the mapping:

```
Switch(config)#int switchport private-vlan mapping 10 add 22-24
Switch(config)#int
```

This example shows how to add a range of secondary VLANs to the trunk mapping:

```
Switch(config)#int switchport private-vlan mapping trunk 10 add 22-24
Switch(config)#int
```

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 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:Off
Access Mode VLAN:1 (default)
Trunking Native Mode VLAN:1 (default)
Voice VLAN:none
Administrative Private VLAN Host Association:none
Administrative Private VLAN Mapping:200 (VLAN0200) 2 (VLAN0002)
Private VLAN Trunk Native VLAN:none
Administrative Private VLAN Trunk Encapsulation:dot1q
Administrative Private VLAN Trunk Normal VLANs:none
Administrative Private VLAN Trunk Private VLANs:none
Operational Private VLANs:
  200 (VLAN0200) 2 (VLAN0002)
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(config)# interface fastethernet 5/2
Switch(config-if)# switchport mode trunk
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 10, 5-4
Switch(config-if)# switchport private-vlan mapping trunk 5 101, 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: 5-4,10
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings:
  5 (VLAN0005) 101 (VLAN0101)  102 (VLAN0102)
Operational private-vlan:
  5 (VLAN0005) 101 (VLAN0101) 102 (VLAN0102)
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
Switch(config)#
```

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 (Optional) Adds 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

Command History	Release	Modification
	12.1(11)EW	Support for this command was introduced on the Catalyst 6500 series switch.

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 mapping trunk** command to configure a port that can carry private VLANs on 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(config)# interface fastethernet 5/2
Switch(config-if)# switchport 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
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 (301) 10 (100)
    Administrative private-vlan trunk mappings: none
    Operational private-vlan: none
    Operational Normal VLANs: none
    Operational private-vlan:
    Protocol VLAN Enabled: 2-1001
    Capture Mode Disabled Capture VLANs Allowed: ALL

    Unknown unicast blocked: disabled
    Unknown multicast blocked: disabled
    Appliance trust: none
Switch(config-if)#
```

This example shows how to configure interface FastEthernet 5/2 as a promiscuous trunk port and to verify the configuration:

```
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 41, 5-4
Switch(config-if)# switchport private-vlan mapping trunk 3 100
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: 4,5
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings:
  3 (VLAN0041) 100 (VLAN0100)
Operational private-vlan:
  3 (VLAN0041) 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
Protected: false
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 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

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.
	12.2(18)EW	Removed **vlan id** keyword.

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)# switchport private-vlan trunk native vlan tag
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 trunk

To set the trunk characteristics when an interface is in trunking mode, use the **switchport trunk** command. To reset all of the trunking characteristics back to the original defaults, use the **no** form of this command.

switchport trunk encapsulation {**isl** | **dot1q** | **negotiate** }

no switchport trunk encapsulation

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

encapsulation isl	Sets the trunk encapsulation format to ISL.
encapsulation dot1q	Sets the trunk encapsulation format to 802.1Q.
encapsulation negotiate	Specifies that if DISL and DTP negotiation do not resolve the encapsulation, ISL is the encapsulation format.
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 eligible 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:

- The encapsulation type is dependent on the platform or interface hardware.
- The access VLANs and trunk interface native VLANs are a default VLAN that corresponds to the platform or the interface hardware.
- All VLAN lists include all VLANs.
- Native VLAN tagging is enabled on the port if enabled globally.

Command Modes

Interface configuration mode

Command History	Release	Modification
	12.1(11b)EW	Support for dot1ucmulti was introduced on the Catalyst 6500 series switch.
	12.1(13)EW	Support for extended addressing was added.
	12.2(18)EW	Support for native VLAN tagging was added.

Usage Guidelines

Then keyword specifies the **all**, **none** | **add** | **except** | **remove** | **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 not 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_atom* is either a single VLAN number from 1 to 4094 or a continuous range of VLANs described by two VLAN numbers (the lesser one first), separated by a hyphen.

The **switchport trunk encapsulation** command is supported only for platforms and interface hardware that can support both ISL and IEEE 802.1Q formats.

If you enter the **negotiate** keywords, and DISL and DTP negotiation do not resolve the encapsulation format, ISL is the selected format. The **no** form of this command reverts the trunk encapsulation format back to the default.

Then form of the **native** vlan command resets the native mode VLAN to the appropriate default VLAN for the device.

Then form of the **allowed vlan** command resets the list to the default list, which allows all VLANs.

Then form of the **pruning vlan** command resets 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 every VLAN in the network can cause spanning-tree loops. We recommend that you leave spanning-tree enabled on the native VLAN of an 802.1Q trunk. If this is not possible, disable 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 information on the native VLAN of the trunk. Cisco switches stop sending the BPDUs on the native VLAN of the trunk only if spanning-tree is disabled on the native VLAN of the trunk or if the native VLAN is one of the VLANs that are not exchanged in the reserved 802.1d spanning-tree multicast MAC address (01-80-C2-00-00-00). The BPDUs on all other VLANs (with the exception of those VLANs that are not exchanged in the reserved 802.1d spanning-tree multicast MAC address (01-80-C2-00-00-00). The BPDUs on all other VLANs (with the exception of those VLANs that are not exchanged in the reserved STP multicast MAC address (01-00-0c-cc-cc-cd).

- Non-Cisco 802.1Q switches maintain only 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 non-Cisco switch and the native VLAN spanning tree of the Cisco switch combine to form a single spanning-tree topology known as CIST.
- Because Cisco switches transmit BPDUs to the SNAP multicast MAC address on the VLANs other than the native VLAN, the non-Cisco switches do not recognize these frames as BPDUs 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 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 ISL trunks or through the access ports. This action causes the switch to place the ISL trunk port or access port into the spanning-tree "port inconsistent" state and no traffic will pass through the port.

Define these guidelines for native VLAN tagging:

- The **no switchport trunk native tag** command disables the native VLAN tagging operation on a port. This overrides the global tagging configuration.
- The **switchport trunk native tag** command can be used to override tagging on a disabled port.
- The **no** option is used 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 trusting mode:

```
Switch>enable|1|6|
Switch>enable|1|6|switchport trunk encapsulation dot1q
Switch>enable|1|6|
```

This example shows how to enable 802.1Q tagging on a port:

```
Switch>enable|1|6|switchport trunk native vlan tag
Switch>enable|1|6|
```

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>enable|1|6|interface gigabitethernet|1|
Switch>enable|1|6|switchport trunk encapsulation dot1q
Switch>enable|1|6|switchport mode trunk
Switch>enable|1|6|switchport port-security
Switch>enable|1|6|switchport port-security maximum 3
```

This example shows how to configure a secure MAC-address on Gigabit Ethernet port 1 in a specific VLAN or range of VLANs:

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport port-security
Switch(config-if)# vlan range 2-4
Switch(config-if-vlan-range)# 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 mode trunk
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 mac-address sticky
Switch(config-if)# vlan range 2-4
Switch(config-if-vlan-range)# port-security mac-address 1.1.1
Switch(config-if-vlan-range)# port-security mac-address sticky 1.1.2
Switch(config-if-vlan-range)# port-security mac-address sticky 1.1.3
```

You can verify your settings by using the **show port-security interface vlan** privileged EXEC command.

Related Commands	Command	Description
	show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.

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

Command History	**Release**	**Modification**
	12.1(11)EW	Support for this command was introduced on the Catalyst 6500 series switch.

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 to18 on model WS-X6418-GB 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 within total Ethernet frame size of up to 1600 bytes.

Examples

This example shows how to set the MTU size to 1550 bytes:

```
Switch# configure 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# configure 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

Command History

Release	Modification
12.2(25)SG	Support for this command on the Catalyst 4500 series switch.

Usage Guidelines The TDR test is supported on Catalyst 4500 series switches running Cisco IOS Release 12.2(25)SG 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 diagnostics 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 fa6/1
Switch#
```

This example shows the message that displays when the TDR test is not supported on a module:

```
Switch#test cable-diagnostics tdr fa6/1
%C4K-IOSD-MSG_NOSUPPORT-4-TDRUNSUPPORTEDMODULE: Active radio
diag tdr test is not supported on this module
Switch#
```

Note The **show cable-diagnostic 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 "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 switch interface.
source-mac-address	MAC address of the trace route from broadcast 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 would take from source to destination. The destination switch, valid VLAN (from 1 to 4094). Use source ending mac.
detail	(Optional) Displays detailed information.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.1(15)SW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

Do not use loading zeros when entering a VLAN ID.

The Layer 2 traceroute feature is available on these switches:

- Catalyst 2950 switches running Release 12.1(12c)EA1 or later
- Catalyst 3550 switches running Release 12.1(12c)EA1 or later
- Catalyst 4500 series switches running Catalyst operating system Release 6.2 or later for the supervisor engine
- Catalyst 4500 series switches running Release 12.1(13)EW or later
- Catalyst 5000 family switches running Catalyst operating system Release 6.1 or later for the supervisor engine
- Catalyst 6500 series switches running Catalyst operating system Release 6.1 or later for the supervisor engine

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 less than one.

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 between the specified source and destination addresses belonging 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 more 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 0000.0201.0801
Source 0000.0201.0601 found on vlan2(0.0.0.0) [2/-2/-4/4]
vlan2 (2.2.2.4) vlan3 vlan3:5
        2/-2/-4/4 ---> 2/-2/-4/4
vlan3 (2.2.3.1)  1 /  [ ] ---> [ ] / [ ]
        2/-2/-2/2 ---> 4/4/0 vlan4:1
Destination 0000.0201.0801 found on vlan4(0.0.0.0) [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 0000.0201.0801 detail
Source 0000.0201.0601 found on vlan2(0.0.0.0) [2/-2/-4/4]
vlan2 (2.2.2.4) vlan3 vlan3:5 [auto, auto]
        fa6/1 [auto, auto] vlan3:5 [auto, auto]
vlan3 ( 60.0.0.60) 2/ [ 2.2.3.1 ]
        fa6/1 [auto, auto] vlan3:5 [auto, auto]
vlan3 ( 60.0.0.60) 2/ 2.2.3.1 ]
        gi2/1 [auto, auto] vlan3:2 [auto, auto]
vlan3 (2.2.3.1)  1 /  [ ] ---> [ ] / [ ]
        gi2/1 [auto, auto] vlan4:1 [auto, auto]
Destination 0000.0201.0801 found on vlan4(0.0.0.0) [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 0001.0201.0501 0000.0201.0801 detail
Source 0001.0201.0501 connected to, tracing source
vlan2 (2.2.2.4) vlan3 vlan3:5 [auto, auto]
vlan3 ( 60.0.0.60) 2/ [ 2.2.3.1 ]
        fa6/1 [auto, auto] vlan3:5 [auto, auto]
vlan3 ( 60.0.0.60) 2/ 2.2.3.1 ]
        gi2/1 [auto, auto] vlan3:2 [auto, auto]
vlan3 (2.2.3.1)  1 /  [ ] ---> [ ] / [ ]
        gi2/1 [auto, auto] vlan4:1 [auto, auto]
Destination 0000.0201.0801 found on vlan4(0.0.0.0) [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 0000.0011.1111 0000.0201.0201
Source 0000.0011.1111 destination was found
Layer2 trace aborted.
Switch#
```

This example shows the Layer 2 path when the source and destination devices are in different VLANs:

```
Switch# traceroute mac 0000.0201.0408 0000.0201.0201
Error:Source and destination macs are in 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 0000.0201.0408 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 0000.0201.0408 0000.0201.0201
Error:Dest 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 fastethernet6/1 0000.0201.0408 Interface fastethernet6/5 0000.0201.0201
Source 0000.0201.0408 found on cat6k2(172.20.52.91) [0.0.0.0]
cat6k2 (0.0.0.0) vlan 999
cat6k2          [2.2.5.1          ]  :  Fa6/5 :cdp2/5
cat6k1          [2.2.1.1          ]  :  Gi5/1 :cdp2/2
cat6k3          [2.2.2.2          ]  :  Gi5/1 :cdp2/1
Destination 0000.0201.0201 found on cat6k3(172.20.52.34) [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 that is taken by the 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.

Syntax Description

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.1(12)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

The Layer 2 traceroute feature is available on these switches:

- Catalyst 2950 switches running Release 12.1(12c)EA1 or later
- Catalyst 3550 switches running Release 12.1(12c)EA1 or later
- Catalyst 4500 series switches running Catalyst operating system Release 6.2 or later for the supervisor engine
- Catalyst 6500 series switches running Release 12.1(2)EW or later
- Catalyst 6500 family switches running Catalyst operating system Release 6.1 or later for the supervisor engine
- Catalyst 6500 series switches running Catalyst operating system Release 6.1 or later for the supervisor engine

For Layer 2 traceroute to functional properly, Cisco Discovery Protocol (CDP) must be enabled on all the switches in the network. Do not disable CDP.

When the switch detects a device in the Layer 2 path that does not support Layer 2 traceroute, the switch continues to send Layer 2 trace queries and lets them time out.

The maximum number of hops identified in the path is ten.

The **traceroute mac** ip command output shows the Layer 2 path when the specified source and destination IP addresses are in the same subnet. When you specify the IP addresses, the switch uses Address Resolution Protocol (ARP) to associate the IP addresses with the corresponding MAC addresses and the VLAN ID.

- 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 address resolution to 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, multiple CDP neighbors are detected on a port). When more than one CDP neighbor is detected on a port, the Layer 2 path is not identified, and an error message appears.

This feature is not supported in Token Ring VLANs.

Examples

This example shows how to display the Layer 2 path by specifying the source and destination IP addresses and by using the **detail** keyword:

```
Switch> traceroute mac ip 2.2.40.40 2.2.20.20 detail
Translating IP to mac ...
2.2.40.40 =>0004.0201.0401
2.2.20.20 =>0004.0201.0501

Source 0004.0201.0401 found on vrf[BE-CEFMS:24-32] (2.2.4.4)
vrf [BE-CEFMS:24-32] / 2.2.4.4 /
        Fa5/1 [auto, auto] vlan[3] [auto, auto]
cisco-7600 [2.2.4.4] / 2.2.4.4 /
        Fa5/1 [auto, auto] vlan[3] [auto, auto]
vrf [BE-CEFMS:32] / 2.2.2.1 /
        Gi1/1 [auto, auto] vlan[2] [auto, auto]
vrf [BE-CEFMS:32] / 2.2.2.2 /
        Gi1/1 [auto, auto] vlan[2] [auto, auto]
Destination 0004.0201.0501 found on vrf[BE-CEFMS:32] (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 vrf1 vrf2
Translating IP to mac ...
2.2.40.40 =>0004.0201.0401
2.2.20.20 =>0004.0201.0501

Source 0004.0201.0401 found on vrf1
vrf1 (2.2.4.4)  [auto] vlan[3]
vrf1                (2.2.4.4)          |  |  Fa5/1 vlan[3]
cisco-7600          (2.2.4.4)          |  |  Gi1/1 vlan[2]
vrf2                (2.2.2.2)          |  |  Gi1/1 vlan[2]
Destination 0004.0201.0501 found on vrf2
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 2.2.40.40 2.2.70.70
Arp failed for destination 2.2.70.70.
Layer 2 trace aborted.
Switch>
```

Related Commands	Command	Description
	show ip source binding	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) value (more 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

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 6500 series switch.

Usage Guidelines

This command is not supported on the Supervisor Engine 6-E and Catalyst 4500M chassis.

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#configure terminal
Switch(config)#policy-map policy1
Switch(config-pmap)#class class1
Switch(config-pmap-c)#trust dscp
Switch(config-pmap-c)#police 1000000 20000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)#exit
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.
	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-size* 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

Command History	**Release**	**Modification**
	12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

This command is not supported on the Supervisor Engine 6-E and Catalyst 4900M chassis.

The bandwidth and shape rates cannot exceed the maximum speed of the interface.

The bandwidth can be configured only on the following:

- Uplink ports on Supervisor Engine III (WS-X4014)
- 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

Only transmit queue 3 can be configured to be a high-priority transmit queue.

Examples

This example shows how to allocate bandwidth on queue 1 to 100 Mbps:

```
Switch(config-if)# tx-queue 1
Switch(config-if)# tx-queue1# bandwidth 100000000
Switch(config-if)# tx-queue1#
```

This example shows how to configure transmit queue 3 to the high priority:

```
Switch(config-if)# tx-queue 3
Switch(config-if)# tx-queue1# priority high
Switch(config-if)# tx-queue1#
```

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-queue1# shape 64000
Switch(config-if)# tx-queue1#
```

Related Commands

Command	Description
show qos interface	Displays QoS 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** command. 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

udld enable | aggressive

no udld enable | aggressive

udld message time *message-timer-time*

no udld message time

Syntax Description	**enable** Enables UDLD in normal mode by default on all the fiber interfaces.
	aggressive Enables UDLD in aggressive mode by default on all the fiber 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.
Defaults	All fiber interfaces are disabled and the message timer time equals 15 seconds.
Command Modes	Global configuration mode

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 6500 series switch.

Usage Guidelines If you enable aggressive mode, once all the neighbors of a port have aged out either in the advertisement or in the detection phase, UDLD resumes the linkup sequence to try to regain frames with any potentially non-sync neighbor and shuts down the port if the bidirectional state of the link is still undetermined.

This command affects the fiber interfaces only. Use the **udld interface configuration mode** command to enable UDLD on the other interface types.

Examples This example shows how to enable UDLD on all the fiber interfaces:

```
Switch (config)# udld enable
Switch (config)#
```

■ **fiber global configuration mode**

Related Commands	Command	Description
	show udld	Displays the administrative and operational UDLD status.
	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.

udld (interface configuration mode)

To enable UDLD on an individual interface or to prevent a fiber interface from being enabled by the **udld (global configuration mode)** command, use the **udld** command. To return to the **udld (global configuration mode)** command setting, or if the port is a nonfiber port to disable UDLD, use the **no** form of this command.

udld {**enable** | **aggressive**| **disable**}

no udld {**enable** | **aggressive** | **disable**}

Syntax Description	**enable** Enables UDLD on this interface.
	aggressive Enables UDLD in aggressive mode on this interface.
	disable Disables UDLD on this interface.

Defaults

The fiber interfaces are enabled per the state of the global **udld** (**enable** or **aggressive**) command, and the nonfiber interfaces are enabled with UDLD disabled.

Command Modes Interface configuration mode

Command History	**Release**	**Modification**
	12.1(8a)EW	Support for this command was introduced on the Catalyst 6500 series switch.

Usage Guidelines

If you enable aggressive mode, once all the neighbors of a port have aged out either in the advertisement or in the detection phase, UDLD restarts the linkup sequence to try to reopen/recover with any persistently out-of-sync neighbor and shuts down the port if the message train from the link is still unidirectional.

Use the **no udld enable** command on the fiber ports to return control of UDLD to the global **udld enable** command or to disable UDLD on the nonfiber ports.

Use the **udld aggressive** command on the fiber ports to override the setting of the global **udld** (**enable** or **aggressive**) command. Use the **no** form on the fiber ports to remove this setting, return control of UDLD enabling back to the **udld** command or to disable UDLD on the nonfiber ports.

The **disable** keyword is supported on the fiber ports only. Use the **no** form of this command to remove this setting and return control of UDLD to the **udld (global configuration mode)** command.

If the port changes from fiber to nonfiber or vice versa, all configuration will be maintained because of a change of module or a GBIC change detected by the platform software.

Examples

This example shows how to cause any port interface to enable UDLD, despite the current global **udld (global configuration mode)** setting:

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

This example shows how to cause any port interface to enable UDLD in aggressive mode, despite the current global **udld** (**enable** or **aggressive**) setting:

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

This example shows how to cause a fiber port interface to disable UDLD, despite the current global **udld (global configuration mode)** setting:

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

Related Commands

Command	Description
show udld	Displays the administrative and operational 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, use the **udld reset** command.

udld reset

Syntax Description This command has no keywords or variables.

Defaults This command has no default settings.

Command Modes Privileged EXEC mode

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 6500 series switch.

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 corrected.

The **udld reset** command permits the traffic to flow on the ports again; other features, such as spanning tree, PAgP, and DTP, operate normally if enabled.

Examples This example shows how to reset all the ports that are shut down by UDLD:

```
Switch(enable) udld reset
Switch(enable)
```

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

Command History	**Release**	**Modification**
	12.2(11)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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# conf t unidirectional
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet 1/1
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*

name	User ID of the user.
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

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 6500 series switch.

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 (xena):

```
Switch(config)# username xena secret 5 warrior
Switch(config)#
```

Find more pages of this command.
Find more pages of this command.

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.
	username (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-file-system:*] [*filename*] [*expected-md5-signature*]

Syntax Description	**md5** (Optional) Verifies the MD5 checksum.
	flash-file-system: (Optional) Device where the flash resides; valid values are **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

Command History	**Release**	**Modification**
	12.1(26)E9	Support for this command was introduced on the Catalyst 6500 series switch.

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 Boot Helper files, which is included with the image on the disk, lists the name, file size, and checksum of the image. Review the contents of the Boot Helper 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 to a server.

Use the **verify md5** command to verify the MD5 signature of a file before using it. This command initializes 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-file-system:*][*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-jsv.bin 6f
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
MD5sum verifying slot0:c6sup-jsv.bin
Computed signature = 6f30e6a8e9d7f6b1276b42f6b6a77f5d5
Embedded signature = 6f
```

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:

```
Switch# verify /md5 cat2_c.cbi
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
File cat2_c2_j1.cbi verified OK.
Switch#
```

This example shows how to manually verify the MD5 signature:

```
Switch# verify /md5 c6-jsv.rom
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
```

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* [*ieee bnp*] [**backupcrf** *mode*] [**bridge** *type* | *bridge-num*] [**media** *type*] [**name** *vlan-name*] [**parent** *parent-vlan-id*] [**ring** *ring-number*] [**ring2** *ring2-number*] [**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.
ieee *bnp*	(Optional) Specifies the maximum number of All Route Explorer bnp for this VLAN; valid values are from 0 to 15. 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 or bridge; valid values are the keyword; valid type values are **crb** and **srt**.
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 **ethernet**, **fd-net**, **fddi**, **trcrf**, and **trbrf**.
name *vlan-name*	(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 *ring-number*	(Optional) Specifies the ring number of FDDI or Token Ring-type VLANs; valid values are from 2 to 1001.
ring2 *ring2-number*	(Optional) Specifies the secondary ring number; valid values are from 2 to 4094 or 0.
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 size-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:
  - fddi—1500
  - trcrf—1500 if V2 is not enabled; 4472 if it is enabled
  - fdnet—1500
  - trbrf—1500 if V2 is not enabled; 4472 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

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

VLANs 1 parameters are factory configured and cannot be changed.

When you define size-name, the name must be unique within the administrative domain.

The said is documented in 802.10. When the **no** form is used, the VLANs 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 (no-op) on other types of VLANs. When the **no** form is used, the VLANs source-route-bridging number returns to the default.

The parent VLAN exists to the default if the parent VLAN is defined 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 a different VLAN type than the affected VLAN. If no 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 VLANs.

Examples

This example shows how to add a new VLAN with all the default parameters to the new VLAN database:

```
Switch(vlan)# vlan 2
```

Note If the VLAN already exists, no action occurs.

This example shows how to cause 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 added:
    Name: VLAN0002
    Media type: ETHERNET
    Parent VLAN: 3
```

This example shows how to delete VLAN 2:

```
Switch(vlan)# no vlan 2
Switch(vlan)#
```

This example shows how to retain the MTU in the default for its type and the translational bridging VLANs to the default:

```
Switch(vlan)# vlan 2 mtu tb-vlan1 tb-vlan2
Switch(vlan)#
```

Related Commands

Command	Description
show vlan	Displays VLAN information.

vlan access-map

To enter VLAN access-map command mode to create a VLAN access-map, use the **vlan access-map** command. To remove a mapping sequence or the entire map, use the **no** form of this command.

vlan access-map *name* [*seq#*ˆ]

no vlan access-map *name* [*seq#*]

Syntax Description	*name*	VLAN access-map tag.
	seq#	(Optional) Map sequence number; valid values are from 0 to 65535.

Defaults This command has no default settings.

Command Modes Global configuration mode

Command History	**Release**	**Modification**
	12.1(14)EW	Support for this command was introduced on the Catalyst 6500 series switch.

Usage Guidelines If you enter the sequence number of an existing map sequence, you enter VLAN access-map mode. If you do not specify a sequence number, a number is automatically assigned. You can enter one match clause and one action clause per map sequence. If you enter the **no vlan access-map name** [*seq#*] command without entering a sequence number, the whole map is removed. Once you enter VLAN access-map mode, the following commands are available:

- **action**—Sets the action to be taken (forward or drop).
- **default**—Returns a command to its default settings.
- **end**—Exits from VLAN access-map configuration mode.
- **exit**—Exits from VLAN access-map configuration mode.
- **match**—Sets the values to match (IP address or MAC address).
- **no**—Negates a command or reverts defaults.

Examples This example shows how to enter VLAN access-map mode:

```
Switch(config)# vlan access-map vlan1
Switch(config-access-map)#
```

Related Commands	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 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

Command History

Release	Modification
12.2(40)SG	This command was introduced on the Catalyst 4500 series switch using a Supervisor Engine 6E.

Usage Guidelines

Configuring of service-policies in this mode is supported on the Supervisor Engine 6-E and Catalyst 4500E chassis.

In Supervisor Engine 5/ through 10GE and earlier, a service-policy has to attach to SVI to apply VLAN-based policies, then 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.

To restore the requirement of creating an SVI, VLAN configuration mode is introduced on the Supervisor Engine 6-E and Catalyst 4500E chassis. With this command you can specify lists of VLANs to which service-policies that are applied. To configure a system in this mode there is no requirement for you to create SVIs, or create VLAN or VTP mode instances. Once the VLAN becomes active the configuration becomes active on that VLAN. 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#conf t 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 2-1000
!
!
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
      police:
        cir 128000 bps, bucket 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

Command History	Release	Modification
	12.1(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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
Switch#
```

This example shows how to delete a VLAN after you are in VLAN configuration mode:

```
Switch(config)# no vlan 100
Deleting VLAN 100...
Switch(config)#
```

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

Command History	Release	Modification
	12.2(18)EW	This command was first introduced on the Catalyst 4500 series switch.

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 ensures that packets in the native VLAN of a 802.1Q trunk port are tagged by tagging the tagged packets. You must set 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-interface)
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	Configures 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*]}

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

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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 *one* VLAN 7 through 9:

```
Switch(config)# vlan filter parts vlan-list 7-9
Switch(config)#
```

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

Command History

Release	Modification
12.1(12)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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 VLAN.

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 a VLAN that conflicts with an existing internal VLAN, the VLAN that you configured is put into a nonoperational status until the internal VLAN 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

Command History	Release	Modification
	12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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 row.

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

Command History	Release	Modification
	12.1(13)E	Support for this command was introduced on the Catalyst 4500 series switch.

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 reason 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:

```
Switch(config)# vmps reconfirm
Switch(config)#
```

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) client.

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

Command History	Release	Modification
	12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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

Command History	**Release**	**Modification**
	12.1(20)EA1	Support for this command was introduced on the Catalyst 4500 series switch.

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 address 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 servers when dynamic-access ports are present, the switch cannot forward the packets from the new sources 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 191.10.49.20 as the primary VMPS server. The servers with IP addresses 191.10.49.21 and 191.10.49.22 are configured as secondary servers:

```
Switch(config)# vmps server 191.10.49.20 primary
Switch(config)# vmps server 191.10.49.21
Switch(config)# vmps server 191.10.49.22
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 vmps	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

Command History	**Release**	**Modification**
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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

Command History	Release	Modification
	12.1(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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

Command History	Release	Modification
	12.1(8a)EW	Support for this command was introduced on the Catalyst 6500 series switch.

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 restore the number except by clearing NVRAM and reloading.

Examples

This example shows how to set the device administrative domain:

```
Switch>(enable)set vtp domain domainname
Switch>(enable)set vtp
```

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 the 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

Command History

Release	Modification
12.1(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.

Examples

This example shows how to create a VTP domain password:

```
Switch(vlan-config)# vtp password DomainSecret
Switch(vlan-config)#
```

This example shows how to delete the VTP domain password:

```
Switch(vlan-config)# no vtp password
Clearing device VLAN database password.
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 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

Command History

Release	Modification
12.1(8a)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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

Command History	Release	Modification
	12.1(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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 **vtp client**, except that it does not retain 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

Command History	Release	Modification
	12.1(12c)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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)#vlan database
Switch(vlan-database)# vtp transparent
Switch(vlan-database)#
```

This example shows how to return the device to VTP server mode:

```
Switch(config)#vlan database
Switch(vlan-database)# no vtp transparent
Switch(vlan-database)#
```

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 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

Command History	Release	Modification
	12.1(20)EW	Support for this command was introduced on the Catalyst 4500 series switch.

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
AnsRT	Automated Packet Recognition and Translation
ARP	Address Resolution Protocol

B

BEM	beer 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-addressible 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 Peroocol
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
SHM	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 contention 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

B

C

F

G

H

Q

R

U

V

W