



Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide

Release IOS XE 3.9.xE and IOS 15.2(5)Ex

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Catalyst 4500 Series Switch Cisco IOS Command Reference

Copyright © 1999–2016 Cisco Systems, Inc. All rights reserved.



Catalyst 4500 Series IOS Commands

New Commands

auto security
auto security-port
show auto security

Revised Commands

A Commands

aaa accounting dot1x default start-stop group radius
aaa accounting system default start-stop group radiusclear mac-address-table
access-group mode
access-list hardware capture mode
access-list hardware entries
access-list hardware region
action
apply
anyp client server
anyp mode client
apply
arp access-list
attach module
authentication control-direction
authentication critical recovery delay
authentication event
authentication fallback
authentication host-mode

authentication open
authentication order
authentication periodic
authentication port-control
authentication priority
authentication timer
authentication violation
auto qos classify
auto qos classify police
auto qos srnd4
auto qos trust
auto qos video
auto qos voip
auto qos voip cisco-softphone
auto security
auto security-port
auto-sync
average-packet-size (netflow-lite monitor submode)

C Commands

call-home (global configuration)
call-home request
call-home send
call-home send alert-group
call-home test
channel-group
channel-protocol
cisp enable
class-map
clear counters
clear errdisable interface
clear hw-module slot password
clear interface gigabitethernet
clear interface vlan
clear ip access-template
clear ip arp inspection log
clear ip arp inspection statistics

clear ip dhcp snooping binding
clear ip dhcp snooping database
clear ip dhcp snooping database statistics
clear ip igmp group
clear ip mfib counters
clear ip mfib fastdrop
clear ip wecp
clear lacp counters
clear netflow-lite exporter statistics
clear netflow-lite monitor statistics interface
clear nmsp statistics
clear mac-address-table dynamic
clear pagp
clear port-security
clear pppoe intermediate-agent statistics
clear qos
clear switch virtual dual-active fast-hello
clear vlan counters
clear vmps statistics
control-plane
cos (netflow-lite exporter submode)
counter

D Commands

debug adjacency
debug backup
debug condition interface
debug condition standby
debug condition vlan
debug device-sensor
debug dot1x
debug etherchnl
debug interface
debug ip dhcp snooping event
debug ip dhcp snooping packet
debug ip verify source packet
debug ipc

debug lacp
debug monitor
debug nmsp
debug nvram
debug pagp
debug platform packet protocol lacp
debug platform packet protocol pagp
debug pm
debug port-security
debug pppoe intermediate-agent
debug redundancy
debug spanning-tree
debug spanning-tree backbonefast
debug spanning-tree switch
debug spanning-tree uplinkfast
debug sw-vlan
debug sw-vlan ifs
debug sw-vlan notification
debug sw-vlan vtp
debug udd
debug vqpc
define interface-range
deny
destination (netflow-lite exporter submode)
device-sensor filter-list
device-sensor filter-list dhcp
device-sensor filter-spec
device-sensor notify
diagnostic fpga soft-error recover
diagnostic monitor action
diagnostic start
dot1x auth-fail max-attempts
dot1x auth-fail vlan
dot1x credentials (global configuration)
dot1x critical
dot1x critical eapol
dot1x critical recovery delay
dot1x critical vlan

dot1x control-direction
dot1x guest-vlan
dot1x guest-vlan supplicant
dot1x host-mode
dot1x initialize
dot1x mac-auth-bypass
dot1x max-reauth-req
dot1x max-req
dot1x port-control
dot1x re-authenticate
dot1x re-authentication
dot1x system-auth-control
dot1x timeout
dscp (netflow-lite exporter submode)
dual-active detection (virtual switch)
duplex
dual-active recovery ip address
duplex

E Commands

erase
errdisable detect cause
errdisable recovery
export-protocol (netflow-lite exporter submode)
exporter (netflow-lite monitor submode)

F Commands

flowcontrol

H Commands

hardware statistics
hw-module beacon
hw-module module start
hw-module module stop
hw-module port-group
hw-module power
hw-module system max-port-num-mode 1/2

hw-module system max-port-num-mode 1/2 switch 1/2/all

hw-module system max-queue-limit

hw-module uplink mode

hw-module uplink select

I Commands

instance

interface

interface (virtual switch)

interface port-channel

interface range

interface vlan

ip admission proxy http refresh-all

ip arp inspection filter vlan

ip arp inspection limit (interface)

ip arp inspection log-buffer

ip arp inspection trust

ip arp inspection validate

ip arp inspection vlan

ip arp inspection vlan logging

ip cef load-sharing algorithm

ip dhcp snooping

ip dhcp snooping binding

ip dhcp snooping database

ip dhcp snooping information option

ip dhcp snooping information option allow-untrusted

ip dhcp snooping limit rate

ip dhcp snooping trust

ip dhcp snooping vlan

ip device tracking maximum

ip igmp filter

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 mfib fastdrop
ip name-server
ip route-cache flow
ip source binding
ip sticky-arp
ip verify header vlan all
ip verify source
ip verify unicast source reachable-via
ip wccp
ip wccp check services all
ip wccp group-listen
ip wccp redirect
p wccp redirect exclude in
ipv6 mld snooping
ipv6 mld snooping last-listener-query-count
ipv6 mld snooping last-listener-query-interval
ipv6 mld snooping listener-message-suppression
ipv6 mld snooping robustness-variable
ipv6 mld snooping tcn
ipv6 mld snooping vlan
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
l2protocol-tunnel drop-threshold
l2protocol-tunnel shutdown-threshold
lACP port-priority
lACP system-priority
license right-to-use activate
license right-to-use deactivate
lldp tlv-select power-management
logging event trunk-status global (global configuration)
logging event link-status global (global configuration)
logging event trunk-status global (global configuration)
logging event link-status global (global configuration)
logging event link-status (interface configuration)
logging event trunk-status (interface configuration)

M Commands

mac access-list extended
mac-address (virtual switch)
mac-address-table aging-time
mac-address-table dynamic group protocols
mac-address-table learning vlan
mac-address-table notification
mac-address-table static
macro apply cisco-desktop
macro apply cisco-phone
macro apply cisco-router
macro apply cisco-switch
macro auto device
macro auto execute (built-in function)
macro auto execute (remotely-defined trigger)
macro auto execute (user-defined function)
macro auto global processing
macro auto mac-address-group
macro auto monitor
macro auto processing
macro auto sticky
macro global apply cisco-global

macro global apply system-cpp
macro global description
macsec network-link
mka
mka policy
main-cpu
match
match flow ip
mdix auto
media-type
mode
monitor capture { access-list | class-map }
monitor capture [clear | export]
monitor capture [interface | vlan | control-plane]
monitor capture file location buffer-size
monitor capture limit
monitor capture mycap match
monitor capture start
monitor session
mtu
mvr (global configuration)
mvr (interface configuration)

N Commands

name
netflow-lite exporter
netflow-lite monitor
netflow-lite sampler
nmsp
nmsp attachment suppress

O Commands

options timeout (netflow-lite exporter submode)

P Commands

packet-offset (netflow-lite sampler submode)
packet-rate (netflow-lite sampler submode)

packet-section size (netflow-lite sampler submode)
pagp learn-method
pagp port-priority
passive-interface
permit
policy-map
port-channel load-balance
port-channel standalone-disable
port-security mac-address
port-security mac-address sticky
port-security maximum
power dc input
power efficient-ethernet auto
power inline
power inline consumption
power inline four-pair forced
power inline logging global
power inline police
power redundancy combined max inputs
power redundancy-mode
pppoe intermediate-agent (global)
pppoe intermediate-agent (interface)
pppoe intermediate-agent (interface vlan-range)
pppoe intermediate-agent format-type (global)
pppoe intermediate-agent limit rate
pppoe intermediate-agent trust
pppoe intermediate-agent vendor-tag strip
priority
private-vlan
private-vlan mapping
private-vlan synchronize
profile
profile flow

Q Commands

qos account layer-all encapsulation
qos account layer2 encapsulation

qos trust
queue-limit

R Commands

redundancy
redundancy force-switchover
redundancy reload
remote login module
remote-span
renew ip dhcp snooping database
reset
revision

S Commands

sampler (netflow-lite monitor submode)
service-policy (interface configuration)
service-policy (policy-map class)
service-policy input (control-plane)
session module
set
set cos
set dscp
set precedence
set qos-group
shape (interface configuration)
shell trigger
snmp ifindex clear
snmp ifindex persist
snmp-server enable traps
snmp-server ifindex persist
snmp-server ifindex persist compress
snmp trap mac-notification change
source (netflow-lite exporter submode)
spanning-tree backbonefast
spanning-tree bpdofilter
spanning-tree bpduguard
spanning-tree bridge assurance

spanning-tree cost
spanning-tree etherchannel guard misconfig
spanning-tree extend system-id
spanning-tree guard
spanning-tree link-type
spanning-tree loopguard default
spanning-tree mode
spanning-tree mst
spanning-tree mst configuration
spanning-tree mst forward-time
spanning-tree mst hello-time
spanning-tree mst max-age
spanning-tree mst max-hops
spanning-tree mst simulate pvst global
spanning-tree mst simulate pvst (interface configuration mode)
spanning-tree mst root
spanning-tree pathcost method
spanning-tree portfast (interface configuration mode)
spanning-tree portfast edge bpdudfilter default
spanning-tree portfast edge bpduguard default
spanning-tree portfast
spanning-tree port-priority
spanning-tree uplinkfast
spanning-tree vlan
speed
storm-control
storm-control broadcast include multicast
switch (virtual switch)
switch convert mode (virtual switch)
switch virtual domain (virtual switch)
switch virtual link (virtual switch)
switchport
switchport access vlan
switchport autostate exclude
switchport block
switchport mode
switchport port-security
switchport private-vlan association trunk

switchport private-vlan host-association
switchport private-vlan mapping
switchport private-vlan trunk allowed vlan
switchport private-vlan trunk native vlan tag
switchport trunk
switchport vlan mapping
system mtu

Show Commands

show access-group mode interface
show adjacency
show ancp multicast
show arp access-list
show authentication
show auto install status
show auto qos
show auto security
show bootflash:
show bootvar
show cable-diagnostics tdr
show call-home
show cdp neighbors
show class-map
show device-sensor cache
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 eigrp plugins
show errdisable detect
show errdisable recovery
show etherchannel
show flowcontrol
show hw-module port-group
show hw-module system max-port-num-mode

show hw-module uplink
show idprom
show interfaces
show interfaces (virtual switch)
show interfaces counters
show interfaces counters (virtual switch)
show interfaces description
show interfaces link
show interfaces mtu
show interfaces private-vlan mapping
show interfaces status
show interfaces switchport
show interfaces transceiver
show interfaces trunk
show ip arp inspection
show ip arp inspection log
show ip 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 ip wccp
show ipc
show ipv6 mld snooping
show ipv6 mld snooping mrouter
show ipv6 mld snooping querier
show ipv6 snooping counters

show issu capability
show issu clients
show issu comp-matrix
show issu endpoints
show issu entities
show issu fsm
show issu message
show issu negotiated
show issu rollback-timer
show issu sessions
show issu state
show l2protocol-tunnel
show lacp
show license
show mab
show mac access-group interface
show mac-address-table address
show mac-address-table aging-time
show mac-address-table count
show mac-address-table dynamic
show mac-address-table interface
show mac address-table learning
show mac-address-table multicast
show mac-address-table notification
show mac-address-table protocol
show mac-address-table static
show mac-address-table vlan
show macro auto mac-address-group
show macro auto device
show macro auto interface
show macro auto monitor clients
show macro auto monitor device
show macro auto monitor type
show module
show monitor
show monitor capture
show monitor capture file
show mvr

show mvr interface
show mvr members
show netflow-lite exporter
show netflow-lite monitor
show netflow-lite sampler
show nmsp
show pagp
show pagp dual-active (virtual switch)
show policy-map
show policy-map control-plane
show policy-map interface
show policy-map interface vlan
show port-security
show power
show power inline police
show qos
show pppoe intermediate-agent interface
show qos
show qos aggregate policer
show qos dbl
show qos interface
show qos maps
show redundancy
show redundancy config-sync
show running-config
show slavebootflash:
show slaveslot0:
show slot0:
show spanning-tree
show spanning-tree mst
show storm-control
show switch virtual (virtual switch)
show system mtu
show tech-support
show udd
show vlan
show vlan access-map
show vlan counters

show vlan dot1q tag native
show vlan group
show vlan internal usage
show vlan mapping
show vlan mtu
show vlan private-vlan
show vlan remote-span
show vmps
show vslp (virtual switch)
show vtp

T Commands

template data timeout (netflow-lite exporter submode)
test cable-diagnostics tdr
traceroute mac
traceroute mac ip
transport udp (netflow-lite exporter submode)
trust
ttl (netflow-lite exporter submode)
tx-queue

U Commands

udld (global configuration mode)
udld (interface configuration mode)
udld reset
unidirectional
username

V Commands

verify
vlan (VLAN Database mode)
vlan access-map
vlan configuration
vlan database
vlan dot1q tag native
vlan filter
vlan group

vlan internal allocation policy
vmps reconfirm (global configuration)
vmps reconfirm (privileged EXEC)
vmps retry
vmps server
vrf (netflow-lite exporter submode)
vslp interval (virtual switch)
vtp (global configuration mode)
vtp client
vtp domain
vtp password
vtp pruning
vtp server
vtp transparent
vtp v2-mode



Preface

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

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

Audience

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

Cisco IOS Software Documentation

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

Organization

This chapter describes the contents of each chapter in this document.

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

Related Documentation

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

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



Note

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

Other documents in the Cisco IOS documentation set include:

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

For information about MIBs, refer to this URL:

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

Command Syntax Conventions

Table 1 describes the syntax used with the commands in this document.

Table 1 **Command Syntax Guide**

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

Table 1 **Command Syntax Guide**

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

Notes use this convention:



Note

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

Cautions use this convention:



Caution

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

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

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

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

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

License Issues

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

OpenSSL License:

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

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

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following 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. Redistributions 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 THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

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

Original SSLeay License:

Copyright © 1995-1998 Eric Young (ey@cryptsoft.com). All rights reserved.

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

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

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, 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. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

“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.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgment: “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/docs/general/whatsnew/whatsnew.html>

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



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 context-sensitive 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
<i>abbreviated-command-entry?</i>	Displays a list of commands that begin with a particular character string. (Do not leave a space between the command and question mark.)
<i>abbreviated-command-entry<Tab></i>	Completes a partial command name.
<i>?</i>	Lists all commands for the command mode.
<i>command ?</i>	Lists all keywords for the command. Leave a space between the command and the question mark.
<i>command keyword ?</i>	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 4500 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> enable Password: <password> Switch#	Enter the enable command and password to access privileged EXEC commands. You are in privileged EXEC mode when the prompt changes to Switch#.
Switch# 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> GigabitEthernet 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 <i>module-number/port-number</i> . 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
<pre>Switch(config-if)#? Interface configuration commands: access-expression Build a bridge boolean access expression apollo Apollo interface subcommands appletalk Appletalk interface subcommands arp Set arp type (arpa, probe, snap) or timeout backup Modify backup parameters bandwidth Set bandwidth informational parameter bgp-policy Apply policy propagated by bgp community string bridge-group Transparent bridging interface parameters carrier-delay Specify delay for interface transitions cdp CDP interface subcommands channel-group Etherchannel/port bundling configuration clns CLNS interface subcommands cmns OSI CMNS custom-queue-list Assign a custom queue list to an interface decnet Interface DECnet config commands default Set a command to its defaults delay Specify interface throughput delay description Interface specific description dlsw DLSw interface subcommands dspu Down Stream PU exit Exit from interface configuration mode fair-queue Enable Fair Queuing on an Interface flowcontrol Configure flow operation. fras DLC Switch Interface Command help Description of the interactive help system hold-queue Set hold queue depth ip Interface Internet Protocol config commands ipx Novell/IPX interface subcommands isis IS-IS commands iso-igrp ISO-IGRP interface subcommands . . .</pre>	<p>Enter a ? to display a list of all the interface configuration commands available for the Gigabit Ethernet interface.</p>
<pre>Switch(config-if)# Switch(config-if)# channel-group ? group channel-group of the interface Switch(config-if)#channel-group</pre>	<p>Enter the command that you want to configure for the controller. In this example, the channel-group command is used.</p> <p>Enter a ? to display what you must enter next on the command line. In this example, you must enter the group keyword.</p> <p>Because a <cr> is not displayed, it indicates that you must enter more information to complete the command.</p>

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

Command	Purpose
<pre>Switch(config-if)# channel-group ? <1-256> Channel group number Switch(config-if)#channel-group</pre>	<p>After you enter the group keyword, enter a ? to display what you must enter next on the command line. In this example, you must enter a channel group number from 1 to 256.</p> <p>Because a <code><cr></code> is not displayed, it indicates that you must enter more information to complete the command.</p>
<pre>Switch(config-if)# channel-group 1 ? mode Etherchannel Mode of the interface Switch(config-if)#</pre>	<p>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.</p> <p>Because a <code><cr></code> is not displayed, it indicates that you must enter more information to complete the command.</p>
<pre>Switch(config-if)# channel-group 1 mode ? auto Enable PAGP only if a PAGP device is detected desirable Enable PAGP unconditionally on Enable Etherchannel only Switch(config-if)#</pre>	<p>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.</p> <p>Because a <code><cr></code> is not displayed, it indicates that you must enter more information to complete the command.</p>
<pre>Switch(config-if)# channel-group 1 mode auto ? <cr> Switch(config-if)#</pre>	<p>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.</p> <p>Because a <code><cr></code> is displayed, it indicates that you can press Return to complete the command. If additional keywords are listed, you can enter more keywords or press Return to complete the command.</p>
<pre>Switch(config-if)# channel-group 1 mode auto Switch(config-if)#</pre>	<p>In this example, press Return to complete the command.</p>

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 global configuration mode. Most EXEC commands are one-time commands, such as **show** commands, which show the current status 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.

ROM-monitor mode is a separate 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 ROM-monitor 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)

Command Mode	Access Method	Prompt	Exit Method
Subinterface configuration	From interface configuration mode, specify a subinterface with an interface command.	Switch(config-subif)#	To exit to global configuration mode, enter the exit command. To enter privileged EXEC mode, enter the end command or press Ctrl-Z .
ROM monitor	From privileged EXEC mode, enter the reload EXEC command. Press the Break key during the first 60 seconds while the system is booting.	Rommon>	To exit ROM-monitor mode, you must reload the image by entering the boot command. If you use the boot command without specifying a file or any other boot instructions, the system boots from the default Flash image (the first image in onboard Flash memory). Otherwise, you can instruct the system 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 reenable a disabled function or to enable a function that is disabled by default. For example, IP routing is enabled by default. To disable IP routing, specify the **no ip routing** command and specify **ip routing** to reenable it. This publication provides the complete syntax for the configuration commands and describes what the **no** form of a command does.

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

Using the CLI String Search

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

With the 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 start 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 00210..., (is), and [Oo]utput.

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 or filter backward 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, anchoring, 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 ~) as 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

[abcdABCD]

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

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

[a-dA-D]

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

[a-dA-D\-]

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

[a-dA-D\-)]

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

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

[^a-dqsv]

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

[^\d]

Multiple-Character Patterns

When creating regular expressions, you can also specify a pattern containing multiple characters. You create multiple-character regular expressions by joining letters, digits, or keyboard characters that do not have special meaning. For example, a4% is a multiple-character regular expression. Put a backslash in front of the keyboard characters that have special meaning when you want to remove their special meaning.

With multiple-character patterns, order is important. The regular expression a4% matches the character a followed by a 4 followed by a % sign. If the string does not have a4%, 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, a!, or a2 are all valid matches for the regular expression.

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

a\.

only the string a. matches this regular expression.

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

telebit 3107 v32bis

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 “multiples” 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, including none:

a*

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

a+

This pattern matches the string bb or bab:

ba?b

This string matches any number of asterisks (*):

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

(ab)*

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

([A-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 A9b3, but not 9Ab3 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

codex | telebit

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

Anchoring

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

Table 1-6 Special Characters Used for Anchoring

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

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

^abcd

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

[^abcd]

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

\$.12

Contrast these anchoring characters with the special character underscore (_). The underscore matches the beginning of a string (^), the end of a string (\$), parentheses (), space (), braces { }, 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’s 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\$ ^1300(space) (space)1300 {1300, ,1300, {1300} ,1300, (1300

with

1300

Parentheses for Recall

As shown in the “Multipliers” section on page 1-9, 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 reuse 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(.)\1\2
```

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

Saving Configuration Changes

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

show platform Commands

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

**Note**

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



CHAPTER 2

Cisco IOS Commands for the Catalyst 4500 Series Switches

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

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

#macro keywords

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

```
#macro keywords [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.

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

```
Switch(config)# macro name test
macro name test
Enter macro commands one per line. End with the character '@'.
#macro keywords $VLAN $MAX
switchport
@

Switch(config)# int gi1/1
Switch(config-if)# macro apply test ?
WORD Keyword to replace with a value e.g $VLAN, $MAX << It is shown as help
<cr>
```

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.

Command Default Accounting is disabled.

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 802.1X accounting requires a RADIUS server.

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

Examples The following 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 receive 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.

Command Default Accounting is disabled.

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 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 reauthenticated, an interim-update accounting notice is sent to the accounting server.

Examples The following example shows how to generate a logoff after a switch reboots:

```
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.

Command Default

PACL override mode

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(19)EW	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

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

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

The following 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.

Command Default The control packets are globally captured.

Command Modes Global configuration mode

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

Usage Guidelines This command is not supported on Supervisor Engine 6-E, Supervisor Engine 6L-E, Catalyst 4900M, Catalyst 4948E, and Catalyst 4948E-F.

Before configuring the capture mode, it is best to examine and modify your configuration to globally disable features such as DHCP snooping or IGMP snooping, and instead enable them on specific VLANs.

When changing to path managed mode, be aware that control traffic may be bridged in hardware or dropped initially until the per-vlan CAM entries are programmed in hardware.

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

The following 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)# end
Switch#
```

The following 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.

Command Default The ACLs are programmed as packed.

Command Modes Global configuration mode

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

Usage Guidelines Two types of hardware resources are used when ACLs are programmed: entries and masks. If one of these resources is consumed, no additional ACLs can be programmed into the hardware. If the masks are consumed, but the entries are available, change the programming algorithm from **packed** to **scattered** to make the masks available. This action allows additional ACLs to be programmed into the hardware. The goal is to use TCAM resources more efficiently; that is, to minimize the number of masks per ACL entries. To compare TCAM utilization when using the **scattered** or **packed** algorithms, 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 The following example shows how to program ACLs into the hardware as packed. After they are programmed, you will need 89 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#
01:15:34: %SYS-5-CONFIG_I: Configured from console by console
Switch#
Switch# show platform hardware acl statistics utilization brief
Entries/Total(%)  Masks/Total(%)
-----
Input  Acl(PortAndVlan)  2016 / 4096 ( 49)   460 /  512 ( 89)
Input  Acl(PortOrVlan)   6 / 4096 (  0)     4 /  512 (  0)
Input  Qos(PortAndVlan)  0 / 4096 (  0)     0 /  512 (  0)
Input  Qos(PortOrVlan)   0 / 4096 (  0)     0 /  512 (  0)
```

```

Output Acl(PortAndVlan)    0 / 4096 ( 0)    0 / 512 ( 0)
Output Acl(PortOrVlan)    0 / 4096 ( 0)    0 / 512 ( 0)
Output Qos(PortAndVlan)   0 / 4096 ( 0)    0 / 512 ( 0)
Output Qos(PortOrVlan)    0 / 4096 ( 0)    0 / 512 ( 0)

```

```
L4Ops: used 2 out of 64
```

```
Switch#
```

The following example shows how to reserve space (scatter) between ACL entries in the hardware. The number of masks required to program 49 percent of the entries has decreased to 49 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#
```

```
01:39:37: %SYS-5-CONFIG_I: Configured from console by console
```

```
Switch#
```

```
Switch# show platform hardware acl statistics utilization brief
```

```

Entries/Total(%)  Masks/Total(%)
-----
Input  Acl(PortAndVlan)  2016 / 4096 ( 49)  252 / 512 ( 49)
Input  Acl(PortOrVlan)   6 / 4096 (  0)   5 / 512 (  0)
Input  Qos(PortAndVlan)  0 / 4096 (  0)   0 / 512 (  0)
Input  Qos(PortOrVlan)  0 / 4096 (  0)   0 / 512 (  0)
Output Acl(PortAndVlan)  0 / 4096 (  0)   0 / 512 (  0)
Output Acl(PortOrVlan)  0 / 4096 (  0)   0 / 512 (  0)
Output Qos(PortAndVlan)  0 / 4096 (  0)   0 / 512 (  0)
Output Qos(PortOrVlan)  0 / 4096 (  0)   0 / 512 (  0)

```

```
L4Ops: 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 QoS.
	input	Specifies adjustment of region balance for input ACL and QoS.
	output	Specifies adjustment of region balance for output ACL and QoS.
	balance <i>bal-num</i>	Specifies relative sizes of the PandV and PorV regions in the TCAM; valid values are between 1 and 99.

Command Default The default region balance for each TCAM is 50.

Command Modes Global configuration mode

Command History	Release	Modification
	12.2(31)SG	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 The following example shows how to enable the MAC notification trap when a MAC address is added to a port:

```
Switch# configure terminal
Switch(config)# access-list hardware region feature input balance 75
Switch(config)#
```

action

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

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

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

Syntax Description

drop	Sets the action to drop packets.
forward	Sets the action to forward packets to their destination.

Command Default

This command has no default settings.

Command Modes

VLAN access-map mode

Command History

Release	Modification
12.1(12c)EW	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

The following example shows how to define a drop action:

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

The following example shows how to define a forward action:

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

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.

Command Default This command has no default settings.

Command Modes cfg-call-home-profile

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

Usage Guidelines By default the profile is enabled upon creation.

Examples The following example shows how to enable the destination profile:

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

Related Commands	Command	Description
	destination address	Configures the destination e-mail address or URL to which Call Home messages will be sent.
	destination message-size-limit bytes	Configures a maximum destination message size for the destination profile.
	destination preferred-msg-format	Configures a preferred message format.
	destination transport-method	Enables the message transport method.
	profile	Enters profile call-home configuration submenu
	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** *vlan number* **interface** *interface*

Syntax Description	Parameter	Description
	<i>identifier name</i>	Identifier used by the ANCP server to specify an interface member of a VLAN.
	<i>vlan number</i>	VLAN identifier.
	<i>interface</i>	Interface member of this VLAN.

Command Default This command has no default settings.

Command Modes Global configuration mode

Command History	Release	Modification
	12.2(50)SG	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 (in hex) 0x01060004[vlan][intf]. For example, VLAN 19 and interface Fast Ethernet 2/3 will provide 0x0106000400130203. 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 box in ANCP client mode with the **ancp mode client** configuration command.

Examples The following example shows how to identify interface FastEthernet 7/3 on VLAN 10 with the string NArmstrong:

```
Switch# ancp client port identifier NArmstrong 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 of server interface interface
```

Syntax Description	
<i>ipaddr of server</i>	IP address of the ANCP server the client must connect with TCP.
<i>interface</i>	Interface to use for the connection.

Command Default This command has no default settings.

Command Modes Global configuration mode

Command History	Release	Modification
	12.2(50)SG	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 this 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 The following example shows how to indicate to the ANCP client the IP address of the ANCP server it needs to connect to:

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

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

ancp mode client

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

ancp mode client

Syntax Description This command has no arguments or keywords.

Command Default This command has no default settings.

Command Modes Global configuration mode

Command History	Release	Modification
	12.2(50)SG	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 The following 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.

Command Default This command has no default settings.

Command Modes VLAN configuration mode

Command History	Release	Modification
	12.1(8a)EW	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 The following 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.

■ apply

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	<i>name</i> Specifies the access control list name.
---------------------------	---

Command Default	This command has no default settings.
------------------------	---------------------------------------

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

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

Examples	<p>The following example shows how to define an ARP access list named static-hosts:</p> <pre>Switch(config)# arp access-list static-hosts Switch(config)#</pre>
-----------------	---

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	<i>mod</i> Target module for the command.
---------------------------	---

Command Default	This command has no default settings.
------------------------	---------------------------------------

Command Modes	Privileged EXEC mode
----------------------	----------------------

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

Usage Guidelines	<p>This command applies only to the Access Gateway Module on Catalyst 4500 series switches.</p> <p>The valid values for <i>mod</i> depend on the chassis that are 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.</p> <p>When you execute the attach module <i>mod</i> command, the prompt changes to Gateway#.</p> <p>This command is identical in the resulting action to the session module <i>mod</i> and the remote login module <i>mod</i> commands.</p>
-------------------------	---

Examples	The following example shows how to remotely log in to an Access Gateway Module:
-----------------	---

```
Switch# attach module 5
Attaching console to module 5
Type 'exit' at the remote prompt to end the session

Gateway>
```

Related Commands	Command	Description
	remote login module	Remotely connects to a specific module.
	session module	Logs in to the 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(50)SG	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(50)SG and later releases:

dot1x control-direction { both | in }

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

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

- **Unidirectional state**—When you configure a port as unidirectional with the **dot1x control-direction** interface configuration command, the port changes to the spanning-tree forwarding state.
When the unidirectional controlled port is enabled, the connected host is in sleeping mode 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 can only receive traffic from other devices in the network.
- **Bidirectional state**—When you configure a port as bidirectional with the **dot1x control-direction** interface configuration command, the port is access-controlled in both directions. In this state, the switch port sends 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

<i>milliseconds</i>	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	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

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

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

Related Commands

Command	Description
show authentication	Displays Authentication Manager information.

authentication event

To configure the actions for authentication 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] | voice | dead action reinitialize [vlan vlan]} }
```

```
authentication event no-response action authorize vlan vlan }
```

```
no authentication event { fail } | { server { alive | dead } } | { no-response }
```

Syntax Description

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

Command Default

The default settings are as follows:

- The *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	This command was introduced.

Usage Guidelines

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

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

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

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

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

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

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

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

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

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

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

Examples

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

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

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

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

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

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

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

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

■ authentication event

Related Commands	Command	Description
	show authentication	Displays Authentication Manager information.

authentication fallback

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

authentication fallback *profile*

Syntax Description	<i>profile</i>	Name to use when failing over to WebAuth (maximum of 200 characters).
---------------------------	----------------	---

Command Default	Disabled
------------------------	----------

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

Command History	Release	Modification
	12.2(50)SG	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(50)SG 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	The following example shows how to enable WebAuth fallback and specify the fallback profile to use when failing over to WebAuth:
-----------------	--

```
Switch(config-if) # authentication fallback fallbacktest1
Switch(config-if) #
```

The following example shows how to disable WebAuth fallback:

```
Switch(config-if) # no authentication fallback fallbacktest1
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(50)SG	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 switching environment refers to the VLAN, and the two supported domains are the DATA domain and the voice domain. Only one client is allowed on a particular domain. So, only two clients (MACs) per port are supported. Each one is required to authenticate separately. Any policies that are downloaded for the client will be applied for that client's MAC/IP only and will not affect the other on the same port. The clients can be authenticated using different methods (such as 802.1X for PC, MAB for IP phone, or vice versa). No restriction exists on the authentication order.

The only caveat 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 enforcement for all types of devices is downloadable ACLs (dACL). The restriction is in place because VLAN assignment is not supported for web-based authentication. Furthermore, if you use dACLs for data devices and not for voice devices, when the user's data falls back to webauth, voice traffic is affected by the ACL that is applied based on the fallback policy. Therefore if webauth is configured as a fallback on an MDA enabled port, dACL is the only supported enforcement method.

Multi-auth mode 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 related to this feature is attached to the host-mode configuration whereby the host-mode itself is significant for the control plane, while the open access configuration is significant for the data plane. Open-access configuration has absolutely no bearing on the session classification. The host-mode configuration still controls this. If the open-access is defined for single-host mode, the port still allows only one MAC address. The port forwards traffic from the start 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

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

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

Related Commands

Command	Description
show 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.

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	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. This command operates per-port rather than globally.

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

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

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

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

Related Commands	Command	Description
	show authentication	Displays Authentication Manager information.

authentication order

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

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

no authentication order

Syntax Description

<i>method1</i>	Authentication method to be attempted. The valid values are as follows: <ul style="list-style-type: none"> dot1x—Adds the dot1x authentication method. mab—Adds the MAB authentication method. webauth—Adds the WebAuth authentication method.
<i>method2</i>	(Optional) Authentication method to be attempted. The valid values are as follows: <ul style="list-style-type: none"> dot1x—Adds the dot1x authentication method. mab—Adds the MAB authentication method. webauth—Adds the WebAuth authentication method.
<i>method3</i>	

Command Default

The default order is dot1x, MAB, then WebAuth.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.2(50)SG	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 run list and no methods may be entered after you enter the **webauth** keyword.

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

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

Examples

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

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

Related Commands

Command	Description
show authentication	Displays Authentication Manager information.

authentication periodic

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

authentication periodic

no authentication periodic

Syntax Description This command has no arguments or keywords.

Command Default Disabled.

Command Modes Interface configuration mode

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

Usage Guidelines The **authentication periodic** command replaces the following dot1x command, which is deprecated in Cisco IOS Release 12.2(50)SG 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 802.1X port-based authentication and causes the port to begin in the unauthorized state.
	force-authorized	(Optional) Disables 802.1X on the interface and causes the port to change to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 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(50)SG	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(50)SG 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

<i>method1</i>	Authentication method to be attempted. The valid values are as follows: <ul style="list-style-type: none"> • dot1x—Adds the dot1x authentication method. • mab—Adds the MAB authentication method. • webauth—Adds the Webauth authentication method.
<i>method2</i> <i>method3</i>	(Optional) Authentication method to be attempted. The valid values are as follows: <ul style="list-style-type: none"> • 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(50)SG	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 <i>value</i>	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 timer value, but configuring the inactivity value higher than the reauthenticate timer 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 <i>value</i>	Specifies the amount of time in seconds after which an automatic reauthentication is initiated. Range is 1 to 65535. Default is 3600.
restart <i>value</i>	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(50)SG	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 command that is deprecated in Cisco IOS Release 12.2(50)SG 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-if)# authentication timer reauthenticate server
Switch(config-if)#
```

Related Commands

Command	Description
show authentication	Displays Authentication Manager information.

authentication violation

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

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

Security violation cannot be triggered in multiplehost or multiauthentication mode.

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

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

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

Command Default 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(50)SG	Command introduced on the Catalyst 4500 series switch.
	12.2(54)SG	Support for replace keyword.

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

Examples The following example shows how to configure violation mode shutdown on a switch:

```
Switch# configure terminal
Switch(config)# authentication violation shutdown
```

A port is error-disabled when a security violation triggers 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: security-violation error detected on <interface name>, putting
<interface name> in err-disable state
```

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

auto qos classify

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

auto qos classify

Syntax Description This command has no arguments or keywords.

Command Default This command has no default settings.

Command Modes Interface configuration mode

Command History	Release	Modification
	15.1(1)SG, 15.1(1)SG IOS-XE 3.3.0	This command was introduced on the Catalyst 4500 series switch.

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

Global Level Commands Generated

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

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

```
ip access-list extended AutoQos-4.0-ACL-Multimedia-Conf
  permit udp any any range 16384 32767
ip access-list extended AutoQos-4.0-ACL-Signaling
  permit tcp any any range 2000 2002
  permit tcp any any range 5060 5061
  permit udp any any range 5060 5061
ip access-list extended AutoQos-4.0-ACL-Transactional-Data
  permit tcp any any eq 443
  permit tcp any any eq 1521
  permit udp any any eq 1521
  permit tcp any any eq 1526
  permit udp any any eq 1526
  permit tcp any any eq 1575
  permit udp any any eq 1575
  permit tcp any any eq 1630
  permit udp any any eq 1630
ip access-list extended AutoQos-4.0-ACL-Bulk-Data
  permit tcp any any eq ftp
  permit tcp any any eq ftp-data
  permit tcp any any eq 22
permit tcp any any eq smtp
  permit tcp any any eq 465
  permit tcp any any eq 143
  permit tcp any any eq 993
  permit tcp any any eq pop3
```

```

    permit tcp any any eq 995
    permit tcp any any eq 1914
ip access-list extended AutoQos-4.0-ACL-Scavenger
    permit tcp any any eq 1214
    permit udp any any eq 1214
    permit tcp any any range 2300 2400
    permit udp any any range 2300 2400
    permit tcp any any eq 3689
    permit udp any any eq 3689
    permit tcp any any range 6881 6999
    permit tcp any any eq 11999
    permit tcp any any range 28800 29100
ip access-list extended AutoQos-4.0-ACL-Default
    permit ip any any

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

```

AutoQos-4.0-VoIP-Data-Cos and AutoQos-4.0-VoIP-Signal-Cos are needed to handle instances when you connect an IP phone to an interface and call the **auto qos voip cisco-phone** command on that interface. In this situation, the input service policy on the interface must match VoIP and signaling packets solely on their CoS markings. This is because switching ASICs on Cisco IP Phones are limited to only remarking the CoS bits of VoIP and the signaling traffic. Matching DSCP markings results in a security vulnerability because a user whose PC was connected to an IP phone connected to a switch would be able to remark DSCP markings of traffic arising from their PC to dscp ef using the NIC on their PC. This causes incorrect placement of non real-time traffic in the priority queue in the egress direction.

B. Template for the **auto qos classify** command input service-policy

```

policy-map AutoQos-4.0-Classify-Input-Policy
    class AutoQos-4.0-Multimedia-Conf-Classify
        set dscp af41
        set cos 4
        set qos-group 34
    class AutoQos-4.0-Signaling-Classify
        set dscp cs3
        set cos 3
        set qos-group 16
    class AutoQos-4.0-Transaction-Classify
        set dscp af21
        set cos 2
        set qos-group 18
    class AutoQos-4.0-Bulk-Data-Classify

```

```

    set dscp af11
    set cos 1
    set qos-group 10
class AutoQos-4.0-Scavenger-Classify
    set dscp cs1
    set cos 1
    set qos-group 8
class AutoQos-4.0-Default-Classify
    set dscp default
    set cos 0

```

C. Template for egress queue classes along with the SRND4 output policy that uses the egress classes to allocate 8 queues. This template is required by all SRND4 commands:

```

class-map match-all AutoQos-4.0-Priority-Queue
    match qos-group 32
class-map match-all AutoQos-4.0-Control-Mgmt-Queue
    match qos-group 16
class-map match-all AutoQos-4.0-Multimedia-Conf-Queue
    match qos-group 34
class-map match-all AutoQos-4.0-Multimedia-Stream-Queue
    match qos-group 26
class-map match-all AutoQos-4.0-Trans-Data-Queue
    match qos-group 18
class-map match-all AutoQos-4.0-Bulk-Data-Queue
    match qos-group 10
class-map match-any AutoQos-4.0-Scavenger-Queue
    match qos-group 8
    match dscp cs1

```

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

```

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

```


Interface Level Commands Generated

For Fa/Gig Ports:

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

Examples

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

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

Related Commands

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

auto qos classify police

To police traffic form an untrusted interface, use the **auto qos classify police** interface command.

auto qos classify police

Syntax Description This command has no arguments or keywords.

Command Default This command has no default settings.

Command Modes Interface configuration mode

Command History	Release	Modification
	15.1(1)SG, 15.1(1)SG IOS-XE 3.3.0	This command was introduced on the Catalyst 4500 series switch.

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

Global Level Commands Generated

Auto QoS srn4 commands, once applied to an interface, generate one or more of the following templates (A, B, and C) at the global configuration level. Typically, a command generates a series of class-maps that either match on ACLs or on DSCP or CoS values to differentiate traffic into application classes. An input policy is generated that matches the generated classes, sets qos-groups on the classes, and in some cases, polices the classes to a set bandwidth. (A qos-group is merely a numerical tag that allows different application classes to be treated as one unit. Outside the switch's context, it has no significance.) Furthermore, eight egress-queue class-maps are generated, matching the qos-groups set in the input policy. The actual egress output policy assigns a queue to each one of these eight egress-queue class-maps.

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

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

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

```
ip access-list extended AutoQos-4.0-ACL-Multimedia-Conf
  permit udp any any range 16384 32767
ip access-list extended AutoQos-4.0-ACL-Signaling
  permit tcp any any range 2000 2002
  permit tcp any any range 5060 5061
  permit udp any any range 5060 5061
ip access-list extended AutoQos-4.0-ACL-Transactional-Data
```

```

    permit tcp any any eq 443
    permit tcp any any eq 1521
    permit tcp any any eq 1521
    permit udp any any eq 1521
    permit tcp any any eq 1526
    permit udp any any eq 1526
    permit tcp any any eq 1575
    permit udp any any eq 1575
    permit tcp any any eq 1630
    permit udp any any eq 1630
ip access-list extended AutoQos-4.0-ACL-Bulk-Data
    permit tcp any any eq ftp
    permit tcp any any eq ftp-data
    permit tcp any any eq 22
permit tcp any any eq smtp
    permit tcp any any eq 465
    permit tcp any any eq 143
    permit tcp any any eq 993
    permit tcp any any eq pop3
    permit tcp any any eq 995
    permit tcp any any eq 1914
ip access-list extended AutoQos-4.0-ACL-Scavenger
    permit tcp any any eq 1214
    permit udp any any eq 1214
    permit tcp any any range 2300 2400
    permit udp any any range 2300 2400
    permit tcp any any eq 3689
    permit udp any any eq 3689
    permit tcp any any range 6881 6999
    permit tcp any any eq 11999
    permit tcp any any range 28800 29100
ip access-list extended AutoQos-4.0-ACL-Default
    permit ip any any

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

```

AutoQos-4.0-VoIP-Data-Cos and AutoQos-4.0-VoIP-Signal-Cos are needed to handle the case in which a user connects an IP phone to an interface and calls the **auto qos voip cisco-phone** command on that interface. In this situation, the input service policy on the interface must match VoIP and signaling packets solely on their CoS markings because switching ASICs on Cisco IP phones are limited to only remarking the CoS bits of VoIP and signaling traffic. Matching DSCP markings would cause a security

vulnerability because user whose PC was connected to an IP phone connected to a switch would be able to re-mark DSCP markings of traffic arising from their PC to dscp ef using the NIC on their PC. This places non real-time traffic in the priority queue in the egress direction.

B. Template for the input service-policy of the **auto qos classify police** command

```

policy-map AutoQos-4.0-Classify-Police-Input-Policy
  class AutoQos-4.0-Multimedia-Conf-Classify
    set dscp af41
    set cos 4
    set qos-group 34
    police cir 5000000 bc 8000
    exceed-action drop
  class AutoQos-4.0-Signaling-Classify
    set dscp cs3
    set cos 3
    set qos-group 16
    police cir 32000 bc 8000
    exceed-action drop
  class AutoQos-4.0-Transaction-Classify
    set dscp af21
    set cos 2
    set qos-group 18
    police cir 10000000 bc 8000
    exceed-action set-dscp-transmit cs1
    exceed-action set-cos-transmit 1
  class AutoQos-4.0-Bulk-Data-Classify
    set dscp af11
    set cos 1
    set qos-group 10
    police cir 10000000 bc 8000
    exceed-action set-dscp-transmit cs1
    exceed-action set-cos-transmit 1
  class AutoQos-4.0-Scavenger-Classify
    set dscp cs1
    set cos 1
    set qos-group 8
    police cir 10000000 bc 8000
    exceed-action drop
  class AutoQos-4.0-Default-Classify
    set dscp default
    set cos 0
    police cir 10000000 bc 8000
    exceed-action set-dscp-transmit cs1
    exceed-action set-cos-transmit 1

```

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

```

class-map match-all AutoQos-4.0-Priority-Queue
  match qos-group 32
class-map match-all AutoQos-4.0-Control-Mgmt-Queue
  match qos-group 16
class-map match-all AutoQos-4.0-Multimedia-Conf-Queue
  match qos-group 34
class-map match-all AutoQos-4.0-Multimedia-Stream-Queue
  match qos-group 26
class-map match-all AutoQos-4.0-Trans-Data-Queue
  match qos-group 18
class-map match-all AutoQos-4.0-Bulk-Data-Queue
  match qos-group 10
class-map match-any AutoQos-4.0-Scavenger-Queue
  match qos-group 8
  match dscp cs1

```

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

```

policy-map AutoQos-4.0-Output-Policy
  bandwidth remaining percent 1
class AutoQos-4.0-Priority-Queue
  priority
  police cir percent 30 bc 33 ms
    conform-action transmit exceed-action drop
class AutoQos-4.0-Control-Mgmt-Queue
  bandwidth remaining percent 10
class AutoQos-4.0-Multimedia-Conf-Queue
  bandwidth remaining percent 10
class AutoQos-4.0-Multimedia-Stream-Queue
  bandwidth remaining percent 10
class AutoQos-4.0-Trans-Data-Queue
  bandwidth remaining percent 10
  db1
class AutoQos-4.0-Bulk-Data-Queue
  bandwidth remaining percent 4
  db1
class class-default
  bandwidth remaining percent 25
  db1

```

Interface Level Commands Generated

For Fa/Gig Ports:

```

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

```

Examples

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

```

Switch(config)# interface gigabitethernet1/1
Switch(config-if)# auto qos classify police
Switch(config-if)# do sh run interface gigabitethernet1
Interface gigabitethernet1
  auto qos classify police
  service-policy input AutoQos-4.0-Classify-Policy-Input-Policy
  service-policy output AutoQos-4.0-Output-Policy
end

```

Related Commands

Command	Description
auto qos voip cisco-softphone	Generates QoS configuration for interfaces connected to PCs running the Cisco IP SoftPhone application and mark police traffic coming from such interfaces.
auto qos classify	Generates a QoS configuration for an untrusted interface.
auto qos srnd4	Generates QoS configurations based on solution reference network design 4.0.

auto qos srnd4

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

auto qos srnd4

Syntax Description This command has no arguments or keywords.

Command Default This command has no default settings.

Command Modes Global configuration

Command History	Release	Modification
	15.1(1)SG, 15.1(1)SG IOS-XE 3.3.0	This command was introduced on the Catalyst 4500 series switch.

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

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

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

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

For interfaces with auto qos voip trust enabled

—Global Level Commands Generated

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

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

```
class-map match-any AutoQos-4.0-VoIP
  match dscp ef
```

```

    match cos 5
class-map match-all AutoQos-4.0-Broadcast-Vid
    match dscp cs5
class-map match-all AutoQos-4.0-Realtime-Interact
    match dscp cs4
class-map match-all AutoQos-4.0-Network-Ctrl
    match dscp cs7
class-map match-all AutoQos-4.0-Internetwork-Ctrl
    match dscp cs6
class-map match-any AutoQos-4.0-Signaling
    match dscp cs3
    match cos 3
class-map match-all AutoQos-4.0-Network-Mgmt
    match dscp cs2
class-map match-any AutoQos-4.0-Multimedia-Conf
    match dscp af41
    match dscp af42
    match dscp af43
class-map match-any AutoQos-4.0-Multimedia-Stream
    match dscp af31
    match dscp af32
    match dscp af33
class-map match-any AutoQos-4.0-Transaction-Data
    match dscp af21
    match dscp af22
    match dscp af23
class-map match-any AutoQos-4.0-Bulk-Data
    match dscp af11
    match dscp af12
    match dscp af13
class-map match-all AutoQos-4.0-Scavenger
    match dscp cs1

```

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

```

policy-map AutoQos-4.0-Input-Policy
    class AutoQos-4.0-VoIP
        set qos-group 32
    class AutoQos-4.0-Broadcast-Vid
        set qos-group 32
    class AutoQos-4.0-Realtime-Interact
        set qos-group 32
    class AutoQos-4.0-Network-Ctrl
        set qos-group 16
    class AutoQos-4.0-Internetwork-Ctrl
        set qos-group 16
    class AutoQos-4.0-Signaling
        set qos-group 16
    class AutoQos-4.0-Network-Mgmt
        set qos-group 16
    class AutoQos-4.0-Multimedia-Conf
        set qos-group 34
    class AutoQos-4.0-Multimedia-Stream
        set qos-group 26
    class AutoQos-4.0-Transaction-Data
        set qos-group 18
    class AutoQos-4.0-Bulk-Data
        set qos-group 10
    class AutoQos-4.0-Scavenger
        set qos-group 8

```

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

```
class-map match-all AutoQos-4.0-Priority-Queue
  match qos-group 32
class-map match-all AutoQos-4.0-Control-Mgmt-Queue
  match qos-group 16
class-map match-all AutoQos-4.0-Multimedia-Conf-Queue
  match qos-group 34
class-map match-all AutoQos-4.0-Multimedia-Stream-Queue
  match qos-group 26
class-map match-all AutoQos-4.0-Trans-Data-Queue
  match qos-group 18
class-map match-all AutoQos-4.0-Bulk-Data-Queue
  match qos-group 10
class-map match-any AutoQos-4.0-Scavenger-Queue
  match qos-group 8
  match dscp cs1
```

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

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

—Interface Level Commands Generated

For Fa/Gig Ports:

If Layer 2 interface:

```
Switch(config-if)# no service-policy input AutoQos-VoIP-Input-Cos-Policy
                  no service-policy output AutoQos-VoIP-Output-Policy
                  service-policy input AutoQos-4.0-Input-Policy
                  service-policy output AutoQos-4.0-Output-Policy
```

If Layer 3 interface:

```
Switch(config-if)# no service-policy input AutoQos-VoIP-Input-Dscp-Policy
                  no service-policy output AutoQos-VoIP-Output-Policy
```



```
service-policy input AutoQos-4.0-Input-Policy
service-policy output AutoQos-4.0-Output-Policy
```

For interfaces with auto qos voip cisco-phone enabled

—Global Level Commands Generated

The global templates defined in A and B (above).

—Interface Level Commands Generated

For Fa/Gig Ports:

```
Switch(config-if)# no qos trust device cisco-phone
no service-policy input AutoQos-VoIP-Input-Cos-Policy
no service-policy output AutoQos-VoIP-Output-Policy
qos trust device cisco-phone
service-policy input AutoQos-4.0-Cisco-Phone-Input-Policy
service-policy output AutoQos-4.0-Output-Policy
```

Examples

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

```
Switch# auto qos srnd4
```

Related Commands

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

auto qos trust

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

auto qos trust

Syntax Description This command has no arguments or keywords.

Command Default This command has no default settings.

Command Modes Interface configuration mode

Command History	Release	Modification
	15.1(1)SG, 15.1(1)SG IOS-XE 3.3.0	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines Global Level Commands Generated

After you apply auto-QoS srnd4 commands to an interface, they generate one or more of the following templates (A and B) at the global configuration level. Typically, a command generates a series of class-maps that either match on ACLs or on DSCP or CoS values to differentiate traffic into application classes. An input policy is generated, which matches the generated classes, sets qos-groups on the classes, and in some cases, polices the classes to a set bandwidth. (A qos-group is simply a numerical tag that allows different application classes to be treated as one unit. Outside the switch's context, it has no significance.) Additionally, eight egress-queue class-maps are generated, matching the qos-groups set in the input policy. The actual egress output policy assigns a queue to each of these eight class-maps.

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

The global templates defined in A and B.

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

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

```
class-map match-any AutoQos-4.0-VoIP
  match dscp ef
  match cos 5
class-map match-all AutoQos-4.0-Broadcast-Vid
  match dscp cs5
class-map match-all AutoQos-4.0-Realtime-Interact
  match dscp cs4
```

```

class-map match-all AutoQos-4.0-Network-Ctrl
  match dscp cs7
class-map match-all AutoQos-4.0-Internetwork-Ctrl
  match dscp cs6
class-map match-any AutoQos-4.0-Signaling
  match dscp cs3
  match cos 3
class-map match-all AutoQos-4.0-Network-Mgmt
  match dscp cs2
class-map match-any AutoQos-4.0-Multimedia-Conf
  match dscp af41
  match dscp af42
  match dscp af43
class-map match-any AutoQos-4.0-Multimedia-Stream
  match dscp af31
  match dscp af32
  match dscp af33
class-map match-any AutoQos-4.0-Transaction-Data
  match dscp af21
  match dscp af22
  match dscp af23
class-map match-any AutoQos-4.0-Bulk-Data
  match dscp af11
  match dscp af12
  match dscp af13
class-map match-all AutoQos-4.0-Scavenger
  match dscp cs1

```

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

```

policy-map AutoQos-4.0-Input-Policy
  class AutoQos-4.0-VoIP
    set qos-group 32
  class AutoQos-4.0-Broadcast-Vid
    set qos-group 32
  class AutoQos-4.0-Realtime-Interact
    set qos-group 32
  class AutoQos-4.0-Network-Ctrl
    set qos-group 16
  class AutoQos-4.0-Internetwork-Ctrl
    set qos-group 16
  class AutoQos-4.0-Signaling
    set qos-group 16
  class AutoQos-4.0-Network-Mgmt
    set qos-group 16
  class AutoQos-4.0-Multimedia-Conf
    set qos-group 34
  class AutoQos-4.0-Multimedia-Stream
    set qos-group 26
  class AutoQos-4.0-Transaction-Data
    set qos-group 18
  class AutoQos-4.0-Bulk-Data
    set qos-group 10
  class AutoQos-4.0-Scavenger
    set qos-group 8

```

B. Templates for egress queue classes and the srnd4 output policy that uses the egress classes to allocate eight queues. This template is required by all srnd4 commands.

```

class-map match-all AutoQos-4.0-Priority-Queue
  match qos-group 32
class-map match-all AutoQos-4.0-Control-Mgmt-Queue

```

```

    match qos-group 16
class-map match-all AutoQos-4.0-Multimedia-Conf-Queue
    match qos-group 34
class-map match-all AutoQos-4.0-Multimedia-Stream-Queue
    match qos-group 26
class-map match-all AutoQos-4.0-Trans-Data-Queue
    match qos-group 18
class-map match-all AutoQos-4.0-Bulk-Data-Queue
    match qos-group 10
class-map match-any AutoQos-4.0-Scavenger-Queue
    match qos-group 8
    match dscp cs1

```

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

```

    policy-map AutoQos-4.0-Output-Policy
class AutoQos-4.0-Scavenger-Queue
    bandwidth remaining percent 1
class AutoQos-4.0-Priority-Queue
    priority
    police cir percent 30 bc 33 ms
        conform-action transmit exceed-action drop
class AutoQos-4.0-Control-Mgmt-Queue
    bandwidth remaining percent 10
class AutoQos-4.0-Multimedia-Conf-Queue
    bandwidth remaining percent 10
class AutoQos-4.0-Multimedia-Stream-Queue
    bandwidth remaining percent 10
class AutoQos-4.0-Trans-Data-Queue
    bandwidth remaining percent 10
    db1
class AutoQos-4.0-Bulk-Data-Queue
    bandwidth remaining percent 4
    db1
class class-default
    bandwidth remaining percent 25

```

Interface Level Commands Generated

For Fa/Gig Ports:

```

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

```

Examples

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

```

Switch(config)# interface gigabitethernet1/1
Switch(config-if)# auto qos trust
Switch(config-if)# do sh running interface interface-id
interface FastEthernet2/1
    auto qos trust
    service-policy input AutoQos-4.0-Input-Policy
    service-policy output AutoQos-4.0-Output-Policy
end

```

Related Commands	Command	Description
	auto qos voip cisco-softphone	Generates QoS configuration for interfaces connected to PCs running the Cisco IP SoftPhone application and mark police traffic coming from such interfaces.
	auto qos classify	Generates a QoS configuration for an untrusted interface.
	auto qos srnd4	Generates QoS configurations based on solution reference network design 4.0.

auto qos video

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

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

Syntax Description

cts	Trust the QoS marking of Cisco Telepresence device.
ip-camera	Trust the QoS marking of Cisco video surveillance camera.

Command Default

This command has no default settings.

Command Modes

Interface configuration mode

Command History

Release	Modification
15.1(1)SG, 15.1(1)SG IOS-XE 3.3.0	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

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

Global Level Commands Generated

When auto-Qos srnd4 commands are applied to an interface, they generate one or more of the following templates at the global configuration level. Typically, a command generates a series of class-maps that either match on ACLs or on DSCP (or CoS) values to differentiate traffic into application classes. An input policy is also generated, which matches the generated classes, sets qos-groups on the classes, and in some cases, polices the classes to a set bandwidth. (A qos-group is simply a numerical tag that allows different application classes to be treated as one unit. Outside the switch's context, it has no significance.) Furthermore, eight egress-queue class-maps are generated, which match the qos-groups set in the input policy. The actual egress output policy assigns a queue to each of the eight egress-queue class-maps.

The srnd4 commands generate the templates only as needed. For example, on first use of the new command, global configurations that define the eight queue egress service-policy are generated. Subsequently, auto-QoS commands applied to other interfaces do not generate templates for egress queuing. This is because all auto-QoS commands rely on the same eight queue model after migration, already generated on first use of the command.

The global templates defined in A and B.

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

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

```

class-map match-any AutoQos-4.0-VoIP
  match dscp ef
  match cos 5
class-map match-all AutoQos-4.0-Broadcast-Vid
  match dscp cs5
class-map match-all AutoQos-4.0-Realtime-Interact
  match dscp cs4
class-map match-all AutoQos-4.0-Network-Ctrl
  match dscp cs7
class-map match-all AutoQos-4.0-Internetwork-Ctrl
  match dscp cs6
class-map match-any AutoQos-4.0-Signaling
  match dscp cs3
  match cos 3
class-map match-all AutoQos-4.0-Network-Mgmt
  match dscp cs2
class-map match-any AutoQos-4.0-Multimedia-Conf
  match dscp af41
  match dscp af42
  match dscp af43
class-map match-any AutoQos-4.0-Multimedia-Stream
  match dscp af31
  match dscp af32
  match dscp af33
class-map match-any AutoQos-4.0-Transaction-Data
  match dscp af21
  match dscp af22
  match dscp af23
class-map match-any AutoQos-4.0-Bulk-Data
  match dscp af11
  match dscp af12
  match dscp af13
class-map match-all AutoQos-4.0-Scavenger
  match dscp cs1

```

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

```

policy-map AutoQos-4.0-Input-Policy
  class AutoQos-4.0-VoIP
    set qos-group 32
  class AutoQos-4.0-Broadcast-Vid
    set qos-group 32
  class AutoQos-4.0-Realtime-Interact
    set qos-group 32
  class AutoQos-4.0-Network-Ctrl
    set qos-group 16
  class AutoQos-4.0-Internetwork-Ctrl
    set qos-group 16
  class AutoQos-4.0-Signaling
    set qos-group 16
  class AutoQos-4.0-Network-Mgmt
    set qos-group 16
  class AutoQos-4.0-Multimedia-Conf
    set qos-group 34
  class AutoQos-4.0-Multimedia-Stream
    set qos-group 26
  class AutoQos-4.0-Transaction-Data
    set qos-group 18
  class AutoQos-4.0-Bulk-Data
    set qos-group 10
  class AutoQos-4.0-Scavenger
    set qos-group 8

```

B. Template for egress queue classes and the srnd4 output policy that uses the egress classes to allocate eight queues. This template is required by all srnd commands:

```
class-map match-all AutoQos-4.0-Priority-Queue
  match qos-group 32
class-map match-all AutoQos-4.0-Control-Mgmt-Queue
  match qos-group 16
class-map match-all AutoQos-4.0-Multimedia-Conf-Queue
  match qos-group 34
class-map match-all AutoQos-4.0-Multimedia-Stream-Queue
  match qos-group 26
class-map match-all AutoQos-4.0-Trans-Data-Queue
  match qos-group 18
class-map match-all AutoQos-4.0-Bulk-Data-Queue
  match qos-group 10
class-map match-any AutoQos-4.0-Scavenger-Queue
  match qos-group 8
  match dscp cs1
```

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

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

Interface Level Commands Generated

For Fa/Gig Ports:

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

Examples

The following example shows how to generate a QoS configuration on the cisco-telepresence interface gigabitethernet1/1:

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



```
Switch(config-if)# do sh running interface gigabitethernet1/1
interface interface-id
  auto qos video cts
  qos trust device cts
  service-policy input AutoQos-4.0-Input-Policy
  service-policy output AutoQos-4.0-Output-Policy
end
```

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

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# auto qos video ip-camera
Switch(config-if)# do sh running interface interface-id
interface interface-id
  auto qos video ip-camera
  qos trust device ip-camera
  service-policy input AutoQos-4.0-Input-Policy
  service-policy output AutoQos-4.0-Output-Policy
end
```

Related Commands

Command	Description
auto qos trust	Generates QoS configurations for trusted interfaces.
auto qos srnd4	Generates QoS configurations based on solution reference network design 4.0.

auto qos voip

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

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

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

Syntax Description

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

Command Default

Auto-QoS is disabled on all interfaces

Command Modes

Interface configuration mode

Command History

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

Usage Guidelines

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

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

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

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

- QoS is globally enabled (**qos** global configuration command).
- DBL is enabled globally (**qos dbl** global configuration command).
- When you enter the **auto qos voip cisco-phone** interface configuration command, the trusted boundary feature is enabled. It uses the Cisco Discovery Protocol (CDP) to detect the presence or absence of a Cisco IP phone. When a Cisco IP phone is detected, the ingress classification on the specific interface is set to trust the CoS label that is received in the packet because some older phones do not mark DSCP. When a Cisco IP phone is absent, the ingress classification is set to not trust the CoS label in the packet.

- When you enter the **auto qos voip trust** interface configuration command, the ingress classification on the specified interface is set to trust the CoS label that is received in the packet provided the specified interface is configured as Layer 2 (and is set to trust DSCP if the interface is configured as Layer 3).

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

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

To disable auto-QoS on an interface, use the **no auto qos voip** interface configuration command. When you enter this command, the switch enables standard QoS and changes the auto-QoS settings to the standard QoS default settings for that interface. This action will not change any global configuration performed by auto-QoS; the global configuration remains the same.

Examples

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

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

The following 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
```

The following example shows how to display the QoS configuration that is automatically generated when auto-QoS is enabled on an interface on a Supervisor Engine 6-E:

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface gigabitethernet3/10
Switch(config-if)#auto qos voip trust
Switch(config-if)#
1d03h: service-policy input AutoQos-VoIP-Input-Cos-Policy
1d03h: service-policy output AutoQos-VoIP-Output-Policy
Switch(config-if)#interface gigabitethernet3/11
Switch(config-if)#auto qos voip
cisco-phone
Switch(config-if)#
1d03h: qos trust device cisco-phone
1d03h: service-policy input AutoQos-VoIP-Input-Cos-Policy
1d03h: service-policy output AutoQos-VoIP-Output-Policy
Switch(config-if)#end
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 trust	Sets the trusted state of an interface.

Command	Description
show auto qos	Displays the automatic quality of service (auto-QoS) configuration that is applied.
show qos	Displays QoS information.
show qos interface	Displays queuing information.
show qos maps	Displays QoS map information.

auto qos voip cisco-softphone

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

auto qos voip cisco-softphone

Syntax Description This command has no arguments or keywords.

Command Default This command has no default settings.

Command Modes Interface configuration mode

Command History	Release	Modification
	15.1(1)SG, 15.1(1)SG IOS-XE 3.3.0	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines Ports configured with **auto qos voip** command are considered untrusted.

Global Level Commands Generated

After auto-QoS `srnd4` commands are applied to an interface, they generate one or more of the following templates (A, B, and C) at the global configuration level. Typically, a command generates a series of class-maps that either match on ACLs or on DSCP (or CoS) values to differentiate traffic into application classes. An input policy is also generated, which matches the generated classes, sets qos-groups on the classes, and in some cases, polices the classes to a set bandwidth. (A qos-group is a numerical tag that allows different application classes to be treated as one unit. Outside the switch's context, it has no significance.) Furthermore, eight egress-queue class-maps are generated, matching the qos-groups set in the input policy. The actual egress output policy assigns a queue to each of these eight class-maps.

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

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

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

```
ip access-list extended AutoQos-4.0-ACL-Multimedia-Conf
  permit udp any any range 16384 32767
ip access-list extended AutoQos-4.0-ACL-Signaling
  permit tcp any any range 2000 2002
  permit tcp any any range 5060 5061
  permit udp any any range 5060 5061
ip access-list extended AutoQos-4.0-ACL-Transactional-Data
  permit tcp any any eq 443
  permit tcp any any eq 1521
```

```

permit udp any any eq 1521
permit tcp any any eq 1526
permit udp any any eq 1526
permit tcp any any eq 1575
permit udp any any eq 1575
permit tcp any any eq 1630
permit udp any any eq 1630
ip access-list extended AutoQos-4.0-ACL-Bulk-Data
permit tcp any any eq ftp
permit tcp any any eq ftp-data
permit tcp any any eq 22
permit tcp any any eq smtp
permit tcp any any eq 465
permit tcp any any eq 143
permit tcp any any eq 993
permit tcp any any eq pop3
permit tcp any any eq 995
permit tcp any any eq 1914
ip access-list extended AutoQos-4.0-ACL-Scavenger
permit tcp any any eq 1214
permit udp any any eq 1214
permit tcp any any range 2300 2400
permit udp any any range 2300 2400
permit tcp any any eq 3689
permit udp any any eq 3689
permit tcp any any range 6881 6999
permit tcp any any eq 11999
permit tcp any any range 28800 29100
ip access-list extended AutoQos-4.0-ACL-Default
permit ip any any

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

```

AutoQos-4.0-VoIP-Data-Cos and AutoQos-4.0-VoIP-Signal-Cos handles those instances when a user connects an IP phone to an interface and enters the **auto qos voip cisco-phone** command on that interface. In this situation, the input service policy on the interface must match VoIP and signaling packets based solely on their CoS markings because switching ASICs on Cisco IP Phones are limited to only remarking the CoS bits of VoIP and signaling traffic. Matching DSCP markings would result in a security vulnerability because a user whose PC was connected to an IP phone connected to a switch

would be able to remark DSCP markings of traffic arriving from their PC to DSCP ef using the NIC on their PC. This results in incorrectly placing non real-time traffic in the priority queue in the egress direction.

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

```

    policy-map AutoQos-4.0-Cisco-Softphone-Input-Policy
class AutoQos-4.0-VoIP-Data
    set dscp ef
    set cos 5
    set qos-group 32
    police cir 128000 bc 8000
    exceed-action set-dscp-transmit cs1
    exceed-action set-cos-transmit 1
        class AutoQos-4.0-VoIP-Signal
            set dscp cs3
            set cos 3
            set qos-group 16
            police cir 32000 bc 8000
            exceed-action set-dscp-transmit cs1
            exceed-action set-cos-transmit 1
class AutoQos-4.0-Multimedia-Conf-Classify
    set dscp af41
    set cos 4
    set qos-group 34
    police cir 5000000 bc 8000
    exceed-action drop
class AutoQos-4.0-Signaling-Classify
    set dscp cs3
    set cos 3
    set qos-group 16
    police cir 32000 bc 8000
    exceed-action drop
class AutoQos-4.0-Transaction-Classify
    set dscp af21
    set cos 2
    set qos-group 18
    police cir 10000000 bc 8000
    exceed-action set-dscp-transmit cs1
    exceed-action set-cos-transmit 1
class AutoQos-4.0-Bulk-Data-Classify
    set dscp af11
    set cos 1
    set qos-group 10
    police cir 10000000 bc 8000
    exceed-action set-dscp-transmit cs1
        exceed-action set-cos-transmit 1
class AutoQos-4.0-Scavenger-Classify
    set dscp cs1
    set cos 1
    set qos-group 8
    police cir 10000000 bc 8000
    exceed-action drop
class AutoQos-4.0-Default-Classify
    set dscp default
    set cos 0

```

C. Template for egress queue classes and the srnd4 output policy that uses the egress classes to allocate eight queues. This template is required by all srnd4 commands:

```

class-map match-all AutoQos-4.0-Priority-Queue
    match qos-group 32
class-map match-all AutoQos-4.0-Control-Mgmt-Queue
    match qos-group 16

```

```

class-map match-all AutoQos-4.0-Multimedia-Conf-Queue
  match qos-group 34
class-map match-all AutoQos-4.0-Multimedia-Stream-Queue
  match qos-group 26
class-map match-all AutoQos-4.0-Trans-Data-Queue
  match qos-group 18
class-map match-all AutoQos-4.0-Bulk-Data-Queue
  match qos-group 10
class-map match-any AutoQos-4.0-Scavenger-Queue
  match qos-group 8
  match dscp cs1

```

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

```

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

```

Interface Level Commands Generated

For Fa/Gig Ports:

```

Switch(config-if)#
  service-policy input AutoQos-4.0-Cisco-Softphone-Input-Policy
  service-policy input AutoQos-4.0-Output-Policy

```

Examples

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

```

Switch(config)# interface gigabitethernet1/1
Switch(config-if)# auto qos voip cisco-softphone
Switch(config-if)# do sh running interface gigabitethernet1/1
interface gigabitethernet1/1
  auto qos voip cisco-phone
  qos trust device cisco-phone

```



```
service-policy input AutoQos-4.0-Cisco-Phone-Input-Policy
service-policy output AutoQos-4.0-Output-Policy
end
```

Related Commands

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

auto security

To enable auto security globally, use the **auto security** command. Use the **no** form of this command to disable auto security.

auto security

no auto security

Syntax Description This command has no arguments or keywords.

Command Default none

Command Modes Interface configuration mode

Command History	Release	Modification
	3.6.0E	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines Relevant baseline security feature CLI as shown in the output of the show auto security command is applied on or removed from access and trunk ports.

Examples The following example shows how to enable auto security globally:

```
Switch(config)# auto security
Switch# show running-config | i security
auto security
```

auto security-port

To enable auto security feature for access (end hosts) or uplink ports, use the **auto security-port** command. To disable the feature, use the **no** form of this command.

auto security-port [host | uplink]

no auto security-port [host | uplink]

Syntax Description	host	Enables auto security on host facing port.
	uplink	Enables auto security on server facing /uplink port.

Command Default	none
-----------------	------

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

Command History	Release	Modification
	3.6.0E	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines	This command is supported on Catalyst 3750X, Catalyst 2960S, and the Catalyst 4500 series starting with Cisco IOS Release 15.2(2)E.
------------------	---

Examples	<p>The following example shows how to enable auto security on a host-facing port:</p> <pre>Switch# conf t Enter configuration commands, one per line. End with CNTL/Z. Switch(config)# int g1/0/18 Switch(config-if)# auto security-port host Switch(config-if)# end Switch# Apr 5 22:16:41.725: %SYS-5-CONFIG_I: Configured from console by consolesh auto security Switch# show auto security Auto Secure is Enabled globally AutoSecure is Enabled on below interface(s): ----- GigabitEthernet1/0/2 GigabitEthernet1/0/3 GigabitEthernet1/0/15 GigabitEthernet1/0/18</pre>
----------	--

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.

Command Default

Standard automatic synchronization of all configuration files

Command Modes

Redundancy main-cpu mode

Command History

Release	Modification
12.1(12c)EW	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

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

```
Switch# config terminal
Switch (config)# redundancy
Switch (config-r)# main-cpu
Switch (config-r-mc)# no auto-sync standard
Switch (config-r-mc)# auto-sync configure-register
Switch (config-r-mc)#
```

Related Commands

Command	Description
redundancy	Enters the redundancy configuration mode.

average-packet-size (netflow-lite monitor submode)



Note

NetFlow-lite is supported only on Catalyst 4948E and Catalyst 4948E-F Ethernet switches.

To specify the average packet size at the observation point in netflow-lite monitor submode, use the **average-packet-size** command. To delete a sampler, use the **no** form of this command.

average-packet-size *average-packet-size*

no average-packet-size *average-packet-size*

Syntax Description	<i>average-packer-size</i>	Specifies the average packet size in bytes expected at the observation point.
--------------------	----------------------------	---

Command Default	0 bytes
-----------------	---------

Command Modes	netflow-lite exporter submode
---------------	-------------------------------

Command History	Release	Modification
	15.0(2)SG	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

You can enter this command in physical port interface mode, port channel interface, or config VLAN mode.

The packet sampling mechanism attempts random 1-in-N sampling. Internally, 2 levels of sampling are performed. The accuracy of the first sampling level depends on the size of the packets arriving at a given interface. Use the **average-packet-size** parameter to tune the accuracy of the algorithm.

The system automatically determines the average packet size at an interface based on observation of input traffic and uses that value in its first level of sampling.

The algorithm requires a range of packet sizes from 64 to 9216 bytes. A value of 0 means that you want an automatic determination of average packet size.

Examples

The following example shows how to configure a monitor on a port interface Gigabit 1/3:

```
Switch# config terminal
Switch(config)# int GigabitEthernet1/3
Switch(config-if)# netflow-lite monitor 1
Switch(config-netflow-lite-monitor)# sampler sampler1
Switch(config-netflow-lite-monitor)# exporter exporter1
Switch(config-netflow-lite-monitor)# average-packet-size 128
Switch(config-netflow-lite-monitor)# exit
Switch(config-if)# exit
Switch(config)# exit
Switch(config)#
```

average-packet-size (netflow-lite monitor submode)

```
Switch# show netflow-lite monitor 1 interface gi1/3
Interface GigabitEthernet1/3:
  Netflow-lite Monitor-1:
    Active:                TRUE
    Sampler:               sampler1
    Exporter:              exporter1
    Average Packet Size:   0
  Statistics:
    Packets exported:      0
    Packets observed:      0
    Packets dropped:       0
    Average Packet Size observed: 64
    Average Packet Size used: 64
```

You can verify your settings with the **show netflow-lite exporter** privileged EXEC command.

Related Commands

Command	Description
sampler (netflow-lite monitor submode)	Activates sampling on an interface in netflow-lite monitor submode.
exporter (netflow-lite monitor submode)	Assigns an exporter in netflow-lite monitor submode.

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

<i>bandwidth-kbps</i>	Amount of bandwidth in kbps assigned to the class. The range is 32 to 16000000.
percent <i>percent</i>	Percentage of available bandwidth assigned to the parent class. The range is 1 to 100.
remaining percent <i>percent</i>	Percentage of remaining bandwidth assigned to parent class. The range is 1 to 100. This command is supported only when priority queuing class is configured, and the priority queuing class is not rate-limited.

Command Default

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

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

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

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

- If the **percent** keyword is used, the sum of the class bandwidth percentages within a single policy map cannot exceed 100 percent. Percentage calculations are based on the bandwidth available on the port.

- The amount of bandwidth configured should be large enough to accommodate Layer 2 overhead.
- A policy map can have all the class bandwidths specified in either kbps or in percentages, but not a mix of both.

Examples

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

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# policy-map polmap6
Switch(config-pmap)# class silver-class
Switch(config-pmap-c)# bandwidth 2000
Switch(config-pmap-c)# end
```

The following 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 50
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
```

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

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# policy-map policy1
Switch(config-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 voice1
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 queueing [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-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.

border

To configure the IP address of the fabric border device in the fabric domain, use the **border ip address** command. The no border IP address command removes reference the association of the border device from the edge device.

border ip address

no border ip address

Syntax Description	<i>ip address</i>	Configures the IP address of the fabric border device.
Command Default	None.	
Command Modes	Fabric-auto-domain configuration	
Command History	Release	Modification
	3.9.01E	This command was introduced on the Catalyst 4500-E series switch using a Supervisor Engines 8-E and 8L-E.

Usage Guidelines

Use this command to configure the IP address of the fabric border device. Border devices in the fabric domain connect traditional Layer 3 networks or different fabric domains to the local domain, and translate reachability and policy (VRF and SGT) information from one domain to another.

This command auto-generates LISP configuration, to orchestrate the fabric overlay. The **show-running configuration** command shows the fabric domain configuration including the auto-generated commands.

Examples

The following configuration is auto-generated when this command is run on your device:

```
Device(config-fabric-auto-domain)#border 198.51.100.4
  ipv4 use-petr 198.51.100.4 priority 10 weight 10
```

capwap-ac address

To configure a Control And Provisioning of Wireless Access Point (CAPWAP) access controller address, use the **capwap-ac address** command in DHCPv6 pool configuration mode. To remove the CAPWAP access controller address, use the **no** form of this command.

capwap-ac address *ipv6-address*

no capwap-ac address *ipv6-address*

Syntax Description	<i>ipv6-address</i>	IPv6 address for the CAPWAP access controller.
---------------------------	---------------------	--

Command Default	Access controller address is not configured.
------------------------	--

Command Modes	DHCPv6 pool configuration (config-dhcpv6)
----------------------	---

Command History	Release	Modification
	Cisco IOS Release 15.2(5)E2	This command was introduced on Cisco Catalyst 4500 series switches.

Usage Guidelines	<p>The CAPWAP protocol allows lightweight access points to use DHCPv6 to discover a Wireless Controller to which it can connect. CAPWAP is a standard, interoperable protocol that enables a controller to manage a collection of wireless access points.</p> <p>Wireless access points use the DHCPv6 option 52 (RFC 5417) to supply the IPv6 management interface addresses of the primary, secondary, and tertiary Wireless Controllers.</p>
-------------------------	---

Examples	The following example shows how to configure an IPv6 address for a CAPWAP access controller:
-----------------	--

```
Device> enable
Device# configure terminal
Device(config)# ipv6 dhcp pool pool1
Device(config-dhcpv6)# capwap-ac address 2001:DB8::1
Device(config-dhcpv6)# end
```

Related Commands	Command	Description
	ipv6 dhcp pool	Configures a DHCPv6 server configuration information pool and enters DHCPv6 pool configuration mode.

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 Supervisor Engine 6E and the Catalyst 4900M.

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.
- **contract-id** *alphanumeric*—Specifies the customer contract 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** *name*—Provides customer identification for Cisco AutoNotify. You can enter up to 256 alphanumeric characters. If you include spaces, you must enclose your entry in quotes (" ").
- **default**—Sets a command to its defaults.
- **exit**—Exits call home configuration mode and returns to global configuration mode.
- **mail-server** { *ipv4-address* | *name* } **priority** *priority*—Assigns the customer's e-mail server address and relative priority. You can enter an IP address or a fully qualified domain name (FQDN), and assign a priority from 1 (highest) to 100 (lowest).

You can define backup e-mail servers by repeating the **mail-server** command and entering different **priority** numbers.

- **no**—Negates a command or 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*—Configures the call-home message rate-limit threshold; valid values are from 1 to 60 messages per minute.
- **sender** {**from** | **reply-to**} *email-address*—Specifies the call-home message sender's e-mail addresses. You can enter up to 128 alphanumeric characters in e-mail address format with no spaces.
- **site-id** *alphanumeric*—Specifies the site identification for Cisco AutoNotify. You can enter up to 256 alphanumeric characters. If you include spaces, you must enclose your entry in quotes (“ ”).
- **street-address** *street-address*—Specifies the street address for the RMA part shipments. You can enter up to 256 alphanumeric characters. If you include spaces, you must enclose your entry in quotes (“ ”).
- **vrf**—Specifies the VPN routing or forwarding instance name; limited to 32 characters.

Examples

This example show how to configure the contact information:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# call-home
Switch(cfg-call-home)# contact-email-addr username@example.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 Site1ManhattanNY
Switch(cfg-call-home)# contract-id Company1234
Switch(cfg-call-home)# exit
Switch(config)#
```

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

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

The following 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
```

The following 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 profile1a
```

The following 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)#
```

The following 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-advisory} [profile name] [ccoid user-id]
```

Syntax Description

output-analysis " <i>show-command</i> "	Sends the output of the specified CLI show command for analysis. The show command must be contained in quotes (" ").
config-sanity bugs-list command-reference product-advisory	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.
profile <i>name</i>	(Optional) Specifies an existing profile to which the request is sent. If no profile is specified, the request is sent to the Cisco TAC profile.
ccoid <i>user-id</i>	(Optional) Specifies the identifier of a registered Smart Call Home user. If a <i>user-id</i> is specified, the resulting analysis report is sent to the e-mail address of the registered user. If no <i>user-id</i> 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 Supervisor Engine 6E and the Catalyst 4900M.

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-advisory**—Product Security Incident Response Team (PSIRT) notices, End of Life (EOL) or End of Sales (EOS) notices, or field notices (FN) that may affect devices in your network.

Examples

The following example shows a request for analysis of a user-specified show command:

```
Switch# call-home request output-analysis "show diagnostic result module all" profile TG
```

Related Commands

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

call-home send

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

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

Syntax Description

"cli-command"	Specifies a CLI command to be executed. The command output is sent by e-mail.
email <i>email-addr</i>	Specifies the e-mail address to which the CLI command output is sent. If no e-mail address is specified, the command output is sent to the Cisco TAC at attach@cisco.com.
service-number <i>SR</i>	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(52)SG	This command was introduced on Supervisor Engine 6E and the Catalyst 4900M.

Usage Guidelines

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

The command output is then sent by e-mail to the specified e-mail address. If no e-mail address is specified, the command output is sent to 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

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

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

Related Commands

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

call-home send alert-group

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

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

Syntax Description

configuration	Sends the configuration alert-group message to the destination profile.
diagnostic module <i>number</i>	Sends the diagnostic alert-group message to the destination profile for a specific module number.
inventory	Sends the inventory call-home message.
profile <i>profile-name</i>	(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 Supervisor Engine 6E and the Catalyst 4900M.

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

The following example shows how to send the configuration alert-group message to the destination profile:

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

The following 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
```

The following 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 Ciscotacl
```

The following 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 [*“test-message”*] **profile** *profile-name*

Syntax Description	
<i>“test-message”</i>	(Optional) Test message text.
profile <i>profile-name</i>	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 Supervisor Engine 6E and the Catalyst 4900M.

Usage Guidelines This command sends a test message to the specified destination profile. If you enter test 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 The following 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

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

Command Default

No channel groups are assigned.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch.
12.1(13)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 when it contains member ports.

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

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

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

**Caution**

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

Examples

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

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

Related Commands

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

channel-protocol

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

channel-protocol { lacp | pagp }

no channel-protocol { lacp | pagp }

Syntax Description

lacp	Enables LACP to manage channeling.
pagp	Enables PAgP to manage channeling.

Command Default

pagp

Command Modes

Interface configuration mode

Command History

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

Usage Guidelines

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

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

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

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

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

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

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

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

Examples

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

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

cisp enable

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

cisp enable

no cisp enable

Syntax Description	Command	Description
	cisp enable	Enable CISP.

Command Default	Default
	None

Command Modes	Mode
	Global configuration

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

Usage Guidelines	Guidelines
	You must enable the CISP protocol (with the global cisp enable command) on both the authenticator and supplicant switch. The CISP protocol is crucial because it conveys the client information from the supplicant switch to the authenticator switch thereby providing access for the clients of the supplicant switch through the authenticator switch.

Examples	Example
	The following example shows how to enable CISP: <pre>switch(config)# cisp enable</pre>

Related Commands	Command	Description
	dot1x credentials (global configuration)	Configures a profile on a supplicant switch.
	show cisp	Displays CISP information for a specified interface. Refer to IOS documentation.

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

<i>class-name</i>	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 <i>class-map-name</i> global configuration command.
-------------------	--

Command Default

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

Command Modes

Policy-map configuration mode

Command History

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

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. The class name that you specify with the **class** command in the policy map ties the characteristics for that class (its policy) to the class map and its match criteria, as configured through the **class-map** global configuration command. You attach the policy map to a port by using the **service-policy (interface configuration)** configuration command.

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

- **bandwidth** Specifies or modifies the minimum bandwidth provided to a class belonging to a policy map. For more information, see the **bandwidth** command.
- **dbl** Enables dynamic buffer limiting for traffic hitting this class. For details on **dbl** parameters refer to the **show 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 (two rates)** and the **police (percent)** command.

- **priority** Enables the strict priority queue for a class of traffic. For more information, see the **priority** command.
- **service-policy (policy-map class)** Creates a service policy as a quality of service (QoS) policy within a policy map (called a hierarchical service policy). For more information, see the **service-policy (policy-map class)** command. This command is effective only in a hierarchical policy map attached to an interface.
- **set** Classifies IP traffic by setting a class of service (CoS), a Differentiated Services Code Point (DSCP) or IP-precedence in the packet. For more information, see the **set** command.
- **shape (class-based queueing)** Sets the token bucket committed information rate (CIR) in a policy map. For more information, see the **shape (class-based queueing)** command.
- **trust** Defines a trust state for a traffic class. For more information, see the **trust** command. This command is not supported on Supervisor Engine 6-E, Supervisor Engine 6L-E, Catalyst 4900M, Catalyst 4948E, and Catalyst 4948E-F.

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 as members of the default traffic class. You configure the default traffic class by specifying **class-default** as the class name in the **class** policy-map class configuration command. You can manipulate the default traffic class (for example, set policies to police or to shape it) just like any other traffic class, but you cannot delete it.

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

Examples

The following 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 bursts of 20 KB. Traffic exceeding the profile is marked down to a Traffic exceeding the profile is marked down to a DSCP value obtained from the policed-DSCP map and then sent.

```
Switch# configure terminal
Switch(config)# class-map class1
Switch(config-cmap)# exit
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 queueing [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 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.
	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.
<i>class-map-name</i>	Name of the class map.

Command Default

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(8a)EW	This command was introduced on the Catalyst 4500 series switch.

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

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

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

The following example shows how to delete the class1 class map:

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

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

Related Commands

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

clear counters

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

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

Syntax Description		
FastEthernet <i>interface_number</i>	(Optional) Specifies the Fast Ethernet interface; valid values are from 1 to 9.	
GigabitEthernet <i>interface_number</i>	(Optional) Specifies the Gigabit Ethernet interface; valid values are from 1 to 9.	
null <i>interface_number</i>	(Optional) Specifies the null interface; the valid value is 0.	
port-channel <i>number</i>	(Optional) Specifies the channel interface; valid values are from 1 to 64.	
vlan <i>vlan_id</i>	(Optional) Specifies the VLAN; valid values are from 1 to 4096.	

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.1(8a)EW	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 enter the **show interface counters** command.

Examples The following example shows how to clear all the interface counters:

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

The following 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#
```

■ clear counters

Related Commands

Command	Description
show interface counters (refer to Cisco IOS documentation)	Displays interface counter information.

clear errdisable interface

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

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

Syntax Description

<i>interface-id</i>	Specifies interface and port.
<i>vlan-list</i>	(Optional) Specifies a list of VLANs to be re-enabled. If not specified, then all VLANs are re-enabled.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)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 the disabled VLANs on an interface.

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

You can re-enable a port by using the **shutdown** and **no shutdown** interface configuration commands, or you can clear error disable for VLANs by using the **clear errdisable interface** command.

Examples

The following example shows how to re-enable all VLANs that were error-disabled on Gigabit Ethernet port 4/0/2.

```
Switch# clear errdisable interface gigabitethernet4/0/2 vlan
```

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

```
Switch# clear errdisable interface ethernet2 vlan 10-15
Switch#
```

Related Commands

Command	Description
errdisable detect cause	Enables error-disabled detection for a specific cause or all causes.
errdisable recovery	Configures the recovery mechanism variables.

Command	Description
show errdisable detect	Displays error-disabled detection status.
show errdisable recovery	Display error-disabled recovery timer information.
show interfaces status	Displays interface status of a list of interfaces in error-disabled state.

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	<i>slot_num</i> Slot on a line module.
---------------------------	--

Command Default	The password is not cleared.
------------------------	------------------------------

Command Modes	Privileged EXEC mode
----------------------	----------------------

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

Usage Guidelines	You only need to change the password once unless the password is reset.
-------------------------	---

Examples	The following example shows how to clear the password from slot 5 on a line module:
-----------------	---

```
Switch# clear hw-module slot 5 password
Switch#
```

Related Commands	Command	Description
	hw-module power	Turns the power off on a slot or line module.

clear interface gigabitethernet

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



Note

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

```
clear interface gigabitethernet mod/port
```

Syntax Description

mod/port Number of the module and port.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

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

Examples

The following 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 status.

clear interface vlan

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

clear interface vlan *number*

Syntax Description	<i>number</i> Number of the VLAN interface; valid values are from 1 to 4094.
---------------------------	--

Command Default	This command has no default settings.
------------------------	---------------------------------------

Command Modes	Privileged EXEC mode
----------------------	----------------------

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

Examples	<p>The following example shows how to clear the hardware logic from a specific VLAN:</p> <pre>Switch# clear interface vlan 5 Switch#</pre>
-----------------	--

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

clear ip access-template

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

clear ip access-template *access-list*

Syntax Description	<i>access-list</i> 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.
---------------------------	---

Command Default	This command has no default settings.
------------------------	---------------------------------------

Command Modes	Privileged EXEC mode
----------------------	----------------------

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

Examples The following 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.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

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

Examples The following 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 <i>vlan-range</i>	(Optional) Specifies the VLAN range.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

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

Examples The following 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.
<i>ip-address</i>	(Optional)	IP address for the DHCP snooping binding entries.
vlan <i>vlan_num</i>	(Optional)	Specifies a VLAN.
interface <i>interface_num</i>	(Optional)	Specifies an interface.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.2(44)SG	This command was introduced on the Catalyst 4500 series switch.

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

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

The following example shows how to clear a specific DHCP snooping binding entry:

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

The following example shows how to clear all the DHCP snooping binding entries on the GigabitEthernet interface 1/1:

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

The following example shows how to clear all the DHCP snooping 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.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

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

Examples The following example shows how to clear the DHCP binding database:

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

Related Commands	Command	Description
		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 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.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

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

Examples The following 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}]
```

Syntax Description		
fastethernet		(Optional) Specifies the Fast Ethernet interface.
<i>mod/port</i>		(Optional) Number of the module and port.
GigabitEthernet		(Optional) Specifies the Gigabit Ethernet interface.
<i>host_name</i>		(Optional) Hostname, as defined in the DNS hosts table or with the ip host command.
<i>group_address</i>		(Optional) Address of the multicast group in four-part, dotted notation.
Loopback <i>interface_number</i>		(Optional) Specifies the loopback interface; valid values are from 0 to 2,147,483,647.
null <i>interface_number</i>		(Optional) Specifies the null interface; the valid value is 0.
port-channel <i>number</i>		(Optional) Specifies the channel interface; valid values are from 1 to 64.
vlan <i>vlan_id</i>		(Optional) Specifies the VLAN; valid values are from 1 to 4094.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.1(8a)EW	This command was introduced on the Catalyst 4500 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 The following example shows how to clear the entries for a specific group from the IGMP cache:

```
Switch# clear ip igmp group 224.0.255.1
Switch#
```

■ clear ip igmp group

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

```
Switch# clear ip igmp group gigabitethernet 2/2
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), use the show ip igmp groups command in EXEC 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 <i>vlan_id</i> (Optional) Specifies a VLAN; valid values are from 1 to 1001 and from 1006 to 4094.
---------------------------	--

Command Default	This command has no default settings.
------------------------	---------------------------------------

Command Modes	Privileged EXEC mode
----------------------	----------------------

Command History	Release	Modification
	12.1(20)EW	This command was introduced on the Catalyst 4500 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	The following 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
	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.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

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

Examples The following 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.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.1(8a)EW	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 The following 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 ip wccp

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

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

Syntax Description	web-cache	(Optional) Directs the router to remove statistics for the web cache service.
	<i>service-number</i>	(Optional) Number of the cache service to be removed. The number can be from 0 to 99.

Command Default No default behavior or values.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	15.0(2)SG	This command was introduced on Supervisor Engine 6-E, Supervisor Engine 6L-E, Catalyst 4900M, Catalyst 4948E, and Catalyst 4948E-F.

Usage Guidelines Use the **show ip wccp** and **show ip wccp detail** commands to display WCCP statistics. Use the **clear ip wccp** command to clear the WCCP counters for all WCCP services in all VRFs.

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

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

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

clear lacp counters

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

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

Syntax Description	<i>channel-group</i> (Optional) Channel-group number; valid values are from 1 to 64.
---------------------------	--

Command Default	This command has no default settings.
------------------------	---------------------------------------

Command Modes	Privileged EXEC mode
----------------------	----------------------

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

Usage Guidelines	<p>If you do not specify a channel group, all channel groups are cleared.</p> <p>If you enter this command for a channel group that contains members in PAgP mode, the command is ignored.</p>
-------------------------	--

Examples	The following 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 <i>mac_addr</i>	(Optional) Specifies the MAC address.
interface <i>interface</i>	(Optional) Specifies the interface and clears the entries associated with it; valid values are FastEthernet and GigabitEthernet .
vlan <i>vlan_id</i>	(Optional) Specifies the VLANs; valid values are from 1 to 4094.
notification	Specifies MAC change notification global counters.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch.
12.1(12c)EW	Support for extended VLAN addresses added.
12.2(31)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-NATIFICATION-MIB.

Examples

The following 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#
```

The following 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.
	main-cpu	Enters the main CPU submode and manually synchronizes the configurations on two supervisor engines.
	show mac-address-table address	Displays the information about the MAC-address table.
	snmp-server enable traps	Enables SNMP notifications.

clear mac-address-table dynamic

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

```
clear mac-address-table dynamic [{address mac_addr} | {interface interface}] [vlan vlan_id]
```

Syntax Description	Parameter	Description
	address <i>mac_addr</i>	(Optional) Specifies the MAC address.
	interface <i>interface</i>	(Optional) Specifies the interface and clears the entries associated with it; valid values are FastEthernet and GigabitEthernet .
	vlan <i>vlan_id</i>	(Optional) Specifies the VLANs; valid values are from 1 to 4094.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.1(8a)EW	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 The following 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.
	main-cpu	Enters the main CPU submode and manually synchronizes the configurations on two supervisor engines.
	show mac-address-table address	Displays the information about the MAC-address table.

clear netflow-lite exporter statistics


Note

NetFlow-lite is supported only on the Catalyst 4948E and Catalyst 4948E-F Ethernet switches.

To clear the collector statistics, use the **clear netflow-lite exporter statistics** command.

clear netflow-lite exporter *exporter-name* **statistics**

Syntax Description

exporter-name Specifies an exporter.

Command Default

None

Command Modes

Privileged EXEC mode

Command History

Release	Modification
15.0(2)SG	Command introduced on on the Catalyst 4948E and Catalyst 4948E-F Ethernet switches.

Examples

The following examples show how to clear statistics of a packet sampler at a monitor:

```
Switch# clear netflow-lite exporter e1 statistics
```

Related Commands

Command	Description
clear netflow-lite monitor statistics interface	Clears statistics of a packet sampler at a monitor.

clear netflow-lite monitor statistics interface


Note

NetFlow-lite is supported only on the Catalyst 4948E and Catalyst 4948E-F Ethernet switches.

To clear statistics of a packet sampler at a monitor, use the **clear netflow-lite monitor statistics interface** command.

```
clear netflow-lite monitor statistics interface vlan-id
```

Syntax Description

<i>vlan-id</i>	Specifies an interface.
----------------	-------------------------

Command Default

None

Command Modes

Privileged EXEC mode

Command History

Release	Modification
15.0(2)SG	Command introduced on the Catalyst 4948E and Catalyst 4948E-F Ethernet switches.

Examples

The following examples show how to clear statistics of a packet sampler at a monitor:

```
Switch# clear netflow-lite monitor 1 statistics int gi1/1
Switch# clear netflow-lite monitor 1 statistics vlan 10
```

Related Commands

Command	Description
clear netflow-lite exporter statistics	Clear the collector statistics.

clear nmosp statistics

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

clear nmosp statistics

Syntax Description This command has no arguments or keywords.

Command Default No default is defined.

Command Modes Privileged EXEC mode

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

Examples The following example shows how to clear NMSP statistics:

```
Switch# clear nmosp statistics
Switch#
```

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

Related Commands	Command	Description
	show nmosp	Displays the NMSP information.

clear pagp

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

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

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

Command Default	This command has no default settings.
-----------------	---------------------------------------

Command Modes	Privileged EXEC mode
---------------	----------------------

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

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

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

The following 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 <i>mac-addr</i>	(Optional)	Deletes the specified secure MAC address.
vlan <i>vlan-id</i>	(Optional)	Deletes the specified secure MAC address from the specified VLAN.
interface <i>interface-id</i>	(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.

Command Default 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(18)EW	This command was first introduced on the Catalyst 4500 series switch.
	12.2(31)SG	Add support for sticky port security.

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

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

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

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

clear port-security

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

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

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

Related Commands

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

clear pppoe intermediate-agent statistics

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

clear pppoe intermediate-agent statistics

Syntax Description

This command has no arguments.

Command Default

This command has no default settings.

Command Modes

Privileged 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 clear PPPoE Intermediate Agent statistics:

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

Related Commands

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

clear qos

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

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

Syntax Description

aggregate-policer <i>name</i>	(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.
<i>mod/interface</i>	(Optional) Number of the module and interface.
vlan <i>vlan_num</i>	(Optional) Specifies a VLAN.
port-channel <i>number</i>	(Optional) Specifies the channel interface; valid values are from 1 to 64.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

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

Usage Guidelines

This command is not supported on Supervisor Engine 6-E, Supervisor Engine 6L-E, Catalyst 4900M, Catalyst 4948E, and Catalyst 4948E-F.



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

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

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

The following 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 switch virtual dual-active fast-hello

To clear counters related to fast-hello interfaces for a virtual switching system (VSS), use the **clear switch virtual dual-active fast-hello** command in EXEC mode.

clear switch virtual dual-active fast-hello [counters | packet]

Syntax Description	counters	(Optional)Clear counters related to exchange of fast-hello packets between fast-hello interfaces.
	packet	(Optional) Clear cumulative counters related to exchange of fast-hello packets between the VSS members.

Command Default This command has no default settings.

Command Modes EXEC (>)

Command History	Release	Modification
	Release IOS XE 3.5.0E and IOS 15.2(1)SG	This command was introduced.

Usage Guidelines Use this command to clear fast-hello counters and packet statistics.

Examples The following example shows how to clear counters related to fast-hello interfaces:

```
Switch# clear switch virtual dual-active fast-hello ?
  counters  Dual-active fast-hello link counters
  packet    Dual-active fast-hello pkt counters
  <cr>
Switch# clear switch virtual dual-active fast-hello counters ?
  interface Interface
  <cr>
```

Related Commands	Command	Description
	dual-active detection (virtual switch)	Enables and configures dual-active detection.
	snmp ifindex clear	Configures the VSS domain number and enter the virtual switch domain configuration submode.

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	<i>vlan-id</i> (Optional) VLAN number
---------------------------	---------------------------------------

Command Default	This command has no default settings.
------------------------	---------------------------------------

Command Modes	Privileged EXEC mode
----------------------	----------------------

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

Usage Guidelines	If you do not specify a <i>vlan-id</i> value; the software-cached counter values for all the existing VLANs are cleared.
-------------------------	--

Examples	The following example shows how to clear the software-cached counter values for a specific VLAN:
-----------------	--

```
Switch# clear vlan 10 counters
Clear "show 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.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

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

Examples The following 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.

Command Default Default service police *system-cpp-policy* is attached.

Command Modes Global configuration mode

Command History	Release	Modification
	12.2(31)SG	This command was introduced on the Catalyst 4500 series switch.
	12.2(50)SG	This command was introduced on Supervisor 6-E and Catalyst 4900M.
	12.2(52)XO	This command was introduced on Supervisor 6L-E
	12.2(54)XO	This command was introduced on Catalyst 4948-E

Usage Guidelines After you enter the **control-plane** command, you can define control plane services for your route 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 trusted host traffic.
Switch(config)# access-list 140 deny tcp host 10.1.1.2 any eq telnet
! Rate limit all other Telnet traffic.
Switch(config)# access-list 140 permit tcp any any eq telnet
! Define class-map "telnet-class."
Switch(config)# class-map telnet-class
Switch(config-cmap)# match access-group 140
Switch(config-cmap)# exit
Switch(config)# policy-map control-plane
Switch(config-pmap)# class telnet-class
Switch(config-pmap-c)# police 32000 1000 conform transmit exceed drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
```

```
! Define aggregate control plane service for the active Route Processor.
Switch(config)# macro global apply system-cpp
Switch(config)# control-plane
Switch(config-cp)# service-police 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 <i>Cisco IOS Release 12.2 Command Reference</i>)	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.

context

To configure layer 3 contexts in the fabric domain, use the **context** *name* **id** *id* command.

context *name*

id *id*

Syntax Description

<i>name</i>	Creates a new layer 3 context in the fabric domain.
<i>id</i>	Assigns an ID to the context.

Command Default

None.

Command Modes

Fabric-auto-domain configuration

Command History

Release	Modification
3.9.01E	This command was introduced on the Catalyst 4500-E series switch using a Supervisor Engines 8-E and 8L-E.

Usage Guidelines

A virtual context provides virtualization at the device level, using virtual routing and forwarding (VRF), to create multiple instances of Layer 3 routing tables. Contexts or VRFs provide segmentation across IP addresses, allowing for overlapped address space and traffic separation.

This command enables the auto-generation of LISP (Locator ID Separation Protocol) and VRF (Virtual Routing and Forwarding) configuration, to orchestrate the fabric overlay. The **show-running configuration** command shows the virtual context configuration including the auto-generated base line commands.

Examples

The following configuration is auto-generated when this command is run on your device:

```
Device(config-fabric-auto-domain)# context guest id 10
ip vrf guest
    description Auto-provisioned vrf for context example-context (source - fabric auto)
router lisp
    eid-table vrf guest instance-id 10
```

control-plane

To configure the IP address of the control-plane device with which the edge device can communicate, in the fabric domain, use the **control-plane** *ip address* *auth-key key* command.

control-plane *ip address*

auth-key *key*

Syntax Description	control-plane ip address	Configures the IP address of the control-plane device, to which the edge device can connect.
	auth-key key	Configures the key to authenticate access to the control-plane device.

Command Default None.

Command Modes Fabric-auto-domain configuration

Command History	Release	Modification
	3.9.01E	This command was introduced on the Catalyst 4500-E series switch using a Supervisor Engines 8-E and 8L-E.

Usage Guidelines Use the command to configure the control-plane device IP address and the authentication key, to allow fabric edge devices in the fabric domain to communicate with the control-plane device .

This command enables the auto-generation of LISP (Locator ID Separation Protocol) and VRF (Virtual Routing and Forwarding) configuration, to orchestrate the fabric overlay. The **show-running configuration** command shows the virtual context configuration including the auto-generated base line commands.

Examples The following configuration is auto-generated when this command is run on your device:

```
Device(config-fabric-auto-domain)#control-plane 2.2.2.2
auth_key examplekey123
r
outer lisp
locator-set default.RLOC
ipv4-interface Loopback0 priority 10 weight 10
exit

disable-ttl-propagate
ipv4 sgt
eid-table default instance-id 0
exit

loc-reach-algorithm lsb-reports ignore
ipv4 itr map-resolver 2.2.2.2
ipv4 itr
```

```
ipv4 etr map-server 2.2.2.2 key examplekey123  
ipv4 etr
```

cos (netflow-lite exporter submode)



Note

NetFlow-lite is supported only on Catalyst 4948E and Catalyst 4948E-F Ethernet switches.

To specify a CoS value for the NetFlow-lite collector, use the **cos** command. To delete the value, use the **no** form of this command.

```
cos cos-value
```

```
no cos cos-value
```

Syntax Description	<i>cos-value</i>	Specifies a CoS value for the NetFlow-lite collector. Valid values from 0 to 7.
--------------------	------------------	---

Command Default	0
-----------------	---

Command Modes	netflow-lite exporter submode
---------------	-------------------------------

Command History	Release	Modification
	15.0(2)SG	This command was introduced on the Catalyst 4948E and Catalyst 4948E-F Ethernet switches.

Usage Guidelines	This option allows you to set the CoS value of VLAN tags for packet samples exported by the fpga alone.
------------------	---

Examples	The following example shows how to specify a CoS value for the NetFlow-lite collector:
----------	--

```
Switch# config terminal
Switch(config)# netflow-lite exporter exporter1
Switch(config-netflow-lite-exporter)# destination 5.5.5.6
Switch(config-netflow-lite-exporter)# source 5.5.5.5
Switch(config-netflow-lite-exporter)# transport udp 8188
Switch(config-netflow-lite-exporter)# ttl 128
Switch(config-netflow-lite-exporter)# cos 7
Switch(config-netflow-lite-exporter)# dscp 32
Switch(config-netflow-lite-exporter)# template data timeout 1
Switch(config-netflow-lite-exporter)# options sampler-table timeout 1
Switch(config-netflow-lite-exporter)# options interface-table timeout 1
Switch(config-netflow-lite-exporter)# export-protocol netflow-v9
Switch(config-netflow-lite-exporter)# exit
Switch(config)#
```



```

Display the exporter
Switch# show netflow-lite exporter exporter1
Netflow-lite Exporter exporter1:
  Network Protocol Configuration:
    Destination IP address: 5.5.5.6
    Source IP Address:    5.5.5.5
    VRF label:
    DSCP:                 0x20
    TTL:                  128
    COS:                  7
  Transport Protocol Configuration:
    Transport Protocol:   UDP
    Destination Port:     8188
    Source Port:         61670
  Export Protocol Configuration:
    Export Protocol:      netflow-v9
    Template data timeout: 60
    Options sampler-table timeout: 1800
    Options interface-table timeout: 1800
  Exporter Statistics:
    Packets Exported:    0

```

You can verify your settings with the **show netflow-lite exporter** privileged EXEC command.

Related Commands	Command	Description
	destination (netflow-lite exporter submode)	Specifies a destination address in netflow-lite submode.
	source (netflow-lite exporter submode)	Specifies a source Layer 3 interface of the NetFlow-lite collector.
	transport udp (netflow-lite exporter submode)	Specifies a UDP transport destination port for a NetFlow-lite collector.
	ttl (netflow-lite exporter submode)	Specifies a ttl value for the NetFlow-lite collector.
	dscp (netflow-lite exporter submode)	Specifies a CoS value for the NetFlow-lite collector.
	template data timeout (netflow-lite exporter submode)	Specifies a template data timeout for the NetFlow-lite collector.
	options timeout (netflow-lite exporter submode)	Specifies an options timeout for the NetFlow-lite collector.
	export-protocol (netflow-lite exporter submode)	Specifies the export protocol for the NetFlow-lite collector.

counter

To assign counters to a Layer 3 interface, use the **counter** interface command. To remove a counter assignment, use the **no** form of this command.

counter {**ipv4** | **ipv6** | **ipv4 ipv6 separate**}

no counter



Note

Supervisor Engine 6-E and Supervisor Engine 6L-E do not support Layer 3 interface counters.

Syntax Description

ipv4	Enables collection of IPv4 statistics only.
ipv6	Enables collection of IPv6 statistics only.
ipv4 ipv6 separate	Enables collection of IPv4 and IPv6 statistics and displays them individually.

Command Default

Not enabled

Command Modes

Interface configuration

Command History

Release	Modification
12.2(40)SG	This command was introduced on the Catalyst 4500 series switch.
12.2(54)SG	Support added for IPv4 and IPv6 counters.

Usage Guidelines

Entering the **counter** command without keywords displays the statistics as a sum.

The total number of switch ports that can possess transmit and receive counters is 4092.

When you change a Layer 3 port assigned with a counter to a Layer 2 port, the hardware counters are cleared. This action is similar to entering the **no counter** command.

Examples

The following example shows how to enable counters on interface VLAN 1:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface vlan 1
Switch(config-if)# counter ipv4
Switch(config-if)# end
Switch#
00:17:15: %SYS-5-CONFIG_I: Configured from console by console
Switch# show run interface vlan 1
Building configuration...
```

```
Current configuration : 63 bytes
!
interface Vlan1
  ip address 10.0.0.1 255.0.0.0
  counter ipv4
end
```

**Note**

To remove the counter assignment, use the **no counter** command.

If you have already assigned the maximum number of counters, the **counter** command fails, displaying the following error message:

```
Switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface fa3/2
Switch(config-if)# no switchport
Switch(config-if)# counter ipv6
Counter resource exhausted for interface fa3/2
Switch(config-if)# end
Switch#
00:24:18: %SYS-5-CONFIG_I: Configured from console by console
```

In this situation, you must release a counter from another interface so the new interface can use it.

dbi

To enable active queue management on a transmit queue used by a class of traffic, use the **dbi** command. Use the **no** form of this command to return to the default setting.

dbi

no dbi

Syntax Description This command has no keywords or arguments.

Command Default Active queue management is disabled.

Command Modes Policy-map class configuration

Command History

Release	Modification
12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch.
12.2(40)SG	Support added on Supervisor Engine 6E.

Usage Guidelines

The semantics of the DBL configuration is similar to the WRED algorithm. The **dbi** command can operate alone on class-default; otherwise, it requires you to configure the **bandwidth** or **shape** commands on the class.

Examples

The following example shows how to enable dbi action in a class:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# dbi
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 **no** form of this command.

debug adjacency [ipc]

no debug adjacency

Syntax Description	ipc (Optional) Displays the IPC entries in the adjacency database.
---------------------------	---

Command Default	This command has no default settings.
------------------------	---------------------------------------

Command Modes	Privileged EXEC mode
----------------------	----------------------

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

Examples	The following example shows how to display the information in the adjacency database:
-----------------	---

```
Switch# debug adjacency
4d02h: ADJ: add 172.20.52.36 (GigabitEthernet1/1) via ARP will expire: 04:00:00
4d02h: ADJ: add 172.20.52.36 (GigabitEthernet1/1) via ARP will expire: 04:00:00
4d02h: ADJ: add 172.20.52.36 (GigabitEthernet1/1) via ARP will expire: 04:00:00
4d02h: ADJ: add 172.20.52.36 (GigabitEthernet1/1) via ARP will expire: 04:00:00
4d02h: ADJ: add 172.20.52.36 (GigabitEthernet1/1) via ARP will expire: 04:00:00
4d02h: ADJ: add 172.20.52.36 (GigabitEthernet1/1) via ARP will expire: 04:00:00
4d02h: ADJ: add 172.20.52.36 (GigabitEthernet1/1) via ARP will expire: 04:00:00
4d02h: ADJ: add 172.20.52.36 (GigabitEthernet1/1) via ARP will expire: 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.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

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

Examples The following 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 no debug backup)	Disables debugging output.

debug condition interface

To limit the debugging output of interface-related activities, use the **debug condition interface** command. To disable the debugging output, use the **no** form of this command.

```
debug condition interface {fastethernet mod/port | GigabitEthernet mod/port |
null interface_num | port-channel interface-num | vlan vlan_id}
```

```
no debug condition interface {fastethernet mod/port | GigabitEthernet mod/port | null
interface_num | port-channel interface-num | vlan vlan_id}
```

Syntax Description		
fastethernet		Limits the debugging to Fast Ethernet interfaces.
<i>mod/port</i>		Number of the module and port.
GigabitEthernet		Limits the debugging to Gigabit Ethernet interfaces.
null <i>interface-num</i>		Limits the debugging to null interfaces; the valid value is 0.
port-channel <i>interface-num</i>		Limits the debugging to port-channel interfaces; valid values are from 1 to 64.
vlan <i>vlan_id</i>		Specifies the VLAN interface number; valid values are from 1 to 4094.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

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

Examples The following 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 mod/port | GigabitEthernet mod/port |  
port-channel interface-num | vlan vlan_id group-number}
```

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

Syntax Description		
fastethernet		Limits the debugging to Fast Ethernet interfaces.
<i>mod/port</i>		Number of the module and port.
GigabitEthernet		Limits the debugging to Gigabit Ethernet interfaces.
port-channel <i>interface_num</i>		Limits the debugging output to port-channel interfaces; valid values are from 1 to 64.
vlan <i>vlan_id</i>		Limits the debugging of a condition on a VLAN interface; valid values are from 1 to 4094.
<i>group-number</i>		VLAN group number; valid values are from 0 to 255.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.1(8a)EW	This command was introduced on the Catalyst 4500 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 removal operation. You can enter **n** to abort the removal or **y** to proceed with the removal. If you remove the only condition set, an excessive number of debugging messages might occur.

Examples The following example shows how to limit the debugging output to group 0 in VLAN 1:

```
Switch# debug condition standby vlan 1 0  
Condition 3 set  
Switch#
```

The following example shows the display if you try to turn off the last standby debug condition:

```
Switch# no debug condition standby vlan 1 0
This condition is the last standby condition set.
Removing all conditions may cause a flood of debugging
messages to result, unless specific debugging flags
are first removed.

Proceed with removal? [yes/no]: n
% Operation aborted
Switch#
```

Related Commands

Command	Description
undebg 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.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch.
12.1(12c)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

The following example shows how to limit the debugging output to VLAN 1:

```
Switch# debug condition vlan 1
Condition 4 set
Switch#
```

The following 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 all conditions may cause a flood of debugging
messages to result, unless specific debugging flags
are first removed.

Proceed with removal? [yes/no]: n
% Operation aborted
Switch#
```

debug condition vlan**Related Commands**

Command	Description
undebug condition vlan (same as no debug condition vlan)	Disables debugging output.

debug device-sensor

To enable debugging for Device Sensor, use the **debug device-sensor** command in privileged EXEC mode.

debug device-sensor errors events

Syntax Description	errors	Displays Device Sensor error messages.
	events	Displays messages for events such as protocol packet arrivals, identity updates, and release events sent to the session manager.

Command Default There are no defaults for this command.

Command Modes Privileged EXEC

Command History	Release	Modification
	IOS XE 3.4.0SG and IOS 15.1(2)SG)	Command introduced on the Catalyst 4500 Series switch.

Usage Guidelines Use the **debug device-sensor** command in conjunction with the **debug authentication all** command to troubleshoot scenarios where device sensor cache entries are not being created for the connected devices

Examples The following is sample output from the **debug device-sensor events** command. The debug output shows how Cisco Discovery Protocol packets and TLVs are received from the device connected to the GigabitEthernet 2/1 interface:

```
Switch# debug device-sensor events

Switch#
*Nov 30 23:58:45.811: DSensor: Received cdp packet from GigabitEthernet2/1:00d0.2bdf.08a5
*Nov 30 23:58:45.811: DSensor: SM returned no or invalid session label for
GigabitEthernet2/1:00d0.2bdf.08a5
*Nov 30 23:58:45.811: DSensor: Updating SM with identity attribute list
  cdp-tlv          0 00 01 00 0B 4A 41 45 30 37 34 31 31 50 53 32
  cdp-tlv          0 00 03 00 03 32 2F 38
  cdp-tlv          0 00 04 00 04 00 00 00 0A
  cdp-tlv          0 00 05 00 68 57 53 2D 43 32 39 34 38 20 53 6F 66 74 77 61 72 65
2C 20 56 65 72 73 69 6F 6E 20 4D 63 70 53 57 3A 20 36 2E 34 28 35 29 0A 43 6F 70 79 72 69 67 68 74 20 28 63 29
30 29 20 4E 6D 70 53 57 3A 20 36 2E 34 28 35 29 0A 43 6F 70 79 72 69 67 68 74 20 28 63 29
20 31 39 39 35 2D 32 30 30 33 20 62 79 20 43 69 73 63 6F 20 53 79 73
74 65 6D 73 2C 20 49 6E 63 2E 0A
  cdp-tlv          0 00 06 00 08 57 53 2D 43 32 39 34 38
  cdp-tlv          0 00 09 00 00
  cdp-tlv          0 00 0A 00 02 00 21
  cdp-tlv          0 00 0B 00 01 01
  cdp-tlv          0 00 12 00 01 00
  cdp-tlv          0 00 13 00 01 00
```

■ debug device-sensor

```

cdp-tlv          0  00 14 00 00
cdp-tlv          0  00 15 00 0A 06 08 2B 06 01 04 01 09 05 2A
cdp-tlv          0  00 16 00 16 00 00 00 02 01 01 CC 00 04 00 00 00 0001 01 CC 00 04
01 01 01 01
cdp-tlv          0  00 17 00 01 00
swidb            0  604702240 (0x240B0620)
clid-mac-addr   0  00 D0 2B DF 08 A5
*Nov 30 23:58:46.831: DSensor: Received cdp packet from
GigabitEthernet2/1:00d0.2bdf.08a5exi
Switch#
*Nov 30 23:58:51.171: %SYS-5-CONFIG_I: Configured from console by console

```

Related Commands

Command	Description
debug authentication all	Displays all debugging information about Authentication Manager and all features.
device-sensor accounting	Adds the Device Sensor protocol data to the accounting records and generates additional accounting events when new sensor data is detected.

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.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC mode

Command History

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

Examples

The following example shows how to enable the 802.1X debugging for all conditions:

```
Switch# debug dot1x all
Switch#
```

Related Commands

Command	Description
show dot1x	Displays dot1x information.
undebug dot1x (same as no debug dot1x)	Disables debugging output.

debug etherchnl

To debug EtherChannel, use the **debug etherchnl** command. To disable the debugging output, use the **no** form of this command.

debug etherchnl [**all** | **detail** | **error** | **event** | **idb** | **linecard**]

no debug etherchnl

Syntax Description

all	(Optional) Displays all EtherChannel debug messages.
detail	(Optional) Displays the detailed EtherChannel debug messages.
error	(Optional) Displays the EtherChannel error messages.
event	(Optional) Debugs the major EtherChannel event messages.
idb	(Optional) Debugs the PAgP IDB messages.
linecard	(Optional) Debugs the SCP messages to the module.

Command Default

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	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

If you do not specify a keyword, all debug messages are displayed.

Examples

The following example shows how to display all the EtherChannel debug messages:

```
Switch# debug etherchnl
PAgP Shim/FEC debugging is on
22:46:30:FEC:returning agport Po15 for port (Fa2/1)
22:46:31:FEC:returning agport Po15 for port (Fa4/14)
22:46:33:FEC:comparing GC values of Fa2/25 Fa2/15 flag = 1 1
22:46:33:FEC:port_attr:Fa2/25 Fa2/15 same
22:46:33:FEC:EC - attrib incompatable for Fa2/25; duplex of Fa2/25 is half, Fa2/15 is full
22:46:33:FEC:pagp_switch_choose_unique:Fa2/25, port Fa2/15 in agport Po3 is incompatable
Switch#
```

The following example shows how to display the EtherChannel IDB debug messages:

```
Switch# debug etherchnl idb
Agport idb related debugging is on
Switch#
```


The following example shows how to disable the debugging:

```
Switch# no debug etherchnl
Switch#
```

Related Commands

Command	Description
undebug etherchnl (same as no debug etherchnl)	Disables debugging output.

debug fabric auto

To troubleshoot your fabric domain configuration, use the **debug fabric auto** command.

```
debug fabric auto {trace | level {error | verbose}}
```

Syntax Description	trace	Enables tracing for the commands auto-generated when the fabric-auto command is executed.
	level error	Displays the errors encountered during fabric overlay provisioning.
	level verbose	Displays the maximum number of messages encountered during fabric overlay provisioning.

Command Default None.

Command Modes Privileged EXEC

Command History	Release	Modification
	3.9.01E	This command was introduced on the Catalyst 4500-E series switch using a Supervisor Engines 8-E and 8L-E.

Usage Guidelines Use these debug commands to troubleshoot your fabric domain configuration, and trace the commands auto-generated by the fabric auto command, and display the errors encountered.

The **no debug fabric auto level verbose** command disables the display of all the messages encountered during fabric provisioning.

debug interface

To abbreviate 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 mod/port | GigabitEthernet mod/port | null |
port-channel interface-num | vlan vlan_id }
```

```
no debug interface { FastEthernet mod/port | GigabitEthernet mod/port | null |
port-channel interface-num | vlan vlan_id }
```

Syntax Description	FastEthernet	Limits the debugging to Fast Ethernet interfaces.
	<i>mod/port</i>	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 <i>interface-num</i>	Limits the debugging to port-channel interfaces; valid values are from 1 to 64.
	vlan <i>vlan_id</i>	Specifies the VLAN interface number; valid values are from 1 to 4094.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

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

Examples The following example shows how to limit the debugging to interface VLAN 1:

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

Related Commands	Command	Description
	debug condition interface	Limits the debugging output of interface-related activities.
	undebug etherchnl (same as no debug etherchnl)	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 nodes.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

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

Examples

The following example shows how to enable the debugging of the IPC events:

```
Switch# debug ipc events
Special Events debugging is on
Switch#
```

Related Commands

Command	Description
undebg 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.

Command Default Debugging of snooping event is disabled.

Command Modes Privileged EXEC mode

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

Examples The following example shows how to enable the debugging for the DHCP snooping events:

```
Switch# debug ip dhcp snooping event
Switch#
```

The following 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.

Command Default Debugging of snooping packet is disabled.

Command Modes Privileged EXEC mode

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

Examples The following example shows how to enable the debugging for the DHCP snooping packets:

```
Switch# debug ip dhcp snooping packet
Switch#
```

The following 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.

Command Default Debugging of snooping security packets is disabled.

Command Modes Privileged EXEC mode

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

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

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

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

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

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.

Command Default

Debugging of LACP activity is disabled.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.1(13)EW	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

The following 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.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

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

Examples

The following 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 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.

Command Default Debugging is disabled.

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 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.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

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

Examples The following example shows how to debug NVRAM:

```
Switch# debug nvram
NVRAM behavior debugging is on
Switch#
```

Related Commands	Command	Description
	undebug nvram (same as no debug nvram)	Disables debugging output.

debug pagp

To debug the PAgP activity, use the **debug pagp** command. To disable the debugging output, use the **no** form of this command.

debug pagp [**all** | **dual-active** | **event** | **fsm** | **misc** | **packet**]

no debug pagp

Syntax Description

all	(Optional) Enables all PAgP debugging.
dual-active	(Optional) Enables the PAgP dual-active debugging.
event	(Optional) Enables the debugging of the PAgP events.
fsm	(Optional) Enables the debugging of the PAgP finite state machine.
misc	(Optional) Enables the miscellaneous PAgP debugging.
packet	(Optional) Enables the PAgP packet debugging.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

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

Usage Guidelines

This command is supported only on the supervisor engine and can be entered only from the Catalyst 4500 series switch console.

Examples

The following example shows how to enable the PAgP miscellaneous debugging:

```
Switch# debug pagp misc
Port Aggregation Protocol Miscellaneous debugging is on
Switch#
*Sep 30 10:13:03: SP: PAgP: pagp_h(Fa5/6) expired
*Sep 30 10:13:03: SP: PAgP: 135 bytes out Fa5/6
*Sep 30 10:13:03: SP: PAgP: Fa5/6 Transmitting information packet
*Sep 30 10:13:03: SP: PAgP: timer pagp_h(Fa5/6) 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 reception debugging functions.
transmit	(Optional)	Enables the platform packet transmission debugging functions.
vlan	(Optional)	Enables the platform packet VLAN debugging functions.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

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

Examples The following example shows how to enable all PM debugging:

```
Switch# debug platform packet protocol lacp
Switch#
```

Related Commands	Command	Description
	undebug platform packet protocol lacp (same as no debug platform packet protocol lacp)	Disables debugging output.

debug platform packet protocol pagp

To debug the PAgP protocol packets, use the **debug platform packet protocol pagp** command. To disable the debugging output, use the **no** form of this command.

debug platform packet protocol pagp [receive | transmit | vlan]

no debug platform packet protocol pagp [receive | transmit | vlan]

Syntax Description

receive	(Optional) Enables the platform packet reception debugging functions.
transmit	(Optional) Enables the platform packet transmission debugging functions.
vlan	(Optional) Enables the platform packet VLAN debugging functions.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

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

Examples

The following example shows how to enable all PM debugging:

```
Switch# debug platform packet protocol pagp
Switch#
```

Related Commands

Command	Description
undebug platform packet protocol pagp (same as no debug platform packet protocol pagp)	Disables debugging output.

debug pm

To debug the port manager (PM) activity, use the **debug pm** command. To disable the debugging output, use the **no** form of this command.

```
debug pm {all | card | cookies | etherchnl | messages | port | registry | scp | sm | span | split |
          vlan | vp}
```

```
no debug pm {all | card | cookies | etherchnl | messages | port | registry | scp | 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 invocations.
	scp	Debugs the SCP 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.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

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

Examples The following example shows how to enable all PM debugging:

```
Switch# debug pm all
Switch#
```

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.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

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

Examples The following example shows how to enable all PM debugging:

```
Switch# debug port-security
Switch#
```

Related Commands	Command	Description
	switchport port-security	Enables port security on an interface.

debug pppoe intermediate-agent

To turn on debugging of the PPPoE Intermediate Agent feature, use the **debug pppoe intermediate-agent** command. To turn off debugging, use the **no** form of this command.

```
debug pppoe intermediate-agent {event | packet | all}
```

```
no debug pppoe intermediate-agent {event | packet | all}
```

Syntax Description

event	Activates event debugging
packet	Activates packet debugging
all	Activates both event and packet debugging

Command Default

All debugging is turned off.

Command Modes

Privileged 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 turn on packet debugging:

```
Switch# debug pppoe intermediate-agent packet
PPPOE IA Packet debugging is on

*Sep  2 06:12:56.133: PPPOE_IA: Process new PPPoE packet, Message type: PADI, input
interface: Gi3/7, vlan : 2 MAC da: ffff.ffff.ffff, MAC sa: aabb.cc00.0000
*Sep  2 06:12:56.137: PPPOE_IA: received new PPPOE packet from inputinterface
(GigabitEthernet3/4)
*Sep  2 06:12:56.137: PPPOE_IA: received new PPPOE packet from inputinterface
(GigabitEthernet3/8)
*Sep  2 06:12:56.137: PPPOE_IA: Process new PPPoE packet, Message type: PADO, input
interface: Gi3/4, vlan : 2 MAC da: aabb.cc00.0000, MAC sa: 001d.e64c.6512
*Sep  2 06:12:56.137: PPPOE_IA: Process new PPPoE packet, Message type: PADO, input
interface: Gi3/8, vlan : 2 MAC da: aabb.cc00.0000, MAC sa: aabb.cc80.0000
*Sep  2 06:12:56.137: PPPOE_IA: received new PPPOE packet from inputinterface
(GigabitEthernet3/7)
*Sep  2 06:12:56.137: PPPOE_IA: Process new PPPoE packet, Message type: PADR, input
interface: Gi3/7, vlan : 2 MAC da: 001d.e64c.6512, MAC sa: aabb.cc00.0000
*Sep  2 06:12:56.145: PPPOE_IA: received new PPPOE packet from inputinterface
(GigabitEthernet3/4)
*Sep  2 06:12:56.145: PPPOE_IA: Process new PPPoE packet, Message type: PADS, input
interface: Gi3/4, vlan : 2 MAC da: aabb.cc00.0000, MAC sa: 001d.e64c.6512
```

The following example shows how to turn off packet debugging:

```
Switch# debug pppoe intermediate-agent packet
PPPOE IA Packet debugging is off
```

■ debug pppoe intermediate-agent

Related Commands	Command	Description
	pppoe intermediate-agent (interface)	Enables the PPPoE Intermediate Agent feature on an interface.
	pppoe intermediate-agent limit rate	Limits the rate of the PPPoE Discovery packets arriving on an interface.
	pppoe intermediate-agent trust	Sets the trust configuration of an interface.

debug redundancy

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

```
debug redundancy {errors | fsm | kpa | msg | progression | status | timer}
```

```
no debug redundancy
```

Syntax Description

errors	Enables the redundancy facility for error debugging.
fsm	Enables the redundancy facility for FSM event debugging.
kpa	Enables the redundancy facility for keepalive debugging.
msg	Enables the redundancy facility for messaging event debugging.
progression	Enables the redundancy facility for progression event debugging.
status	Enables the redundancy facility for status event debugging.
timer	Enables the redundancy facility for timer event debugging.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.1(12c)EW	This command was introduced on the Catalyst 4500 series switch (Catalyst 4507R only).

Examples

The following example shows how to debug the redundancy facility timer event debugging:

```
Switch# debug redundancy timer
Redundancy timer debugging is on
Switch#
```

debug spanning-tree

To debug the spanning tree activities, use the **debug spanning-tree** command. To disable the debugging output, use the **no** form of this command.

```
debug spanning-tree {all | backbonefast | bpdu | bpdu-opt | 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 spanningtree BPDU.
bpdu-opt	Debugs the optimized BPDU handling.
etherchannel	Debugs the spanning tree EtherChannel support.
config	Debugs the spanning tree configuration changes.
events	Debugs the TCAM events.
exceptions	Debugs the spanning tree exceptions.
general	Debugs the general spanning tree activity.
ha	Debugs the HA events.
mstp	Debugs the multiple spanning tree events.
pvst+	Debugs the PVST+ events.
root	Debugs the spanning tree root events.
snmp	Debugs the spanning tree SNMP events.
switch	Debugs the switch debug events.
synchronization	Debugs the STP state synchronization events.
uplinkfast	Debugs the UplinkFast events.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

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

Examples

The following 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
	undebg 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.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

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

Usage Guidelines

This command is supported only on the supervisor engine and enterable only from the switch console.

Examples

The following 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.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

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

Usage Guidelines This command is supported only on the supervisor engine and enterable only from the switch console.

Examples

The following 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 08:47:33: SP: STP SW: TX: bpdu of type ieee-st size 92 on FastEthernet5/9 303
*Sep 30 08:47:33: SP: STP SW: TX: bpdu of type ieee-st size 92 on FastEthernet5/9 304
*Sep 30 08:47:33: SP: STP SW: TX: bpdu of type ieee-st size 92 on FastEthernet5/9 305
*Sep 30 08:47:33: SP: STP SW: TX: bpdu of type ieee-st size 92 on FastEthernet5/9 349
*Sep 30 08:47:33: SP: STP SW: TX: bpdu of type ieee-st size 92 on FastEthernet5/9 350
*Sep 30 08:47:33: SP: STP SW: TX: bpdu of type ieee-st size 92 on FastEthernet5/9 351
*Sep 30 08:47:33: SP: STP SW: TX: bpdu of type ieee-st size 92 on FastEthernet5/9 801
<... output truncated...>
Switch#
```

Related Commands

Command	Description
undebg 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.				
Command Default	This command has no default settings.				
Command Modes	Privileged EXEC mode				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.1(8a)EW</td> <td>This command was introduced on the Catalyst 4500 series switch.</td> </tr> </tbody> </table>	Release	Modification	12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch.
Release	Modification				
12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch.				
Usage Guidelines	This command is supported only on the supervisor engine and enterable only from the switch console.				
Examples	<p>The following example shows how to debug the spanning tree UplinkFast exceptions:</p> <pre>Switch# debug spanning-tree uplinkfast exceptions Spanning Tree uplinkfast exceptions debugging is on Switch#</pre>				
Related Commands	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>undebug spanning-tree uplinkfast (same as no debug spanning-tree uplinkfast)</td> <td>Disables debugging output.</td> </tr> </tbody> </table>	Command	Description	undebug spanning-tree uplinkfast (same as no debug spanning-tree uplinkfast)	Disables debugging output.
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.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

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

Examples

The following 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

To enable the VLAN manager Cisco IOS file system (IFS) error tests, use the **debug sw-vlan ifs** command. To disable the debugging output, use the **no** form of this command.

```
debug sw-vlan ifs {open {read | write} | read {1 | 2 | 3 | 4} | write}
```

```
no debug sw-vlan ifs {open {read | write} | read {1 | 2 | 3 | 4} | write}
```

Syntax Description

open	Enables the VLAN manager IFS debugging of errors in an IFS file-open operation.
read	Debugs the errors that occurred when the IFS VLAN configuration file was open for reading.
write	Debugs the errors that occurred when the IFS VLAN configuration file was open for writing.
{1 2 3 4}	Determines the file-read operation. See the “Usage Guidelines” section for information about operation levels.
write	Debugs the errors that occurred during an IFS file-write operation.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

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

Usage Guidelines

The following are four types of file read operations:

- Operation **1**—Reads the file header, which contains the header verification word and the file version number.
- Operation **2**—Reads the main body of the file, which contains most of the domain and VLAN information.
- Operation **3**—Reads TLV descriptor structures.
- Operation **4**—Reads TLV data.

Examples

The following 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#
```

debug sw-vlan ifs**Related Commands**

Command	Description
undebug sw-vlan ifs (same as no debug sw-vlan ifs)	Disables debugging output.

debug sw-vlan notification

To enable the 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 { accfwdchange | allowedvlanfgchange | fwdchange | linkchange |
modechange | pruningfgchange | statechange }
```

```
no debug sw-vlan notification { accfwdchange | allowedvlanfgchange | fwdchange | linkchange
| modechange | pruningfgchange | statechange }
```

Syntax Description	Parameter	Description
	accfwdchange	Enables the VLAN manager notification of aggregated access interface STP forward changes.
	allowedvlanfgchange	Enables the VLAN manager notification of changes to allowed VLAN configuration.
	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.
	pruningfgchange	Enables the VLAN manager notification of changes to pruning configuration.
	statechange	Enables the VLAN manager notification of interface state changes.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

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

Examples The following 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
	undebg 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 that the Cisco IOS VTP platform-dependent layer to send.
xmit	Displays the contents of all outgoing VTP packets that the VTP code will request that the Cisco IOS VTP platform-dependent layer to send; does not include pruning packets.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.1(8a)EW	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

The following example shows how to debug the software VLAN outgoing 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 udd

To enable the debugging of UDLD activity, use the **debug udd** command. To disable the debugging output, use the **no** form of this command.

```
debug udd {events | packets | registries}
```

```
no debug udd {events | packets | registries}
```

Syntax Description

events	Enables the debugging of UDLD process events as they occur.
packets	Enables the debugging of the UDLD process as it receives packets from the packet queue and attempts to transmit packets at the request of the UDLD protocol code.
registries	Enables the debugging of the UDLD process as it processes registry upcalls from the UDLD process-dependent module and other feature modules.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

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

Usage Guidelines

This command is supported only on the supervisor engine and enterable only from the switch console.

Examples

The following example shows how to debug the UDLD events:

```
Switch# debug udd events
UDLD events debugging is on
Switch#
```

The following example shows how to debug the UDLD packets:

```
Switch# debug udd packets
UDLD packets debugging is on
Switch#
```

The following example shows how to debug the UDLD registry events:

```
Switch# debug udd registries
UDLD registries debugging is on
Switch#
```

■ **debug udd****Related Commands**

Command	Description
undebug udd (same as no debug udd)	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.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

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

Examples The following example shows how to enable all VQP debugging:

```
Switch# debug vqpc all
Switch#
```

Related Commands	Command	Description
	vmpls 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	
<i>macro-name</i>	Name of the interface range macro; up to 32 characters.
<i>interface-range</i>	List of valid ranges when specifying interfaces; see the “Usage Guidelines” section.

Command Default This command has no default settings.

Command Modes Global configuration mode

Command History	Release	Modification
	12.1(8a)EW	This command was introduced on the Catalyst 4500 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 The following example shows how to create a multiple-interface macro:

```
Switch(config)# define interface-range macro1 gigabitethernet 4/1-6, fastethernet 2/1-5
Switch(config)#
```

Related Commands	Command	Description
	interface range	Runs a command on multiple ports at the same time.

deny

To deny an ARP packet based on matches against the DHCP bindings, use the **deny** command. To remove the specified ACEs from the access list, use the **no** form of this command.

```
deny {[request] ip {any | host sender-ip | sender-ip sender-ip-mask} mac {any | host sender-mac | sender-mac sender-mac-mask} | response ip {any | host sender-ip | sender-ip sender-ip-mask} [{any | host target-ip | target-ip target-ip-mask}] mac {any | host sender-mac | sender-mac sender-mac-mask} [{any | host target-mac | target-mac target-mac-mask}] [log]
```

```
no deny {[request] ip {any | host sender-ip | sender-ip sender-ip-mask} mac {any | host sender-mac | sender-mac sender-mac-mask} | response ip {any | host sender-ip | sender-ip sender-ip-mask} [{any | host target-ip | target-ip target-ip-mask}] mac {any | host sender-mac | sender-mac sender-mac-mask} [{any | host target-mac | target-mac target-mac-mask}] [log]
```

Syntax Description

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 <i>sender-ip</i>	Specifies that only a specific sender IP address will be accepted.
<i>sender-ip sender-ip-mask</i>	Specifies that a specific range of sender IP addresses will be accepted.
mac	Specifies the sender MAC address.
host <i>sender-mac</i>	Specifies that only a specific sender MAC address will be accepted.
<i>sender-mac sender-mac-mask</i>	Specifies that a specific range of sender MAC addresses will be accepted.
response	Specifies a match for the ARP responses.
ip	Specifies the IP address values for the ARP responses.
host <i>target-ip</i>	(Optional) Specifies that only a specific target IP address will be accepted.
<i>target-ip target-ip-mask</i>	(Optional) Specifies that a specific range of target IP addresses will be accepted.
mac	Specifies the MAC address values for the ARP responses.
host <i>target-mac</i>	(Optional) Specifies that only a specific target MAC address will be accepted.
<i>target-mac target-mac-mask</i>	(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).

Command Default

At the end of the ARP access list, there is an implicit **deny ip any mac any** command.

Command Modes

arp-nacl configuration mode

deny

Command History

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

Usage Guidelines

Deny clauses can be added to forward or drop ARP packets based on some matching criteria.

Examples

The following example shows a host with a MAC address of 0000.0000.abcd and an IP address of 1.1.1.1. The following 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 (netflow-lite exporter submode)



Note

NetFlow-lite is supported only on Catalyst 4948E and Catalyst 4948E-F Ethernet switches.

To specify a destination address in netflow-lite submode, use the **destination** command. To delete an exporter, use the **no destination** form of this command.

destination *destination-address*

no destination *destination-address*

Syntax Description	<i>destination-address</i>	Specifies a destination address of a NetFlow-lite collector.
--------------------	----------------------------	--

Command Default	None
-----------------	------

Command Modes	netflow-lite exporter submode
---------------	-------------------------------

Command History	Release	Modification
	15.0(2)SG	This command was introduced on on the Catalyst 4948E and Catalyst 4948E-F Ethernet switches.

Usage Guidelines	One of the mandatory parameters for a minimally configured exporter along with the source Layer 3 interface and the UDP destination port of the collector.
------------------	--

Examples	The following example shows how to specify a destination address in netflow-lite submode:
----------	---

```
Switch# config terminal
Switch(config)# netflow-lite exporter exporter1
Switch(config-netflow-lite-exporter)# destination 5.5.5.6
Switch(config-netflow-lite-exporter)# source 5.5.5.5
Switch(config-netflow-lite-exporter)# transport udp 8188
Switch(config-netflow-lite-exporter)# ttl 128
Switch(config-netflow-lite-exporter)# cos 7
Switch(config-netflow-lite-exporter)# dscp 32
Switch(config-netflow-lite-exporter)# template data timeout 1
Switch(config-netflow-lite-exporter)# options sampler-table timeout 1
Switch(config-netflow-lite-exporter)# options interface-table timeout 1
Switch(config-netflow-lite-exporter)# export-protocol netflow-v9
Switch(config-netflow-lite-exporter)# exit
Switch(config)#
```

destination (netflow-lite exporter submode)

```

Display the exporter
Switch# show netflow-lite exporter exporter1
Netflow-lite Exporter exporter1:
  Network Protocol Configuration:
    Destination IP address: 5.5.5.6
    Source IP Address:    5.5.5.5
    VRF label:
    DSCP:                 0x20
    TTL:                  128
    COS:                  7
  Transport Protocol Configuration:
    Transport Protocol:   UDP
    Destination Port:     8188
    Source Port:         61670
  Export Protocol Configuration:
    Export Protocol:      netflow-v9
    Template data timeout: 60
    Options sampler-table timeout: 1800
    Options interface-table timeout: 1800
  Exporter Statistics:
    Packets Exported:    0

```

You can verify your settings with the **show netflow-lite exporter** privileged EXEC command.

Related Commands

Command	Description
cos (netflow-lite exporter submode)	Specifies a CoS value for the NetFlow-lite collector.
source (netflow-lite exporter submode)	Specifies a source Layer 3 interface of the NetFlow-lite collector.
transport udp (netflow-lite exporter submode)	Specifies a UDP transport destination port for a NetFlow-lite collector.
ttl (netflow-lite exporter submode)	Specifies a ttl value for the NetFlow-lite collector.
dscp (netflow-lite exporter submode)	Specifies a CoS value for the NetFlow-lite collector.
template data timeout (netflow-lite exporter submode)	Specifies a template data timeout for the NetFlow-lite collector.
options timeout (netflow-lite exporter submode)	Specifies an options timeout for the NetFlow-lite collector.
export-protocol (netflow-lite exporter submode)	Specifies the export protocol for the NetFlow-lite collector.

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 <i>email-address</i>	Specifies the destination e-mail address in 1 to 200 characters.
http <i>url</i>	Specifies the destination HTTP URL in 2 to 200 characters.

Command Default

This command has no default settings.

Command Modes

cfg-call-home-profile

Command History

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

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

The following example shows how to set the destination to the e-mail address **callhome@cisco.com**:

```
Switch(config)# call-home
Switch(cfg-call-home)# profile cisco
Switch(cfg-call-home-profile)# destination address email callhome@cisco.com
```

Related Commands

Command	Description
destination message-size-limit bytes	Configures a maximum destination message size for the destination profile.
destination preferred-msg-format	Configures a preferred message format.
destination transport-method	Enables the message transport method.
profile	Enters profile call-home configuration submode
subscribe-to-alert-group all	Subscribes to all available alert groups.
subscribe-to-alert-group configuration	Subscribes this destination profile to the Configuration alert group.
subscribe-to-alert-group diagnostic	Subscribes this destination profile to the Diagnostic alert group.

destination address

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.

Command Default 3145728 bytes

Command Modes cfg-call-home-profile

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

Usage Guidelines To enter profile call-home configuration submenu, use the **profile** command in call-home configuration mode.

Examples The following example shows how to configure the maximum message size for the destination profile as 3000000:

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

Related Commands	Command	Description
	destination address	Configures the destination e-mail address or URL to which Call Home messages will be sent.
	destination preferred-msg-format	Configures a preferred message format.
	destination transport-method	Enables the message transport method.
	profile	Enters profile call-home configuration submenu
	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.

■ destination message-size-limit bytes

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.

Command Default xml

Command Modes cfg-call-home-profile

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

Usage Guidelines To enter profile call-home configuration submode, use the **profile** command in call-home configuration mode.

Examples The following example shows how to configure the preferred message format as long text:

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

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

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.

Command Default	e-mail
-----------------	--------

Command Modes	cfg-call-home-profile
---------------	-----------------------

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

Usage Guidelines	To enter profile call-home configuration submode, use the profile command in call-home configuration mode.
------------------	---

Examples	The following example shows how to set the transport method to HTTP:
----------	--

```
Switch(config)# call-home
Switch(cfg-call-home)# profile cisco
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 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.

device-sensor filter-list

To create a CDP or Link Layer Discovery Protocol (LLPD) filter list that contains a list of Type-Length-Value (TLV) fields to be included or excluded in the Device Sensor output, use the **device-sensor filter-list** command in global configuration mode. To remove the filter list, use the **no** form of this command.

```
device-sensor filter-list cdp | lldp list list-name
```

```
no device-sensor filter-list cdp | lldp list list-name
```

Syntax Description	list	Contains a discovery protocol filter list.
	<i>list-name</i>	Name of the filter list.

Command Default Protocol TLV fields filter list is not available.

Command Modes Global configuration

Command History	Release	Modification
	IOS XE 3.4.0SG and IOS 15.1(2)SG)	Command introduced on the Catalyst 4500 Series switch.

Usage Guidelines Use the **device-sensor filter-list** command to configure the name of the protocol filter list and enter into discovery protocol sensor configuration mode. You can configure the list of TLVs in discovery protocol sensor configuration mode using the **tlv {name tlv-name | number tlv-number}** command. Use the **name tlv-name** keyword-argument pair to specify the name of the TLV. Enter **?** to query the available TLV names or refer to the following tables.

Table 2-1 CDP TLV Names

CDP TLV Name	Description
Global configuration mode	
app	Enable application TLV
forward	Forward CDP packets to another interface
location	Enable location information
Interface configuration mode	
app	Enable application TLV
location	Enable location information
server-location	Enable CDP location server on interface

Table 2-2 LLDP TLVs

LLPP TLV Name	Description
Global configuration mode	
4-wire-power-management	Cisco 4-wire power with MDI TLV
mac-phy-cfg	IEEE 802.3 MAC/PHY configuration status TLV
management-address	Management address TLV
port-description	Port description TLV
port-vlan	Port VLAN ID TLV
power-management	IEEE 802.3 DTE power with MDI TLV
system-capabilities	System capabilities TLV
system-description	System description TLV
system-name	System name TLV
Interface configuration mode	
inventory-management	LLDP Media Endpoint Devices (MED) inventory management TLV
location	LLDP MED location TLV
network-policy	LLDP MED network policy TLV

Use the **number** *tlv-name* keyword-argument pair to specify the TLV number to be added to the TLV filter list.

Use the **no tlv** {**name** *tlv-name* | **number** *tlv-number*} command to remove individual TLVs from the TLV filter list.

Use the **no device-sensor filter-list lldp list** *tlv-list-name* command to remove the entire TLV list containing all of the TLVs.

The following example shows how to create an LLDP filter containing a list of TLVs:

```
Switch> enable
Switch# configure terminal
Switch(config)# device-sensor filter-list lldp list lldp-list
Switch(config-sensor-llldplist)# tlv name mac-phy-config
Switch(config-sensor-llldplist)# tlv name system-name
Switch(config-sensor-llldplist)# end
```

Examples

The following example shows how to create an LLDP filter containing a list of TLVs:

```
Switch> enable
Switch# configure terminal
Switch(config)# device-sensor filter-list lldp list lldp-list
Switch(config-sensor-llldplist)# tlv name mac-phy-config
Switch(config-sensor-llldplist)# tlv name system-name
Switch(config-sensor-llldplist)# end
```


Related Commands	Command	Description
	debug device-sensor	Enables debugging for Device Sensor.
	device-sensor accounting	Adds the Device Sensor protocol data to accounting records and generates additional accounting events when new sensor data is detected.
	device-sensor filter-list dhcp	Creates a DHCP filter containing a list of options that can be included or excluded in the Device Sensor output.
	show device-sensor cache	Displays Device Sensor cache entries.

device-sensor filter-list dhcp

To create a DHCP filter containing a list of options that can be included or excluded in the Device Sensor output, use the **device-sensor filter-list dhcp** command in global configuration mode. To remove the DHCP filter containing the list of options, use the **no** form of this command.

device-sensor filter-list dhcp list *option-list-name*

no device-sensor filter-list dhcp list *option-list-name*

Syntax Description

list	Contains a DHCP options filter list.
<i>option-list-name</i>	DHCP options filter list name.

Command Default

DHCP options filter list is not available.

Command Modes

Global configuration

Command History

Release	Modification
IOS XE 3.4.0SG and IOS 15.1(2)SG	Command introduced on the Catalyst 4500 Series switch.

Usage Guidelines

Use the **device-sensor filter-list dhcp** command to configure the name of the DHCP options filter list and enter into DHCP sensor configuration mode. You can configure the list of options in DHCP sensor configuration mode using the **option** {**name** *option-name* | **number** *option-number*} command. Use the **name** *option-name* keyword-argument pair to specify the name of the DHCP option. Use the **number** *option-number* keyword-argument pair to specify the TLV number to be added to the DHCP options filter list.

Use the **no option** {**name** *option-name* | **number** *option-number*} command to remove individual options from the DHCP options filter list.

Use the **no device-sensor filter-list dhcp list** *option-list-name* command to remove the entire options filter list.

Examples

The following example shows how to create a DHCP filter containing a list of options:

```
Switch> enable
Switch# configure terminal
Switch(config)# device-sensor filter-list dhcp list dhcp-list
Switch(config-sensor-dhcplist)# option name domain-name
Switch(config-sensor-dhcplist)# option name host-name
Switch(config-sensor-dhcplist)# option number 50
Switch(config-sensor-dhcplist)# end
```

Related Commands	Command	Description
	debug device-sensor	Enables debugging for Device Sensor.
	device-sensor accounting	Adds the Device Sensor protocol data to accounting records and generates additional accounting events when new sensor data is detected.
	device-sensor filter-list	Creates a CDP or LLDP filter containing a list of options that can be included or excluded in the Device Sensor output.
	show device-sensor cache	Displays Device Sensor cache entries.

device-sensor filter-spec

To apply a protocol filter list to the Device Sensor output, use the **device-sensor filter-spec** command in global configuration mode. To remove the protocol filter list from the device sensor output, use the **no** form of this command.

device-sensor filter-spec {cdp | lldp | dhcp} {exclude {all | list *list-name*} | include list *list-name*}

Syntax Description

cdp	Applies a CDP TLV filter list to the device sensor output.
lldp	Applies a LLDP TLV filter list to the device sensor output.
dhcp	Applies a DHCP options filter list to the device sensor output.
exclude	Specifies the protocol TLVs or DHCP options to be excluded from the device sensor output.
all	Disables all notifications for the associated protocol.
list <i>list-name</i>	Specified the name of the filter list.
include	Specifies the TLVs or DHCP options that should be included in the Device Sensor output.

Command Default

All TLVs or DHCP options are included in notifications and will trigger notifications.

Command Modes

Global configuration

Command History

Release	Modification
IOS XE 3.4.0SG and IOS 15.1(2)SG	Command introduced on the Catalyst 4500 Series switch.

Usage Guidelines

Use the **device-sensor filter-spec** command to specify a list of CDP or LLDP TLV fields or DHCP options to be included in Device Sensor outputs.

Certain TLVs and message types such as DISCOVER, OFFER, REQUEST, ACK, and IP address are unconditionally excluded. These excluded TLVs and message types are used as transport for higher layer protocols, which change frequently and convey little useful information about endpoints. OFFER messages are also excluded because they can be received from multiple servers, and therefore, do not convey useful endpoint data.

Examples

The following example shows how to apply a CDP TLV filter list to the Device Sensor output:

```
Switch> enable
Switch# configure terminal
Switch(config)# device-sensor filter-spec cdp include cdp-list1
```

Related Commands

Command	Description
debug device-sensor	Enables debugging for Device Sensor.
device-sensor accounting	Adds the Device Sensor protocol data to accounting records and generates additional accounting events when new sensor data is detected.
device-sensor filter-list	Creates a CDP or LLDP filter containing a list of options that can be included or excluded in the Device Sensor output.
device-sensor filter-list dhcp	Creates a DHCP filter containing a list of options that can be included or excluded in the Device Sensor output.
show device-sensor cache	Displays Device Sensor cache entries.

device-sensor notify

To enable client notifications and events for TLV changes, use the **device-sensor notify** command in global configuration mode. To disable client notifications and accounting events for TLV changes, use the **no** form of this command.

device-sensor notify all-changes | new-tlvs

no device-sensor notify all-changes | new-tlvs

Syntax Description

all-changes	Enables client notifications and accounting events for all TLV changes.
new-tlvs	Enables client notifications and accounting events for only new TLV changes.

Command Default

Client notifications and accounting events are generated only for new TLVs.

Command Modes

Global configuration

Command History

Release	Modification
IOS XE 3.4.0SG and IOS 15.1(2)SG	Command introduced on the Catalyst 4500 Series switch.

Usage Guidelines

By default, for each supported peer protocol, client notifications and accounting events will only be generated when an incoming packet includes a TLV that has not been previously received in the context of a given session.

To enable client notifications and accounting events for all TLV changes, where either a new TLV has been received or a previously received TLV has been received with a different value, use the **device-sensor notify all-changes** command.

To return to the default behavior, use the **device-sensor notify new-tlvs** or the **default device-sensor notify** command.

Examples

The following example shows how to enable client notifications and accounting events for all TLV change:

```
Switch> enable
Switch# configure terminal
Switch(config)# device-sensor notify all-changes
```

Related Commands

Command	Description
debug device-sensor	Enables debugging for Device Sensor.
device-sensor filter-list	Creates a CDP or LLDP filter containing a list of options that can be included or excluded in the Device Sensor output.

Command	Description
device-sensor filter-list dhcp	Creates a DHCP filter containing a list of options that can be included or excluded in the Device Sensor output.
show device-sensor cache	Displays Device Sensor cache entries.

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 event as the cause of the reload.

Command Default

A switch exhibits the default SEU behavior when this command is not configured. On redundant switches that have reached SSO, 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(53)SG3, 12.2(54)SG, 15.0(2)SG XE 3.1.1SG	This command was provided on the Catalyst 4500 series switch.
12.2(53)SG6 15.0(2)SG2 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

The following example shows how to configure the SEU behavior as conservative:

```
Switch(config)# diagnostic fpga soft-error recover conservative
```

The following 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 events, but will take no other action.
	normal	(Optional) Specifies that the SRAM diagnostics operate as in conservative mode, except that an ongoing failure resets the supervisor engine; allows for the bootup tests to map out the affected memory.
	aggressive	(Optional) Specifies that the SRAM diagnostics operate as in 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.

Command Default 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 The following example shows how to configure the switch to initiate an RPR switchover when an ongoing failure occurs:

```
Switch# configure terminal
Switch (config)# diagnostic monitor action normal
```

Related Commands	Command	Description
	show diagnostic result module test 2	Displays the module-based diagnostic test results.
	show diagnostic result 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	Parameter	Description
	module num	Module number.
	test	Specifies a test to run.
	<i>test-id</i>	Specifies an identification number for the test to be run; can be the cable diagnostic <i>test-id</i> , or the cable-tdr keyword.
	port num	(Optional) Specifies the interface port number.

Command Default 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.

Examples The following 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-tdr port 3
diagnostic start module 1 test cable-tdr port 3
module 1: Running test(s) 5 Run interface level cable diags
module 1: Running test(s) 5 may disrupt normal system operation
Do you want to continue? [no]: yes
yes
Switch#
2d16h: %DIAG-6-TEST_RUNNING: module 1: Running online-diag-tdr{ID=5} ...
2d16h: %DIAG-6-TEST_OK: module 1: online-diag-tdr{ID=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.

domain

To configure the fabric domain and enter fabric-auto-domain configuration mode, use the **domain** command. The **no** version of this command deletes the fabric domain.

domain {**default** | **name** *name*

no domain

Syntax Description	default	Configures the default fabric domain and enters fabric-auto domain configuration mode.
	name <i>name</i>	Configures a new fabric domain and enters fabric-auto domain configuration mode.

Command Default None.

Command Modes Fabric-auto configuration

Command History	Release	Modification
	3.9.01E	This command was introduced on the Catalyst 4500-E series switch using a Supervisor Engines 8-E and 8L-E.

Usage Guidelines We recommend that you use the default domain, unless your network requires you to create a new domain. This command allows you to enter fabric-auto domain configuration mode where you can configure edge devices in the fabric domain.

Examples

```
Device(config-fabric-auto)#domain default
Device(config-fabric-auto)#domain name exampledomain
```

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	<i>max-attempts</i>	Specifies a maximum number of attempts before a port is moved to the auth-fail VLAN in the range of 1 to 10.
---------------------------	---------------------	--

Command Default	Default is 3.
------------------------	---------------

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

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

Examples The following 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# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet4/3
Switch(config-if)# dot1x auth-fail max-attempts 5
Switch(config-if)# end
Switch#
```

Related Commands	Command	Description
	dot1x max-reauth-req	Sets the maximum number of times that the switch will retransmit an EAP-Request/Identity frame to the client before restarting the authentication process.
	show dot1x	Displays 802.1x information.

dot1x auth-fail vlan

To enable the auth-fail VLAN on a port, use the **dot1x auth-fail vlan** command. To return to the default setting, use the **no** form of this command.

```
dot1x auth-fail vlan vlan-id
```

```
no dot1x auth-fail vlan vlan-id
```

Syntax Description	<i>vlan-id</i>	Specifies a VLAN in the range of 1 to 4094.
--------------------	----------------	---

Command Default	This command has no default settings.
-----------------	---------------------------------------

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

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

Examples The following 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 in-bound traffic on a port.
	both	(Optional) Specifies controlling both in-bound and out-bound traffic on a port.

Command Default Both in-bound and out-bound traffic will be controlled.

Command Modes Interface configuration mode

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

Usage Guidelines You can manage remote systems using unidirectional control. Unidirectional control enables you to turn on systems remotely using a specific Ethernet packet, known as a magic packet.

Using unidirectional control enables you to remotely manage systems using 802.1X ports. In the past, the port became unauthorized after the systems was turned off. In this state, the port only allowed the receipt and transmission of EAPoL packets. Therefore, there was no way for the unidirectional control magic packet to reach the host and without being turned on there was no way for the system to authenticate and open the port.

Examples The following example shows how to enable unidirectional control on incoming packets:

```
Switch(config-if)# dot1x control-direction in
Switch(config-if)#
```

Related Commands	Command	Description
	show dot1x	Displays dot1x information.

dot1x credentials (global configuration)

Use the **dot1x credentials** global configuration command to configure a profile on a supplicant switch.

dot1x credentials *profile*

no dot1x credentials *profile*

Syntax Description	<i>profile</i>	Specify a profile for the supplicant switch.
---------------------------	----------------	--

Command Default	No profile is configured for the switch.	
------------------------	--	--

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

Command History	Release	Modification
	12.2(54)SG	This command was introduced.

Usage Guidelines	You must have another switch set up as the authenticator for this switch to be the supplicant.	
-------------------------	--	--

Examples	The following example shows how to configure a switch as a supplicant:	
-----------------	--	--

```
Switch(config)# dot1x credentials profile
```

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

Related Commands	Command	Description
	cisp enable	Enables Client Information Signalling Protocol (CISP).
show cisp	Displays CISP information for a specified interface.	
	Refer to IOS documentation.	

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.

Command Default Critical authentication is disabled.

Command Modes Interface configuration mode

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

Examples The following example shows how to enable 802.1x critical authentication:

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

Related Commands	Command	Description
	dot1x critical eapol	Enables sending EAPOL success packets when a port is critically authorized partway through an EAP exchange.
	dot1x critical recovery delay	Sets the time interval between port reinitializations.
	dot1x critical vlan	Assigns a critically authenticated port to a specific VLAN.
	show dot1x	Displays dot1x information.

dot1x critical eapol

To enable sending EAPOL success packets when a port is critically authorized partway through an EAP exchange, use the **dot1x critical eapol** command. To return to the default setting, use the **no** form of this command.

dot1x critical eapol

no dot1x critical eapol

Syntax Description This command has no keywords or variables.

Command Default The default is to not send EAPOL success packets.

Command Modes Global configuration mode

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

Examples The following example shows how to enable sending EAPOL success packets:

```
Switch(config-if)# dot1x critical eapol
Switch(config-if)#
```

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	<i>delay-time</i>	Specifies the interval between port reinitializations when AAA transition occurs; valid values are from 1 to 10,000 milliseconds.
---------------------------	-------------------	---

Command Default	Delay time is set to 100 milliseconds.
------------------------	--

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

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

Examples The following example shows how to set the 802.1x critical recovery delay time to 500:

```
Switch(config-if)# dot1x critical recovery delay 500
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 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	<i>vlan-id</i> (Optional) Specifies the VLANs; valid values are from 1 to 4094.
---------------------------	---

Command Default	Critical authentication is disabled on a ports VLAN.
------------------------	--

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

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

Usage Guidelines	<p>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 routed port, no VLAN may be specified.</p> <p>This command is not supported on platforms such as Layer 3 switches that do not include the Critical Auth VLAN subsystem.</p>
-------------------------	--

Examples	The following example shows how to enable 802.1x critical authentication on a ports VLAN:
-----------------	---

```
Switch(config-if)# dot1x critical vlan 350
Switch(config-if)#
```

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

<i>vlan-id</i>	Specifies a VLAN in the range of 1 to 4094.
----------------	---

Command Default

This command has no default settings.; the guest VLAN feature is disabled.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(19)EW	This command was introduced on the Catalyst 4500 series switch.
12.2(25)EWA	Support for secondary VLAN as 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

The following 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)# dot1x port-control auto
Switch(config-if)# dot1x guest-vlan 26
Switch(config-if)# end
Switch(config)# end
Switch#
```

Related Commands

Command	Description
dot1x max-reauth-req	Sets the maximum number of times that the switch will retransmit an EAP-Request/Identity frame to the client before restarting the authentication process.
show dot1x	Displays dot1x information.

dot1x guest-vlan supplicant

To place an 802.1X-capable supplicant (host) into a guest VLAN, use the **dot1x guest-vlan supplicant** global configuration command. To return to the default setting, use the **no** form of this command.

dot1x guest-vlan supplicant

no dot1x guest-vlan supplicant

Syntax Description This command has no arguments or keywords.

Command Default 802.1X-capable hosts are not put into a guest VLAN.

Command Modes Global configuration mode

Command History	Release	Modification
	12.2(25)EWA	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 supplicant behavior 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 The following example shows how to place an 802.1X-capable supplicant (host) into a guest VLAN:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# dot1x guest-vlan supplicant
Switch(config)# end
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.

Command Default

The default is single-host mode.

Command Modes

Interface configuration mode

Command History

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

The following example shows how to enable IEEE 802.1x authentication and to enable multiple-hosts mode:

```
Switch# configure t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitEthernet6/1
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-host
Switch(config-if)# end
Switch#
```

The following 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 FastEthernet6/1
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	<i>interface</i>	Number of the interface.
---------------------------	------------------	--------------------------

Command Default	This command has no default settings.	
------------------------	---------------------------------------	--

Command Modes	Privileged EXEC mode	
----------------------	----------------------	--

Command History	Release	Modification
	12.1(12c)EW	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 fresh authentication.	
-------------------------	---	--

Examples	The following 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.
--------------------	-----	--

Command Default	There is no default setting.
-----------------	------------------------------

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

Command History	Release	Modification
	12.2(31)SG	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 authentication state of a port. If the port is in unauthenticated state, it remains unauthenticated, and if MAB is active, the authentication will revert back to the 802.1X Authenticator. If the port is authorized with a MAC address, and the MAB configuration is removed the port remains authorized until re-authentication takes place. When re-authentication occurs the MAC address is removed in favor of an 802.1X supplicant, which is detected on the wire.
------------------	--

Examples	The following example shows how to enable EAP MAC address authentication:
----------	---

```
Switch(config-if)# dot1x mac-auth-bypass
Switch(config-if)#
```

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

<i>count</i>	Number of times that the switch retransmits EAP-Request/Identity frames before restarting the authentication process; valid values are from 1 to 10.
--------------	--

Command Default

The switch sends a maximum of two retransmissions.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(19)EW	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

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

Related Commands

Command	Description
show dot1x	Displays dot1x information.

dot1x max-req

To set the maximum number of times that the switch retransmits an Extensible Authentication Protocol (EAP)-Request frame of types other than EAP-Request/Identity to the client before restarting the authentication process, use the **dot1x max-req** command. To return to the default setting, use the **no** form of this command.

dot1x max-req *count*

no dot1x max-req

Syntax Description

count Number of times that the switch retransmits EAP-Request frames of types other than EAP-Request/Identity before restarting the authentication process; valid values are from 1 to 10.

Command Default

The switch sends a maximum of two retransmissions.

Command Modes

Interface configuration mode

Command History

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

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

The following 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)#
```

The following 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.

Command Default

The port 802.1X authorization is disabled.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(12c)EW	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 ports. You can use the **auto** keyword only if the port is not configured as follows:

- Trunk port—If you try to enable 802.1X on a trunk port, an error message appears, and 802.1X is not enabled. If you try to change the mode of an 802.1X-enabled port to trunk, the port mode is not changed.
- Dynamic ports—A port in dynamic mode can negotiate with its neighbor to become a trunk port. If you try to enable 802.1X on a dynamic port, an error message appears, and 802.1X is not enabled. If you try to change the mode of an 802.1X-enabled port to dynamic, the port mode is not changed.
- EtherChannel port—Before enabling 802.1X on the port, you must first remove it from the EtherChannel. If you try to enable 802.1X on an EtherChannel 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

The following example shows how to enable 802.1X on Gigabit Ethernet 1/1:

```
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 int** 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 <i>interface-id</i> (Optional) Module and port number of the interface.
---------------------------	--

Command Default	This command has no default settings.
------------------------	---------------------------------------

Command Modes	Privileged EXEC mode
----------------------	----------------------

Command History	Release	Modification
	12.1(12c)EW	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 (<i>re-authperiod</i>) and automatic reauthentication.
-------------------------	---

Examples	The following 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.

Command Default The periodic reauthentication is disabled.

Command Modes Interface configuration mode

Command History	Release	Modification
	12.1(12c)EW	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 The following example shows how to disable the periodic reauthentication of the client:

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

The following example shows how to enable the periodic reauthentication and set the number of seconds between the reauthentication attempts to 4000 seconds:

```
Switch(config-if)# dot1x re-authentication
Switch(config-if)# dot1x timeout re-authperiod 4000
Switch#
```

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

Related Commands	Command	Description
	dot1x timeout	Sets the reauthentication timer.
	show dot1x	Displays dot1x information.

dot1x system-auth-control

To enable 802.1X authentication on the switch, use the **dot1x system-auth-control** command. To disable 802.1X authentication on the system, use the **no** form of this command.

dot1x system-auth-control

no dot1x system-auth-control

Syntax Description This command has no arguments or keywords.

Command Default The 802.1X authentication is disabled.

Command Modes Global configuration mode

Command History	Release	Modification
	12.1(12c)EW	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 port-control auto** command on each specific port on which you want the 802.1X access controls to be used.

Examples The following example shows how to enable 802.1X authentication:

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

Related Commands	Command	Description
	dot1x initialize	Unauthorizes an interface before reinitializing 802.1X.
	show dot1x	Displays dot1x information.

dot1x timeout

To set the reauthentication timer, 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 <i>seconds</i>	Number of seconds between reauthentication attempts; valid values are from 1 to 65535. See the “Usage Guidelines” section for more information.
reauth-period server	Number of seconds between reauthentication attempts; valid values are from 1 to 65535 as derived from the Session-Timeout RADIUS attribute. See the “Usage Guidelines” section for more information.
quiet-period <i>seconds</i>	Number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client; valid values are from 0 to 65535 seconds.
tx-period <i>seconds</i>	Number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request; valid values are from 1 to 65535 seconds.
supp-timeout <i>seconds</i>	Number of seconds that the switch waits for the retransmission of EAP-Request packets; valid values are from 30 to 65535 seconds.
server-timeout <i>seconds</i>	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.

Command Default

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(12)EW	This command was introduced on the Catalyst 4500 series switch.
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

The following example shows how to set 60 as the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet4/3
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.

The following 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 fastethernet4/3
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.

dscp (netflow-lite exporter submode)



Note

NetFlow-lite is supported only on Catalyst 4948E and Catalyst 4948E-F Ethernet switches.

To specify a CoS value for the NetFlow-lite collector, use the **dscp** command. To delete the value, use the **no** form of this command.

```
dscp dscp-value
```

```
no dscp dscp-value
```

Syntax Description

<i>dscp-value</i>	Specifies a DSCP value for the NetFlow-lite collector. Valid values from 0 to 63
-------------------	--

Command Default

0

Command Modes

netflow-lite exporter submode

Command History

Release	Modification
15.0(2)SG	This command was introduced on the Catalyst 4948E and Catalyst 4948E-F Ethernet switches.

Examples

The following example shows how to specify a CoS value for the NetFlow-lite collector:

```
Switch# config terminal
Switch(config)# netflow-lite exporter exporter1
Switch(config-netflow-lite-exporter)# destination 5.5.5.6
Switch(config-netflow-lite-exporter)# source 5.5.5.5
Switch(config-netflow-lite-exporter)# transport udp 8188
Switch(config-netflow-lite-exporter)# ttl 128
Switch(config-netflow-lite-exporter)# cos 7
Switch(config-netflow-lite-exporter)# dscp 32
Switch(config-netflow-lite-exporter)# template data timeout 1
Switch(config-netflow-lite-exporter)# options sampler-table timeout 1
Switch(config-netflow-lite-exporter)# options interface-table timeout 1
Switch(config-netflow-lite-exporter)# export-protocol netflow-v9
Switch(config-netflow-lite-exporter)# exit
Switch(config)#
```

Display the exporter

```
Switch# show netflow-lite exporter exporter1
Netflow-lite Exporter exporter1:
  Network Protocol Configuration:
    Destination IP address: 5.5.5.6
    Source IP Address:     5.5.5.5
    VRF label:
```

```

DSCP:                0x20
TTL:                 128
COS:                 7
Transport Protocol Configuration:
Transport Protocol:   UDP
Destination Port:    8188
Source Port:         61670
Export Protocol Configuration:
Export Protocol:      netflow-v9
Template data timeout: 60
Options sampler-table timeout: 1800
Options interface-table timeout: 1800
Exporter Statistics:
Packets Exported:    0

```

You can verify your settings with the **show netflow-lite exporter** privileged EXEC command.

Related Commands	Command	Description
	cos (netflow-lite exporter submode)	Specifies a CoS value for the NetFlow-lite collector.
	source (netflow-lite exporter submode)	Specifies a source Layer 3 interface of the NetFlow-lite collector.
	transport udp (netflow-lite exporter submode)	Specifies a UDP transport destination port for a NetFlow-lite collector.
	ttl (netflow-lite exporter submode)	Specifies a ttl value for the NetFlow-lite collector.
	destination (netflow-lite exporter submode)	Specifies a destination address in netflow-lite submode.
	template data timeout (netflow-lite exporter submode)	Specifies a template data timeout for the NetFlow-lite collector.
	options timeout (netflow-lite exporter submode)	Specifies an options timeout for the NetFlow-lite collector.
	export-protocol (netflow-lite exporter submode)	Specifies the export protocol for the NetFlow-lite collector.

dual-active detection (virtual switch)

To enable and configure dual-active detection, use the **dual-active detection** command in virtual switch configuration submode. To disable dual-active detection, use the **no** form of this command.

```
dual-active detection { pagp [trust channel-group num] } | fast-hello }
```

```
no dual-active detection { pagp | fast-hello }
```

Syntax Description

pagp	Configures Port Aggregation Protocol (PAgP) as the dual-active detection method. Default: enabled.
trust channel-group <i>num</i>	(Optional) Specifies the EtherChannel/port bundling to be used for PAgP dual-active detection. Range: 1 to 256. Default: disabled.
fast-hello	Configures fast hello packet detection as the dual-active detection method. Default: enabled.

Command Default

Detection methods (pagp and fast-hello) are enabled and trust is disabled by default.

Command Modes

Virtual switch configuration submode (config-vs-domain)

Command History

Release	Modification
12.2(52)SG	This command was introduced on the Catalyst 4500 series switch.
Release IOS XE 3.5.0E and IOS 15.2(1)SG	Support extended to fast-hello option.

Usage Guidelines

If PAgP is running on the MECs between the VSS and its access switches, the VSS can use enhanced PAgP messaging to detect dual-active scenario. The MEC must have links from both chassis of the VSS to the access switch. By default, PAgP dual-active detection is enabled. However, the enhanced messages are only sent on channel groups with trust mode enabled.

If you configure the fast hello dual-active detection mechanism, you must also configure dual-active interface pairs to act as fast hello dual-active messaging links. See the **dual-active fast-hello (virtual switch)** command.

When you enter the optional **trust channel-group** *num* keywords and argument, the following applies:

- You can configure trust mode on a port channel even if there are no interfaces on the port channel or the port channel is a protocol type other than PAgP. The trust mode status is displayed in the **show pagp dual-active** command output, but no interfaces are displayed.
- Configuring trust mode requires that the port channel exists. If the port channel does not exist, the following error message is displayed:

```
Router(config-vs-domain)# dual-active trust pagp channel-group 30
Port-channel 30 not configured
```

- If a trusted port is deleted, the trust-mode configuration is deleted and the following warning message is displayed:

```
Port-channel num is a trusted port-channel for PAgP
dual-active detection. Restricting this
port-channel has deleted the dual-active trust
channel-group configuration associated with it.
```

- If a trusted port is changed to a virtual switch port, the trust mode configuration is deleted when the port becomes restricted and the following warning message is displayed:

```
Port-channel num is a trusted port-channel for PAgP
dual-active detection. Deletion of this
port-channel has deleted the dual-active trust
channel-group configuration associated with it.
```

- If you enter the **dual-active detection pagp trust port-channel** command on a virtual switch port channel, the following error message is displayed:

```
Cannot configure dual-active trust mode on a virtual switch port-channel
```

Examples

The following example shows how to configure interfaces for PAgP dual-active detection:

```
Router(config)# switch virtual domain domain-id
Router (config-vs-domain)# dual-active detection pagp
Router (config-vs-domain)#
```

The following example shows how to specify that EtherChannel/port bundling to be used for PAgP dual-active detection;

```
Router(config)# switch virtual domain domain-id
Router (config-vs-domain)# dual-active detection pagp trust port-channel 20
Router (config-vs-domain)#
```

The following example shows how to configure an interface for fast hello dual-active detection:

```
Router(config)# switch virtual domain domain-id
Router (config-vs-domain)# dual-active detection fast-hello
Router (config-vs-domain)# exit
Router(config)# interface fastethernet 1/2/40
Router(config-if)# dual-active fast-hello
WARNING: Interface FastEthernet1/2/40 placed in restricted config mode. All extraneous
configs removed!
Router(config-if)# no shutdown
```

Related Commands

Command	Description
dual-active fast-hello (virtual switch)	Configures dual-active detection.
show switch virtual (virtual switch)	Displays information about dual-active detection configuration and status.

dual-active fast-hello (virtual switch)

To enable an interface to be a fast hello dual-active messaging link, use the **dual-active detection** command in interface configuration mode. To disable dual-active detection on an interface, use the **no** form of this command.

dual-active fast-hello

no dual-active fast-hello

Syntax Description This command has no arguments or keywords.

Command Default Fast hello dual-active detection is disabled on all interfaces by default.

Command Modes Interface configuration mode (config-if)

Command History	Release	Modification
	Release IOS XE 3.5.0E and IOS 15.2(1)SG	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines This command automatically removes all other configuration from the interface and restricts the interface to dual-active configuration commands.

Examples The following example shows how to configure an interface as a fast hello dual-active messaging link:

```
Router(config)# switch virtual domain domain-id
Router (config-vs-domain)# dual-active detection fast-hello
Router (config-vs-domain)# exit
Router(config)# interface fastethernet 1/2/40
Router(config-if)# dual-active fast-hello
WARNING: Interface FastEthernet1/2/40 placed in restricted config mode. All extraneous
configs removed!
Router(config-if)# no shutdown
```

Related Commands	Command	Description
	dual-active detection (virtual switch)	Configure dual-active detection on the virtual switch.
	show switch virtual (virtual switch)	Displays information about dual-active detection configuration and status.

dual-active recovery ip address

To configure an IP address for the management interface when the switch is in recovery mode, use the **dual-active recovery ip address** command in virtual-switch configuration submode. To remove the IP address, use the **no** form of this command.

```
dual-active recovery [switch num] ip address ip-address ip-mask
```

```
no dual-active recovery ip address ip-address ip-mask
```

Syntax Description

switch num	(Optional) The virtual switch number of the chassis for which the IP address must be used. If unspecified, the same IP address is used for either switch.
<i>ip-address</i>	Specifies an IP address.
<i>ip-mask</i>	Specifies an IP address mask.

Command Default

This command has no default settings.

Command Modes

Virtual switch configuration submode (config-vs-domain)

Command History

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

Usage Guidelines

The command accepts up to three IP addresses - one for switch 1, one for switch 2 and one global IP address. When a switch enters recovery mode, it picks up the configured switch-specific recovery IP address for its management interface. If the switch-specific IP address is unconfigured, the global recovery IP address is used. If neither the switch-specific nor global recovery IP addresses are configured, the fastEthernet1 management interface on the switch has no IP address active, when the switch enters recovery mode.

The normal IP address configured for fastEthernet1 in interface configuration mode is retained in the configuration.

Examples

The following example shows how to configure global recovery IP address:

```
Switch(config)# switch virtual domain domain-id
Switch(config-vs-domain)# dual-acti
ve recovery ip address 192.168.1.5 255.255.255.0
Switch(config-vs-domain)# exit
```

Related Commands

■ dual-active recovery ip address

Command	Description
dual-active detection (virtual switch)	Configure dual-active detection on the virtual switch.
show switch virtual (virtual switch)	Displays information about dual-active detection configuration and status.

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.

Command Default

Half-duplex operation

Command Modes

Interface configuration mode

Command History

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

Usage Guidelines

Table 2-1 lists the supported command options by interface.

Table 2-1 Supported duplex Command Options

Interface Type	Supported Syntax	Default Setting	Guidelines
10/100-Mbps module	duplex [half full]	half	If the speed is set to auto , you will not be able to set the duplex mode. If the speed is set to 10 or 100 , and you do not configure the duplex setting, the duplex mode is set to half duplex.
100-Mbps fiber modules	duplex [half full]	half	
Gigabit Ethernet Interface	Not supported.	Not supported.	Gigabit Ethernet interfaces are set to full duplex.
10/100/1000	duplex [half full]		If the speed is set to auto or 1000 , you will not be able to set duplex . If the speed is set to 10 or 100 , and you do not configure the duplex setting, the duplex mode is set to half duplex.

If the transmission speed on a 16-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 reenables 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 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

The following example shows how to configure the interface for full-duplex operation:

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

Related Commands

Command	Description
speed	Configures the interface speed.
interface (refer to Cisco IOS documentation)	Configures an interface.
show controllers (refer to Cisco IOS documentation)	Displays controller information.
show interfaces	Displays interface information.

epm access control

To configure access control, use the **epm access control [open | default]** command.

epm access control [open | default]

Syntax Description	open	Specifies open access control.
	default	Specifies default access control.

Command Default If the **epm access control** command is not configured, the behavior defaults to the **epm access control default** command. Nothing is nvgened.

Command Modes Configuration mode

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

Usage Guidelines When you enter the **epm access control** command, it is nvgen'd.

If no ACLs are downloaded from the ACS server when a host is authenticated, the host is restricted by the port ACLs and do not receive additional permissions. In such a scenario, if you enter the **epm access control open** command, a **permit ip host** any entry is created for the host after authentication. This entry is created only if no ACLs are downloaded from the ACS.

The **epm access control open** command is particularly useful in authentication open mode. Traffic from a host is allowed to pass even before the host is authenticated. This traffic is restricted by the port ACL. In such a scenario, if no ACLs are downloaded from the ACS, the host will not receive any additional permissions. Even after authentication, the host is still restricted by the port ACL. If **epm access control open** is configured, complete access is granted upon authentication.

If **epm access control default** is configured and no ACL is downloaded, port ACL is the only ACL on the port. This is how access control functioned prior to Cisco IOS Release 12.2(54)SG.

Examples The following example shows how to enable open access control:

```
Switch(config)# epm access control open
```

The following example shows how to enable default access control:

```
Switch(config)# epm access control default
```

Related Commands	Command	Description
	show ipv6 snooping counters	Displays the number of packets dropped per port due to RA Guard.

erase

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

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

Syntax Description	
/all nvram:	Erases everything in nvram:.
/all non-default	Erases files and configuration in nonvolatile storage including nvram:, bootflash:, cat4000_flash:, and crashinfo: of the local supervisor engine. Resets the Catalyst 4500 series switch to the factory default settings. Note This command option is intended to work only on a standalone supervisor engine.
cat4000_flash:	Erases the VLAN database configuration file.
nvram:	Erases the startup-config and private-config file in NVRAM.
startup-config:	Erases the startup-config and private-config file in NVRAM.

Command Default 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



When you use the **erase** command to erase a file system, you cannot recover the files in the file system.

In addition to the command options shown above, options with the prefix slave that are used to identify nvram: and flash (such as slavenvram: and slavecat4000_flash:) appear in the command help messages on the dual supervisor engine redundancy switch.

The **erase nvram:** command replaces the **write erase** and the **erase startup-config** commands. This command erases both the startup-config and the private-config file.

The **erase /all nvram:** command erases all files in nvram: in addition to startup-config file and private-config file.

The **erase cat4000_flash:** command erases the VLAN database configuration file.

The **erase /all non-default** command facilitates 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 mentioned in the Cisco IOS library as well as those set by the **erase /all non-default** command (vtp mode=transparent, and the ROMMON variables: ConfigReg=0x2101, PS1= "rommon ! >" and EnableAutoConfig=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/configfun/command/reference/ffun_r.html



Caution

The **erase /all non-default** command can erase Cisco IOS images in bootflash:. Ensure that a Cisco IOS image can be copied back to the bootflash: (such as, 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

The following example shows how to erase the files and configuration in a nonvolatile storage and reset the switch to factory default settings:

```
Switch# erase /all non-default
Switch#
Erase and format operation will destroy all data in non-volatile storage. Continue?
[confirm]
Formatting bootflash: ...

Format of bootflash complete
Erasing nvram:
Erasing cat4000_flash:
Clearing crashinfo:data
Clearing the last power failure timestamp
Clearing all ROMMON variables
Setting default ROMMON variables:
    ConfigReg=0x2101
    PS1=rommon ! >
    EnableAutoConfig=1
Setting vtp mode to transparent
%WARNING! Please reboot the system for the changes to take effect
Switch#
00:01:48: %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#
```

The following example shows how to erase the contents in nvram.

```
Switch# erase /all nvram:
Erasing the nvram filesystem will remove all files! Continue? [confirm]
[OK]
Erase of nvram: complete
Switch#
00:38:10: %SYS-7-NV_BLOCK_INIT: Initalized the geometry of nvram
Switch#
```

The following example shows how to erase filesystem cat4000_flash.

```
Switch# erase cat4000_flash:
Erasing the cat4000_flash filesystem will remove all files! Continue? [confirm]
[OK]
Erase of cat4000_flash:complete
Switch#
```

Related Commands	Command	Description
	boot config (refer to Cisco IOS documentation)	Specifies the device and filename of the configuration file.
	delete (refer to Cisco IOS documentation)	Deletes a file from a flash memory device or NVRAM.
	show bootvar	Displays BOOT environment variable information.
	undelete (refer to Cisco IOS documentation)	Recovers a file marked “deleted” on a Class a flash file system.

errdisable detect cause

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

```
errdisable detect cause {all | arp-inspection | bpduguard | dhcp-rate-limit | dtp-flap |
gbic-invalid | inline-power | l2ptguard | link-flap | loopback | pagp-flap | psp |
security-violation shutdown vlan | sfp-config-mismatch }
```

```
no errdisable detect cause {all | arp-inspection | bpduguard | dhcp-rate-limit | dtp-flap |
gbic-invalid | inline-power | l2ptguard | link-flap | loopback | pagp-flap | psp |
security-violation shutdown vlan | sfp-config-mismatch }
```

For the bridge protocol data unit (BPDU) guard and port security, you can use this command to configure the switch to disable only a specific VLAN on a port instead of disabling the entire port.

When the per-VLAN error-disable feature is turned off and a BPDU guard violation occurs, the entire port is disabled. Use the **no** form of this command to disable the per-VLAN error-disable feature.

```
errdisable detect cause bpduguard shutdown vlan
```

```
no errdisable detect cause bpduguard shutdown vlan
```

Syntax Description

all	Enable error detection for all error-disabled causes.
arp-inspection	Enable error detection for dynamic Address Resolution Protocol (ARP) inspection.
bpduguard shutdown vlan	Enable per-VLAN error-disable for BPDU guard.
dhcp-rate-limit	Enable error detection for DHCP snooping.
dtp-flap	Enable error detection for the Dynamic Trunking Protocol (DTP) flapping.
gbic-invalid	Enable error detection for an invalid Gigabit Interface Converter (GBIC) module. Note This error refers to an invalid small form-factor pluggable (SFP) module.
inline-power	Enable error detection for the Power over Ethernet (PoE) error-disabled cause. This keyword is supported only on switches with PoE ports.
l2ptguard	Enable error detection for a Layer 2 protocol-tunnel error-disabled cause.
link-flap	Enable error detection for link-state flapping.
loopback	Enable error detection for detected loopbacks.
pagp-flap	Enable error detection for the Port Aggregation Protocol (PAgP) flap error-disabled cause.
psp	Enable error detection for protocol storm protection
security-violation shutdown vlan	Enable voice aware 802.1x security.
sfp-config-mismatch	Enable error detection on an SFP configuration mismatch.

Command Default Detection is enabled for all causes. All causes, except for per-VLAN error disabling, are configured to shut down the entire port.

Command Modes Global configuration

Command History	Release	Modification
	12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch.
	12.2(52)SG	Added support for per-VLAN error-disable detection.
	IOS XE 3.5.0E and IOS 15.2(1)E	The security-violation shutdown vlan keyword was introduced.

Usage Guidelines A cause (**link-flap**, **dhcp-rate-limit**, and so forth) is the reason for the error-disabled state. When a cause is detected on an interface, the interface is placed in an error-disabled state, an operational state that is similar to a link-down state.

When a port is error-disabled, it is effectively shut down, and no traffic is sent or received on the port. For the BPDU guard, voice aware 802.1x security, and port-security features, you can configure the switch to shut down just the offending VLAN on the port when a violation occurs, instead of shutting down the entire port.

If you set a recovery mechanism for the cause by entering the **errdisable recovery** global configuration command for the cause, the interface is brought out of the error-disabled state and allowed to retry the operation when all causes have timed out. If you do not set a recovery mechanism, you must enter the **shutdown** and then the **no shutdown** commands to manually recover an interface from the error-disabled state.

For protocol storm protection, excess packets are dropped for a maximum of two virtual ports. Virtual port error disabling using the **psp** keyword is not supported for EtherChannel and Flexlink interfaces.

To verify your settings, enter the **show errdisable detect** privileged EXEC command.

Examples The following example shows how to enable error-disabled detection for the link-flap error-disabled cause:

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

This command shows how to globally configure BPDU guard for per-VLAN error disable:

```
switch(config)# errdisable detect cause bpduguard shutdown vlan
```

This command shows how to globally configure voice aware 802.1x security for per-VLAN error disable:

```
Switch(config)# errdisable detect cause security-violation shutdown vlan
```

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

Related Commands	Command	Description
	show errdisable detect	Displays error-disabled detection information.
	show interfaces status	Displays interface status or a list of interfaces in the error-disabled state.
	clear errdisable interface	Clears the error-disabled state from a port or VLAN that was error disabled by the per-VLAN error disable feature.

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.

Use the **errdisable recovery** command to configure the recovery mechanism variables. To return to the default setting, use the **no** form of this command.

```
errdisable recovery [cause {all | arp-inspection | bpduguard | channel-misconfig |
dhcp-rate-limit | dtp-flap | gbic-invalid | l2ptguard | link-flap | pagp-flap |
psecure-violation | security-violation | storm-control | udld | unicastflood | vmps}
[arp-inspection] [interval {interval}]]
```

```
no errdisable recovery [cause {all | arp-inspection | bpduguard | channel-misconfig |
dhcp-rate-limit | dtp-flap | gbic-invalid | l2ptguard | link-flap | pagp-flap |
psecure-violation | 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 timers for all error-disable causes.
arp-inspection	(Optional) Enables the recovery timer for the ARP inspection cause.
bpduguard	(Optional) Enables the recovery timer for the BPDU guard error-disable cause.
channel-misconfig	(Optional) Enables the recovery timer for the channel-misconfig error-disable cause.
dhcp-rate-limit	(Optional) Enables the recovery timer for the DHCP rate limit error-disable cause.
dtp-flap	(Optional) Enables the recovery timer for the DTP flap error-disable cause.
gbic-invalid	(Optional) Enables the recovery timer for the GBIC invalid error-disable cause.
l2ptguard	(Optional) Enables the recovery timer for the Layer 2 protocol-tunnel error-disable cause.
link-flap	(Optional) Enables the recovery timer for the link flap error-disable cause.
pagp-flap	(Optional) Enables the recovery timer for the PAgP flap error-disable cause.
psecure-violation	(Optional) Enables the recovery timer for the psecure violation error-disable cause.
security-violation	(Optional) Enables the automatic recovery of ports disabled due to 802.1X security violations.
storm-control	(Optional) Enables the timer to recover from storm-control error-disable state.
udld	(Optional) Enables the recovery timer for the UDLD error-disable cause.
unicastflood	(Optional) Enables the recovery timer for the unicast flood error-disable cause.
vmps	(Optional) Enables the recovery timer for the VMPS error-disable cause.
arp-inspection	(Optional) Enables the ARP inspection cause and recovery timeout.
interval interval	(Optional) Specifies the time to recover from a specified error-disable cause; valid values are from 30 to 86400 seconds.

Command Default Error disable recovery is disabled.
The recovery interval is set to 300 seconds.

Command Modes Global configuration mode

Command History	Release	Modification
	12.1(8a)EW	This command was introduced on the Catalyst 4500 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 operational state that is similar to the link-down state). If you do not enable error-disable recovery for the cause, the interface stays in the error-disabled state until a shutdown and no shutdown occurs. If you enable recovery for a cause, the interface is brought out of the error-disabled state and allowed to retry operation again once all the causes have timed out.

You must enter the **shutdown** command and then the **no shutdown** command to recover an interface manually from error disable.

Examples The following example shows how to enable the recovery timer for the BPDU guard error disable cause:

```
Switch(config)# errdisable recovery cause bpduguard
Switch(config)#
```

The following example shows how to set the timer to 300 seconds:

```
Switch(config)# errdisable recovery interval 300
Switch(config)#
```

The following 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
l2ptguard              Disabled
psecure-violation     Disabled
gbic-invalid           Disabled
dhcp-rate-limit       Disabled
unicast-flood         Disabled
storm-control         Disabled
arp-inspection        Enabled
```

■ **errdisable recovery**

Timer interval: 300 seconds

Interfaces that will be enabled at the next timeout:

Switch#

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.

export-protocol (netflow-lite exporter submode)



Note

NetFlow-lite is supported only on Catalyst 4948E and Catalyst 4948E-F Ethernet switches.

To specify the export protocol for the NetFlow-lite collector, use the **export-protocol** command. To delete the value, use the **no** form of this command.

```
export-protocol { netflow-v9 | ipfix }
```

```
no export-protocol { netflow-v9 | ipfix }
```

Syntax Description	netflow-v9	Specifies export format of Netflow V9.
	ipfix	Specifies export format of Netflow V10 or IPFIX.

Command Default netflow-v9

Command Modes netflow-lite exporter submode

Command History	Release	Modification
	15.0(2)SG	This command was introduced on the Catalyst 4948E and Catalyst 4948E-F Ethernet switches.

Usage Guidelines By default the export protocol is Netflow V9. IPFIX or Netflow V10 is a newer export format. They support variable length encoding that allows for more efficient packaging of packet samples according to the actual packet section bytes extracted from the original sampled packet.

Examples The following example shows how to specify the export protocol for the NetFlow-lite collector:

```
Switch# config terminal
Switch(config)# netflow-lite exporter exporter1
Switch(config-netflow-lite-exporter)# destination 5.5.5.6
Switch(config-netflow-lite-exporter)# source 5.5.5.5
Switch(config-netflow-lite-exporter)# transport udp 8188
Switch(config-netflow-lite-exporter)# ttl 128
Switch(config-netflow-lite-exporter)# cos 7
Switch(config-netflow-lite-exporter)# dscp 32
Switch(config-netflow-lite-exporter)# template data timeout 1
Switch(config-netflow-lite-exporter)# options sampler-table timeout 1
Switch(config-netflow-lite-exporter)# options interface-table timeout 1
Switch(config-netflow-lite-exporter)# export-protocol netflow-v9
Switch(config-netflow-lite-exporter)# exit
Switch(config)#
```

■ export-protocol (netflow-lite exporter submode)

```

Display the exporter
Switch# show netflow-lite exporter exporter1
Netflow-lite Exporter exporter1:
  Network Protocol Configuration:
    Destination IP address: 5.5.5.6
    Source IP Address:    5.5.5.5
    VRF label:
    DSCP:                 0x20
    TTL:                  128
    COS:                  7
  Transport Protocol Configuration:
    Transport Protocol:   UDP
    Destination Port:     8188
    Source Port:         61670
  Export Protocol Configuration:
    Export Protocol:      netflow-v9
    Template data timeout: 60
    Options sampler-table timeout: 1800
    Options interface-table timeout: 1800
  Exporter Statistics:
    Packets Exported:    0

```

You can verify your settings with the **show netflow-lite exporter** privileged EXEC command.

Related Commands

Command	Description
netflow-lite exporter	Defines an exporter and to enter NetFlow-lite exporter submode.
destination (netflow-lite exporter submode)	Specifies a destination address in netflow-lite submode.
source (netflow-lite exporter submode)	Specifies a source Layer 3 interface of the NetFlow-lite collector.
transport udp (netflow-lite exporter submode)	Specifies a UDP transport destination port for a NetFlow-lite collector.
ttl (netflow-lite exporter submode)	Specifies a ttl value for the NetFlow-lite collector.
cos (netflow-lite exporter submode)	Specifies a CoS value for the NetFlow-lite collector.
dscp (netflow-lite exporter submode)	Specifies a CoS value for the NetFlow-lite collector.
template data timeout (netflow-lite exporter submode)	Specifies a template data timeout for the NetFlow-lite collector.
options timeout (netflow-lite exporter submode)	Specifies an options timeout for the NetFlow-lite collector.

exporter (netflow-lite monitor submode)



Note

NetFlow-lite is supported only on Catalyst 4948E and Catalyst 4948E-F Ethernet switches.

To assign an exporter in netflow-lite monitor submode, use the **exporter** command. To delete a sampler, use the **no exporter** form of this command.

```
exporter exporter-name
```

```
no exporter exporter-name
```

Syntax Description	<i>exporter-name</i>	Specifies an exporter.
--------------------	----------------------	------------------------

Command Default	None
-----------------	------

Command Modes	netflow-lite exporter submode
---------------	-------------------------------

Command History	Release	Modification
	15.0(2)SG	This command was introduced on the Catalyst 4948E and Catalyst 4948E-F Ethernet switches.

Usage Guidelines	You can enter this command under the physical port interface mode, port channel interface, or config VLAN mode.
------------------	---

Examples	The following example shows how to configure a monitor on a port interface Gigabit 1/3:
----------	---

```
Switch# config terminal
Switch(config)# int GigabitEthernet1/3
Switch(config-if)# netflow-lite monitor 1
Switch(config-netflow-lite-monitor)# sampler sampler1
Switch(config-netflow-lite-monitor)# average-packet-size 128
Switch(config-netflow-lite-monitor)# exporter exporter1
Switch(config-netflow-lite-monitor)# exit
Switch(config-if)# exit
Switch(config)# exit
Switch# show netflow-lite monitor 1 interface gi1/3
Interface GigabitEthernet1/3:
  Netflow-lite Monitor-1:
    Active:                TRUE
    Sampler:                sampler1
    Exporter:              exporter1
    Average Packet Size:   0
  Statistics:
    Packets exported:      0
    Packets observed:      0
```

■ exporter (netflow-lite monitor submode)

```

Packets dropped:          0
Average Packet Size observed: 64
Average Packet Size used: 64

```

You can verify your settings with the **show netflow-lite exporter** privileged EXEC command.

Related Commands	Command	Description
	sampler (netflow-lite monitor submode)	Activate sampling on an interface in netflow-lite monitor submode.
	average-packet-size (netflow-lite monitor submode)	Specifies the average packet size at the observation point.
	exporter (netflow-lite monitor submode)	Assigns an exporter in netflow-lite monitor submode.

fabric auto

To enable automatic fabric provisioning and enter automatic fabric configuration mode, use the **fabric auto command** in global configuration mode.

fabric auto

Syntax Description	fabric auto	Enables automatic fabric provisioning and enters fabric-auto configuration mode.
---------------------------	--------------------	--

Command Default	None.
------------------------	-------

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

Command History	Release	Modification
	3.9.01E	This command was introduced on the Catalyst 4500-E series switch using a Supervisor Engines 8-E and 8L-E.

Usage Guidelines	Use this command to configure all the elements in your fabric domain automatically. The fabric auto command enables the auto-generation of LISP, VLAN, VRF configuration to orchestrate the fabric overlay. The show-running configuration command shows the fabric domain configuration including the and auto-generated base line commands.
-------------------------	---

Examples	Device(config)# fabric auto
-----------------	-----------------------------

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.

Command Default

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-X4416-2GB-TX	All ports except for the oversubscribed ports	Off
WS-X4418-GB	Uplink ports (1–2)	Off
WS-X4418-GB	Oversubscribed ports (3–18)	On
WS-X4412-2GB-TX	Uplink ports (13–14)	Off
WS-X4412-2GB-TX	Oversubscribed ports (1–12)	On
WS-X4416-2GB-TX	Uplink ports (17–18)	Off

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(8a)EW	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-T	Negotiation always enabled	Configured flow control always negotiated
1000BASE-X	No speed nonnegotiation	Configured flow control negotiated
1000BASE-X	Speed nonnegotiation	Configured flow control forced

Examples

The following example shows how to enable send flow control:

```
Switch(config-if)# flowcontrol receive on
Switch(config-if)#
```

The following example shows how to disable send flow control:

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

The following example shows how to set receive flow control to desired:

```
Switch(config-if)# flowcontrol receive desired
Switch(config-if)#
```

Related Commands	Command	Description
	interface port-channel	Accesses or creates a port-channel interface.
	interface range	Runs a command on multiple ports at the same time.
	show flowcontrol	Displays the per-interface status and statistics related to flow control.
	show running-config	Displays the running-configuration for a switch.
	speed	Configures the interface speed.

hardware statistics

To enable TCAM hardware statistics in your ACLs use the **hardware statistics** command. To disable TCAM hardware statistics, use the **no** form of this command.

hardware statistics

no hardware statistics

Syntax Description This command has no arguments or keywords.

Command Default Hardware statistics is disabled.

Command Modes Global configuration mode

Command History	Release	Modification
	12.2(40)SG	Support introduced on Supervisor Engine 6-E and Catalyst 4900M.

Usage Guidelines TCAM hardware on Supervisor Engine 6-E, Supervisor Engine 6L-E, Catalyst 4900M, Catalyst 4948E, and Catalyst 4948E-F do not have sufficient hardware statistics entries for every classification/QoS cam entry. Therefore, the statistics for each cam entry needs to be enabled as needed.

Examples The following example shows how to enable TCAM hardware statistics in your ACLs ace:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#ip access-list extended myv4
Switch(config-ext-nacl)#permit ip any any
Switch(config-ext-nacl)#hardware statistics
Switch(config-ext-nacl)#end
```

Related Commands	Command	Description
	ip access list (refer to Cisco IOS documentation)	Creates an IP ACL (Access Control List).
	ipv6 access list (refer to Cisco IOS documentation)	Creates an IPv6 ACL.
	mac access-list extended	Defines the extended MAC access lists.

host-pool name

To create an IP pool to group endpoints in the fabric domain, and enter host-pool configuration mode, use the **host-pool name** *name* command in global configuration mode.

```
host-pool name name {host-vlan id} {gateway ip address mask} [context name name] {use-dhcp ip address}
```

Syntax Description	Parameter	Description
	host-vlan id	Configures a VLAN ID to associate with the host-pool.
	gateway ipv4 address mask	Configures the routing gateway IP address and subnet mask for the host-pool.
	context name name	Associates a context or a VRF to the host-pool.
	use-dhcp ipv4 address	Configures a DHCP server for the host-pool.

Command Default None.

Command Modes Fabric-auto-domain configuration

Command History	Release	Modification
	3.9.01E	This command was introduced on the Catalyst 4500-E series switch using a Supervisor Engines 8-E and 8L-E.

Usage Guidelines Use this command to group endpoints in the fabric domain into IP pools, and identify them with a VLAN ID, an IP subnet, and optionally, to a context or VRF in the fabric domain.

This command auto-generates LISP configuration, to orchestrate the fabric overlay. The **show-running configuration** command shows the fabric domain configuration including the auto-generated commands.

Examples This example configures a host-pool in your fabric domain.

```
device(config-fabric-auto-domain)#host-pool name VOICE_DOMAIN
device(config-fabric-auto-domain-host-pool)#vlan 10
device(config-fabric-auto-domain-host-pool)#gateway 192.168.1.254/24
device(config-fabric-auto-domain-host-pool)#context name example-context
device(config-fabric-auto-domain-host-pool)#use-dhcp 172.10.1.1
device(config-fabric-auto-domain-host-pool)#exit
```

This configuration is auto-generated when you configure a host-pool:

```
ip dhcp relay information option vpn
ip dhcp relay information option
ip dhcp snooping vlan 10
ip dhcp snooping
```



```
vlan 10
name VOICE_DOMAIN
interface Vlan10
ip vrf forwarding example-context
ip dhcp relay source-interface Loopback0
ip address 192.168.1.254 255.255.255.0
ip helper-address global 209.65.201.6
no ip redirects
ip local-proxy-arp
ip route-cache same-interface
no lisp mobility liveness test
lisp mobility example-context.EID.VOICE_DOMAIN
!
router lisp
eid-table vrf example-context
dynamic-eid example-context.EID.VOICE_DOMAIN
database-mapping 192.168.1.0/24 locator-set default.RLOC
```

hw-module beacon



Note

The **hw-module beacon** command is enabled only on the uplink modules of the WS-C4500X-32.

To control the beacon LED in conjunction with the beacon button, enter the **hw-module beacon** command:

```
hw-module beacon [on | off]
```

Syntax Description

on	Turns on the LED.
off	Turns off the LED.

Command Default

none

Command Modes

global configuration

Command History

Release	Modification
IOS-XE 3.3.0SG (15.1(1)SG)	This command was introduced on WS-C4500X-32.

Usage Guidelines

Either press the beacon button on the front side of the switch or enter the **hw-mod beacon** command, so the switch is identifiable when the operator walks around the isle to the back side of the switch. (The LED and the CLI function as switch identifiers when multiple units are present.)

Pressing the blue beacon LED switch toggles the beacon LED state.

Examples

If numerous WS-C4500X-32 chassis are in close proximity and you want to remove a transceiver from one chassis' port 11, you can identify it with the **hw-module beacon on** command:

```
Switch# hw-module beacon on
Switch#
*Feb 16 13:12:24.418: %C4K_IOSMODPORTMAN-6-BEACONTURNEDON: Beacon has been turned on
```

The WS-C4500X-32 whose beacon was turned on is the switch you are looking for.

After you complete the necessary service on a switch with the beacon LED turned on, you should either press the beacon button to turn it off, or enter the **hw-module beacon off** command to turn the LED off.

```
Switch# hw-module beacon off
Switch#
*Feb 16 13:12:18.083: %C4K_IOSMODPORTMAN-6-BEACONTURNEDOFF: Beacon has been turned off
```

hw-module module start



Note

The **hw-module module start** command is enabled only on the uplink modules of the WS-C4500X-32.

To boot a module after if it has been stopped, use the **hw-module module start** command:

```
hw-module module number start
```

Syntax Description

<i>number</i>	Uplink module ID. The only applicable value for WS-C4500 is 2.
---------------	--

Command Default

none

Command Modes

global configuration

Command History

Release	Modification
IOS-XE 3.3.0SG (15.1(1)SG)	This command was introduced on WS-C4500X-32.

Usage Guidelines

To bring up a module that has been stopped using the **hw-module module *number* stop** command or by pressing the **OIR button**, you either enter the **hw-module module *number* start** command or physically remove and reinsert.

Examples

The following example shows what happens if a module has been stopped and you enter this command:

```
Switch# hw-module module 2 start
Switch#
*Feb  5 16:36:27.352: %C4K_IOSMODPORTMAN-6-MODULEINSERTED: Module 2 is inserted
*Feb  5 16:37:15.902: %C4K_IOSMODPORTMAN-6-MODULEONLINE: Module 2 (WS-X4908X-10G-TIM S/N:
JAE15340C0J Hw: 0.1) is online
Switch#show module
Chassis Type : WS-C4500X-32

Power consumed by backplane : 0 Watts

Mod Ports Card Type                               Model                               Serial No.
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
  1    32  4500X-32 10GE (SFP+)                   WS-C4900X-32P-10G                 JAE153505E9
  2     8   10GE SFP+                               WS-X4908X-10G-TIM                 JAE15340C0J

M MAC addresses                               Hw  Fw                               Sw                               Status
-----+-----+-----+-----+-----+-----+-----+-----+
  1 0022.bde2.1061 to 0022.bde2.1080 0.2 15.0(1r)SG(0 0.DEV-0             Ok
  2 0022.bde2.1579 to 0022.bde2.1580 0.1                               Ok

Switch#
```

hw-module module start

The following example shows what happens if a module has not been stopped and you enter this command:

```
Switch# hw-module module 2 start  
% Module 2 not stopped
```

Related Commands

Command	Description
hw-module module stop	Shuts down a module and makes it safe for removal.

hw-module module stop



Note

The **hw-module module stop** command is enabled only on the uplink modules of the WS-C4500X-32.

To shut down a module and make it safe for removal, enter the **hw-module module stop** command:

```
hw-module module number stop
```

Syntax Description

<i>number</i>	Uplink module ID. The only applicable value for WS-C4500 is 2.
---------------	--

Command Default

none

Command Modes

global configuration

Command History

Release	Modification
IOS-XE 3.3.0SG (15.1(1)SG)	This command was introduced on WS-C4500X-32.

Usage Guidelines

To initiate uplink module OIR w/o pressing the OIR button.

Examples

The following example shows what happens if a module is up and you enter the **hw-module module stop** command:

```
Switch# hw-module module 2 stop
Proceed with module stop? [confirm]
Switch#
*Feb  5 16:34:37.325: %C4K_IOSMODPORTMAN-6-MODULEOFFLINE: Module 2 is offline
Switch#show module
Chassis Type : WS-C4500X-32

Power consumed by backplane : 0 Watts

Mod Ports Card Type                               Model                               Serial No.
---+-----+-----+-----+-----+-----+-----+-----+-----+-----+
 1    32  4500X-32 10GE (SFP+)                       WS-C4900X-32P-10G                 JAE153505E9
 2     8  Module being held in reset                WS-X4908X-10G-TIM                 JAE15340C0J

M MAC addresses                                Hw Fw                               Sw                               Status
---+-----+-----+-----+-----+-----+-----+-----+-----+-----+
 1 0022.bde2.1061 to 0022.bde2.1080 0.2 15.0(1r)SG(0 0.DEV-0           Ok
 2 0022.bde2.1579 to 0022.bde2.1580 0.1                               In Reset

Switch#
```

hw-module module stop

The following example shows what happens if a module is already stopped and you enter the **hw-module module stop** command:

```
Switch# hw-module module 2 stop
% Module 2 stopped
```

Related Commands

Command	Description
hw-module module start	Boots a module after if it has been stopped.

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	Specifies a line module.
<i>number</i>	Specifies a module which supports TwinGig converter.
port-group <i>number</i>	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.

Command Default

10 Gigabit.

Command Modes

Global configuration mode

Command History

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

Usage Guidelines

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

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

```
Switch# config 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.
<i>number</i>	Slot or module number.

Command Default

After a boot up, the power is on.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch.
12.2(18)EW	Add slot and module keywords.

Usage Guidelines

After you enter **no hw-mod mod x power** command and OIR the linecard, the configuratio persists and is valid for any slot in the chassis it is applied to.

Examples

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

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

Related Commands

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

hw-module system max-port-num-mode 1/2



Note

This command is supported only on a 10-slot chassis.

To enable support for the WS-X4640-CSFP-E linecard in a 10-slot chassis, use the **hw-module system max-port-num-mode 2** command. To restore the default mode, use **hw-module system max-port-num-mode 1** command or use the **no** form of the commands.

[no] **hw-module system max-port-num-mode 1**

OR

[no] **hw-module system max-port-num-mode 2**

Syntax Description

hw-module system max-port-num-mode 2	Enables a chassis with 80 ports and 5 Line card slots.
hw-module system max-port-num-mode 1	Restores the default mode (48 ports and 8 Line card slots).
no hw-module system max-port-num-mode 1	Restores the default mode (48 ports and 8 Line card slots).
no hw-module system max-port-num-mode 2	Restores the default mode (48 ports and 8 Line card slots).

Command Default

Unless **max-port-num-mode** is configured to 2, system assumes **max-port-num-mode 1** as the default mode with 48 ports and 8 LC slots.

Command Modes

Global configuration mode

Command History

Release	Modification
Release IOS XE 3.5.0E and IOS 15.2(1)E	This command was introduced on the Catalyst 4500 series switch.

Examples

The following example shows how to enable support for the WS-X4640-CSFP-E linecard in a 10-slot chassis:

```
Switch# enable
Switch# config terminal
Switch(config)# hw-module system max-port-num-mode ?
 1 Select this to enable Chassis with 48 ports and 8 Line card slots
 2 Select this to enable Chassis with 80 ports and 5 Line card slots
Switch(config)# hw-module system max-port-num-mode 2
A reload of the active supervisor is required to apply the new configuration.
After reload, last 3 Line card slots will not be active
```

```
hw-module system max-port-num-mode 1/2
```

```
Switch(config)# end
```

hw-module system max-port-num-mode 1/2 switch 1/2/all



Note

This command is supported only in VSS mode on a 10-slot chassis.

To enable support for the WS-X4640-CSFP-E linecard in a 10-slot chassis which is present in VSS, use **hw-module system max-port-num-mode 2 switch 1**, **hw-module system max-port-num-mode 2 switch 2**, or **hw-module system max-port-num-mode 2 switch All** commands. (1, 2, and All (both switches) specify the switch number to which **max-port-num-mode** applies.)

To restore the default mode, use **hw-module system max-port-num-mode 1 switch 1**, **hw-module system max-port-num-mode 1 switch 2**, **hw-module system max-port-num-mode 1 switch All** or the **no** form of the commands.

[no] hw-module system max-port-num-mode 1 switch 1.

[no] hw-module system max-port-num-mode 1 switch 2,

[no] hw-module system max-port-num-mode 1 switch All

[no] hw-module system max-port-num-mode 2 switch 1

[no] hw-module system max-port-num-mode 2 switch 2,

[no] hw-module system max-port-num-mode 2 switch All

Syntax Description

hw-module system max-port-num-mode 2 switch 1	Enables a chassis with 80 ports and five linecard slots for switch 1.
hw-module system max-port-num-mode 2 switch 2	Enables a chassis with 80 ports and five linecard slots for switch 2.
hw-module system max-port-num-mode 2 switch All	Enables a chassis with 80 ports and five linecard slots for switch 1 and 2.
hw-module system max-port-num-mode 1 switch 1	Restores the default mode (48 ports and 8 Line card slots) for switch 1.
hw-module system max-port-num-mode 1 switch 2	Restores the default mode (48 ports and 8 Line card slots) for switch 2.
hw-module system max-port-num-mode 1 switch All	Restores the default mode (48 ports and 8 Line card slots) for switches 1 and 2.
no hw-module system max-port-num-mode 1 switch 1	Restores the default mode (48 ports and 8 Line card slots) for switch 1.
no hw-module system max-port-num-mode 1 switch 2	Restores the default mode(48 ports and 8 Line card slots) for switch 2.
no hw-module system max-port-num-mode 1 switch All	Restores the default mode (48 ports and 8 Line card slots) for switches 1 and 2.
no hw-module system max-port-num-mode 2 switch 1	Restores the default mode (48 ports and 8 Line card slots) for switch 1.

no hw-module system max-port-num-mode 2 switch 2	Restores the default modes(48 ports and 8 Line card slots) for the switch 2.
no hw-module system max-port-num-mode 2 switch All	Restore the default mode (48 ports and 8 Line card slots) for switches 1 and 2.

Command Default

Unless max-port-num-mode is set to 2, switch 1 assumes max-port-num-mode1 as the default mode with 48 ports and 8 linecard slots. Switch 2 behaves similarly.

Command Modes

Global configuration mode

Command History

Release	Modification
Release IOS XE 3.5.0E and IOS 15.2(1)E	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

This command can be applied for individual switches or for all the switches in VSS by specifying the switch number. The switch number option is visible on the active switch provided a 10-slot chassis is present in the VSS mode.

The switch mode conversion from stand-alone to virtual and virtual to stand-alone automatically converts **max-port-num-mode** to the default mode (mode 1), irrespective of the existing mode configuration. **max-port-num-mode** is configured separately for VSS and the stand-alone switch after a switch mode conversion and reboot. Moreover the VSL port configured in WS-X4640-CSFP-E linecard in stand-alone mode is unavailable after a switch mode conversion from stand-alone to virtual.

VSS operations cannot be performed in mode 2 where the VSL port is configured beyond the 5th linecard (7th slot).

Examples

The following example shows how to enable support for the WS-X4640-CSFP-E linecard in a 10-slot chassis:

```
Switch# config terminal
Switch(config)# hw-module system max-port-num-mode 2 switch ?
  1  Switch Number One
  2  Switch Number Two
  All Both switches
Switch(config)# hw-module system max-port-num-mode 2 switch 2
A 'redundancy reload shelf' or power-cycle of chassis is required to apply the new
configuration.
  After reload, last 3 Line card slots will not be active in Switch 2
Switch(config)# end
```

hw-module system max-queue-limit

To enable a user to change the queue limit for all interfaces globally use the **hw-module system max-queue-limit** command. To cancel the global setting, use the **no** form of the command.

hw-module system max-queue-limit *max-queue-limit*

no hw-module system max-queue-limit *max-queue-limit*

Syntax Description	<i>max-queue-limit</i>	Specifies the queue limit for all interfaces. Valid values are from 1024 to 8184. This parameter must be a multiple of 8.
---------------------------	------------------------	---

Command Default	Not enabled by default
------------------------	------------------------

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

Command History	Release	Modification
	15.0(2)SG1, and 3.2.1SG	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines	<p>This command allows you to change the queue limit for all interfaces globally rather than apply a policy with a queue limit to all the interfaces.</p> <p>This is a global configuration command. It can be overridden by the per port, per class, queue-limit command.</p> <p>For a standalone supervisor engine, you must reboot the engine after applying this command. For a redundant supervisor engine, you must enter the redundancy reload shelf command to enforce a reboot on both the supervisor engines.</p>
-------------------------	---

Examples The following example shows how to set the queue limit globally to 1024:

```
Switch> enable
Switch# configure terminal
Switch(config)# hw-module system max-queue-limit 1024
Need to reboot to take effect max queue limit
Switch(config)# exit
Switch# reload (for standalone supervisors)
Switch# redundancy reload shelf (for redundancy supervisors in SSO mode)
or
Switch# redundancy force-switchover (followed by another redundancy force-switchover, for
redundancy supervisors in RPR mode)
```

hw-module uplink mode

To change the uplink mode so that you can use the shared-backplane or the tengigabitethernet mode. To disable shared-backplane uplink mode, use the **no** form of the command.

hw-module uplink mode [**shared-backplane** | **tengigabitethernet**]

no hw-module uplink mode [**shared-backplane** | **tengigabitethernet**]

Syntax Description

shared-backplane	(Optional) Specifies the four Ten-Gigabit Ethernet uplinks as blocking ports on the Supervisor Engine 6-E and Catalyst 4900 M chassis when operating in redundant mode.
tengigabitethernet	(Optional) Specifies the two Ten-Gigabit Ethernet uplinks on Supervisor Engine 6-E with the WS-X4640-CSFP-E linecard.

Command Default

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(44)SG	Support for shared-backplane keyword was introduced on the Catalyst 4500 series switch
IOS-XE 3.3.0SG (15.1(1)SG)	Support for tengigabitethernet keyword was introduced on the Supervisor Engine 6-E.

Usage Guidelines

When changing the uplink mode using the **hw-module uplink mode shared-backplane** command, you must reload the system. A message appears on the console to reflect this.

On a Supervisor Engine 6-E in a 6 or 7-slot chassis (Catalyst 4506-E, 4507R-E, and 4507R+E), the default uplink mode does not allow a WS-X4640-CSFP-E linecard to boot in the last slot because of a hardware limitation. After you use the **hw-module uplink mode tengigabitethernet** command, you must reload the system to enable TenGig mode. The configuration is NVGEN'd after you save the running configuration to the startup configuration. You can use the **show run | incl uplink** command to check the uplink configuration before reloading the system. Furthermore, you can enter the **show hw-module uplink** command to display the uplink mode. It reports the current uplink mode, as well as the mode after the system reloads.

In uplink TenGig mode, the uplink is limited to two 10-Gigabit Ethernet interfaces in non-redundant and in redundant mode; Gigabit Ethernet interfaces are not supported. The WS-X4640-CSFP-E linecard boots in the last slot on 6 and 7-slot chassis. To return to default mode, reload the system from tengigabitethernet mode. SharedBackplane mode can be selected from Default mode, where a system reload is required as well.

The **hw-module module x port-group x select gigabitethernet** command is blocked in uplink TenGig mode, preventing you from selecting gigabitethernet mode.

Examples

The following 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)# exit
Switch#
```

The following 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)# exit
Switch#
```

The following 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 hw-module uplink	Displays hardware-module uplink information.

hw-module uplink select

To select the 10-Gigabit Ethernet, or Gigabit Ethernet uplinks on a Supervisor Engine V-10GE in a WS-C4510R chassis, or Supervisor 7L-E in a WS-C4507R chassis, use the **hw-module uplink select** command.


Note

Supervisor Engine 7L-E is not supported on a ten-slot chassis (WS-C4510R).

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

```
hw-module uplink select { tengigabitethernet | gigabitethernet } (Sup-7L-E only)
```


Note

Option **all** is not supported on Supervisor Engine 7L-E.

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).

Command Default

tengigabitethernet

Command Modes

Global configuration mode

Command History

Release	Modification
12.2(25)EW	This command was introduced on the Catalyst 4500 series switch.
12.2(25)SG	Support for the all keyword was added.
15.0(2)XO	The number of uplink ports for Supervisor Engine 7L-E in a WS-C4507R chassis depends on the supervisor engine mode (single or redundant) and the uplink mode configuration (1-Gigabit or 10-Gigabit).

Usage Guidelines

On a Supervisor Engine V-10GE (WS-X4516-10GE) in a 10-slot chassis (Catalyst 4510R and 4510R-E), if a startup 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 through the command interface 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 II+10GE, all uplink ports are always available. Similarly, when a Supervisor Engine V-10GE is plugged into a W-C4503, W-4506, or W-4507R chassis, all uplink ports are always available. When a Supervisor Engine V-10GE is plugged into a W-4510R

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 tenth slot will support only the WS-X4302-GB 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 tenth slot is either empty or has a WS-X4302-GB switching module.

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

For Supervisor Engine 7L-E in a WS-C4507R chassis, the number of uplink options depends on the supervisor engine mode (single or redundant) and the uplink mode configuration (1-Gigabit or 10-Gigabit)

Single Supervisor Mode

In single supervisor mode, Supervisor Engine 7L-E supports the uplink configuration of at most either two 10-Gigabit or four 1-Gigabit ports (Table 2-6).

Table 2-6 Uplink Options for Single Supervisor Mode

Slot 1	Slot 2	Slot 3	Slot 4	Speeds Achievable with the Following Combination of Pluggables (Band Width)
Choose 10-Gigabit operation through the command line interface.				
SFP+	SFP+	—	—	20 Gbps
SFP+	SFP	—	—	11 Gbps
SFP	SFP+	—	—	11 Gbps
SFP	SFP	—	—	2 Gbps
Choose 1-Gigabit operation through the command line interface.				
SFP	SFP	SFP	SFP	4 Gbps

Redundant Supervisor Mode

In redundant supervisor mode, Supervisor Engine 7L-E support 1+1 (in 10-Gigabit mode) and 2+2 (in 1-Gigabit mode) (Table 2-7).



Note

No redundancy support exists for slots 3 and 4.

Table 2-7 Uplink Options for Redundant Supervisor Mode

Active Supervisor Uplink Ports				Standby Supervisor Uplink Ports				Speeds Achievable with this Combination of Pluggables
A1	A2	A3	A4	B1	B2	B3	B4	
Choose 10-Gigabit operation through the command line interface.								
SFP+	—	—	—	SFP+	—	—	—	20 Gbps

Table 2-7 Uplink Options for Redundant Supervisor Mode

Active Supervisor Uplink Ports				Standby Supervisor Uplink Ports				Speeds Achievable with this Combination of Pluggables
A1	A2	A3	A4	B1	B2	B3	B4	
SFP+	—	—	—	SFP	—	—	—	11 Gbps
SFP	—	—	—	SFP+	—	—	—	11 Gbps
SFP	—	—	—	SFP	—	—	—	2 Gbps
Choose 1-Gigabit operation through the command line interface.								
SFP	SFP	—	—	SFP	SFP	—	—	4 Gbps

Examples

The following 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.

The following 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.

The following 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.

The following 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 disable slot10.
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 Drome 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		
	<i>instance-id</i>	MST instance to which the specified VLANs are mapped; valid values are from 0 to 15.
	vlan <i>vlan-range</i>	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.

Command Default Mapping is disabled.

Command Modes MST configuration mode

Command History	Release	Modification
	12.1(12c)EW	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

The following example shows how to map a range of VLANs to instance 2:

```
Switch(config-mst)# instance 2 vlans 1-100
Switch(config-mst)#
```

The following example shows how to map a VLAN to instance 5:

```
Switch(config-mst)# instance 5 vlans 1100
Switch(config-mst)#
```

The following example shows how to move a range of VLANs from instance 2 to the CIST instance:

```
Switch(config-mst)# no instance 2 vlans 40-60
Switch(config-mst)#
```

The following 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.

■ instance

interface

To select an interface to configure and to enter interface configuration mode, use the **interface** command.

interface *type number*

Syntax Description	<i>type</i>	Type of interface to be configured; see Table 2-8 for valid values.
	<i>number</i>	Module and port number.

Command Default 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 2-8](#) lists the valid values for *type*.

Table 2-8 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

The following example shows how to enter the interface configuration mode on the Fast Ethernet interface 2/4:

```
Switch(config)# interface fastethernet2/4  
Switch(config-if)#
```

Related Commands

Command	Description
show interfaces	Displays interface information.

interface (virtual switch)

To select an interface to configure and enter interface configuration mode, use the **interface** global configuration mode command.

```
interface [interface switch-num/slot/port.subinterface]
```

Syntax Description	Parameter	Description
	<i>interface</i>	Specifies the interface to be configured; see Table 2-9 for valid values.
	<i>switch-num</i>	Specifies a switch ID.
	<i>slot</i>	Specifies a slot number.
	<i>port</i>	Specifies a port number.
	<i>.subinterface</i>	Specifies the port subinterface number.

Command Default No interface types are configured.

Command Modes Global configuration mode

Command History	Release	Modification
	12.2(52)SG	Support introduced on the Catalyst 4500 Series Switch.

Usage Guidelines [Table 2-9](#) lists the valid values for *type*.

Table 2-9 Valid type Values

Keyword	Definition
fastethernet	Fast Ethernet 802.3
gigabitethernet	Gigabit Ethernet IEEE 802.3z interface.
tengigabitethernet	10-Gigabit Ethernet IEEE 802.3ae interface.
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 .
tunnel	Tunnel interface

Examples

The following example shows how to enter the interface configuration mode on the GigabitEthernet interface for switch 1, module 2, port 4:

```
Router(config)# interface gigabitethernet 1/2/4  
Router(config)#
```

Related Commands

Command	Description
show interfaces (virtual switch)	Displays the traffic that is seen by a specific interface.

set ip next-hop verify-availability

To configure policy routing to verify the reachability of the next hop of a route map before the device performs policy routing to that next hop, use the **set ip next-hop verify-availability** command in route-map configuration mode. To disable this function, use the no form of this command.

set ip next-hop verify-availability [*next-hop-address sequence track object*]

no set ip next-hop verify-availability [*next-hop-address sequence track object*]

Syntax Description

<i>next-hop address</i>	(Optional) IP address of the next hop to which packets will be forwarded.
<i>sequence</i>	(Optional) Sequence of next hops. The acceptable range is from 1 to 65535.
track	(Optional) The tracking method is track.
<i>object</i>	(Optional) Object number that the tracking subsystem is tracking. The acceptable range is from 1 to 500.

Command Default

The reachability of the next hop of a route map before the device performs policy routing, is not verified.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
Cisco IOS XE 3.8.0E and IOS 15.2(4)E	This command was introduced.

Usage Guidelines

The **set ip next-hop verify-availability** command can be used with policy-based routing (PBR) to verify next hop reachability to support object tracking using Internet Control Message Protocol (ICMP) ping to verify if a remote device is reachable.

Examples

The following example shows you how to verify the next-hop IP address in a route map:

```
Switch# enable
Switch# configure terminal
Switch(config)# track 100 ip sla 100
Switch(config)# ip sla 100
switch(config-ip-sla)# icmp-echo 172.19.255.253 source-ip 172.19.255.47
switch(config-ip-sla-echo)# timeout 1500
switch(config-ip-sla-echo)# threshold 1000
switch(config-ip-sla-echo)# frequency 2
switch(config)# ip sla schedule 100 life forever start-time now
switch(config)# route-map alpha permit 10
switch(config-route-map)# match ip address exlist
switch(config-route-map)# set ip next-hop verify-availability 95.1.1.2 1 track 100
switch# show route-map alpha
switch# show track 100
```

Related Commands

Command	Description
show route-map	Displays the configured route maps.
show track	Displays information about objects that are tracked by the tracking process.
track	Tracks the state of an interface, an ip route, or a response time reporter.

interface port-channel

To access or create a port-channel interface, use the **interface port-channel** command.

```
interface port-channel channel-group
```

Syntax Description	<i>channel-group</i> Port-channel group number; valid values are from 1 to 64.
---------------------------	--

Command Default	This command has no default settings.
------------------------	---------------------------------------

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

Command History	Release	Modification
	12.1(8a)EW	This command was introduced on the Catalyst 4500 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 want to use CDP, you must configure it only on the physical Fast Ethernet interface and not on the port-channel interface.

Examples	This example creates a port-channel interface with a channel-group number of 64:
-----------------	--

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

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

interface range

To run a command on multiple ports at the same time, use the **interface range** command.

```
interface range {vlan vlan_id - vlan_id} {port-range | macro name}
```

Syntax Description		
vlan <i>vlan_id - vlan_id</i>	Specifies a VLAN range; valid values are from 1 to 4094.	
<i>port-range</i>	Port range; for a list of valid values for <i>port-range</i> , see the “Usage Guidelines” section.	
macro <i>name</i>	Specifies the name of a macro.	

Command Default This command has no default settings.

Command Modes Global configuration mode
Interface configuration mode

Command History	Release	Modification
	12.1(8a)EW	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 VLAN SVIs only. To display the VLAN SVIs, enter the **show running config** command. The VLANs that are not displayed cannot be used in the **interface range** command.

The values that are entered with the **interface range** command are applied to all the existing VLAN SVIs.

Before you can use a macro, you must define a range using the **define interface-range** command.

All configuration changes that are made to a port range are saved to NVRAM, but the port ranges that are created with the **interface range** command do not get saved to NVRAM.

You can enter the port range in two ways:

- Specifying up to five port ranges
- Specifying a previously defined macro

You can either specify the ports or the name of a port-range macro. A port range must consist of the same port type, and the ports within a range cannot span the modules.

You can define up to five port ranges on a single command; separate each range with a comma.

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

```
interface range gigabitethernet 5/1 -20, gigabitethernet4/5 -20.
```

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*

Although the port-channel interface range is 1 to 256, in a VSS setup, there is a discrepancy in the way the range is displayed on the CLI when you enter the beginning of the interface range before you enter the ? prompt. This discrepancy is not seen on a standalone switch.

When you enter the beginning of the interface range, the CLI output is displayed as follows:

```
Switch(config)# interface range port-channel 1 -?
<1-128> end interface number
```

To continue, you have to enter the beginning of the next number range:

```
Switch(config)# interface range port-channel 129 - ?
<129-256> end interface number
```

If you do not enter the beginning of the interface range, the CLI output is displayed as follows:

```
Switch (config)# interface range port-channel ?
<1-256> Port-channel interface number
```

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

The following example shows how to use the **interface range** command to interface to FE 5/18 - 20:

```
Switch(config)# interface range fastethernet 5/18 - 20
Switch(config-if)#
```

This command shows how to run a port-range macro:

```
Switch(config)# interface range macro macro1
Switch(config-if)#
```

Related Commands

Command	Description
define interface-range	Creates a macro of interfaces.
show running config (refer to Cisco IOS documentation)	Displays the running configuration for a switch.

interface vlan

To create or access a Layer 3 switch virtual interface (SVI), use the **interface vlan** command. To delete an SVI, use the **no** form of this command.

```
interface vlan vlan_id
```

```
no interface vlan vlan_id
```

Syntax Description	<i>vlan_id</i> Number of the VLAN; valid values are from 1 to 4094.
---------------------------	---

Command Default	Fast EtherChannel is not specified.
------------------------	-------------------------------------

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

Command History	Release	Modification
	12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW	Support for extended addressing was added.

Usage Guidelines	<p>The SVIs are created the first time that you enter the interface vlan <i>vlan_id</i> command for a particular VLAN. The <i>vlan_id</i> 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.</p>
-------------------------	---

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	<p>The following example shows the output when you enter the interface vlan <i>vlan_id</i> command for a new VLAN number:</p>
-----------------	--

```
Switch(config)# interface vlan 23
% Creating new VLAN interface.
Switch(config)#
```


ip admission proxy http refresh-all

To ensure that you see a customized WebAuth login page with the same name in the switch system directory as a same-named prior login page, use the **ip admission proxy http refresh-all** command.

ip admission proxy http [success | failure | refresh-all | login [expired | page]]

Syntax Description		
success		Successful authentication proxy.
failure		Failed authentication proxy.
refresh-all		Refresh all custom html pages.
login expired		Specify expired webpage
login page		Specify customized login webpage

Command Default If you do not enter this command, if any of the customized web-based authentication page files with the file of same name have been changed, you see the old login page rather than the new file.

Command Modes Global configuration mode

Command History	Release	Modification
	15.0(2)SG	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines You should enter this command whenever the customized web-based authentication page has been changed in the system directory.

Examples The following example shows how to enter this command:

```
Switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip admission proxy http [success | failure | refresh-all | login]
Switch(config)# end
Switch#
```

<The new html page is observed.>

ip arp inspection filter vlan

To permit ARPs from hosts that are configured for static IP when DAI is enabled and to define an ARP access list and apply it to a VLAN, use the **ip arp inspection filter vlan** command. To disable this application, use the **no** form of this command.

```
ip arp inspection filter arp-acl-name vlan vlan-range [static]
```

```
no ip arp inspection filter arp-acl-name vlan vlan-range [static]
```

Syntax Description

<i>arp-acl-name</i>	Access control list name.
<i>vlan-range</i>	VLAN number or range; valid values are from 1 to 4094.
<i>static</i>	(Optional) Specifies that the access control list should be applied statically.

Command Default

No defined ARP ACLs are applied to any VLAN.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(19)EW	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 the IP-to-Ethernet MAC bindings are compared against the ACLs. All other packet types are bridged in the incoming VLAN without validation.

This command specifies that the incoming ARP packets are compared against the ARP access control list, and the packets are permitted only if the access control list permits them.

If the access control lists deny the packets because of explicit denials, the packets are dropped. If the packets are denied because of an implicit deny, they are then matched against the list of DHCP bindings if the ACL is not applied statically.

Examples

The following 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      : Enabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
```

```

Vlan      Configuration      Operation      ACL Match      Static ACL
-----
      1      Enabled      Active      static-hosts      No

Vlan      ACL Logging      DHCP Logging
-----
      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 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 <i>pps</i>	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 <i>seconds</i>	(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.

Command Default

The rate is set to 15 packets per second on the untrusted interfaces, assuming that the network is a switched network with a host connecting to as many as 15 new hosts per second.

The rate is unlimited on all the trusted interfaces.

The burst interval is set to 1 second by default.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(19)EW	This command was introduced on the Catalyst 4500 series switch.
12.1(20)EW	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 timeout feature can be used to remove the port from the error-disabled state. The rate applies to both the trusted and nontrusted interfaces. Configure appropriate rates on trunks to handle the packets across multiple DAI-enabled VLANs or use the **none** keyword to make the rate unlimited.

The rate of the incoming ARP packets on the channel ports is equal to the sum of the incoming rate of packets from all the channel members. Configure the rate limit for the channel ports only after examining the rate of the incoming ARP packets on the channel members.

After a switch receives 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

The following example shows how to limit the rate of the incoming ARP requests to 25 packets per second:

```
Switch# config terminal
Switch(config)# interface fa6/3
Switch(config-if)# ip arp inspection limit rate 25
Switch(config-if)# end
Switch# show ip arp inspection interfaces fastEthernet 6/3
Interface      Trust State      Rate (pps)
-----
Fa6/3          Trusted          25
Switch#
```

The following example shows how to limit the rate of the incoming ARP requests to 20 packets per second and to set the interface monitoring interval to 5 consecutive seconds:

```
Switch# config terminal
Switch(config)# interface fa6/1
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

To configure the parameters that are associated with the logging buffer, use the **ip arp inspection log-buffer** command. To disable the parameters, use the **no** form of this command.

```
ip arp inspection log-buffer { entries number | logs number interval seconds }
```

```
no ip arp inspection log-buffer { entries | logs }
```

Syntax Description

entries <i>number</i>	Number of entries from the logging buffer; the range is from 0 to 1024.
logs <i>number</i>	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 <i>seconds</i>	Logging rate; the range is from 0 to 86400 (1 day). A 0 value indicates an immediate log.

Command Default

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(19)EW	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

The following 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 Log Buffer Size : 45
Syslog rate : 5 entries per 1 seconds.
No entries in log buffer.
Switch#
```

The following 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 : 45
Syslog rate : 10 entries per 3 seconds.
No entries in log buffer.
Switch#
```

Related Commands

Command	Description
arp access-list	Defines an ARP access list or adds clauses at the end of a predefined list.
show ip arp inspection	Displays the status of dynamic ARP inspection for a specific range of VLANs.

ip arp inspection trust

To set a per-port configurable trust state that determines the set of interfaces where incoming ARP packets are inspected, use the **ip arp inspection trust** command. To make the interfaces untrusted, use the **no** form of this command.

ip arp inspection trust

no ip arp inspection trust

Syntax Description This command has no arguments or keywords.

Command Default This command has no default settings.

Command Modes Interface configuration mode

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

Examples The following example shows how to configure an interface to be trusted:

```
Switch# config 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 src-mac is enabled, packets with different MAC addresses are classified as invalid and are dropped.
dst-mac	(Optional) Checks the destination MAC address in the Ethernet header against the target MAC address in ARP body. This checking is done for ARP responses. Note When dst-mac is enabled, the packets with different MAC addresses are classified as invalid and are dropped.
ip	(Optional) Checks the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses. The sender IP addresses are checked in all ARP requests and responses and target IP addresses are checked only in ARP responses.

Command Default

Checks are disabled.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(19)EW	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 **no** form of this command.

ip arp inspection vlan *vlan-range*

no ip arp inspection vlan *vlan-range*

Syntax Description

vlan-range VLAN number or range; valid values are from 1 to 4094.

Command Default

ARP inspection is disabled on all VLANs.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(19)EW	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

The following 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#
```

The following 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 ACL. 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.

Command Default

All denied or dropped packets are logged.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(19)EW	This command was introduced on the Catalyst 4500 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 two options that are available to you are as follows:

- **acl-match**—Logging on ACL matches is reset to log on deny
- **dhcp-bindings**—Logging on DHCP binding compared is reset to log on deny

Examples

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

```
Switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip arp inspection vlan 1 logging acl-match matchlog
Switch(config)# end
Switch# show ip arp inspection vlan 1

Source Mac Validation      : 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       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 <i>source</i>	Specifies the source port in the load-balancing hash functions.
destination <i>dest</i>	Specifies the destination port in the load-balancing 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.

Command Default

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(12c)EW	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

The original algorithm, tunnel algorithm, and universal algorithm are routed 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

The following 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)#
```

The following example shows how to configure the IP CEF 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	<i>number</i> Specifies the number of bindings created in the IP device tracking table for a port, valid values are from 0 to 2048.
---------------------------	---

Command Default	This command has no default settings.
------------------------	---------------------------------------

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

Command History	Release	Modification
	12.2(37)SG	This command was introduced on the Catalyst 4500 series switch.

Examples The following example shows how to enable IP port security with IP-MAC filters on a Layer 2 access port:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip device tracking
Switch(config)# interface fastethernet 4/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 1
Switch(config-if)# 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.

Command Default DHCP snooping is disabled.

Command Modes Global configuration mode

Command History	Release	Modification
	12.1(12c)EW	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 The following example shows how to enable DHCP snooping:

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

The following 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

<i>mac-address</i>	Specifies a MAC address.
vlan <i>vlan-#</i>	Specifies a valid VLAN number.
<i>ip-address</i>	Specifies an IP address.
interface <i>interface</i>	Specifies an interface type and number.
expiry <i>seconds</i>	Specifies the interval (in seconds) after which binding is no longer valid.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.1(19)EW	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

The following example shows how to generate a DHCP binding configuration on interface gigabitethernet1/1 in VLAN 1 with an expiration time of 1000 seconds:

```
Switch# ip dhcp snooping binding 0001.1234.1234 vlan 1 172.20.50.5 interface gi1/1 expiry 1000
Switch#
```

Related Commands

Command	Description
ip dhcp snooping	Globally enables DHCP snooping.
ip dhcp snooping information option	Enables DHCP option 82 data insertion.
ip dhcp snooping trust	Enables DHCP snooping on a trusted VLAN.
ip dhcp snooping vlan	Enables DHCP snooping on a VLAN or a group of VLANs.

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

<i>url</i>	Specifies the URL in one of the following forms: <ul style="list-style-type: none"> • tftp://<host>/<filename> • ftp://<user>:<password>@<host>/<filename> • rcp://<user>@<host>/<filename> • nvram:/<filename> • bootflash:/<filename>
timeout <i>seconds</i>	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 <i>seconds</i>	Specifies the duration for which the transfer should be delayed after a change to the binding database.

Command Default

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	This command was introduced on the Catalyst 4500 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 on 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, an RPR/SSO standby supervisor engine can take over the binding list when a switchover occurs.

Examples

The following example shows how to store a database file with the IP address 10.1.1.1 within a directory called directory. A file named file must be present on the TFTP server.

```
Switch# config terminal
Switch(config)# ip dhcp snooping database tftp://10.1.1.1/directory/file
Switch(config)# end
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 : Yes
Delay Timer Expiry : Not Running
Abort Timer Expiry : Not Running

Last Succeeded Time : None
Last Failed Time : None
Last Failed Reason : No failure recorded.

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

ip dhcp snooping information option

To enable DHCP option 82 data insertion, use the **ip dhcp snooping information option** command. To disable DHCP option 82 data insertion, use the **no** form of this command.

ip dhcp snooping information option format remote-id {hostname | string {word}}

no ip dhcp snooping information option format remote-id {hostname | string {word}}

Syntax Description

format	Specifies the option 82 information format.
remote-id	Specifies the remote ID for option 82.
hostname	Specifies the user-configured hostname for the remote ID.
string word	Specifies the user-defined string for the remote ID. The word string can be from 1 to 63 characters long with no spaces.

Command Default

DHCP option 82 data insertion is enabled.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(12c)EW	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

The following example shows how to enable DHCP option 82 data insertion:

```
Switch(config)# ip dhcp snooping information option
Switch(config)#
```

The following example shows how to disable DHCP option 82 data insertion:

```
Switch(config)# no ip dhcp snooping information option
Switch(config)#
```

The following example shows how to configure the hostname as the remote ID:

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

The following example shows how to enable DHCP Snooping on VLAN 500 through 555 and option 82 remote ID:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip dhcp snooping
```

```

Switch(config)# ip dhcp snooping vlan 500 555
Switch(config)# ip dhcp snooping information option format remote-id string switch123
Switch(config)# interface GigabitEthernet 5/1
Switch(config-if)# ip dhcp snooping trust
Switch(config-if)# ip dhcp snooping limit rate 100
Switch(config-if)# ip dhcp snooping vlan 555 information option format-type circuit-id
string customer-555
Switch(config-if)# interface FastEthernet 2/1
Switch(config-if)# ip dhcp snooping vlan 555 information option format-type circuit-id
string customer-500
Switch(config)# end

```

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 limit rate	Configures the number of the DHCP messages that an interface can receive per second.
ip dhcp snooping trust	Enables DHCP snooping on a trusted VLAN.
ip dhcp snooping vlan	Enables DHCP snooping on a VLAN or a group of VLANs.
ip dhcp snooping vlan information option format-type circuit-id string	Enables circuit-id (a sub-option of DHCP snooping option-82) on a VLAN.
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.

ip dhcp snooping information option allow-untrusted

To allow DHCP packets with option 82 data inserted to be received from a snooping untrusted port, use the **ip dhcp snooping information option allow-untrusted** command. To disallow receipt of these DHCP packets, use the **no** form of this command.

ip dhcp snooping information option allow-untrusted

no ip dhcp snooping information option allow-untrusted

Syntax Description

This command has no arguments or keywords.

Command Default

DHCP packets with option 82 are not allowed on snooping untrusted ports.

Command Modes

Global configuration mode

Command History

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

Examples

The following 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.

Command Default

DHCP snooping rate limiting is disabled.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(12c)EW	This command was introduced on the Catalyst 4500 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 interfaces aggregate all DHCP traffic in the switch, and you will need to adjust the rate limit of the interfaces to a higher value.

Examples

The following example shows how to enable the DHCP message rate limiting:

```
Switch(config-if)# ip dhcp snooping limit rate 150
Switch(config)#
```

The following example shows how to disable the DHCP message rate limiting:

```
Switch(config-if)# no ip dhcp snooping limit rate
Switch(config)#
```

Related Commands

Command	Description
ip dhcp snooping	Globally enables DHCP snooping.
ip dhcp snooping information option	Enables DHCP option 82 data insertion.
ip dhcp snooping trust	Enables DHCP snooping on a trusted VLAN.
ip dhcp snooping vlan	Enables DHCP snooping on a VLAN or a group of VLANs.
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.

ip dhcp snooping trust

To configure an interface as trusted for DHCP snooping purposes, use the **ip dhcp snooping trust** command. To configure an interface as untrusted, use the **no** form of this command.

ip dhcp snooping trust

no ip dhcp snooping trust

Syntax Description This command has no arguments or keywords.

Command Default DHCP snooping trust is disabled.

Command Modes Interface configuration mode

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

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

```
Switch(config-if) # ip dhcp snooping trust
Switch(config) #
```

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

```
Switch(config-if) # no ip dhcp snooping trust
Switch(config) #
```

Related Commands	Command	Description
	ip dhcp snooping	Globally enables DHCP snooping.
	ip dhcp snooping information option	Enables DHCP option 82 data insertion.
	ip dhcp snooping limit rate	Configures the number of the DHCP messages that an interface can receive per second.
	ip dhcp snooping vlan	Enables DHCP snooping on a VLAN or a group of VLANs.
	show ip dhcp snooping	Displays the DHCP snooping configuration.
	show ip dhcp snooping binding	Displays the DHCP snooping binding entries.

ip dhcp snooping vlan

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

ip dhcp snooping [*vlan number*]

no 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.
---------------------------	--

Command Default	DHCP snooping is disabled.
------------------------	----------------------------

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

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

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

Examples	The following example shows how to enable DHCP snooping on a VLAN:
-----------------	--

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

The following example shows how to disable DHCP snooping on a VLAN:

```
Switch(config)# no ip dhcp snooping vlan 10
Switch(config)#
```

The following example shows how to enable DHCP snooping on a group of VLANs:

```
Switch(config)# ip dhcp snooping vlan 10 55
Switch(config)#
```

The following example shows how to disable DHCP snooping on a group of VLANs:

```
Switch(config)# no ip dhcp snooping vlan 10 55
Switch(config)#
```

Related Commands	Command	Description
	ip dhcp snooping	Globally enables DHCP snooping.
	ip dhcp snooping information option	Enables DHCP option 82 data insertion.
	ip dhcp snooping limit rate	Configures the number of the DHCP messages that an interface can receive per second.
	ip dhcp snooping trust	Enables DHCP snooping on a trusted VLAN.
	ip dhcp snooping vlan information option format-type circuit-id string	Enables circuit-id (a suboption of DHCP snooping option-82) on a VLAN.
	show ip dhcp snooping	Displays the DHCP snooping configuration.
	show ip dhcp snooping binding	Displays the DHCP snooping binding entries.

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

To enable circuit-id (a suboption of DHCP snooping option 82) on a VLAN, use the **ip dhcp snooping vlan information option format-type circuit-id string** command. To disable circuit-id on a VLAN, use the **no** form of this command.

```
ip dhcp snooping vlan number information option format-type circuit-id [override] string
string
```

```
no ip dhcp snooping vlan number information option format-type circuit-id [override] string
```

Syntax Description	
number	Specifies single or range of VLANs; valid values are from 1 to 4094.
override	(Optional) Specifies an override string.
string string	Specifies a user-defined string for the circuit ID; range of 3 to 63 ASCII characters with no spaces.

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

Command Modes Interface configuration

Command History	Release	Modification
	12.2(40)SG	This command was introduced on the Catalyst 4500 series switch.
	12.2(54)SG	Added the override option

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

This command allows you to configure a string of ASCII characters to be the circuit ID. When you want to override the vlan-mod-port format type and instead use the circuit-ID to define subscriber information, use the **override** keyword.

Examples The following example shows how to enable DHCP snooping on VLAN 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 5/1
Switch(config-if)# ip dhcp snooping trust
Switch(config-if)# ip dhcp snooping limit rate 100
```

```
Switch(config-if)# ip dhcp snooping vlan 555 information option format-type circuit-id
string customer-555
Switch(config-if)# interface FastEthernet 2/1
Switch(config-if)# ip dhcp snooping vlan 555 information option format-type circuit-id
string customer-500
Switch(config)# end
```

The following example shows how to configure the option-82 circuit-ID override suboption:

```
Switch(config-if)# ip dhcp snooping vlan 250 information option format-type circuit-id
override string testcustomer
```

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


Note

The **show ip dhcp snooping** user EXEC command only displays the global command output, including a remote-ID configuration. It does not display any per-interface, per-VLAN string that you have configured for the circuit ID.

Related Commands

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 429496795.

Command Default

Profiles are not applied.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(11b)EW	This command was introduced on the Catalyst 4500 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

The following 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	<i>number</i>	Maximum number of IGMP groups that an interface can join; valid values are from 0 to 4294967294.
---------------------------	---------------	--

Command Default	No maximum limit.
------------------------	-------------------

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

Command History	Release	Modification
	12.1(11b)EW	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	<p>The following example shows how to limit the number of IGMP groups that an interface can join to 25:</p> <pre>Switch(config)# interface gigabitethernet1/1 Switch(config-if)# ip igmp max-groups 25 Switch(config-if)</pre>
-----------------	--

ip igmp profile

To create an IGMP profile, use the **ip igmp profile** command. To delete the IGMP profile, use the **no** form of this command.

ip igmp profile *profile number*

no ip igmp profile *profile number*

Syntax Description	<i>profile number</i> IGMP profile number being configured; valid values are from 1 to 4294967295.
---------------------------	--

Command Default	No profile created.
------------------------	---------------------

Command Modes	Global configuration mode IGMP profile configuration
----------------------	---

Command History	Release	Modification
	12.1(11b)EW	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	The following example shows how to configure IGMP profile 40 that permits the specified range of IP multicast addresses:
-----------------	--

```
Switch # config terminal
Switch(config)# ip igmp profile 40
Switch(config-igmp-profile)# permit
Switch(config-igmp-profile)# range 233.1.1.1 233.255.255.255
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	<i>seconds</i>	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.
---------------------------	----------------	---

Command Default	The query interval is set to 60 seconds.
------------------------	--

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

Command History	Release	Modification
	12.1(8a)EW	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 **ip igmp query-timeout** command), the switch becomes the querier.



Note

Changing the timeout period may severely impact multicast forwarding.

Examples The following 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 querier-timeout (refer to Cisco IOS documentation)	Configures the timeout 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 configurations.
flood	(Optional) Specifies to flood the spanning tree table to the network when a topology change occurs.
query	(Optional) Specifies the TCN query configurations.
count <i>count</i>	(Optional) Specifies how often the spanning tree table is flooded; valid values are from 1 to 10.
solicit	(Optional) Specifies an IGMP general query.

Command Default

IGMP snooping is enabled.

Command Modes

Global configuration mode
Interface configuration mode

Command History

Release	Modification
12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch.
12.1(11)EW	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

The following example shows how to enable IGMP snooping:

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

The following example shows how to disable IGMP snooping:

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

The following example shows how to enable the flooding of the spanning tree table to the network after nine topology changes have occurred:

```
Switch(config)# ip igmp snooping tcn flood query count 9
Switch(config)#
```

The following 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)#
```

The following example shows how to enable an IGMP general query:

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

The following 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 the **no** form of this command.

ip igmp snooping report-suppression

no igmp snooping report-suppression

Syntax Description This command has no arguments or keywords.

Command Default IGMP snooping report-suppression is enabled.

Command Modes Global configuration mode

Command History	Release	Modification
	12.1(12c)EW	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 The following example shows how to enable report suppression:

```
Switch(config)# ip igmp snooping report-suppression
Switch(config)#
```

The following example shows how to disable report suppression:

```
Switch(config)# no ip igmp snooping report-suppression
Switch(config)#
```

The following example shows how to display the system status for report suppression:

```
Switch# show ip igmp snoop
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	<i>vlan-id</i> Number of the VLAN; valid values are from 1 to 1001 and from 1006 to 4094.
---------------------------	---

Command Default	IGMP snooping is disabled.
------------------------	----------------------------

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

Command History	Release	Modification
	12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch.
12.1(12c)EW	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	The following example shows how to enable IGMP snooping on a VLAN:
-----------------	--

```
Switch(config)# ip igmp snooping vlan 200  
Switch(config)#
```

The following example shows how to disable IGMP snooping on a VLAN:

```
Switch(config)# no ip igmp snooping vlan 200  
Switch(config)#
```

Related Commands	Command	Description
	ip igmp snooping vlan immediate-leave	Enable IGMP immediate-leave processing.
	ip igmp snooping vlan mrouter	Configures a Layer 2 interface as a multicast router interface for a VLAN.
	ip igmp snooping vlan static	Configures a Layer 2 interface as a member of a group.

ip igmp snooping vlan explicit-tracking

To enable per-VLAN explicit host tracking, use the **ip igmp snooping vlan explicit-tracking** command. To disable explicit host tracking, use the **no** form of this command.

ip igmp snooping vlan *vlan-id* explicit-tracking

no ip igmp snooping vlan *vlan-id* explicit-tracking

Syntax Description	<i>vlan_id</i> (Optional) Specifies a VLAN; valid values are from 1 to 1001 and from 1006 to 4094.
---------------------------	--

Command Default	Explicit host tracking is enabled.
------------------------	------------------------------------

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

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

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

```
Switch(config)# no ip igmp snooping vlan 200 explicit-tracking
Switch(config)# end
Switch# show ip igmp snooping vlan 200 | include explicit tracking
Global IGMP Snooping configuration:
-----
IGMP snooping           : Enabled
IGMPv3 snooping        : Enabled
Report suppression     : Enabled
TCN solicit query      : Disabled
TCN flood query count   : 2

Vlan 2:
-----
IGMP snooping           : Enabled
IGMPv2 immediate leave : Disabled
Explicit host tracking   : Disabled
Multicast router learning mode : pim-dvmrp
CGMP interoperability mode : IGMP_ONLY
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 multicast 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

<i>vlan_num</i>	Number of the VLAN; valid values are from 1 to 4094.
immediate-leave	Enables immediate leave processing.

Command Default

Immediate leave processing is disabled.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(8a)EW	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

The following example shows how to enable IGMP immediate-leave processing on VLAN 4:

```
Switch(config)# ip igmp snooping vlan 4 immediate-leave
Switch(config)#
```

The following 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
<code>show ip igmp interface</code>	Displays the information about the IGMP-interface status and configuration.
<code>show mac-address-table multicast</code>	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 <i>vlan-id</i>	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 switch.
fastethernet <i>slot/port</i>	Specifies the Fast Ethernet interface; number of the slot and port.
gigabitethernet <i>slot/port</i>	Specifies the Gigabit Ethernet interface; number of the slot and port.
tengigabitethernet <i>slot/port</i>	Specifies the 10-Gigabit Ethernet interface; number of the slot and port.
port-channel <i>number</i>	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.

Command Default

Multicast switch snooping PIM-DVMRP packets are specified.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(8a)EW	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

The following 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) #
```

The following 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		
<i>vlan_num</i>		Number of the VLAN.
<i>mac-address</i>		Group MAC address.
interface		Specifies the next-hop interface to multicast switch.
fastethernet <i>slot/port</i>		Specifies the Fast Ethernet interface; number of the slot and port.
gigabitethernet <i>slot/port</i>		Specifies the Gigabit Ethernet interface; number of the slot and port.
tengigabitethernet <i>slot/port</i>		Specifies the 10-Gigabit Ethernet interface; number of the slot and port.
port-channel <i>number</i>		Port-channel number; valid values are from 1 through 64.

Command Default This command has no default settings.

Command Modes Global configuration mode

Command History	Release	Modification
	12.1(8a)EW	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.

Examples The following example shows how to configure a host statically on an interface:

```
Switch(config)# ip igmp snooping vlan 4 static 0100.5e02.0203 interface fastethernet 5/11
Configuring port FastEthernet5/11 on group 0100.5e02.0203 vlan 4
Switch(config)#
```

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

Command	Description
<code>ip igmp snooping vlan mrouter</code>	Configures a Layer 2 interface as a multicast router interface for a VLAN.
<code>show mac-address-table multicast</code>	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.

Command Default Local proxy ARP is disabled.

Command Modes Interface configuration mode

Command History	Release	Modification
	12.1(8a)EW	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 The following example shows how to enable the local proxy ARP feature:

```
Switch(config-if) # ip local-proxy-arp
Switch(config-if) #
```

ip mfib fastdrop

To enable MFIB fast drop, use the **ip mfib fastdrop** command. To disable MFIB fast drop, use the **no** form of this command.

ip mfib fastdrop

no ip mfib fastdrop

Syntax Description This command has no arguments or keywords.

Command Default MFIB fast drop is enabled.

Command Modes Privileged EXEC mode

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

Examples The following example shows how to enable MFIB fast drops:

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

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 [s-g-hash {basic | next-hop-based}]
```

```
no ip multicast [vrf vrf-name] multipath [s-g-hash {basic | next-hop-based}]
```

Syntax Description

vrf <i>vrf-name</i>	(Optional) Enables ECMP multicast load splitting for IP multicast traffic associated with the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRP) instance specified for the <i>vrf-name</i> argument.
s-g-hash basic next-hop-based	(Optional) Enables ECMP multicast load splitting based on source and group address or on source, group, and next-hop address. The basic keyword enables a simple hash based on source and group address. This algorithm is referred to as the basic S-G-hash algorithm. The next-hop-based keyword enables a more complex hash based on source, group, and next-hop address. This algorithm is referred to as the next-hop-based S-G-hash algorithm.

Command Default

If multiple equal-cost paths exist, multicast traffic will not be load-split across those paths.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(53)SG	The s-g-hash keyword was introduced on the Catalyst 4500 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 more than one neighbor has the same metric.

When you configure load splitting with the **ip multicast multipath** command, the system splits multicast traffic across multiple equal-cost paths based on source address using the S-hash algorithm. When the **ip multicast multipath** command is configured and multiple equal-cost paths exist, the path in which

multicast traffic will travel is selected based on the source IP address. Multicast traffic from different sources will be load-split across the different equal-cost paths. Load splitting will not occur across equal-cost paths for multicast traffic from the same source sent to different multicast groups.

**Note**

The **ip multicast multipath** command load splits the traffic but does not load balance the traffic. Traffic from a source will use only one path, even if the traffic greatly exceeds traffic from other sources.

If the **ip multicast multipath** command is configured with the **s-g-hash** keyword and multiple equal-cost paths exist, load splitting will occur across equal-cost paths based on source and group address or on source, group, and next-hop address. If you specify the optional **s-g-hash** keyword for load splitting IP multicast traffic, you must select the algorithm used to calculate the equal-cost paths by specifying one of the following keywords:

- **basic**—The basic S-G-hash algorithm is predictable because no randomization is used in calculating the hash value. The basic S-G-hash algorithm, however, is subject to polarization because for a given source and group the same hash is always chosen irrespective of the router that the hash is being calculated on.
- **next-hop-based**—The next-hop-based S-G-hash algorithm is predictable because no randomization is used to determine the hash value. Unlike the S-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 name-server

To configure the IP address of the domain name server (DNS), use the **ip name-server** command. To delete the name server use the **no** form of this command.

ip name-server *server-address1* [*server-address2...server-address6*]

no name-server *server-address1* [*server-address2...server-address6*]

Syntax Description

server-address1 IPv4 or IPv6 addresses of a name server to use for name and address resolution.
 [*server-address2...ip-address6*] (Optional) IP addresses of additional name servers (a maximum of six name servers)

Command Default

No name server addresses are specified.

Command Modes

Global configuration mode

Command History

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

Usage Guidelines

Separate each server address with a space. The first server specified is the primary server. The switch sends DNS queries to the primary server first. If that query fails, the backup servers are queried.

For the Application Visibility Control (AVC) with Domain Name System as an Authoritative Source (DNS-AS) feature (AVC with DNS-AS), ensure that at least the first two IP addresses in the sequence are IPv4 addresses, because the AVC with DNS-AS feature will use only these. See the example below, here the first two addresses are IPv4 (192.0.2.1 and 192.0.2.2), the third one (2001:DB8::1) is an IPv6 address. AVC with DNS-AS will use the first two:

```
Switch(config)# ip name-server 192.0.2.1 192.0.2.2 2001:DB8::1
```

Enter the **show ip name-server** command to display all the name server IP addresses that have been maintained.

Examples

The following example shows how to specify IPv4 hosts 172.16.1.111 and 172.16.1.2 as the name servers:

```
Switch(config)# ip name-server 192.0.2.1 192.0.2.2
```

The following example shows how to specify IPv6 hosts 3FFE:C00::250:8BFF:FEE8:F800 and 2001:0DB8::3 as the name servers:

```
Switch(config)# ip name-server 3FFE:C00::250:8BFF:FEE8:F800 2001:0DB8::3
```

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.
---------------------------	---

Command Default	NetFlow statistics is disabled. Inferred information is excluded.
------------------------	--

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

Command History	Release	Modification
	12.1(13)EW	This command was introduced on the Catalyst 4500 series switches.
	12.1(19)EW	Command enhanced to support infer fields.

Usage Guidelines	<p>To use these commands, you need to install the Supervisor Engine IV and the NetFlow Service Card.</p> <p>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.</p>
-------------------------	--

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 fields 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

The following example shows how to enable NetFlow switching on the switch:

```
Switch# config terminal
Switch(config)# ip route-cache flow
Switch(config)# exit
Switch#
```

**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

<i>ip-address</i>	Binding IP address.
<i>mac-address</i>	Binding MAC address.
vlan <i>vlan-id</i>	VLAN number.
interface <i>interface-name</i>	Binding interface.

Command Default

This command has no default settings.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(19)EW	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

The following example shows how to configure the static IP source binding:

```
Switch# conf t
Switch(config)# ip source binding 11.0.0.1 0000.000A.000B vlan 10 interface
fastethernet6/10
Switch(config)#
```

Related Commands

Command	Description
show ip source binding	Displays IP source bindings that are configured on the system.

ip sticky-arp

To enable sticky ARP, use the **ip sticky-arp** command. Use the **no** form of this command to disable sticky ARP.

ip sticky-arp

no ip sticky-arp

Syntax Description This command has no arguments or keywords.

Command Default Enabled

Command Modes Global configuration mode

Command History	Release	Modification
	12.1(12c)EW	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 **reboot** and **restart** commands.

Examples The following example shows how to enable sticky ARP:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config) ip sticky-arp
Switch(config)# end
Switch#
```

The following example shows how to disable sticky ARP:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config) no ip sticky-arp
Switch(config)# end
Switch#
```

Related Commands	Command	Description
	arp (refer to Cisco IOS documentation)	Enables Address Resolution Protocol (ARP) entries for static routing over the Switched Multimegabit Data Service (SMDS) network.
	show arp (refer to Cisco IOS documentation)	Displays ARP information.

ip verify header vlan all

To enable IP header validation for Layer 2-switched IPv4 packets, use the **ip verify header vlan all** command. To disable the IP header validation, use the **no** form of this command.

ip verify header vlan all

no ip verify header vlan all

Syntax Description This command has no default settings.

Command Default The IP header is validated for bridged and routed IPv4 packets.

Command Modes Global configuration mode

Command History	Release	Modification
	12.1(20)EW	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 IPv4 access lists also are not applied to the IP headers.

Examples The following 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 learning on a port.
port-security	(Optional) Filters both source IP and MAC addresses using the port security feature.

Command Default IP source guard is disabled.

Command Modes Global configuration mode

Command History	Release	Modification
	12.1(19)EW	This command was introduced on the Catalyst 4500 series switch.
	12.2(37)SG	Added support for IP port security and tracking.

Examples The following 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 fastethernet6/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk native vlan 10
Switch(config-if)# switchport trunk allowed vlan 11-20
Switch(config-if)# no ip dhcp snooping trust
Switch(config-if)# ip verify source vlan dhcp-snooping
Switch(config)# end
Switch# show ip verify source interface f6/1
Interface  Filter-type  Filter-mode  IP-address  Mac-address  Vlan
-----  -
Fa6/1     ip-mac      active      10.0.0.1   10
Fa6/1     ip-mac      active      deny-all   11-20
Switch#
```

The following example shows how to enable IP port security with IP-MAC filters on a Layer 2 access port:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip device tracking
Switch(config)# interface fastEthernet 4/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 1
Switch(config-if)# 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 delete a static IP source binding entry.
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.
show ip source binding	Displays IP source bindings that are configured on the system.
show ip verify source	Displays the IP source guard configuration and filters on a particular interface.

ip verify unicast source reachable-via

To enable and configure unicast RPF checks on a IPv4 interface, use the **ip verify unicast source reachable-via** command. To disable unicast RPF, use the **no** form of this command.

ip verify unicast source reachable-via rx allow-default

no ip verify unicast source reachable-via

Syntax Description	rx	Verifies that the source address is reachable on the interface where the packet was received.
	allow-default	Verifies that the default route matches the source address.

Command Default Disabled

Command Modes Interface configuration mode

Command History	Release	Modification
	12.2(40)SG	Support introduced on Catalyst 4900M chassis and a Catalyst 4500 with a Supervisor Engine 6-E.

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

Unicast RPF is an input function and is applied only on the input interface of a router at the upstream end of a connection.

Do not use unicast RPF on internal network interfaces. Internal interfaces might have routing asymmetry, which means that there are multiple routes to the source of a packet. Apply unicast RPF only where there is natural or configured symmetry.

Examples The following example shows how to enable unicast RPF exist-only checking mode:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip verify unicast source reachable-via rx allow-default
Switch(config-if)# end
Switch#
```

Related Commands	Command	Description
	ip cef (refer to Cisco IOS documentation)	Enables Cisco Express Forwarding (CEF) on the switch.
	show running-config	Displays the current running configuration for a switch.

ip wccp

To enable support of the specified Web Cache Communication Protocol (WCCP) service for participation in a service group, use the **ip wccp** command in global configuration mode. To disable the service group, use the **no** form of this command.

```
ip wccp { web-cache | service-number } [accelerated] [group-address multicast-address]
[redirect-list access-list] [group-list access-list] [password [0 | 7] password]
```

```
no ip wccp { web-cache | service-number } [accelerated] [group-address multicast-address]
[redirect-list access-list] [group-list access-list] [password [0 | 7] password]
```

Syntax Description

web-cache	Specifies the web-cache service. Note Web cache counts as one service. The maximum number of services, including those assigned with the <i>service-number</i> argument, are 8.
<i>service-number</i>	Dynamic service identifier, which means the service definition is dictated by the cache. The dynamic service number can be from 0 to 254. The maximum number of services is 8, which includes the web-cache service specified with the web-cache keyword. Note If Cisco cache engines are being used in your service group, the reverse-proxy service is indicated by a value of 99.
accelerated	(Optional) This option applies only to hardware-accelerated routers. This keyword configures the service group to prevent a connection being formed with a cache engine unless the cache engine is configured in a way that allows redirection on the router to benefit from hardware acceleration.
group-address <i>multicast-address</i>	(Optional) Multicast IP address that communicates with the WCCP service group. The multicast address is used by the router to determine which cache engine should receive redirected messages.
redirect-list <i>access-list</i>	(Optional) Access list that controls traffic redirected to this service group. The <i>access-list</i> argument should consist of a string of no more than 64 characters (name or number) that specifies the access list.
group-list <i>access-list</i>	(Optional) Access list that determines which cache engines are allowed to participate in the service group. The <i>access-list</i> argument specifies either the number or the name of a standard or extended access list.
password [0 7] <i>password</i>	(Optional) Message digest algorithm 5 (MD5) authentication for messages received from the service group. Messages that are not accepted by the authentication are discarded. The encryption type can be 0 or 7, with 0 specifying not yet encrypted and 7 for proprietary. The <i>password</i> argument can be up to eight characters in length.

Command Default

WCCP services are not enabled on the router.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(31)SG	Support introduced on the Catalyst 4500 series switch.
15.0(2)SG/3.2(0)SG	Supported extended to Supervisor Engine 6-E, Supervisor Engine 6L-E, Catalyst 4900M, and Catalyst 4948E, and Catalyst 4948E-F.
15.0(2)SG1	Support for redirect-list keyword.
IOS XE 3.3.0 SG (15.1(1)SG)	Supported extended to Supervisor Engine 7-E and Supervisor Engine 7L-E.

Usage Guidelines

This command instructs a router to enable or disable the support for the specified service number or the web-cache service name. A service number can be from 0 to 254. Once the service number or name is enabled, the router can participate in the establishment of a service group.

When the **no ip wccp** command is entered, the router terminates participation in the service group, deallocates space if none of the interfaces still has the service configured, and terminates the WCCP task if no other services are configured.

The keywords following the **web-cache** keyword and the *service-number* argument are optional and may be specified in any order, but only may be specified once. The following sections outline the specific usage of each of the optional forms of this command.

ip wccp { **web-cache** | *service-number* } **group-address** *multicast-address*

A WCCP group address can be configured to set up a multicast address that cooperating routers and web caches can use to exchange WCCP protocol messages. If such an address is used, IP multicast routing must be enabled so that the messages that use the configured group (multicast) addresses are received correctly.

This option instructs the router to use the specified multicast IP address to coalesce the “I See You” responses for the “Here I Am” messages that it has received on this group address. The response is sent to the group address as well. The default is for no group address to be configured, in which case all “Here I Am” messages are responded to with a unicast reply.

ip wccp { **web-cache** | *service-number* } **redirect-list** *access-list*

This option instructs the router to use an access list to control the traffic that is redirected to the web caches of the service group specified by the service name given. The *access-list* argument specifies either the number or the name of a standard or extended access list. The access list itself specifies which traffic is permitted to be redirected. The default is for no redirect list to be configured (all traffic is redirected).

WCCP requires that the following protocol and ports not be filtered by any access lists:

- User Datagram Protocol (UDP) (protocol type 17) port 2048. This port is used for control signaling. Blocking this type of traffic will prevent WCCP from establishing a connection between the router and cache engines.

ip wccp { **web-cache** | *service-number* } **group-list** *access-list*

This option instructs the router to use an access list to control the cache engines that are allowed to participate in the specified service group. The *access-list* argument specifies either the number of a standard or extended access list or the name of any type of named access list. The access list itself specifies which cache engines are permitted to participate in the service group. The default is for no group list to be configured, in which case all cache engines may participate in the service group.

**Note**

The **ip wccp {web-cache | service-number} group-list** command syntax resembles the **ip wccp {web-cache | service-number} group-listen** command, but these are entirely different commands. The **ip wccp group-listen** command is an interface configuration command used to configure an interface to listen for multicast notifications from a cache cluster. Refer to the description of the **ip wccp group-listen** command in the *Cisco IOS IP Application Services Command Reference*.

ip wccp {web-cache | service-number} password password

This option instructs the router to use MD5 authentication on the messages received from the service group specified by the service name given. Use this form of the command to set the password on the router. You must also configure the same password separately on each web cache. The password can be up to a maximum of eight characters. Messages that do not authenticate when authentication is enabled on the router are discarded. The default is for no authentication password to be configured and for authentication to be disabled.

Examples

The following example shows how to configure a router to run WCCP reverse-proxy service, using the multicast address of 239.0.0.0:

```
Router(config)# ip multicast-routing
Router(config)# ip wccp 99 group-address 239.0.0.0
Router(config)# interface gigabitethernet 3/1
Router(config-if)# ip wccp 99 group-listen
```

The following example shows how to configure a router to redirect web-related packets without a destination of 10.168.196.51 to the web cache:

```
Router(config)# access-list 100 deny ip any host 10.168.196.51
Router(config)# access-list 100 permit ip any any
Router(config)# ip wccp web-cache redirect-list 100
Router(config)# interface gigabitethernet 3/2
Router(config-if)# ip wccp web-cache redirect out
```

Related Commands

Command	Description
ip wccp check services all	Enables all WCCP services.
ip wccp version	Specifies which version of WCCP you wish to use on your router.
show ip wccp	Displays global statistics related to WCCP.

ipv6 wccp

To enable support of the specified Web Cache Communication Protocol (WCCP) service for participation in a service group, use the **ipv6 wccp** command in global configuration mode. To disable the service group, use the **no** form of this command.

```
ipv6 wccp vrf vrf-name [group-address groupaddress] [redirect-list access-list] [group-list access-list]
```

Syntax Description

vrf <i>vrf name</i>	(Optional) Specifies a virtual routing and forwarding (VRF) instance to associate with a service group.
group-address <i>groupaddress</i>	(Optional) IP address that communicates with the WCCP service group. The multicast address is used by the device to determine which cache engine should receive redirected messages.
redirect-list <i>access-list</i>	(Optional) Access list that controls traffic redirected to this service group. The <i>access-list</i> argument should consist of a string of no more than 64 characters (name or number) that specifies the access list.
group-list <i>access-list</i>	(Optional) Access list that determines which cache engines are allowed to participate in the service group. The <i>access-list</i> argument specifies either the number or the name of a standard or extended access list.

Command Default

WCCP services are not enabled on the router.

Command Modes

Global configuration (config)

Command History

Release	Modification
IOS XE 3.8.0E and 15.2(4)E	This command was introduced.

Usage Guidelines

This command instructs a device to enable or disable the support for the specified service number or the VRF. A service number can be from 0 to 254. Once the service number or name is enabled, the router can participate in the establishment of a service group.

When the **no ipv6 wccp** command is entered, the device terminates participation in the service group, deallocates space if none of the interfaces still has the service configured, and terminates the WCCP task if no other services are configured.

The following sections outline the specific usage of each of the optional forms of this command.

```
ipv6 wccp vrf vrf name group-address groupaddress
```

The **vrf** *vrf-name* keyword and argument pair is optional. It allows you to specify a VRF to associate with a service group. You can then specify a web-cache service name or service number.

A WCCP group address can be configured to set up a multicast address that cooperating devices can use to exchange WCCP protocol messages. If such an address is used, IP multicast routing must be enabled so that the messages that use the configured group (multicast) addresses are received correctly.

This option instructs the device to use the specified multicast IP address to coalesce the “I See You” responses for the “Here I Am” messages that it has received on this group address. The response is sent to the group address as well. The default is for no group address to be configured, in which case all “Here I Am” messages are responded to with a unicast reply.

ipv6 wccp vrf *vrf name* **redirect-list** *access-list*

This option instructs the device to use an access list to control the traffic that is redirected to the service group specified by the service name given. The *access-list* argument specifies either the number or the name of a standard or extended access list. The access list itself specifies which traffic is permitted to be redirected. The default is for no redirect list to be configured (all traffic is redirected).

WCCP requires that the following protocol and ports not be filtered by any access lists:

- User Datagram Protocol (UDP) (protocol type 17) port 2048. This port is used for control signaling. Blocking this type of traffic will prevent WCCP from establishing a connection between the router and cache engines.

ipv6 wccp vrf *vrf name* **group-list** *access-list*

This option instructs the router to use an access list to control the cache engines that are allowed to participate in the specified service group. The *access-list* argument specifies either the number of a standard or extended access list or the name of any type of named access list. The access list itself specifies which cache engines are permitted to participate in the service group. The default is for no group list to be configured, in which case all cache engines may participate in the service group.

Examples

The following example shows how to configure the TCP promiscuous service for IPv4 VRF interfaces, where VLAN 40 represents the server interface and VLAN 50 represents the content engine interface:

```
Switch# configure terminal
Switch(config)# ipv6 wccp vrf abc 91
Switch(config)# ipv6 wccp vrf abc 92
Switch(config)# interface vlan 30
Switch(config-if)# vrf forwarding abc s
Switch(config-if)# ipv6 wccp vrf abc 91 redirect in
Switch(config)# interface vlan 40
Switch(config-if)# vrf forwarding abc
Switch(config-if)# ipv6 wccp vrf abc 92 redirect in
Switch(config)# interface vlan 50
Switch(config-if)# vrf forwarding abc
```

Related Commands

Command	Description
show ipv6 wccp	Displays global statistics related to WCCP.

ip wccp check services all

To enable all Web Cache Communication Protocol (WCCP) services, use the **ip wccp check services all** command in global configuration mode. To disable all services, use the **no** form of this command.

ip wccp check services all

no ip wccp check services all

Syntax Description This command has no arguments or keywords.

Command Default WCCP services are not enabled on the router.

Command Modes Global configuration (config)

Command History	Release	Modification
	12.2(31)SG	Support introduced on the Catalyst 4500 series switch.
	IOS XE 3.2(0)SG (15.0(2)SG)	Support extended to Supervisor Engine 6-E, Supervisor Engine 6L-E, Catalyst 4900M, Catalyst 4948E, and Catalyst 4948E-F.
	IOS XE 3.3.0 SG (15.1(1)SG)	Supported extended to Supervisor Engine 7-E and Supervisor Engine 7L-E.

Usage Guidelines With the **ip wccp check services all** command, WCCP can be configured to check all configured services for a match and perform redirection for those services if appropriate. The caches to which packets are redirected can be controlled by a redirect ACL access control list (ACL) as well as by the priority value of the service.

It is possible to configure an interface with more than one WCCP service. When more than one WCCP service is configured on an interface, the precedence of a service depends on the relative priority of the service compared to the priority of the other configured services. Each WCCP service has a priority value as part of its definition.

If no WCCP services are configured with a redirect ACL, the services are considered in priority order until a service is found which matches the IP packet. If no services match the packet, the packet is not redirected. If a service matches the packet and the service has a redirect ACL configured, then the IP packet will be checked against the ACL. If the packet is rejected by the ACL, the packet will not be passed down to lower priority services unless the **ip wccp check services all** command is configured. When the **ip wccp check services all** command is configured, WCCP will continue to attempt to match the packet against any remaining lower priority services configured on the interface.



Note

The priority of a WCCP service group is determined by the web cache appliance. The priority of a WCCP service group cannot be configured via Cisco IOS software.

**Note**

The **ip wccp check services all** command is a global WCCP command that applies to all services and is not associated with a single service.

Examples

The following example shows how to configure all WCCP services:

```
Router(config)# ip wccp check services all
```

Related Commands

Command	Description
ip wccp	Enables support of the specified WCCP service for participation in a service group.
ip wccp group-listen	Configures an interface on a router to enable or disable the reception of IP multicast packets for Web Cache Communication Protocol (WCCP).
ip wccp redirect	Enables packet redirection on an inbound or outbound interface using Web Cache Communication Protocol (WCCP).
ip wccp redirect exclude in	Configure an interface to exclude packets received on an interface from being checked for redirection.
ip wccp version	Specifies which version of WCCP you wish to use on your router.

ip wccp group-listen

To configure an interface on a router to enable or disable the reception of IP multicast packets for Web Cache Communication Protocol (WCCP), use the **ip wccp group-listen** command in interface configuration mode. To disable the reception of IP multicast packets for WCCP, use the **no** form of this command.

ip wccp {web-cache | service-number} group-listen

no ip wccp {web-cache | service-number} group-listen

Syntax Description

web-cache	The web cache service.
<i>service-number</i>	WCCP service number; valid values are from 0 to 254.

Command Default

This command is disabled by default.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(31)SG	Support introduced on the Catalyst 4500 series switch.
IOS XE 3.2(0)SG (15.0(2)SG)	Support extended to Supervisor Engine 6-E, Supervisor Engine 6L-E, Catalyst 4900M, Catalyst 4948E, and Catalyst 4948E-F.
IOS XE 3.3.0 SG (15.1(1)SG)	Supported extended to Supervisor Engine 7-E and Supervisor Engine 7L-E.

Usage Guidelines

On routers that are to be members of a Service Group when IP multicast is used, the following configuration is required:

- Configure the IP multicast address for use by the WCCP Service Group.
- Configure the interfaces on which the router wishes to receive the IP multicast address with the **ip wccp {web-cache | service-number} group-listen** interface configuration command.

Examples

The following example shows how to enable the multicast packets for a web cache with a multicast address of 224.1.1.100:

```
Switch# configure terminal
Switch(config)# ip wccp web-cache group-address 224.1.1.100
Switch(config)# interface gigabitethernet 3/1
Switch(config-if)# ip wccp web-cache group-listen
```


Related Commands	Command	Description
	ip wccp	Enables support of the WCCP service for participation in a service group.
	ip wccp check services all	Enables all Web Cache Communication Protocol (WCCP) services.
	ip wccp redirect	Enables WCCP redirection on an interface.
	ip wccp redirect	Enables packet redirection on an inbound or outbound interface using Web Cache Communication Protocol (WCCP).
	ip wccp redirect exclude in	Configures an interface to exclude packets received on an interface from being checked for redirection.
	ip wccp version	Specifies which version of WCCP you wish to use on your router.

ip wccp redirect

To enable packet redirection on an inbound or outbound interface using Web Cache Communication Protocol (WCCP), use the **ip wccp redirect** command in interface configuration mode. To disable WCCP redirection, use the **no** form of this command.

```
ip wccp {web-cache | service-number} redirect {in | out}
```

```
no ip wccp {web-cache | service-number} redirect {in | out}
```

Syntax Description

web-cache	Enables the web cache service.
<i>service-number</i>	Identification number of the cache engine service group; valid values are from 0 to 254. If Cisco cache engines are used in the cache cluster, the reverse proxy service is indicated by a value of 99.
in	Specifies packet redirection on an inbound interface.
out	Specifies packet redirection on an outbound interface.

Command Default

Redirection checking on the interface is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(31)SG	Support introduced on the Catalyst 4500 series switch.
IOS XE 3.2(0)SG (15.0(2)SG)	Support extended to Supervisor Engine 6-E, Supervisor Engine 6L-E, Catalyst 4900M, Catalyst 4948E, and Catalyst 4948E-F.
15.0(2)SG1	web-cache and service-number keywords supports on Supervisor Engine 6-E, Supervisor Engine 6L-E, Catalyst 4900M, Catalyst 4948E, and Catalyst 4948E-F.
IOS XE 3.3.0 SG (15.1(1)SG)	Supported extended to Supervisor Engine 7-E and Supervisor Engine 7L-E.

Usage Guidelines

The **ip wccp {web-cache | service-number} redirect in** command allows you to configure WCCP redirection on an interface receiving inbound network traffic. When the command is applied to an interface, all packets arriving at that interface will be compared against the criteria defined by the specified WCCP service. If the packets match the criteria, they will be redirected.

Likewise, the **ip wccp {web-cache | service-number} redirect out** command allows you to configure the WCCP redirection check at an outbound interface.



Tips

Be careful not to confuse the **ip wccp {web-cache | service-number} redirect {out | in}** interface configuration command with the **ip wccp redirect exclude in** interface configuration command.

Examples

The following example shows how to configure a session in which reverse proxy packets on Ethernet interface 3/1 are being checked for redirection and redirected to a Cisco Cache Engine:

```
Switch(config)# ip wccp 99
Switch(config)# interface gigabitethernet 3/1
Switch(config-if)# ip wccp 99 redirect out
```

The following example shows how to configure a session in which HTTP traffic arriving on GigabitEthernet interface 3/1 is redirected to a Cache Engine:

```
Switch(config)# ip wccp web-cache
Switch(config)# interface gigabitethernet 3/1
Switch(config-if)# ip wccp web-cache redirect in
```

Related Commands

Command	Description
ip wccp check services all	Configures an interface on a router to enable or disable the reception of IP multicast packets for Web Cache Communication Protocol (WCCP).
ip wccp group-listen	Configures an interface on a router to enable or disable the reception of IP multicast packets for Web Cache Communication Protocol (WCCP).
ip wccp redirect exclude in	Enables redirection exclusion on an interface.
show ip interface	Displays the usability status of interfaces that are configured for IP.
show ip wccp	Displays the WCCP global configuration and statistics.

p wccp redirect exclude in

To configure an interface to exclude packets received on an interface from being checked for redirection, use the **ip wccp redirect exclude in** command in interface configuration mode. To disable the ability of a router to exclude packets from redirection checks, use the **no** form of this command.

ip wccp redirect exclude in

no ip wccp redirect exclude in

Syntax Description This command has no arguments or keywords.

Command Default Redirection exclusion is disabled.

Command Modes Interface configuration (config-if)

Command History

Release	Modification
12.2(31)SG	Support introduced on the Catalyst 4500 series switch.
IOS XE 3.2(0)SG (15.0(2)SG)	Support extended to Supervisor Engine 6-E, Supervisor Engine 6L-E, Catalyst 4900M, Catalyst 4948E, and Catalyst 4948E-F.
IOS XE 3.3.0 SG (15.1(1)SG)	Supported extended to Supervisor Engine 7-E and Supervisor Engine 7L-E.

Usage Guidelines

This configuration command instructs the interface to exclude inbound packets from any redirection check. Note that the command is global to all the services and should be applied to any inbound interface that will be excluded from redirection.

This command is intended to be used to accelerate the flow of packets from a cache engine to the Internet as well as allow for the use of the Web Cache Communication Protocol (WCCP) v2 packet return feature.

Examples

In the following example, packets arriving on GigabitEthernet interface 3/1 are excluded from WCCP output redirection checks:

```
Router (config)# interface gigabitethernet 3/1
Router (config-if)# ip wccp redirect exclude in
```

Related Commands

Command	Description
ip wccp	Enables support of the WCCP service for participation in a service group.
ip wccp redirect	Enable packet redirection on an inbound or outbound interface using Web Cache Communication Protocol (WCCP).
ip wccp redirect out	Configures redirection on an interface in the outgoing direction.

Command	Description
<code>ip wccp check services all</code>	Configures an interface on a router to enable or disable the reception of IP multicast packets for Web Cache Communication Protocol (WCCP).
<code>ip wccp group-listen</code>	Configures an interface on a router to enable or disable the reception of IP multicast packets for Web Cache Communication Protocol (WCCP).
<code>ip wccp redirect exclude in</code>	Enables redirection exclusion on an interface.
<code>show ip interface</code>	Displays the usability status of interfaces that are configured for IP.
<code>show ip wccp</code>	Displays the WCCP global configuration and statistics.

ipv6 dhcp-lrda

To enable Lightweight DHCPv6 Relay Agent (LDRA) functionality on an access node, use the **ipv6 dhcp-lrda** command in global configuration mode. To disable the LDRA functionality, use the **no** form of this command.

```
ipv6 dhcp-lrda {enable | disable | remote-id remote-id}
```

```
no ipv6 dhcp-lrda {enable | disable | remote-id remote-id}
```

Syntax Description

enable	Enables LDRA functionality on an access node.
disable	Disables LDRA functionality on an access node.
remote-id <i>remote-id</i>	Configures the DHCPV6 LDRA remote ID globally.

Command Default

If the remote ID is not configured, a system generated remote ID is used.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS Release 15.2(5)E2	This command was introduced on the Catalyst 4500 series switches.

Usage Guidelines

You must configure the LDRA functionality globally using the **ipv6 dhcp-lrda** command before configuring it on a VLAN or an access node (such as a Digital Subscriber Link Access Multiplexer [DSLAM] or an Ethernet switch) interface.

To enable LDRA, configure the **ipv6 dhcp-lrda** command. To disable LDRA, configure either the **no ipv6 dhcp-lrda enable** or the **ipv6 dhcp-lrda disable** command. Configuring the **no ipv6 dhcp-lrda** command will not disable LDRA globally, and as a result, there is no carriage return after the **no ipv6 dhcp-lrda** command.

Examples

The following example shows how to enable the LDRA functionality:

```
Device> enable
Device# configure terminal
Device(config)# ipv6 dhcp-lrda enable
Device(config)# exit
```

Related Commands

Command	Description
ipv6 dhcp relay destination	Specifies a destination address to which client messages are forwarded and to enable DHCPv6 relay service on the interface.

ipv6 dhcp-ldra interface-id

To configure Lightweight DHCPv6 Relay Agent (LDRA) interface ID on a port or an interface, use the **ipv6 dhcp-ldra interface-id** command in interface configuration mode. To disable LDRA interface ID on an interface or port, use the **no** form of this command.

ipv6 dhcp-ldra interface-id *interface-id*

no dhcp-ldra interface-id *interface-id*

Syntax Description

<i>interface-id</i>	Interface identifier. Valid length for this argument is from 2 to 23 characters.
---------------------	--

Command Default

If the interface ID is not configured, the system uses a short name for an interface (for example, the system uses eth0/0 for Ethernet 0/0) as the interface ID.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS Release 15.2(5)E2	This command was introduced on the Catalyst 4500 series switches.

Examples

The following example shows how to configure an LDRA interface ID:

```
Device> enable
Device# configure terminal
Device(config)# ipv6 dhcp-ldra enable
Device(config)# interface gigabitethernet 0/0
Device(config-if)# switchport
Device(config-if)# ipv6 dhcp-ldra interface-id 20
Device(config-if)# exit
```

Related Commands

Command	Description
ipv6 dhcp-ldra	Enables LDRA functionality on an access node.
ipv6 dhcp ldra attach-policy (VLAN)	Specifies a VLAN number and enters VLAN configuration mode.

ipv6 dhcp-ldra attach-policy

To enable Lightweight DHCPv6 Relay Agent (LDRA) functionality on a port or interface, use the **ipv6 dhcp-ldra attach-policy** command in interface configuration mode. To disable LDRA functionality on an interface or port, use the **no** form of this command.

```
ipv6 dhcp-ldra attach-policy { client-facing-trusted | client-facing-untrusted |
client-facing-disable | server-facing }
```

```
no ipv6 dhcp-ldra attach-policy { client-facing-trusted | client-facing-untrusted |
client-facing-disable | server-facing }
```

Syntax Description

client-facing-trusted	Specifies client-facing interfaces or ports as trusted.
client-facing-untrusted	Specifies client-facing interfaces or ports as untrusted.
client-facing-disable	Disables LDRA functionality on an interface or port.
server-facing	Specifies an interface or port as server facing.

Command Default

LDRA functionality is not enabled on an interface or port.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS Release 15.2(5)E2	This command was introduced on the Catalyst 4500 series switches.

Usage Guidelines

You need to configure the LDRA functionality globally using the **ipv6 dhcp-ldra** command in global configuration mode before configuring it on an interface or port.

The **ipv6 dhcp-ldra attach-policy** command enables LDRA functionality on a specific interface or port. Instead of configuring LDRA individually on all the client-facing interfaces or ports individually, use the **ipv6 dhcp-ldra attach-policy** command to configure LDRA on an entire VLAN.

Examples

The following example shows how to enable LDRA functionality on an interface and specify it as server facing:

```
Device> enable
Device# configure terminal
Device(config)# ipv6 dhcp-ldra enable
Device(config)# interface gigabitethernet 0/0
Device(config-if)# switchport
Device(config-if)# ipv6 dhcp-ldra attach-policy server-facing
Device(config-if)# exit
```


Related Commands	Command	Description
	ipv6 dhcp-ldra	Enables LDRA functionality on an access node.
	ipv6 dhcp ldra attach-policy (VLAN)	Enables LDRA functionality on a VLAN.

ipv6 dhcp ldra attach-policy (VLAN)

To enable Lightweight DHCPv6 Relay Agent (LDRA) functionality on a VLAN, use the **ipv6 dhcp ldra attach-policy** command in VLAN configuration mode. To disable LDRA functionality on a VLAN, use the **no** form of this command.

```
ipv6 dhcp ldra attach-policy { client-facing-trusted | client-facing-untrusted }
```

```
no ipv6 dhcp ldra attach-policy { client-facing-trusted | client-facing-untrusted }
```

Syntax Description

client-facing-trusted	Specifies client-facing interfaces or ports as trusted.
client-facing-untrusted	Specifies client-facing interfaces or ports as untrusted.

Command Default

The LDRA functionality is not enabled on a VLAN.

Command Modes

VLAN configuration (config-vlan-config)

Command History

Release	Modification
Cisco IOS Release 15.2(5)E2	This command was introduced on the Catalyst 4500 series switches in a release prior to Cisco IOS Release 15.2(5)E2.

Usage Guidelines

You need to configure the LDRA functionality globally using the **ipv6 dhcp-ldra** command before configuring it on a VLAN.

In a typical deployment, a majority of the interfaces or ports on a device are client facing. Instead of configuring LDRA individually on all the client facing interfaces and ports, use the **ipv6 dhcp ldra attach-policy** command to configure LDRA on the entire VLAN. As a result, all the ports or interfaces associated with the VLAN will be configured as client facing.

Examples

The following example shows how to enable LDRA functionality on a VLAN:

```
Device> enable
Device# configure terminal
Device(config)# ipv6 dhcp-ldra enable
Device(config)# vlan configuration 5
Device(config-vlan-config)# ipv6 dhcp ldra attach-policy client-facing-trusted
Device(config-vlan-config)# exit
```

Related Commands	Command	Description
	ipv6 dhcp-lrdra	Enables LDRA functionality on an access node.
	vlan configuration	Enables SNMP MAC address notifications.

ipv6 dhcp relay destination

To specify a destination address to which client messages are forwarded and to enable Dynamic Host Configuration Protocol Version 6 (DHCPv6) relay service on the interface, use the **ipv6 dhcp relay destination** command in interface configuration mode. To remove a relay destination on the interface or to delete an output interface for a destination, use the **no** form of this command.

ipv6 dhcp relay destination { *ipv6-address* | **global** *ipv6-address* | **vrf** *vrfname* *ipv6-address* }
 [*interface-type* *interface-number*] [**link-address** *link-address*] [**source-address**
source-address]

no ipv6 dhcp relay destination { *ipv6-address* | **global** *ipv6-address* | **vrf** *vrfname* *ipv6-address* }
 [*interface-type* *interface-number*] [**link-address** *link-address*] [**source-address**
source-address]

Syntax Description		
	<i>ipv6-address</i>	Relay destination address. There are two types of relay destination address: <ul style="list-style-type: none"> • Link-scoped unicast or multicast IPv6 address. User must specify an output interface for this kind of address. • Global or site-scoped unicast or multicast IPv6 address.
	global	Specifies the relay destination when the relay destination is in the global address space and when the relay source is in a virtual routing and forwarding (VRF) instance.
	vrf <i>vrfname</i>	Specifies the VRF instance associated with the relay destination IPv6 address.
	<i>interface-type</i> <i>interface-number</i>	(Optional) Interface type and number that specifies the output interface for a destination. If this argument is configured, client messages are forwarded to the destination address through the link to which the output interface is connected.
	link-address <i>link-address</i>	(Optional) Specifies the DHCPv6 link address. The link-address must be an IPv6 globally scoped address configured on the network interface where the DHCPv6 relay is operational.
	source-address <i>source-address</i>	(Optional) Specifies the network interface source address. The source-address can be any IPv6 global-scoped address on a device.

Command Default The relay function is disabled, and there is no relay destination on an interface.

Command Modes Interface configuration (config-if)

Command History	Release	Modification
	Cisco IOS Release 15.2(5)E2	This command was introduced on the Catalyst 4500 series switches in a release prior to Cisco IOS Release 152(5)E2.

Usage Guidelines

The **ipv6 dhcp relay destination** command specifies a destination address to which client messages are forwarded, and it enables DHCPv6 relay service on the interface. When relay service is enabled on an interface, a DHCPv6 message received on that interface is forwarded to all configured relay destinations. The incoming DHCPv6 message may have come from a client on that interface, or relayed by another relay agent.

The relay destination can be a unicast address of a server or another relay agent, or it may be a multicast address. There are two types of relay destination addresses:

- A link-scoped unicast or multicast IPv6 address, for which a user must specify an output interface
- A global or site-scoped unicast or multicast IPv6 address. A user can optionally specify an output interface for this kind of address.

If no output interface is configured for a destination, the output interface is determined by routing tables. In this case, it is recommended that a unicast or multicast routing protocol be running on the device.

Multiple destinations can be configured on one interface, and multiple output interfaces can be configured for one destination. When the relay agent relays messages to a multicast address, it sets the hop limit field in the IPv6 packet header to 32.

Unspecified, loopback, and node-local multicast addresses are not acceptable as the relay destination. If any one of them is configured, the message "Invalid destination address" is displayed.

Note that it is not necessary to enable the relay function on an interface for it to accept and forward an incoming relay reply message from servers. By default, the relay function is disabled, and there is no relay destination on an interface. The no form of the command removes a relay destination on an interface or deletes an output interface for a destination. If all relay destinations are removed, the relay service is disabled on the interface.

The DHCPv6 client, server, and relay functions are mutually exclusive on an interface. When one of these functions is already enabled, and a user tries to configure a different function on the same interface, one of the following messages is displayed: "Interface is in DHCP client mode," "Interface is in DHCP server mode," or "Interface is in DHCP relay mode."

Examples

The following example sets the relay destination address on Ethernet interface 4/3:

```
Device# configure terminal
Device(config)# interface gigabitethernet 0/0
Device(config-if)# ipv6 dhcp relay destination FE80::250:A2FF:FEBF:A056
gigabitethernet 4/3
```

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
ipv6 dhcp-ldra	Enables LDRA functionality on an access node.

ipv6 mld snooping

To enable IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping globally or on the specified VLAN, use the **ipv6 mld snooping** command without keywords. To disable MLD snooping on a switch or the VLAN, use the **no** form of this command.

ipv6 mld snooping [vlan *vlan-id*]

no ipv6 mld snooping [vlan *vlan-id*]

Syntax Description

vlan <i>vlan-id</i>	(Optional) Enables or disables IPv6 MLD snooping on the specified VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094.
----------------------------	--

Command Default

MLD snooping is globally disabled on the switch.

MLD snooping is enabled on all VLANs. However, MLD snooping must be globally enabled before VLAN snooping can take place.

Command Modes

Global configuration mode

Command History

Release	Modification
12.2(40)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

The following example shows how to globally enable MLD snooping:

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

The following 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 reset 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 <i>vlan-id</i>	(Optional) Configures last-listener query count on the specified VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094.
	<i>integer_value</i>	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 to hosts belonging to the multicast group. If a host wants to leave a multicast group, it can silently leave or it can respond to the query with a Multicast Listener Done message (equivalent to an IGMP Leave message). When Immediate Leave is not configured (it should not be configured if multiple clients for a group exist on 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

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

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ipv6 mld snooping last-listener-query-count 1
Switch(config)# end
Switch#
```

The following 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	Configures IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping last-listener query interval on the switch or on a VLAN.
show ipv6 mld snooping	Displays IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping configuration of the switch or the VLAN.
show ipv6 mld snooping querier	Displays IP version 6 (IPv6) MLD snooping querier-related information most recently received by the switch or the VLAN.

ipv6 mld snooping 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 <i>vlan-id</i>	(Optional) Configures last-listener query interval on the specified VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094.
<i>integer_value</i>	Sets the time period (in thousandths of a second) that a multicast switch 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(40)SG	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

The following example shows how to globally set the last-listener query interval to 2 seconds:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ipv6 mld snooping last-listener-query-interval 2000
Switch(config)# end
Switch#
```

The following 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#
```

You can verify your settings by entering the **show ipv6 MLD snooping [vlan *vlan-id*]** user EXEC command.

Related Commands

Command	Description
ipv6 mld snooping last-listener-query-count	Configures IP version 6 (IPv6) Multicast Listener Discovery Multicast Address Specific Queries (MASQs) that will be sent before aging out a client.
show ipv6 mld snooping querier	Displays IP version 6 (IPv6) MLD snooping querier-related information most recently received by the switch or the VLAN.

ipv6 mld snooping listener-message-suppression

To enable IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping listener message suppression, use the **ipv6 mld snooping listener-message-suppression** command. To disable MLD snooping listener message suppression, use the **no** form of this command.

ipv6 mld snooping listener-message-suppression

no ipv6 mld snooping listener-message-suppression

Command Default

The default is for MLD snooping listener message suppression to be disabled.

Command Modes

Global configuration mode

Command History

Release	Modification
12.2(40)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 switches only once in every report-forward time. This prevents the forwarding of duplicate reports.

Examples

The following 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#
```

The following 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 <i>vlan-id</i>	(Optional) Configures the robustness variable on the specified VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094.
<i>integer_value</i>	The robustness value ranges 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(40)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

The following 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# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ipv6 mld snooping robustness-variable 3
Switch(config)# end
Switch#
```

The following example shows how to configure the robustness variable for VLAN 1. This value overrides the global configuration for the VLAN:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
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*]** user EXEC command.

Related Commands

Command	Description
ipv6 mld snooping last-listener-query-count	Configures IP version 6 (IPv6) Multicast Listener Discovery Multicast Address Specific Queries (MASQs) that will be sent before aging out a client.
show ipv6 mld snooping	Displays IP version 6 (IPv6) MLD snooping configuration of the switch or the VLAN.

ipv6 mld snooping tcn

To configure IP version 6 (IPv6) Multicast Listener Discovery (MLD) Topology Change Notifications (TCNs), use the **ipv6 mld snooping tcn** commands. To reset 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 <i>integer_value</i>	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)SG	This command was introduced on the Catalyst 4500.

Examples

The following 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#
```

The following 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
ip-address interface interface-id]
```

Syntax Description		
vlan <i>vlan-id</i>		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 <i>ipv6-multicast-address</i>		(Optional) Configures a multicast group with the specified IPv6 multicast address.
interface <i>interface-id</i>		Adds a Layer 2 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(40)SG	This command was introduced on the Catalyst 4500.

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

The following example shows how to enable MLD Immediate-Leave processing on VLAN 1:

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

The following example shows how to disable MLD Immediate-Leave processing on VLAN 1:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# no ipv6 mld snooping vlan 1 immediate-leave
Switch(config)# end
Switch#
```

The following example shows how to configure a port as a multicast switch port:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ipv6 mld snooping vlan 1 mrouter interface GigabitEthernet1/1
Switch(config)# end
Switch#
```

The following example shows how to configure a static multicast group:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ipv6 mld snooping vlan 2 static FF12::34 interface GigabitEthernet1/1
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.

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		
<i>active-slot</i>		Specifies the slot number for the current standby supervisor engine.
<i>active-image-new</i>		(Optional) Name of the new image present in the current standby supervisor engine.

Command Default There are no default settings

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.2(31)SGA	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 load version (LV) 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 The following example shows how you can reset and reload the standby supervisor engine:

```
Switch# issu abortversion 2
Switch#
```

Related Commands	Command	Description
	issu acceptversion	Halts the rollback timer and ensures that the new Cisco IOS software image is not automatically stopped during the ISSU process.
	issu commitversion	Loads the new Cisco IOS software image into the new standby supervisor engine.
	issu loadversion	Starts the ISSU process.

Command	Description
issu runversion	Forces a change from the active supervisor engine to the standby supervisor engine and causes the newly active supervisor engine to run the new image specified.
show issu state	Displays the ISSU state and current booted image name during the ISSU process.

issu acceptversion

To halt the rollback timer and to ensure that the new Cisco IOS software image is not automatically stopped during the ISSU process, use the **issu acceptversion** command.

issu acceptversion *active-slot* [*active-image-new*]

Syntax Description		
	<i>active-slot</i>	Specifies the slot number for the currently active supervisor engine.
	<i>active-image-new</i>	(Optional) Name of the new image on the currently active supervisor engine.

Command Default Rollback timer resets automatically 45 minutes after you enter the **issu runversion** command.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.2(31)SGA	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 ISSU process is automatically rolled back to the previous version of the software. The rollback timer starts immediately after you enter the **issu runversion** command.

If the rollback timer expires before the standby supervisor engine goes to a hot standby state, the timer is automatically extended by up to 15 minutes. If the standby state goes to a hot-standby state within this extension time or the 15 minute extension expires, the switch aborts the ISSU process. A warning message that requires your intervention is displayed every 1 minute of the timer extension.

If the rollback timer is set to a long period of time, such as the default of 45 minutes, and the standby supervisor engine goes into the hot standby state in 7 minutes, you have 38 minutes (45 minus 7) to roll back if necessary.

Use the **issu set rollback-timer** to configure the rollback timer.

Examples The following example shows how to halt the rollback timer and allow the ISSU process to continue:

```
Switch# issu acceptversion 2
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 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		
	<i>standby-slot</i>	Specifies the slot number for the currently active supervisor engine.
	<i>standby-image-new</i>	(Optional) Name of the new image on the currently active supervisor engine.

Command Default	
	Enabled by default.

Command Modes	
	Privileged EXEC mode

Command History	Release	Modification
	12.2(31)SGA	This command was introduced on the Catalyst 4500 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 run version (RV) state. If these conditions are met, the following actions take place:

- The standby supervisor engine is reset and booted with the new version of Cisco IOS software.
- The standby supervisor engine moves into the Stateful Switchover (SSO) mode and is fully stateful for all clients and applications with which the standby supervisor engine is compatible.
- The supervisor engines are moved into final state, which is the same as initial state.

Entering the **issu commitversion** command completes the In Service Software Upgrade (ISSU) process. This process cannot be stopped or reverted to its original state without starting a new ISSU process.

Entering the **issu commitversion** command without entering the **issu acceptversion** command is equivalent to entering both the **issu acceptversion** and the **issu commitversion** commands. Use the **issu commitversion** command if you do not intend to run in the current state for an extended period of time and are satisfied with the new software version.

Examples	
	The following 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
	issu acceptversion	Halts the rollback timer and ensures that the new Cisco IOS software image is not automatically stopped during the ISSU process.
	issu commitversion	Loads the new Cisco IOS software image into the new standby supervisor engine.
	issu loadversion	Starts the ISSU process.
	issu runversion	Forces a change from the active supervisor engine to the standby supervisor engine and causes the newly active supervisor engine to run the new image specified.
	show issu state	Displays the ISSU state and current booted image name during the ISSU process.

issu 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		
	<i>active-slot</i>	Specifies the slot number for the currently active supervisor engine.
	<i>active-image-new</i>	Specifies the name of the new image on the currently active supervisor engine.
	<i>standby-slot</i>	Specifies the standby slot on the networking device.
	<i>standby-image-new</i>	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.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.2(31)SGA	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 The following example shows how to initiate the ISSU process:

```
Switch# issu loadversion 1 bootflash:new-image 2 slavebootflash:new-image
Switch#
```

Related Commands	Command	Description
	issu abortversion	Cancels the ISSU upgrade or the downgrade process in progress and restores the switch to its state before the start of the process.
	issu acceptversion	Halts the rollback timer and ensures that the new Cisco IOS software image is not automatically stopped during the ISSU process.

Command	Description
issu commitversion	Loads the new Cisco IOS software image into the new standby supervisor engine.
issu runversion	Forces a change from the active supervisor engine to the standby supervisor engine and causes the newly active supervisor engine to run the new image specified.
show issu state	Displays the ISSU state and current booted image name during the ISSU process.

issu runversion

To force a change from the active supervisor engine to the standby supervisor engine and to cause the newly active supervisor engine to run the new image specified in the **issu loadversion** command, use the **issu runversion** command.

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

Syntax Description

<i>standby-slot</i>	Specifies the standby slot on the networking device.
<i>standby-image-new</i>	(Optional) Specifies the name of the new image on the standby supervisor engine.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.2(31)SGA	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

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

The following example shows how to force a change of the active-supervisor engine to standby-supervisor engine:

```
Switch# issu runversion 2
Switch#
```

Related Commands

Command	Description
issu abortversion	Cancels the ISSU upgrade or the downgrade process in progress and restores the switch 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 loadversion	Starts the ISSU process.
show issu state	Displays the ISSU state and current booted image name during the ISSU process.

issu set rollback-timer

To configure the In Service Software Upgrade (ISSU) rollback timer value, use the `issu set rollback-timer` command.

`issu set rollback-timer seconds`

Syntax Description	<code>seconds</code>	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.
---------------------------	----------------------	--

Command Default Rollback timer value is 2700 seconds.

Command Modes Global configuration mode

Command History	Release	Modification
	12.2(31)SGA	This command was introduced on the Catalyst 4500 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 init state.

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

```
Switch# configure terminal
Switch(config)# issu set rollback-timer 3600
Switch(config)# end
Switch#
```

Related Commands	Command	Description
	issu acceptversion	Halts the rollback timer and ensures that the new Cisco IOS software image is not automatically stopped during the ISSU process.
	issu set rollback-timer	Configures the In Service Software Upgrade (ISSU) rollback timer value.

key chain macsec

To create or modify a macsec keychain, and enter keychain-macsec configuration mode, use the **key chain** *key-chain-name* **macsec** command

To disable this feature, use the **no** form of this command.

key chain *key-chain-name* **macsec**

no key chain

Syntax Description	<i>key-chain-name</i> Specifies the name of the keychain. The maximum length is 32.								
Command Default	None.								
Command Modes	Global configuration mode								
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>3.9.0E</td> <td>This command was introduced on the Cisco Catalyst 4500-E and 4500-X series switches.</td> </tr> </tbody> </table>	Release	Modification	3.9.0E	This command was introduced on the Cisco Catalyst 4500-E and 4500-X series switches.				
Release	Modification								
3.9.0E	This command was introduced on the Cisco Catalyst 4500-E and 4500-X series switches.								
Examples	<p>The following example shows how to enable protocol tunneling for the CDP packets:</p> <pre>Switch(config terminal)# key chain mac_chain macsec Switch(config-keychain-macsec)#</pre>								
Related Commands	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Command	Description						
Command	Description								

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.

Command Default

The default is that no Layer 2 protocol packets are tunneled.

Command Modes

Interface configuration mode

Command History

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

Usage Guidelines

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

Layer 2 protocol tunneling across a service-provider network ensures that Layer 2 information is propagated across the network to all customer locations. When protocol tunneling is enabled, protocol packets are encapsulated with a well-known Cisco multicast address for transmission across the network. When the packets reach their destination, the well-known MAC address is replaced by the Layer 2 protocol MAC address.

You can enable Layer 2 protocol tunneling for CDP, STP, and VTP individually or for all three protocols.

Examples

The following example shows how to enable protocol tunneling for the CDP packets:

```
Switch(config-if)# l2protocol-tunnel cdp
Switch(config-if)#
```

Related Commands

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

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	<i>value</i> Specifies the CoS priority value for tunneled Layer 2 protocol packets. The range is 0 to 7, with 7 being the highest priority.
---------------------------	--

Command Default	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
	12.2(18)EW	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	The following 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.
<i>value</i>	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.

Command Default

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	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

The following 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
<code>l2protocol-tunnel</code>	Enables protocol tunneling on an interface.
<code>l2protocol-tunnel cos</code>	Configures the class of service (CoS) value for all tunneled Layer 2 protocol packets.
<code>l2protocol-tunnel shutdown-threshold</code>	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.
	<i>value</i>	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.

Command Default 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(18)EW	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines The **l2-protocol-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 option is specified with the keyword, the threshold is applied to each of the tunneled Layer 2 protocol types. If you also set a drop threshold 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 l2ptguard** command, the interface 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 **l2ptguard**, the interface stays in the error-disabled state until you enter the **shutdown** and **no shutdown** commands.

Examples The following example shows how to configure the maximum rate:

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

Related Commands	Command	Description
	l2protocol-tunnel	Enables protocol tunneling on an interface.
	l2protocol-tunnel cos	Configures the class of service (CoS) value for all tunneled Layer 2 protocol packets.
	l2protocol-tunnel 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-channel min-links

To define the minimum number of LACP ports that must be bundled in the link-up state and bundled in the EtherChannel in order that a port channel becomes active, use the `port-channel min-links` command in interface configuration mode. To return to the default setting, use the `no` form of this command.

port-channel min-links min_links_number

Syntax Description	
	<i>min_links_number</i> The minimum number of active LACP ports in the port channel. The range is 2 to 8. The default is 1.

Command Default	
	None.

Command Modes	
	Interface configuration mode

Command History	Release	Modification
	IOS XE 3.8.0E and IOS 15.2(4)E	This command was introduced.

Usage Guidelines	
	For switches in VSS mode, when configuring min-links, ensure that the port-channel has the same number of links on the active switch and the standby switch.

Examples	
	The following example shows how to specify a minimum of three active LACP ports before port channel 2 becomes active:

```
Switch(config)# interface port-channel 2
Switch(config-if)# port-channel min-links 3
```

Related Commands	Command	Description
	show lacp	Displays LACP information.

lacp port-priority

To set the LACP priority for the physical interfaces, use the **lacp port-priority** command.

lacp port-priority *priority*

Syntax Description	<i>priority</i> Priority for the physical interfaces; valid values are from 1 to 65535.
---------------------------	---

Command Default	Priority is set to 32768.
------------------------	---------------------------

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

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

Usage Guidelines

You must assign each port in the switch a port priority that can be specified automatically or by entering the **lacp port-priority** command. The port priority is used with the port number to form the port identifier. The port priority is used to decide which ports should be put in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.

Although this command is a global configuration command, the *priority* value is supported only on port channels with LACP-enabled physical interfaces. This command is supported on LACP-enabled interfaces.

When setting the priority, the higher numbers indicate lower priorities.

Examples

The following example shows how to set the priority for the interface:

```
Switch(config-if) # lacp port-priority 23748
Switch(config-if) #
```

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 rate

To set the rate at which Link Aggregation Control Protocol (LACP) control packets are received by an LACP-supported interface, use the **lacp rate** command in interface configuration mode. To return to the default settings, use the no form of this command.

lacp rate {normal | fast}

no lacp rate

Syntax Description	normal	fast
	Specifies that LACP control packets are received at the normal rate (every 30 seconds).	Specifies that LACP control packets are received at the fast rate (once every 1 second).

Command Default 30 seconds

Command Modes Interface configuration mode

Command History	Release	Modification
	IOS XE 3.7.1E and IOS 15.2(3)E1	This command was introduced.

Usage Guidelines Using the **lacp rate** command, you can set the LACP rate to a default of 30 seconds or to the fast rate of 1 second. This command is supported only on LACP-enabled interfaces.

Examples The following example shows how to set the lacp rate for an interface:

```
Switch(config)# interface gigabitEthernet 2/1
Switch(config-if)# lacp rate fast
```

Related Commands	Command	Description
	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	<i>priority</i> Priority of the system; valid values are from 1 to 65535.
---------------------------	---

Command Default	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 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 The following example shows how to set the system priority:

```
Switch(config)# lACP system-priority 23748
Switch(config)#
```

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.

license right-to-use activate


Note

This command applies only to Catalyst 4500X, as well as Supervisor Engine 7-E, 7L-E, and 8-E.

To activate PRTU licenses use the **license right-to-use activate** command.

license right-to-use activate *feature-name* [**acceptEula**]

Syntax Description

<i>feature-name</i>	Specifies the feature name (e.g., entservices, ipbase, lanbase)
acceptEula	(Optional). Activates the PRTU license. The End User License Agreement is accepted but does not display.

Command Default

PRTU licenses are inactive

Command Modes

privileged EXEC mode

Command History

Release	Modification
IOS XE 3.4.2SG	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

Use this command to activate PRTU licenses that are *inactive*.

Downloading the license file from cisco portal and installing the license are not required. The PRTU licenses are bundled with image. Because the PRTU license is of highest precedence, when the PRTU license is activated, other license of the same feature switch to inactive state.

Examples

The following example shows how to activate PRTU licenses:

```
Switch# license right-to-use activate entservices
```

Related Commands

Command	Description
license right-to-use deactivate	Deactivates the PRTU license

license right-to-use deactivate



Note

This command applies only to Catalyst 4500X, as well as Supervisor Engine 7-E, 7L-E, and 8-E.

To deactivate the PRTU license use the **license right-to-use deactivate** command.

license right-to-use deactivate *feature-name*

Syntax Description

feature-name Specifies the feature name (e.g., entservices, ipbase, lanbase)

Command Default

PRTU licenses are inactive

Command Modes

privileged EXEC mode

Command History

Release	Modification
IOS XE 3.4.2SG	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

Use this command to deactivate the PRTU licenses that are *active*.

The PRTU licenses can be deactivated provided any other valid license is available for the same feature.

For example, to deactivate a entservices PRTU license, the switch should contain a valid evaluation license. Else, the deactivation will fail.

Examples

The following example shows how to deactivate PRTU licenses:

```
Switch# license right-to-use deactivate entservices
```

Related Commands

Command	Description
<code>license right-to-use activate</code>	Activates the PRTU license

link state group

To configure the link state group, use the **link state group** command in interface configuration mode.

link state group [*number*] {**upstream** | **downstream**}

Syntax Description	<i>number</i>	Specifies a link-state group. Valid values are from 1 to 20; the default value is 1.
	upstream	Configures the interface as an upstream interface in the group.
	downstream	Configures the interface as a downstream interface in the group.

Command Default The group number is 1

Command Modes Interface configuration

Command History	Release	Modification
	15.1(1)S	This command was introduced.
	3.8.0E and 15.2.(4)E	The upper limit of the group number values was increased from 10 to 20.

Usage Guidelines You can configure a maximum of 20 link state groups per switch.
To disable a link-state group, use the **no link state track** *number* global configuration command.

Examples The following example shows how to configure the link state groups.

```
Switch# configure terminal
Switch(config)# link state track 1
Switch(config)# interface gigabitethernet3/1
Switch(config-if)# link state group 1 upstream
Switch(config-if)# interface gigabitethernet3/3
Switch(config-if)# link state group 1 upstream
Switch(config-if)# interface gigabitethernet3/5
Switch(config-if)# link state group 1 downstream
Switch(config-if)# interface gigabitethernet3/7
Switch(config-if)# link state group 1 downstream
```

Related Commands	Command	Description
	link state track	Configures the link state group and enables link state tracking.
	show link state group	Displays the link state group information.

link state track

To configure the link state group and enable link state tracking, use the **link state track** command in interface configuration mode.

link state track *[number]*

no link state track *[number]*

Syntax Description	<i>number</i>	Specifies a link-state group and enables link state tracking. Valid values are from 1 to 20; the default value is 1.
--------------------	---------------	--

Command Default	The link state track number is 1
-----------------	----------------------------------

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

Command History	Release	Modification
	15.1(1)S	This command was introduced.
	3.8.0E and 15.2.(4)E	The upper limit of the group number values was increased from 10 to 20.

Usage Guidelines	When you configure LST for the first time, add upstream interfaces to the link state group before adding the downstream interface, otherwise the downstream interfaces move into the error-disable mode. To restore the default link-state track, use the no link state track <i>number</i> global configuration command.
------------------	---

Examples	The following example shows how to configure the link state tracking number.
----------	--

```
Switch# configure terminal
Switch(config)# link state track 1
```

Related Commands	Command	Description
	link state group	Configures the link state group and the interface as either an upstream or downstream interface in the group.
	show link state group	Displays the link state group information.

lldp tlv-select power-management

To enable power negotiation through LLDP, use the **lldp tlv-select power-management** interface command.

lldp tlv-select power-management

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

Command Default	Enabled on POEP ports
------------------------	-----------------------

Command Modes	Interface level
----------------------	-----------------

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

Usage Guidelines	<p>You need to disable this feature if you do not want to perform power negotiation through LLDP.</p> <p>This feature is not supported on non-POEP ports; the CLI is suppressed on such ports and TLV is not exchanged.</p>
-------------------------	---

Examples	<p>The following example shows how to enable LLDP power negotiation on interface Gigabit Ethernet 3/1:</p> <pre>Switch# config t Enter configuration commands, one per line. End with CNTL/Z. Switch(config)# int gi 3/1 Switch(config-if)# lldp tlv-select power-management</pre>
-----------------	---

Related Commands	Command	Description
	lldp run	Cisco IOS Command Reference library.

logging event link-status global (global configuration)

To change the default switch-wide global link-status event messaging settings, use the **logging event link-status global** command. Use the **no** form of this command to disable the link-status event messaging.

logging event link-status global

no logging event link-status global

Syntax Description

This command has no arguments or keywords.

Command Default

The global link-status messaging is disabled.

Command Modes

Global configuration mode

Command History

Release	Modification
12.2(25)SG	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

The following 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

Command Default Global link-status messaging is enabled.

Command Modes Interface configuration mode

Command History	Release	Modification
	12.2(25)SG	This command was introduced on the Catalyst 4500 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 The following example shows how to enable logging event state-change events on interface gi1/1:

```
Switch# config 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#
```

The following example shows how to turn off logging event link status regardless of the global setting:

```
Switch# config 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#
```

The following example shows how to enable the global event link-status setting on interface gi11/1:

```
Switch# config terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Switch(config)# interface gi11/1  
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.

Command Default Global trunk-status messaging is disabled.

Command Modes Global configuration mode

Command History	Release	Modification
	12.2(25)SG	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 The following example shows how to globally enable link status messaging on each interface:

```
Switch# config 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

Command Default Global trunk-status messaging is enabled.

Command Modes Interface configuration mode

Command History	Release	Modification
	12.2(25)SG	This command was introduced on the Catalyst 4500 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 The following example shows how to enable logging event state-change events on interface g11/1:

```
Switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface g11/1
Switch(config-if)# logging event trunk-status
Switch(config-if)# end
Switch#
```

The following example shows how to turn off logging event trunk status regardless of the global setting:

```
Switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface g11/1
Switch(config-if)# no logging event trunk-status
Switch(config-if)# end
Switch#
```

The following example shows how to enable the global event trunk-status setting on interface gi11/1:

```
Switch# config terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Switch(config)# interface gi11/1  
Switch(config-if)# logging event trunk-status use-global  
Switch(config-if)# end  
Switch#
```

Related Commands

Command	Description
logging event trunk-status global (global configuration)	Enables the trunk-status event messaging on an interface.

mab

To enable and configure MAC authorization 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(50)SG	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 authenticator learns the MAC address of the host and uses that information to query an authentication server to see whether this MAC address will be granted access.

Examples

The following example shows how to enable MAB on a port:

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

The following example shows how to enable and configure MAB on a port:

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

The following example shows how to disable MAB on a port:

```
Switch(config-if)# no mab
Switch(config-if)#
```

Related Commands	Command	Description
	show authentication	Displays Authentication Manager information.
	show mab	Displays MAB information.
	show running-config	Displays the running configuration information.

mac access-list extended

To define the extended MAC access lists, use the **mac access-list extended** command. To remove the MAC access lists, use the **no** form of this command.

mac access-list extended *name*

no mac access-list extended *name*

Syntax Description

name ACL to which the entry belongs.

Command Default

MAC access lists are not defined.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(12c)EW	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 use the following subset to create or delete entries in a MAC layer access list:

```
[no] {permit | deny} {{src-mac mask | any} [dest-mac mask]} [protocol-family {appletalk | arp-non-ipv4 | decnet | ipx | ipv6 | rarp-ipv4 | rarp-non-ipv4 | vines | xns} | <arbitrary ethertype> | name-coded ethertype].
```

[Table 2-10](#) describes the syntax of the **mac access-list extended** subcommands.

Table 2-10 *mac access-list extended Subcommands*

Subcommand	Description
any	Specifies any source-host or destination-host.
<i>arbitrary ethertype</i>	(Optional) Specifies an arbitrary ethertype in the range 1536 to 65535 (Decimal or Hexadecimal)
deny	Prevents access if the conditions are matched.

Table 2-10 *mac access-list extended Subcommands (continued)*

Subcommand	Description
<i>dest-mac mask</i>	(Optional) Specifies a destination MAC address of the form: <i>dest-mac-address dest-mac-address-mask</i> .
<i>name-coded ethertype</i>	(Optional) Denotes a predefined <i>name-coded ethertype</i> for common protocols: aarp—AppleTalk ARP amber—DEC-Amber appletalk—AppleTalk/EtherTalk dec-spanning—DEC-Spanning-Tree decnet-iv—DECnet Phase IV diagnostic—DEC-Diagnostic dsm—DEC-DSM etype-6000—0x6000 etype-8042—0x8042 lat—DEC-LAT lavc-sca—DEC-LAVC-SCA mop-console—DEC-MOP Remote Console mop-dump—DEC-MOP Dump msdos—DEC-MSDOS mumps—DEC-MUMPS netbios—DEC-NETBIOS protocol-family An Ethernet protocol family vines-echo—VINES Echo vines-ip—VINES IP xns-idp—XNS IDP
no	(Optional) Deletes a statement from an access list.
permit	Allows access if the conditions are matched.
<i>protocol-family</i>	(Optional) Name of the protocol family. Table 2-11 lists which packets are mapped to a particular protocol family.
<i>src-mac mask</i>	Source MAC address in the form: <i>source-mac-address source-mac-address-mask</i> .

[Table 2-11](#) describes mapping an Ethernet packet to a protocol family.

Table 2-11 *Mapping an Ethernet Packet to a Protocol Family*

Protocol Family	Ethertype in Packet Header
Appletalk	0x809B, 0x80F3
Arp-Non-Ipv4	0x0806 and protocol header of Arp is a non-IP protocol family
Decnet	0x6000-0x6009, 0x8038-0x8042

Table 2-11 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 is Ipv4
Rarp-Non-Ipv4	0x8035 and protocol header of Rarp is a non-Ipv4 protocol family
Vines	0x0BAD, 0x0BAE, 0x0BAF
Xns	0x0600, 0x0807

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

- Enter the MAC addresses as three 4-byte values in dotted hexadecimal format such as 0030.9629.9f84.
- Enter the MAC address masks as three 4-byte values in dotted hexadecimal format. Use 1 bit as a wildcard. For example, to match an address exactly, use 0000.0000.0000 (can be entered as 0.0.0).
- For the optional *protocol* parameter, you can enter either the EtherType or the keyword.
- Entries without a *protocol* parameter match any protocol.
- The access 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 to an existing list are placed at the end of the list. You cannot add entries to the middle of a list.

Examples

The following example shows how to create a MAC layer access list named `mac_layer` that denies traffic from 0000.4700.0001, which is going to 0000.4700.0009, and permits all other traffic:

```
Switch(config)# mac access-list extended mac_layer
Switch(config-ext-macl)# deny 0000.4700.0001 0.0.0 0000.4700.0009 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 (virtual switch)

To specify a Media Access Control (MAC) address to use as the common router MAC address for interfaces on the active and standby chassis, use the **mac-address** virtual switch configuration submode command. To return to the default setting, use the **no** form of this command.

mac-address {*mac-address* | **use-virtual** | **chassis**}

no mac-address {*mac-address* | **use-virtual** | **chassis**}

Syntax Description

mac-address	Specifies the MAC address in hexadecimal format.
use-virtual	Specifies the MAC address range reserved for the virtual switch system (VSS).
chassis	Specifies a MAC address derived from the chassis.

Command Default

The router MAC address is derived from the Cisco pool of virtual switch specific MAC addresses intended for the domain 1-255.

Command Modes

Virtual switch configuration submode (config-vs-domain)

Command History

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

Usage Guidelines

When a virtual switch boots, the router MAC address is derived from the Cisco pool of virtual switch specific MAC addresses. The router address is used as the common router MAC address for interfaces on both the active and the standby chassis. Between switchovers, this MAC address is maintained on the new active switch. You can enter the **mac-address mac-address** command to specify a MAC address to use or the **mac-address use-virtual** command to use the MAC address range reserved for the VSS.

The MAC address range reserved for the VSS is derived from a reserved pool of addresses with the domain ID encoded in the leading 6 bits of the last octet and trailing 2 bits of the previous octet of the mac-address. The last two bits of the first octet is allocated for the protocol mac-address that is derived by adding the protocol ID (0 to 3) to the router MAC address.



Note

You must reload the virtual switch for the new router MAC address to take effect. If the MAC address you configured is different from the current MAC address, the following message is displayed:

Console (enable)#

Examples

The following example shows how to specify the MAC address to use in hexadecimal format:

```
Router(config)# switch virtual domain test-mac-address
Router(config-vs-domain)# mac-address 0000.0000.0000
Router(config-vs-domain)#
```


The following example shows how to specify the MAC address range reserved for the VSS:

```
Router(config)# switch virtual domain test-mac-address
Router(config-vs-domain)# mac-address use-virtual
Router(config-vs-domain)#
```

Related Commands

Command	Description
switch virtual domain (virtual switch)	Assigns a switch number and enters virtual switch domain configuration submode.

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	<i>seconds</i>	Aging time in seconds; valid values are 0 and from 10 to 1000000 seconds.
	vlan <i>vlan_id</i>	(Optional) Single VLAN number or a range of VLANs; valid values are from 1 to 4094.

Command Default Aging time is set to 300 seconds.

Command Modes Global configuration mode

Command History	Release	Modification
	12.1(8a)EW	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 The following example shows how to configure the aging time to 400 seconds:

```
Switch(config)# mac-address-table aging-time 400
Switch(config)#
```

The following example shows how to disable aging:

```
Switch(config)# mac-address-table aging-time 0
Switch(config)
```

Related Commands	Command	Description
	show mac-address-table aging-time	Displays MAC address table aging information.

mac-address-table dynamic group protocols

To enable the learning of MAC addresses 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.

Command Default The group learning feature is disabled.

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 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 unicast 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 The following example shows that the MAC addresses are initially assigned to either the “ip” or the “other” protocol bucket:

```
Switch# show mac-address-table dynamic
Unicast Entries
  vlan  mac address      type           protocols      port
-----+-----+-----+-----+-----
   1    0000.0000.5000    dynamic other           GigabitEthernet1/1
   1    0001.0234.6616    dynamic ip             GigabitEthernet3/1
   1    0003.3178.ec0a     dynamic assigned      GigabitEthernet3/1
   1    0003.4700.24c3     dynamic ip             GigabitEthernet3/1
   1    0003.4716.f475     dynamic ip             GigabitEthernet3/1
   1    0003.4748.75c5     dynamic ip             GigabitEthernet3/1
   1    0003.47f0.d6a3     dynamic ip             GigabitEthernet3/1
   1    0003.47f6.a91a     dynamic ip             GigabitEthernet3/1
```

```

1    0003.ba06.4538    dynamic ip           GigabitEthernet3/1
1    0003.fd63.3eb4    dynamic ip           GigabitEthernet3/1
1    0004.2326.18a1    dynamic ip           GigabitEthernet3/1
1    0004.5a5d.de53    dynamic ip           GigabitEthernet3/1
1    0004.5a5e.6ecc    dynamic ip           GigabitEthernet3/1
1    0004.5a5e.f60e    dynamic ip           GigabitEthernet3/1
1    0004.5a5f.06f7    dynamic ip           GigabitEthernet3/1
1    0004.5a5f.072f    dynamic ip           GigabitEthernet3/1
1    0004.5a5f.08f6    dynamic ip           GigabitEthernet3/1
1    0004.5a5f.090b    dynamic ip           GigabitEthernet3/1
1    0004.5a88.b075    dynamic ip           GigabitEthernet3/1
1    0004.c1bd.1b40    dynamic ip           GigabitEthernet3/1
1    0004.c1d8.b3c0    dynamic ip           GigabitEthernet3/1
1    0004.c1d8.bd00    dynamic ip           GigabitEthernet3/1
1    0007.e997.74dd    dynamic ip           GigabitEthernet3/1
1    0007.e997.7e8f    dynamic ip           GigabitEthernet3/1
1    0007.e9ad.5e24    dynamic ip           GigabitEthernet3/1
1    000b.5f0a.f1d8    dynamic ip           GigabitEthernet3/1
1    000b.fdf3.c498    dynamic ip           GigabitEthernet3/1
1    0010.7be8.3794    dynamic assigned    GigabitEthernet3/1
1    0012.436f.c07f    dynamic ip           GigabitEthernet3/1
1    0050.0407.5fe1    dynamic ip           GigabitEthernet3/1
1    0050.6901.65af    dynamic ip           GigabitEthernet3/1
1    0050.da6c.81cb    dynamic ip           GigabitEthernet3/1
1    0050.dad0.af07    dynamic ip           GigabitEthernet3/1
1    00a0.ccd7.20ac    dynamic ip           GigabitEthernet3/1
1    00b0.64fd.1c23    dynamic ip           GigabitEthernet3/1
1    00b0.64fd.2d8f    dynamic assigned    GigabitEthernet3/1
1    00d0.b775.c8bc    dynamic ip           GigabitEthernet3/1
1    00d0.b79e.de1d    dynamic ip           GigabitEthernet3/1
1    00e0.4c79.1939    dynamic ip           GigabitEthernet3/1
1    00e0.4c7b.d765    dynamic ip           GigabitEthernet3/1
1    00e0.4c82.66b7    dynamic ip           GigabitEthernet3/1
1    00e0.4c8b.f83e    dynamic ip           GigabitEthernet3/1
1    00e0.4cbc.a04f    dynamic ip           GigabitEthernet3/1
1    0800.20cf.8977    dynamic ip           GigabitEthernet3/1
1    0800.20f2.82e5    dynamic ip           GigabitEthernet3/1
Switch#

```

The following example shows how to assign MAC addresses that belong to either the “ip” or the “other” bucket to both buckets:

```

Switch(config)# mac-address-table dynamic group protocols ip other
Switch(config)# exit
Switch# show mac address-table dynamic
Unicast Entries
-----+-----+-----+-----+-----+
vlan  mac address      type      protocols      port
-----+-----+-----+-----+-----+
1      0000.0000.5000      dynamic  ip,other       GigabitEthernet1/1
1      0001.0234.6616      dynamic  ip,other       GigabitEthernet3/1
1      0003.4700.24c3      dynamic  ip,other       GigabitEthernet3/1
1      0003.4716.f475      dynamic  ip,other       GigabitEthernet3/1
1      0003.4748.75c5      dynamic  ip,other       GigabitEthernet3/1
1      0003.47c4.06c1      dynamic  ip,other       GigabitEthernet3/1
1      0003.47f0.d6a3      dynamic  ip,other       GigabitEthernet3/1
1      0003.47f6.a91a      dynamic  ip,other       GigabitEthernet3/1
1      0003.ba0e.24a1      dynamic  ip,other       GigabitEthernet3/1
1      0003.fd63.3eb4      dynamic  ip,other       GigabitEthernet3/1
1      0004.2326.18a1      dynamic  ip,other       GigabitEthernet3/1
1      0004.5a5d.de53      dynamic  ip,other       GigabitEthernet3/1
1      0004.5a5d.de55      dynamic  ip,other       GigabitEthernet3/1
1      0004.5a5e.6ecc      dynamic  ip,other       GigabitEthernet3/1
1      0004.5a5e.f60e      dynamic  ip,other       GigabitEthernet3/1
1      0004.5a5f.08f6      dynamic  ip,other       GigabitEthernet3/1

```

```
1 0004.5a5f.090b dynamic ip,other GigabitEthernet3/1
1 0004.5a64.f813 dynamic ip,other GigabitEthernet3/1
1 0004.5a66.1a77 dynamic ip,other GigabitEthernet3/1
1 0004.5a6b.56b2 dynamic ip,other GigabitEthernet3/1
1 0004.5a6c.6a07 dynamic ip,other GigabitEthernet3/1
1 0004.5a88.b075 dynamic ip,other GigabitEthernet3/1
1 0004.c1bd.1b40 dynamic ip,other GigabitEthernet3/1
1 0004.c1d8.b3c0 dynamic ip,other GigabitEthernet3/1
1 0004.c1d8.bd00 dynamic ip,other GigabitEthernet3/1
1 0005.dce0.7c0a dynamic assigned GigabitEthernet3/1
1 0007.e997.74dd dynamic ip,other GigabitEthernet3/1
1 0007.e997.7e8f dynamic ip,other GigabitEthernet3/1
1 0007.e9ad.5e24 dynamic ip,other GigabitEthernet3/1
1 0007.e9c9.0bc9 dynamic ip,other GigabitEthernet3/1
1 000b.5f0a.f1d8 dynamic ip,other GigabitEthernet3/1
1 000b.fdf3.c498 dynamic ip,other GigabitEthernet3/1
1 0012.436f.c07f dynamic ip,other GigabitEthernet3/1
1 0050.0407.5fe1 dynamic ip,other GigabitEthernet3/1
1 0050.6901.65af dynamic ip,other GigabitEthernet3/1
1 0050.da6c.81cb dynamic ip,other GigabitEthernet3/1
1 0050.dad0.af07 dynamic ip,other GigabitEthernet3/1
1 00a0.ccd7.20ac dynamic ip,other GigabitEthernet3/1
1 00b0.64fd.1b84 dynamic assigned GigabitEthernet3/1
1 00d0.b775.c8bc dynamic ip,other GigabitEthernet3/1
1 00d0.b775.c8ee dynamic ip,other GigabitEthernet3/1
1 00d0.b79e.de1d dynamic ip,other GigabitEthernet3/1
1 00e0.4c79.1939 dynamic ip,other GigabitEthernet3/1
1 00e0.4c7b.d765 dynamic ip,other GigabitEthernet3/1
1 00e0.4c82.66b7 dynamic ip,other GigabitEthernet3/1
1 00e0.4c8b.f83e dynamic ip,other GigabitEthernet3/1
1 00e0.4c8c.0861 dynamic ip,other GigabitEthernet3/1
1 0800.20d1.bf09 dynamic ip,other GigabitEthernet3/1
Switch#
```

mac-address-table learning vlan

To enable MAC address learning on a VLAN, use the **mac-address-table learning** global configuration command. Use the **no** form of this command to disable MAC address learning on a VLAN to control which VLANs can learn MAC addresses.

mac-address-table learning vlan *vlan-id*

no mac-address-table learning vlan *vlan-id*

Syntax Description

<i>vlan-id</i>	Specifies a single VLAN ID or a range of VLAN IDs separated by a hyphen or comma. Valid VLAN IDs are 1 to 4094.
----------------	---

Command Default

Enabled on all VLANs

Command Modes

Global configuration

Command History

Release	Modification
12.2(54)SG	This command was modified to support the disable learning feature on the Catalyst 4500 series switch.

Usage Guidelines

When you control MAC address learning on a VLAN, you can manage the available table space by controlling which VLANs, and which ports can learn MAC addresses.

You can disable MAC address learning on a single VLAN ID (for example, by entering **no mac-address-table learning vlan 223**) or on a range of VLAN IDs (for example, by entering **no mac-address-table learning vlan 1-20, 15**.)

Before you disable MAC address learning, familiarize yourself with the network topology and the switch system configuration. If you disable MAC address learning on a VLAN, flooding may occur in the network. For example, if you disable MAC address learning on a VLAN with a configured switch virtual interface (SVI), the switch floods all IP packets in the Layer 2 domain. If you disable MAC address learning on a VLAN that includes more than two ports, every packet entering the switch is flooded in that VLAN domain. Disable MAC address learning only in VLANs that contain two ports. Use caution before disabling MAC address learning on a VLAN with an SVI.

You cannot disable MAC address learning on a VLAN that the switch uses internally. This action causes the switch to generate an error message and rejects the **no mac-address-table learning vlan** command. To view used internal VLANs, enter the **show vlan internal usage** privileged EXEC command.

If you disable MAC address learning on a VLAN configured as a PVLAN primary or a secondary VLAN, the MAC addresses are still learned on the VLAN (primary or secondary) associated with the PVLAN.

You cannot disable MAC address learning on an RSPAN VLAN. The configuration is not allowed.

If you disable MAC address learning on a VLAN that includes a secure port, MAC address learning is not disabled on the secure port. If you later disable port security on the interface, the disabled MAC address learning state is enabled.

To display the MAC address learning status of a specific VLAN or for all VLANs, enter the **show mac-address-table learning vlan** command.

Examples

The following example shows how to disable MAC address learning on VLAN 2003:

```
Switch(config)# no mac-address-table learning vlan 2003
```

Related Commands

Command	Description
show mac address-table learning	Displays the MAC address learning status on all VLANs or on the specified VLAN.

mac-address-table notification

To enable MAC address notification on a switch, use the **mac-address-table notification** command. To return to the default setting, use the **no** form of this command

```
mac-address-table notification [[change [history-size hs_value | interval intv_value]] |
  [mac-move] | [threshold [limit percentage | interval time]] | [learn-fail [interval time | limit
  num_fail]]
```

```
no mac-address-table notification [[change [history-size hs_value | interval intv_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 <i>hs_value</i>	(Optional) Sets a maximum number of entries in the MAC change notification history table. The range is 0 to 500 entries.
interval <i>intv_value</i>	(Optional) Sets a notification trap interval: the set interval time between two consecutive traps. The range is 0 to 2,147,483,647 seconds.
mac-move	(Optional) Specifies enabling MAC move notification.
threshold	(Optional) Specifies enabling MAC threshold notification.
limit <i>percentage</i>	(Optional) Specifies the percentage of MAT utilization threshold; valid values are from 1 to 100 percent.
interval <i>time</i>	(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) notifications of failures to install MAC addresses learned in software into hardware. Disabled by default.
interval <i>time</i>	(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 <i>num_fail</i>	(Optional) Specifies the number of hardware MAC learning failures to be allowed in a notification interval.

Command Default

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(31)SG	This command was introduced on the Catalyst 4500 series switch.
	12.2(52)SG	Support introduced for the learn-fail keyword on Supervisor Engine 6-E and Catalyst 4900M.

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 The following 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)#
```

The following 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)#
```

The following example shows how to enable hardware MAC address learning failure syslog notification:

```
Switch(config)# mac address-table notification learn-fail
```

The following example shows how to set the interval of hardware MAC address learning failure syslog notification to 30 seconds:

```
Switch(config)# mac address-table notification learn-fail interval 30
```

Related Commands	Command	Description
	clear mac-address-table	Clears the global counter entries from the Layer 2 MAC address table.
	mac-address-table notification	Enables MAC address notification on a switch.
	snmp-server enable traps	Enables SNMP notifications.
	snmp trap mac-notification change	Enables SNMP MAC address notifications.

mac-address-table static

To configure the static MAC addresses for a VLAN interface or drop unicast traffic for a MAC address for a VLAN interface, use the **mac-address-table static** command. To remove the static MAC address 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		
<i>mac-addr</i>	MAC address; optional when using the no form of this command.	
vlan <i>vlan-id</i>	VLAN and valid VLAN number; valid values are from 1 to 4094.	
interface <i>type</i>	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.	

Command Default This command has no default settings.

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

- When a static MAC address is installed, it is associated with a port.
- The output interface specified must be a Layer 2 interface and not an SVI.
- If you do not enter a protocol type, an entry is automatically created for each of the four protocol types.
- Entering the **no** form of this command does not remove the system MAC addresses.
- When removing a MAC address, entering **interface int** 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

The following example shows how to add the static entries to the MAC address table:

```
Switch(config)# mac-address-table static 0050.3e8d.6400 vlan 100 interface fastethernet5/7
Switch(config)#
```

Related Commands	Command	Description
	show mac-address-table static	Displays the static MAC address table entries only.

macro apply cisco-desktop

To enable the Cisco-recommended features and settings that are suitable for connecting a switch port to a standard desktop, use the **macro apply cisco-desktop** command.

macro apply cisco-desktop \$AVID access_vlanid

Syntax Description	\$AVID access_vlanid Specifies an access VLAN ID.				
Command Default	This command has no default settings.				
Command Modes	Interface configuration mode				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.2(18)EW</td> <td>This command was introduced on the Catalyst 4500 series switch.</td> </tr> </tbody> </table>	Release	Modification	12.2(18)EW	This command was introduced on the Catalyst 4500 series switch.
Release	Modification				
12.2(18)EW	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

The following example shows how to enable the Cisco-recommended features and settings on port fa2/1:

```
Switch(config)# interface FastEthernet2/1
Switch(config-if)# macro apply cisco-desktop $AVID 50
Switch(config-if)#
```

The contents of this macro are as follows:

```
# Basic interface - Enable data VLAN only
# Recommended value for access vlan (AVID) should not be 1
switchport access vlan $AVID [access_vlanid]
switchport mode access
# Enable port security limiting port to a single
# MAC address -- that of desktop
switchport port-security
# Ensure port-security age is greater than one minute
# and use inactivity timer
# "Port-security maximum 1" is the default and will not
# Show up in the config
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity
# Configure port as an edge network port
spanning-tree portfast
spanning-tree bpduguard enable
```

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.

macsec network-link

To enable MKA MACsec on switch-to-switch links using EAP-TLS, use the **macsec network-link** command.

macsec network-link

Syntax Description	macsec network-link	Enables MKA MACsec on switch-to-switch links using Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) method.
Command Default	This command has no default settings.	
Command Modes	Interface configuration mode	
Command History	Release	Modification
	Cisco IOS XE 3.9.0E	This command was introduced on Cisco Catalyst 4500-E with Supervisor Engine 8-E, and on Cisco Catalyst 4500-X series switches.
Usage Guidelines	This command cannot be used to configure multi-point to multi-point links.	
Examples	The following example shows how to enable the Cisco-recommended features and settings on port fa2/1: <pre>Switch(config)# interface FastEthernet2/1 Switch(config-if)# macsec network-link Switch(config-if)# exit</pre>	

mka

To apply an MACsec Key Agreement policy on an interface, and to configure MKA MACsec on a interface using a PSK, use the **mka** command.

```
mka {default-policy | policy policy name [pre-shared-key {key-chain key-chain-name}]
```

Syntax Description		
	default-policy	Enables MKA MACsec using the default MKA policy on the interface.
	policy <i>policy name</i>	Enables MKA MACsec using a configured MKA policy on the interface.
	pre-shared-key	Enables MKA MACsec using a pre-shared key on the interface.
	key-chain	
	<i>key-chain-name</i>	

Command Default The default MKA policy is applied on the interface.

Command Modes Interface configuration mode

Command History	Release	Modification
	Cisco IOS XE 3.9.0E	This command was introduced on Cisco Catalyst 4500-E with Supervisor Engine 8-E, and on Cisco Catalyst 4500-X series switches.

Examples The following example shows how to enable the Cisco-recommended features and settings on port fa2/1:

```
Switch(config)# interface FastEthernet2/1
Switch(config-if)# mka pre-shared-key key-chain kc1
Switch(config-if)# exit
```

mka policy

To configure MACsec Key Agreement policy options, and enter mka-policy configuration mode, use the **mka policy** command.

```
mka policy policy name [confidentiality-offset default | key-server priority priority |
macsec-cipher-suite {gcm-aes-128 | gcm-aes-256}]
```

Syntax Description		
confidentiality-offset <i>offset-value</i>	Identifies a confidentiality (encryption) offset value for the MKA policy. Valid values are 0, 30, and 50 octets (bytes).	
default	Sets the policy to use the default confidentiality-offset, key-server priority and cipher suite.	
key-server priority <i>priority</i>	Sets the MKA key-server priority between 0 and 255. Note that 255 is not used as the key-server.	
macsec-cipher-suite	Configures the cipher suite for SAK derivation.	

Command Default None.

Command Modes Global Configuration

Command History	Release	Modification
	Cisco IOS XE 3.9.0E	This command was introduced on Cisco Catalyst 4500-E with Supervisor Engine 8-E, and on Cisco Catalyst 4500-X series switches.

Examples

The following example shows how to configure MKA policy options:

```
Switch(config)# mka policy policy1
Switch(config-mka-policy)# confidentiality-offset 0
Switch(config-mka-policy)# key-server priority 245
Switch(config-mka-policy)# gcm-aes-128
Switch(config-mka-policy)# exit
```

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 \$AVID *access_vlanid* \$VVID *voice_vlanid*

Syntax Description

\$AVID <i>access_vlanid</i>	Specifies an access VLAN ID.
\$VVID <i>voice_vlanid</i>	Specifies a voice VLAN ID.

Command Default

This command has no default settings.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.2(18)EW	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

The following example shows how to enable the Cisco-recommended features and settings on port fa2/1:

```
Switch(config)# interface FastEthernet2/1
Switch(config-if)# macro apply cisco-phone $AVID 10 $VVID 50
Switch(config-if)#
```

The contents of this macro are as follows:

```
# VoIP enabled interface - Enable data VLAN
# and voice VLAN (VVID)
# Recommended value for access vlan (AVID) should not be 1\
switchport access vlan $AVID [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 $VVID [voice_vlan_id]
# Enable port security limiting port to a 3 MAC
# addressees -- One for desktop and two for phone
switchport port-security
switchport port-security maximum 3
# Ensure port-security age is greater than one minute
# and use inactivity timer
switchport port-security violation restrict
switchport port-security aging time 2
```



```
switchport port-security aging type inactivity
# Enable auto-gos to extend trust to attached Cisco phone
auto qos voip cisco-phone
# Configure port as an edge network port
spanning-tree portfast
spanning-tree bpduguard enable@
```

Related Commands

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

macro apply cisco-router

To enable the Cisco-recommended features and settings that are suitable for connecting a switch port to a router, use the **macro apply cisco-router** command.

macro apply cisco-router *\$NVID native_vlanid*

Syntax Description	<i>\$NVID native_vlanid</i> Specifies a native VLAN ID.
---------------------------	---

Command Default	This command has no default settings.
------------------------	---------------------------------------

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

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

Usage Guidelines	<p>This command can only be viewed and applied; it cannot be modified.</p> <p>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.</p>
-------------------------	--

Examples	The following 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 $NVID 80
Switch(config-if)#
```

The contents of this macro are as follows:

```
# Access Uplink to Distribution
switchport trunk encapsulation dot1q
# Define unique Native VLAN on trunk ports
# Recommended value for native vlan (NVID) should not be 1
switchport trunk native vlan $NVID [native_vlan_id]
# Update the allowed VLAN range (VRANGE) such that it
# includes data, voice and native VLANs
# switchport trunk allowed vlan $VRANGE [vlan_range]
# Hardcode trunk and disable negotiation to
# speed up convergence
# Hardcode speed and duplex to router
switchport mode trunk
switchport nonegotiate
speed 100
duplex full
# Configure qos to trust this interface
auto qos voip trust
qos trust dscp
```

```
# Ensure fast access to the network when enabling the interface.  
# Ensure that switch devices cannot 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 \$NVID *native_vlanid*

Syntax Description	\$NVID <i>native_vlanid</i> Specifies a native VLAN ID.
---------------------------	---

Command Default	This command has no default settings.
------------------------	---------------------------------------

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

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

Usage Guidelines	<p>This command can only be viewed and applied; it cannot be modified.</p> <p>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.</p>
-------------------------	---

Examples	The following 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 $NVID 45
Switch(config-if)#
```

The contents of this macro are as follows:

```
# Access Uplink to Distribution
switchport trunk encapsulation dot1q
# Define unique Native VLAN on trunk ports
# Recommended value for native vlan (NVID) should not be 1
switchport trunk native vlan $NVID [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
# Configure qos to trust this interface
auto qos voip trust
# 802.1w defines the link as pt-pt for rapid convergence
spanning-tree link-type point-to-point
```

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

macro auto device

Use the **macro auto device** command to simplify changing the parameters for a built-in functions for a device type. Use the **no** form of this command to revert to the initial parameter values.

macro auto device *device_type* [*params values*]

no macro auto device *device_type* [*params values*]

Syntax Description

<i>device_type</i>	Specifies the device type. <ul style="list-style-type: none"> phone—Apply interface configs on detecting a phone switch—Apply interface configs on detecting a switch router—Apply interface configs on detecting a router ap—Apply interface configs on detecting an ap lwap—Apply interface configs on detecting a light weight ap dmp—Apply interface configs on detecting a DMP ipvsc—Apply interface configs on detecting a IPVSC
<i>param name=value</i>	(Optional) <i>parameter=value</i> —Replace default values that begin with \$. Enter new values in the form of name value pair separated by a space: [<i><name1>=<value1> <name2>=<value2>...</i>]. Default values are shown in parenthesis.

Command Modes

Global configuration

Command History

Release	Modification
12.2(54)SG	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

Although you can use the **macro auto execute** command to produce the same effect as the **macro auto device** command, the later is simpler.

Examples

The following example shows how to change the access VLAN and voice VLAN from their default value to user defined values for phone devices.

```
(config)# macro auto device phone ACCESS_VLAN=10 VOICE_VLAN=20
```

Related Commands

Command	Description
macro auto execute (built-in function)	Changes built-in function default values or to map user-defined triggers to built-in functions, and to pass the parameter values.
macro auto execute (remotely-defined trigger)	Maps a trigger to a remotely defined functions.

Command	Description
macro auto execute (user-defined function)	Maps a trigger to a user-defined function.
macro auto global processing	Enables Auto Smartports on a switch.
macro auto processing	Enables Auto SmartPorts macros on a specific interface.
macro auto sticky	Specifies not to remove configurations applied by ASP across link flaps and device removal.
shell trigger	Creates a user defined trigger.

macro auto execute (built-in function)

Use the **macro auto execute** configuration command to change built-in function default values or to map user-defined triggers to built-in functions and to pass the parameter values. Use the **no** form of this command to unmap the trigger.

macro auto execute *event_trigger* **builtin** *shell_function* [*param name=values*]

no macro auto execute *event_trigger* **builtin** *shell_function* [*param name=values*]

Syntax Description

[*event_trigger*](#)

Defines mapping from an event trigger to a built-in macro.

Specify an *event trigger*:

- CISCO_PHONE_EVENT
- CISCO_SWITCH_EVENT
- CISCO_ROUTER_EVENT
- CISCO_WIRELESS_AP_EVENT
- CISCO_WIRELESS_LIGHTWEIGHT_AP_EVENT
- CISCO_DMP_EVENT
- CISCO_IPVSC_EVENT
- WORD—Apply a user-defined event trigger.

[*shell_function*](#)

Specifies a built-in macro name:

- CISCO_PHONE_AUTO_SMARTPORT
(Optional) Specify the parameter values: \$ACCESS_VLAN=(1) and \$VOICE_VLAN=(2).
- CISCO_SWITCH_AUTO_SMARTPORT
(Optional) Specify the parameter values: \$NATIVE_VLAN=(1).
- CISCO_ROUTER_AUTO_SMARTPORT
(Optional) Specify the parameter values: \$NATIVE_VLAN=(1).
- CISCO_AP_AUTO_SMARTPORT
(Optional) Specify the parameter values: \$NATIVE_VLAN=(1).
- CISCO_LWAP_AUTO_SMARTPORT
(Optional) Specify the parameter values: \$ACCESS_VLAN=(1).
- CISCO_DMP_AUTO_SMARTPORT
- CISCO_IP_CAMERA_AUTO_SMARTPORT

[*param name=value*](#)

(Optional) Specifies values for the parameters that are to be used in the function body.

Command Default

Auto Smartports is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(54)SG	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

The switch automatically maps from builtin event triggers to builtin functions. The builtin functions are system-defined functions in the software image.

Use the **macro auto execute** global configuration command to replace the builtin function default values with values specific to your switch.

You can also create user-defined triggers and use this command to map the triggers to builtin functions.

You can create user-defined event triggers by entering the **shell trigger** global configuration command. Use the **show shell** privileged EXEC command to display the contents of the builtin and user-defined triggers and functions.

Examples

The following example shows how to use two built-in Auto Smartports macros for connecting Cisco switches and Cisco IP phones to the switch. It modifies the default voice VLAN, access VLAN, and native VLAN for the trunk interface:

```
Switch# configure terminal
Switch(config)#!!! the next command modifies the access and voice vlans
Switch(config)#!!! for the built in Cisco IP phone auto smartport macro
Switch(config)# macro auto execute CISCO_PHONE_EVENT builtin CISCO_PHONE_AUTO_SMARTPORT
ACCESS_VLAN=10 VOICE_VLAN=20
Switch(config)#
Switch(config)#!!! the next command modifies the native vlan
Switch(config)#!!! for the built in switch auto smartport macro
Switch(config)# macro auto execute CISCO_SWITCH_EVENT builtin CISCO_SWITCH_AUTO_SMARTPORT
NATIVE_VLAN=10
Switch(config)#!!! the next example creates a user-defined trigger and maps it to a
builtin functions
Switch(config)# shell trigger myTrigger "user-defined trigger"
Switch(config)# macro auto execute myTrigger builtin CISCO_PHONE_AUTO_SMARTPORT_ACCESSVLAN
voice_vlan
Switch(config)#!!! the next command enables auto smart ports globally
Switch(config)# macro auto global processing fallback CDP

Switch# !!! here's the running configuration of the interface connected
Switch# !!! to another Cisco Switch after the Macro is applied
Switch#
Switch# show running-config interface Gi1/0/1
Building configuration...

Current configuration : 284 bytes
!
interface GigabitEthernet1/0/1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 10
 switchport mode trunk
 srr-queue bandwidth share 10 10 60 20
 queue-set 2
 priority-queue out
 mls qos trust cos
 auto qos voip trust
 macro description CISCO_SWITCH_EVENT
end
```

Related Commands	Command	Description
	macro auto device	Simplifies changing the parameters for a built-in functions for a device type.
	macro auto execute (remotely-defined trigger)	Maps a trigger to a remotely defined functions.
	macro auto execute (user-defined function)	Maps a trigger to a user-defined function.
	macro auto global processing	Enables Auto Smartports on a switch.
	macro auto processing	Enables Auto SmartPorts macros on a specific interface.
	macro auto sticky	Specifies not to remove configurations applied by ASP across link flaps and device removal.
	shell trigger	Creates a user defined trigger.

macro auto execute (remotely-defined trigger)

Use the **macro auto execute** configuration command to map a trigger to a remotely defined function. Use the **no** form of this command to unmap the trigger.

```
macro auto execute trigger_name remote url
```

```
no macro auto execute trigger_name remote url
```

Syntax Description		
	<i>trigger_name</i>	Specifies the trigger name.
	<i>url</i>	Specifies the remotely-defined URL

Command Default	None
-----------------	------

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

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

Usage Guidelines	This command enables you to store shell functions in a central location and utilized by ASP on many switches. This alleviates the problem of updating functions on every switch for each modification.
------------------	--

Triggering of the remotely defined function requires network connectivity to the URL, which is accessed for each execution of the function.

Examples	The following example shows how to map a trigger to the remotely defined function myfunction - the filename that contains the function body:
----------	---

```
Switch(config)# macro auto execute mytrigger remote tftp://dir/tftpboot/myfunction
```

Related Commands	Command	Description
	macro auto device	Simplifies changing the parameters for a built-in functions for a device type.
	macro auto execute (built-in function)	Changes built-in function default values or to map user-defined triggers to built-in functions, and to pass the parameter values.
	macro auto execute (user-defined function)	Maps a trigger to a user-defined function.
	macro auto global processing	Enables Auto Smartports on a switch.
	macro auto processing	Enable Auto SmartPorts macros on a specific interface.

Command	Description
<code>macro auto sticky</code>	Specifies not to remove configurations applied by ASP across link flaps and device removal.
<code>shell trigger</code>	Create a user defined trigger.

macro auto execute (user-defined function)

Use the **macro auto execute** configuration command to map a trigger to a user-defined function. Use the **no** form of this command to unmap the trigger.

```
macro auto execute trigger_name [param_name=value] {function body}
```

```
no macro auto execute trigger_name [param_name=value]
```

Syntax Description		
	<i>trigger_name</i>	Specifies the trigger name.
	<i>param_name=value</i>	(Optional) Specifies values for the parameters that are to be used in the function body.
	<i>function_body</i>	Shell functions with CLIs.

Command Default None.

Command Modes Global configuration

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

Usage Guidelines Because the function defined in this command does not have a name, you cannot use it to map to another trigger. This is the only way that you can map a trigger to a user defined function. Shell functions defined in the non-configure mode can not be used to map triggers.

Examples The following example shows how to map the user-defined event trigger **Cisco Digital Media Player (DMP)** to a user-defined macro.

- Connect the DMP to an 802.1x- or MAB-enabled switch port.
- On the RADIUS server, set the attribute-value pair to **auto-smart-port=CISCO_DMP_EVENT**.
- On the switch, create the event trigger CISCO_DMP_EVENT, and enter the user-defined macro commands shown below.
- The switch recognizes the attribute-value pair=CISCO_DMP_EVENT response from the RADIUS server and applies the macro associated with this event trigger.

```
Switch(config)# shell trigger CISCO_DMP_EVENT Cisco DMP player
Switch(config)# macro auto execute CISCO_DMP_EVENT {
if [[ $LINKUP -eq YES ]]; then
conf t
interface $INTERFACE
macro description $TRIGGER
switchport access vlan 1
switchport mode access
switchport port-security
```

```

switchport port-security maximum 1
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity
spanning-tree portfast
spanning-tree bpduguard enable
exit
fi
if [[ $LINKUP -eq NO ]]; then
conf t
interface $INTERFACE
    no macro description $TRIGGER
    no switchport access vlan 1
    if [[ $AUTH_ENABLED -eq NO ]]; then
        no switchport mode access
    fi
    no switchport port-security
    no switchport port-security maximum 1
    no switchport port-security violation restrict
    no switchport port-security aging time 2
    no switchport port-security aging type inactivity
    no spanning-tree portfast
    no spanning-tree bpduguard enable
    exit
fi
}
Switch(config)# end

```

Related Commands

Command	Description
macro auto device	Simplifies changing the parameters for a built-in functions for a device type.
macro auto execute (built-in function)	Changes built-in function default values or to map user-defined triggers to built-in functions, and to pass the parameter values.
macro auto execute (remotely-defined trigger)	Maps a trigger to a remotely defined functions.
macro auto global processing	Enables Auto Smartports on a switch.
macro auto processing	Enables Auto SmartPorts macros on a specific interface.
macro auto sticky	Specifies not to remove configurations applied by ASP across link flaps and device removal.
shell trigger	Creates a user defined trigger.

macro auto global processing

Use the **macro auto global processing** global configuration command to enable Auto SmartPorts macros on the switch. Use the **no** form of this command to disable Auto SmartPorts (ASP) macros globally.

macro auto global processing [cdp | lldp]

no macro auto global processing [cdp | lldp]



Note Starting with Release 15.0(2)SG, the **fallback** option has been deprecated.

Syntax Description	cdp	Selects CDP as fallback mode.
	lldp	Selects LLDP as fallback mode.

Command Default Auto Smartports is disabled.

Command Modes Global configuration

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

Usage Guidelines Use the **macro auto global processing** global configuration command to globally enable Auto Smartports macros on the *switch*. To disable ASP macros on a specific *port*, use the **no macro auto processing** command in the interface mode before ASP is enabled globally.

Auto Smartports macros dynamically configure ports based on the device type detected on the port. When the switch detects a new device on a port it applies the appropriate ASP macro. When a link-down event occurs on a port, the switch removes the macro. For example, when you connect a Cisco IP phone to a port, ASP automatically applies the IP phone macro. The IP phone macro enables quality of service (QoS), security features, and a dedicated voice VLAN to ensure proper treatment of delay-sensitive voice traffic.

ASP uses event triggers to map devices to macros. The most common event triggers are based on Cisco Discovery Protocol (CDP) messages received from connected devices. The detection of a device invokes a CDP event trigger: Cisco IP phone, Cisco wireless access point, Cisco switch, or Cisco router. Other event triggers use MAC authentication bypass (MAB) and 802.1X authentication messages.

Use CDP if port authentication is enabled and the RADIUS server does not send an event trigger.

Select LLDP to apply auto configuration if authentication fails.

If authentication is enabled on a port, a switch ignores CDP and LLDP messages unless the **cdp** keyword is enabled.

When using 802.1X or MAB authentication, configure the RADIUS server to support the Cisco attribute-value (AV) pair **auto-smart-port=event trigger**.

When CDP-identified devices advertise multiple capabilities, a switch chooses a capability in this priority order: switch, router, access point, lightweight access point, phone, host.

To verify that an ASP macro is applied to an interface, use the **show running config** command.

The **macro auto global processing cdp** and **macro auto global processing lldp** commands enables ASP globally if it is not already enabled, and set the fallback to CDP or LLDP, respectively. However, the **no macro auto global processing [cdp | lldp]** command only removes the fallback mechanism. It does not disable ASP globally; only the **no macro auto global processing** command disables ASP globally.

The keywords **cdp** and **lldp** are also controlled at the interface level; by default, CDP is the fallback mechanism on an interface. If you prefer LLDP, first enter the **no macro auto processing cdp** command, then enter the **macro auto processing lldp** command.

If you want to activate both CDP and LLDP, you must enable them in sequence. For example, you would first enter the **macro auto processing cdp** command, then the **macro auto processing lldp** command.

Examples

The following example shows how enable ASP on a switch and to disable the feature on Gi1/0/1:

```
Switch(config)# interface interface Gi1/0/1
Switch(config-if)# no macro auto processing
Switch(config)# macro auto global processing
```

Related Commands

Command	Description
macro auto device	Simplifies changing the parameters for a built-in functions for a device type.
macro auto execute (built-in function)	Changes built-in function default values or to map user-defined triggers to built-in functions, and to pass the parameter values.
macro auto execute (remotely-defined trigger)	Maps a trigger to a remotely defined functions.
macro auto execute (user-defined function)	Maps a trigger to a user-defined function.
macro auto processing	Enables ASP macros on a specific interface.
macro auto sticky	Enables a user to not remove configurations applied by ASP across link flaps and device removal.
shell trigger	Creates a user defined trigger.

macro auto mac-address-group

Use the **macro auto mac-address-group** command to configure a group of MAC-address or OUIs as a trigger. Use the **no** form of this command to unconfigure the group.

macro auto mac-address-group *grp_name*

no macro auto mac-address-group *grp_name1*

Syntax Description	<i>grp_name</i>	Specifies the group name.
---------------------------	-----------------	---------------------------

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

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

Usage Guidelines This command changes the mode to config-mac-addr-grp, in which you can add or remove a MAC address or OUI from the group.

You can specify a list of MACs or OUIs, or a range of OUIs (maximum of 5 in the range).

Examples The following example shows how to configure **testGroup** as a trigger:

```
Switch(config)# macro auto mac-address-group testGroup
Switch(config-addr-grp-mac)# mac-address list 1111.1111.1111 2222.2222.2222
Switch(config-addr-grp-mac)# exit
Switch(config)# exit
```

Related Commands	Command	Description
	macro auto execute (built-in function)	Changes built-in function default values or to map user-defined triggers to built-in functions, and to pass the parameter values.
	macro auto execute (remotely-defined trigger)	Maps a trigger to a remotely defined functions.
	macro auto execute (user-defined function)	Maps a trigger to a user-defined function.
	macro auto global processing	Enables Auto Smartports on a switch.
	macro auto processing	Enables Auto SmartPorts macros on a specific interface.
	macro auto sticky	Specifies not to remove configurations applied by ASP across link flaps and device removal.
	shell trigger	Creates a user defined trigger.

macro auto monitor

To enable the device classifier, use the **macro auto monitor** global configuration command. Use the **no** form of this command to disable the device classifier.

macro auto monitor

no macro auto monitor

Syntax Description This command has no arguments or keywords.

Command Default Device classifier is enabled.

Command Modes Global configuration

Command History	Release	Modification
	Release IOS XE 3.3.0 SG (15.1(1)SG)	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines Use the **no macro auto monitor** global configuration command to disable the device classifier. You cannot disable the device classifier while it is being used by features such as ASP.

Examples The following example shows how to enable the ASP device classifier on a switch:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# macro auto monitor
Switch(config)# end
```

Related Commands	Command	Description
	show macro auto monitor clients	Displays the clients using the device classifier facility on the switch.
	show macro auto monitor device	Displays the devices connected to a switch, along with their properties and classifications.
	show macro auto monitor type	Displays all the device types known to the device classification agent.

macro auto processing



Note

Only use this command when Auto SmartPorts (ASP) is enabled globally; when ASP is disabled globally, interface-level control has no effect.

Use the **macro auto processing** interface configuration command to enable ASP macros on a specific interface. Use the **no** form of this command to disable ASP on a specific interface before ASP is enabled globally.

macro auto processing [fallback cdp] [fallback lldp]

no macro auto processing [fallback cdp] [fallback lldp]

Syntax Description

fallback cdp	Specifies as CDP as the fallback mechanism.
fallback lldp	Specifies as LLDP as the fallback mechanism.

Command Default

Fallback mechanism is CDP.

Command Modes

Interface level configuration

Command History

Release	Modification
12.2(54)SG	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

The **no macro auto processing** command should be configured on all interfaces where ASP is not desirable (such as Layer 3 and EtherChannel interfaces) before ASP is enabled globally.

At the interface level, the default fallback mechanism is CDP. To change the mechanism to LLDP, enter the **no macro auto processing fallback cdp** command, followed by the **macro auto processing fallback lldp** command.

Examples

The following example shows how to enable the feature on an interface:

```
Switch(config)# interface Gi3/1
Switch(config-if)# macro auto processing
```

Related Commands

Command	Description
macro auto execute (built-in function)	Configures mapping from an event trigger to a built-in macro.
shell trigger	Creates a user defined trigger.
show shell functions	Displays configurations included for all the builtin functions including user created and built-in functions.

Command	Description
show shell triggers	Displays detail for all supported user created and built-in triggers.
macro auto execute (built-in function)	Changes built-in function default values or to map user-defined triggers to built-in functions, and to pass the parameter values.
macro auto execute (remotely-defined trigger)	Maps a trigger to a remotely defined functions.
macro auto execute (user-defined function)	Maps a trigger to a user-defined function.
macro auto global processing	Enables Auto Smartports on a switch.

macro auto sticky

Use the **macro auto sticky** configuration to specify not to remove configurations applied by ASP across link flaps and device removal.

macro auto sticky

Syntax Description	This command has no arguments or keywords.	
Command Default	Not sticky (macros are removed)	
Command Modes	Global configuration	
Command History	Release	Modification
	12.2(54)SG	This command was introduced on the Catalyst 4500 series switch.
Usage Guidelines	This command enables you to avoid unnecessary removal of ASP configurations when a feature intentionally shuts down a link (like EnergyWise, which shuts down inactive links to save energy). When such a feature is enabled, you don't want ASP macros to be applied and removed unnecessarily. So you configure the sticky feature.	
Examples	The following example shows how to specify not to remove configurations: <pre>Switch(config)# macro auto sticky</pre>	
Related Commands	Command	Description
	macro auto execute (built-in function)	Changes built-in function default values or to map user-defined triggers to built-in functions, and to pass the parameter values.
	macro auto execute (remotely-defined trigger)	Maps a trigger to a remotely defined functions.
	macro auto execute (user-defined function)	Maps a trigger to a user-defined function.
	macro auto global processing	Enables Auto Smartports on a switch.
	macro auto processing	Enables Auto SmartPorts macros on a specific interface.
	shell trigger	Creates a user defined trigger.

macro global apply cisco-global

To apply the system-defined default template to the switch, use the **macro global apply cisco-global** global configuration command on the switch stack or on a standalone switch.

macro global apply cisco-global

Syntax Description This command has no keywords or variables.

Command Default This command has no default setting.

Command Modes Global configuration mode

Command History	Release	Modification
	12.2(31)SG	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 gsg-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.

Command Default This command has no default setting.

Command Modes Global configuration mode

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

Examples The following 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

<i>text</i>	Enters a description about the macros that are applied to the switch.
-------------	---

Command Default

This command has no default setting.

Command Modes

Global configuration mode

Command History

Release	Modification
12.2(31)SG	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

The following example shows how to add a description to a switch:

```
Switch(config)# macro global description udld aggressive mode enabled
```

You can verify your settings by entering the **show parser macro description** privileged EXEC command.

Related Commands

Command	Description
macro 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 two supervisor engines, use the **main-cpu** command.

main-cpu

Syntax Description This command has no arguments or keywords.

Command Default This command has no default settings.

Command Modes Redundancy mode

Command History	Release	Modification
	12.1(12c)EW	This command was introduced on the Catalyst 4500 series switch. (Catalyst 4507R only).

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 configuration between the primary and secondary route processors based on the primary configuration. In addition, you can use all of the redundancy commands that are applicable to the main CPU.

Examples The following example shows how to reenable the default automatic synchronization feature using the auto-sync standard command to synchronize the startup-config and config-register configuration of the active supervisor engine with the standby supervisor engine. The updates for the boot variables are automatic and cannot be disabled.

```
Switch(config)# redundancy
Switch(config-red)# main-cpu
Switch(config-r-mc)# auto-sync standard
Switch(config-r-mc)# end
Switch# copy running-config startup-config
Switch#
```

Related Commands	Command	Description
	auto-sync	Enables automatic synchronization of the configuration files in NVRAM.

match

To specify a match clause by selecting one or more ACLs for a VLAN access-map sequence, use the **match** subcommand. To remove the match clause, use the **no** form of this command.

```
match {ip address {acl-number | acl-name}} | {mac address acl-name}
```

```
no match {ip address {acl-number | acl-name}} | {mac address acl-name}
```



Note

If a match clause is not specified, the action for the VLAN access-map sequence is applied to all packets. All packets are matched against that sequence in the access map.

Syntax Description

ip address <i>acl-number</i>	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 <i>acl-name</i>	Selects an IP ACL by name.
mac address <i>acl-name</i>	Selects one or more MAC ACLs for a VLAN access-map sequence.

Command Default

This command has no default settings.

Command Modes

VLAN access-map mode

Command History

Release	Modification
12.1(12c)EW	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

The following example shows how to define a match clause for a VLAN access map:

```
Switch(config)# vlan access-map ganymede 10
Switch(config-access-map)# match ip address 13
Switch(config-access-map)#
```

Related Commands	Command	Description
	show vlan access-map	Displays the contents of a VLAN access map.
	vlan access-map	Enters VLAN access-map command mode to create a VLAN access map.

match (class-map configuration)

To define the match criteria for a class map, use the **match** class-map configuration command. To remove the match criteria, use the **no** form of this command.

```
match { access-group acl-index-or-name | cos cos-list | [ip] dscp dscp-list | [ip] precedence
ip-precedence-list | qos-group value | protocol [ip | ipv6 | arp]
```

```
no match { access-group acl-index-or-name | cos cos-list | [ip] dscp dscp-list | [ip] precedence
ip-precedence-list | qos-group value | protocol [ip | ipv6 | arp]
```

Syntax Description					
access-group <i>acl-index-or-name</i>	Number or name of an IP standard or extended access control list (ACL) or MAC ACL. For an IP standard ACL, the ACL index range is 1 to 99 and 1300 to 1999. For an IP extended ACL, the ACL index range is 100 to 199 and 2000 to 2699.				
cos <i>cos-list</i>	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 <i>dscp-list</i>	(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 <i>ip-precedence-list</i>	(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 <i>value</i>	Specifies the internally generated qos-group value assigned to a packet on the input qos classification.				
protocol ip	Specifies IP in the Ethernet header. 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. Though visible in the command-line help strings the only protocol types supported are IP, IPv6, and ARP.				
protocol arp	Specifies ARP in the Ethernet header. Though visible in the command-line help strings the only protocol types supported are IP, IPv6, and ARP.				
Command Default	No match criteria are defined.				
Command Modes	Class-map configuration mode				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.1(8a)EW</td> <td>This command was introduced on the Catalyst 4500 series switches.</td> </tr> </tbody> </table>	Release	Modification	12.1(8a)EW	This command was introduced on the Catalyst 4500 series switches.
Release	Modification				
12.1(8a)EW	This command was introduced on the Catalyst 4500 series switches.				

Release	Modification
12.2(40)SG	Support extended to Supervisor Engine 6-E and the Catalyst 4900M chassis.
12.2(46)SG	Added support for the match protocol arp command on the Supervisor Engine 6-E and Catalyst 4900M 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 ip dscp dscp-list** or the **match ip precedence ip-precedence-list** command, you can enter a mnemonic name for a commonly used value. For example, you can enter the **match ip dscp af11** command, which is the same as entering the **match ip dscp 10** command. You can enter the **match ip precedence critical** command, which is the same as entering the **match ip precedence 5** command. For a list of supported mnemonics, enter the **match ip dscp ?** or the **match ip precedence ?** command to see the command-line help strings.

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 cos cos-list**, **match ip 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 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 2-96](#).

Examples

The following example shows how to create a class map called class2, which matches all the inbound traffic with DSCP values of 10, 11, and 12:

```
Switch# configure terminal
Switch(config)# class-map class2
Switch(config-cmap)# match ip dscp 10 11 12
Switch(config-cmap)# exit
Switch#
```

The following example shows how to create a class map called class3, 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 class3
Switch(config-cmap)# match ip precedence 5 6 7
Switch(config-cmap)# exit
Switch#
```

The following example shows how to delete the IP-precedence match criteria and to classify traffic using acl1:

```
Switch# configure terminal
Switch(config)# class-map class2
Switch(config-cmap)# match ip precedence 5 6 7
Switch(config-cmap)# no match ip precedence
Switch(config-cmap)# match access-group acl1
Switch(config-cmap)# exit
Switch#
```

The following 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 af21
Switch(config-cmap)# match protocol ipv6
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 treat flows with a unique source or destination address as new flows, use the **match flow ip** command. To disable this function, use the **no** form of this command.

```
match flow ip {source-address [ip destination-address ip protocol L4 source-address L4 destination-address] | destination-address}
```

```
no match flow ip {source-address [ip destination-address ip protocol L4 source-address L4 destination-address] | destination-address}
```

Syntax Description

source-address	Establishes a new flow from a flow with a unique IP source address.
ip destination-address ip protocol L4 source-address L4 destination-address	(Optional) Comprises the full flow keyword; treats each flow with unique IP source, destination, protocol, and Layer 4 source and destination address as a new flow.
destination-address	Establishes a new flow from a flow with a unique IP destination address.

Command Default

This command has no default settings..

Command Modes

class-map configuration submenu

Command History

Release	Modification
12.2(25)EW	This command was introduced on the Catalyst 4500 series switch.
12.2(25)SG	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 a flow-based policy map as a child to an aggregate policy map, use the **service-policy** command.



Note

The **match flow** command is available on the Catalyst 4500 series switch only when Supervisor Engine 6-E or 6L-E is present.

Examples

The following 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#
Switch# show class-map c1
Class Map match-all c1 (id 2)
  Match flow ip source-address
Switch#
```

The following 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-c)# police 1000000 9000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet6/1
Switch(config-if)# service-policy input p1
Switch(config-if)# end
Switch# write memory

Switch# show policy-map interface
FastEthernet6/1

Service-policy input: p1

Class-map: c1 (match-all)
  15432182 packets
  Match: flow ip source-address
  police: Per-interface
    Conform: 64995654 bytes Exceed: 2376965424 bytes

Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets
Switch#
```


The following example shows two active 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 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 destination-address
Switch(config-cmap)# exit
Switch(config)# policy-map p1
Switch(config-pmap)# class c1
Switch(config-pmap-c)# police 1000000 9000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface 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)
  2965072 packets
  Match: flow ip destination-address
  police: Per-interface
    Conform: 6105636 bytes Exceed: 476652528 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:

SrcIp	DstIp	IpProt	SrcL4Port	DstL4Port
192.168.10.10	192.168.20.20	20	6789	81
192.168.10.10	192.168.20.20	20	6789	21

With 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 because they have the same source and destination address.

```
Switch# conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# class-map c1
Switch(config-cmap)# match flow ip source-address ip destination-address ip protocol 14
source-port 14 destination-port
Switch(config-cmap)# exit
Switch(config)# policy-map p1
Switch(config-pmap)# class c1
Switch(config-pmap-c)# police 1000000 9000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastEthernet 6/1
```

```

Switch(config-if)# service-policy input p1
Switch(config-if)# end
Switch# write memory
Switch# show policy-map interface
FastEthernet6/1

class-map c1
  match flow ip source-address ip destination-address ip protocol 14 source-port 14
  destination-port
!
  policy-map p1
    class c1
      police 1000000 bps 9000 byte conform-action transmit exceed-action drop
!
interface FastEthernet 6/1
  service-policy input p1

Switch# show class-map c1
Class Map match-all c1 (id 2)
  Match flow ip source-address ip destination-address ip protocol 14 source-port 14
  destination-port

Switch# show policy-map p1
Policy Map p1
  Class c1
    police 1000000 bps 9000 byte conform-action transmit exceed-action drop

Switch# show policy-map interface
FastEthernet6/1

  Service-policy input: p1

    Class-map: c1 (match-all)
      15432182 packets
      Match: flow ip source-address ip destination-address ip protocol 14 source-port 14
  destination-port
      police: Per-interface
        Conform: 64995654 bytes Exceed: 2376965424 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.

Command Default Auto-MDIX is enabled.

Command Modes Interface configuration mode

Command History	Release	Modification
	12.2(31)SGA	This command was introduced on the Catalyst 4500 series switch.
	12.2(46)SG	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-X4124-RJ45, WS-X4148-RJ45 (hardware revision 3.0 or higher), and WS-X4232-GB-RJ45 (hardware revision 3.0, or higher), WS-X4920-GE-RJ45, and WS-4648-RJ45V+E (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 turned off using an **mdix** CLI command include: WS-X4448-GB-RJ45, WS-X4548-GB-RJ45, WS-X4424-GB-RJ45, and WS-X4412-2GB-T.

Linecards that cannot support auto-MDIX functionality, either by default or CLI commands, include: WS-X4548-GB-RJ45V, WS-X4524-GB-RJ45V, WS-X4506-GB-T, WS-X4148-RJ, WS-X4248-RJ21V, WS-X4248-RJ45V, WS-X4224-RJ45V, and WS-X4232-GB-RJ.

When you enable auto-MDIX on an interface, you must also set the interface speed to be autonegotiated so that the feature operates correctly.

When auto-MDIX (and autonegotiation of speed) is enabled on one or both of connected interfaces, link up occurs even if the cable type (straight-through or crossover) is incorrect.

Examples The following example shows how to enable auto MDIX on a port:

```
Switch# configure terminal
Switch(config)# interface FastEthernet6/3
Switch(config-if)# speed auto
Switch(config-if)# mdix auto
Switch(config-if)# end
```

Related Commands	Command	Description
	speed	Configures the interface speed.
	show interfaces	Displays traffic on a specific interface.
	show interfaces (virtual switch)	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	Parameter	Description
	rj45	Uses the RJ-45 connector.
	sfp	Uses the SFP connector.

Command Default sfp

Command Modes Interface configuration mode

Command History	Release	Modification
	12.2(20)EWA	This command was introduced for the WS-X4306-GB-T module and the WS-X4948 chassis.

Usage Guidelines This command is supported on all ports on the WS-X4306-GB-T module and ports 1/45-48 on the WS-X4948 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 The following example shows how to configure port 5/45 on a WS-X4948 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.

Command Default

If you are upgrading the current supervisor engine from Cisco IOS Release 12.2(18)EW or an earlier release to 12.2(20)EWA, and the RPR mode has been saved to the startup configuration, both supervisor engines will continue to operate in RPR mode after the software upgrade. To use SSO mode, you must manually change the redundancy mode to SSO.

Command Modes

Redundancy configuration mode

Command History

Release	Modification
12.2(20)EWA	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

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

The following example shows how to set the redundancy mode to SSO:

```
Switch(config)# redundancy
Switch(config-red)# mode sso
Switch(config-red)#
```

Related Commands

Command	Description
<code>redundancy</code>	Enters the redundancy configuration mode.
<code>redundancy force-switchover</code>	Forces a switchover from the active to the standby supervisor engine.
<code>show redundancy</code>	Displays redundancy facility information.
<code>show running-config</code>	Displays the running configuration of a switch.

monitor capture {access-list | class-map}

To specify an access list or class map as the core filter, use the **monitor capture** {**access-list** | **class-map**} command. To remove the filter, use the **no** form of this command.

monitor capture *name* {**access-list** *name* | **class-map** *name*}

no monitor capture *name* {**access-list** *name* | **class-map** *name*}

Syntax Description	<i>name</i>	Specifies a capture point.
	access-list <i>name</i>	Specifies access list name
	class-map <i>name</i>	Specifies class map name

Command Default None

Command Modes Privileged EXEC mode

Command History	Release	Modification
	IOS XE 3.3.0SG/ 15.1(1)SG	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines The access list or class map is defined with configuration commands. The access list or class map should be defined prior to entering the **monitor capture** command. We can specify the core filter as a class map, access list, or an explicit in-line filter. If the filter has already been specified when you enter the **monitor capture** command, it replaces the older one.

Examples The following example shows how to define a core system filter using an existing ACL or class-map:

```
Switch# monitor capture mycap filter access-list myacl
```

```
Switch# monitor capture mycap filter class-map mycm
```

```
Switch# no monitor capture mycap filter class-map mycm
```


monitor capture [clear | export]

To clear capture buffer contents or to store the packets to a file, use the **monitor capture [clear | export filename]** command.

monitor capture *name* [**clear**] [**export** *filename*]

Syntax Description		
<i>name</i>		Specifies a capture point.
clear		Clears all the packets in the capture buffer.
export <i>filename</i>		Store all the packets in capture buffer to a .pcap file.

Command Default none

Command Modes Privileged EXEC mode

Command History	Release	Modification
	IOS XE 3.3.0SG/15.1(1)SG	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines The **clear** option empties the capture buffer and the **export** option stores the packets in the capture buffer to the file. You should use these commands only when the storage destination is a capture buffer. These commands are usable either during capture or when it has stopped either because one or more end conditions has been met or you entered the **stop** command. If you enter the **clear** command after the capture has stopped, further **export** (or **decode**) and **display** commands have no impact because the buffer has no packets.

Examples The following example shows how to associate or disassociate a capture file:

```
Switch# monitor capture mycap export bootflash:mycap.pcap
Switch# monitor capture mycap clear
```

monitor capture [interface | vlan | control-plane]

To specify one or more attachment points with direction, use the **monitor capture** [interface | vlan | control-plane] command. To remove the attachment point, use the **no** form of this command.

monitor capture *name* [{**interface name** | **vlan num** | **control-plane**} {**in** | **out** | **both**}]

no monitor capture *name* [{**interface name** | **vlan num** | **control-plane**} {**in** | **out** | **both**}]

Syntax Description		
	<i>name</i>	Specifies a capture point.
	interface name	Specifies an interface. Interface range is allowed.
	vlan num	Specifies a VLAN.
	control-plane	Specifies control plane.
	input output both	Specific traffic direction.

Command Default None

Command Modes Privileged EXEC mode

Command History	Release	Modification
	IOS XE 3.3.0SG/ 15.1(1)SG	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines Specifies one or more attachment points with direction. We can specify a range of interfaces also. The command can be repeated as many times as needed to add multiple attachment points. We need to mention at least one attachment point. For VLAN, the direction has to be set to both.

Examples The following example shows how to add an attachment point:

```
Switch# monitor capture mycap interface gigabitEthernet 3/1 in
```

The following example shows how to remove an attachment point:

```
Switch# no monitor capture mycap interface gigabitEthernet 3/1 in
```

monitor capture file location buffer-size

To specify the capture destination, use the **monitor capture** command. To remove the details, use the **no** form of this command.

```
monitor capture name [[file location filename [buffer-size <1-100>] [ring <2-10>] [size <1-100>]] | [buffer [circular] size <1-100>]]
```

```
no monitor capture name [file | buffer]
```

Syntax Description

file location <i>filename</i>	Specifies filename of location.
buffer-size <1-100>	Specifies bufer size in MB.
ring <2-10>	Specifies number of files.
size <1-100>	Specifies the file size.
buffer [circular] size <1-100>	Specifies that the capture destination is a buffer. By default, the mode is linear. The keyword circular sets the buffer mode to circular. The keyword size specifies the buffer size.

Command Default

The default buffer size is one MB.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
IOS XE 3.3.0SG/ 15.1(1)SG	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

The capture destination can be a file in storage disk or a memory buffer. This command specifies the parameters related to packet storage.

The **file** option specifies that the packets must be stored to a file. To reduce or avoid any loss in packet capture, you can use the **buffer-size** option. The capture and store operations require more CPU, limiting the capture throughput.

You can increase the throughput by triggering **lock-step** mode, wherein the packets are first captured in the buffer. Within this mode, the “duration” parameter defines the capture duration. Once the buffer is full or the duration closes, the buffer is written to the file, greatly increasing the capture throughput. The lock-step mode is automatically triggered by specifying the buffer size to 32MB or higher.

The size of the capture file can be limited with the **size** option. The file location must one of the following:

- Internal bootflash (bootflash:)
- External flash (slot0:)
- USB (usb0:)

Do not specify any other devices.

The destination file can be a ring of files rather than a single file. The **ring** option specifies the number of files in the ring whereas **size** specifies the total size of all the files. In ring file mode, when the file size limit has reached, it accommodates space for new packets by removing the oldest file.

If the capture destination is a buffer, you must use the **show** command to decode and display the packets from the buffer. If the circular option is specified, capture continues until you explicitly issue the **stop** command. If no space exists in the buffer, oldest packet(s) are removed to accommodate the new ones. If the **circular** option is not provided, newer packets are discarded when the capture buffer is full.

Examples

The following example usages show how to specify a file or a ring of files as the capture destination:

```
Switch# monitor capture mycap associate buffer-size 1000000file location
bootflash:mycap.pcap
Switch# monitor capture mycap file location bootflash:mycap.pcap size 40
Switch# monitor capture mycap file location bootflash:mycap.pcap ring 4 size 40
Switch# monitor capture mycap file location bootflash:mycap.pcap buffer-size 8
Switch# monitor capture mycap file location bootflash:mycap.pcap ring 4 size 40
buffer-size 16
Switch# no monitor capture mycap file
```

The following example shows how to setup capture in lock-step mode:

```
Switch# monitor capture mycap file location bootflash:mycap.pcap buffer-size 64
Switch# no monitor capture mycap file
```

The following example shows how to make a circular buffer as the capture destination and operate on the buffer:

```
Switch# monitor capture mycap int gi 3/1 in match ipv4 any any
Switch# monitor capture mycap buffer circular size 1
Switch# monitor capture mycap start
Switch#
Switch# sh monitor capture mycap buffer
0.000000 10.1.1.164 -> 20.1.1.2      UDP Source port: 20001 Destination port: 20002
1.000000 10.1.1.165 -> 20.1.1.2      UDP Source port: 20001 Destination port: 20002
2.000000 10.1.1.166 -> 20.1.1.2      UDP Source port: 20001 Destination port: 20002
3.000000 10.1.1.167 -> 20.1.1.2      UDP Source port: 20001 Destination port: 20002
4.000000 10.1.1.168 -> 20.1.1.2      UDP Source port: 20001 Destination port: 20002
5.000000 10.1.1.169 -> 20.1.1.2      UDP Source port: 20001 Destination port: 20002
6.000000 10.1.1.170 -> 20.1.1.2      UDP Source port: 20001 Destination port: 20002
7.000000 10.1.1.171 -> 20.1.1.2      UDP Source port: 20001 Destination port: 20002
8.000000 10.1.1.172 -> 20.1.1.2      UDP Source port: 20001 Destination port: 20002
9.000000 10.1.1.173 -> 20.1.1.2      UDP Source port: 20001 Destination port: 20002
10.000000 10.1.1.174 -> 20.1.1.2     UDP Source port: 20001 Destination port: 20002
11.000000 10.1.1.175 -> 20.1.1.2     UDP Source port: 20001 Destination port: 20002
12.000000 10.1.1.176 -> 20.1.1.2     UDP Source port: 20001 Destination port: 20002
```

```
Switch# sh monitor capture mycap buffer detailed
Frame 1: 256 bytes on wire (2048 bits), 256 bytes captured (2048 bits)
Arrival Time: Apr 12, 2012 10:59:06.255983000 PDT
Epoch Time: 1334253546.255983000 seconds
[Time delta from previous captured frame: 0.000000000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 0.000000000 seconds]
Frame Number: 1
Frame Length: 256 bytes (2048 bits)
Capture Length: 256 bytes (2048 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ip:udp:data]
```

```

Ethernet II, Src: 00:00:00:00:03:01 (00:00:00:00:03:01), Dst: 54:75:d0:3a:85:3f
(54:75:d0:3a:85:3f)
  Destination: 54:75:d0:3a:85:3f (54:75:d0:3a:85:3f)
    Address: 54:75:d0:3a:85:3f (54:75:d0:3a:85:3f)
      .... 0 .... = IG bit: Individual address (unicast)
      .... 0 .... = LG bit: Globally unique address (factory default)
  Source: 00:00:00:00:03:01 (00:00:00:00:03:01)
    Address: 00:00:00:00:03:01 (00:00:00:00:03:01)
      .... 0 .... = IG bit: Individual address (unicast)
      .... 0 .... = LG bit: Globally unique address (factory default)
...
Switch# sh monitor capture mycap buffer dump
0.000000 10.1.1.164 -> 20.1.1.2 UDP Source port: 20001 Destination port: 20002

0000 54 75 d0 3a 85 3f 00 00 00 00 03 01 08 00 45 00 Tu...?.....E.
0010 00 ee 00 00 00 00 40 11 59 58 0a 01 01 a4 14 01 .....@.YX.....
0020 01 02 4e 21 4e 22 00 da 6e 13 00 01 02 03 04 05 ..N!N".n.....
0030 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 .....
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 ..... !"#$$%
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 &'()*+,-./012345
0060 36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45 6789:;<=>?@ABCDE
0070 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 FGHIJKLMNOPQRSTU
0080 56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 VWXYZ[\]^_`abcde
0090 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 fghijklmnopqrstu
00a0 76 77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85 vwxyz{|}~.....
00b0 86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95 .....
00c0 96 97 98 99 9a 9b 9c 9d 9e 9f a0 a1 a2 a3 a4 a5 .....
00d0 a6 a7 a8 a9 aa ab ac ad ae af b0 b1 b2 b3 b4 b5 .....
00e0 b6 b7 b8 b9 ba bb bc bd be bf c0 c1 c2 c3 c4 c5 .....
00f0 c6 c7 c8 c9 ca cb cc cd ce cf d0 d1 63 24 51 ee .....c$Q.

1.000000 10.1.1.165 -> 20.1.1.2 UDP Source port: 20001 Destination port: 20002
...
Switch# monitor capture mycap clear
Switch# sh monitor capture mycap buffer detailed
...
Switch# monitor capture mycap stop

```

monitor capture limit

To specify capture limits, use the **monitor capture limit** command. To remove the limits, use the **no** form of this command.

monitor capture *name* **limit** { **duration** *seconds* } [**packet-length** *size*] [**packets** *num*]

no monitor capture *name* **limit** [**duration**] [**packet-length**] [**packets**]

Syntax Description

<i>name</i>	Specifies a capture point.
duration <i>seconds</i>	Specifies duration in seconds.
packet-length <i>size</i>	Specifies packet length. If the actual packet is longer, only the first <i>size</i> bytes are stored.
packets <i>num</i>	Specifies number of packets to be processed.

Command Default

Entire packet is processed if packet-length is not specified.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
IOS XE 3.3.0SG/ 15.1(1)SG	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

Specifies session duration, packet segment length and number of packets to be stored

Examples

The following example shows how to associate/disassociate a capture file:

```
Switch# monitor capture mycap limit duration 10
```

```
Switch# monitor capture mycap limit packet-length 128
```

```
Switch# monitor capture mycap limit packets 100
```

```
Switch# no monitor capture mycap limit duration packet-length packets
```

```
Switch# monitor capture mycap limit duration 10 packet-length 128 packets 100
```

```
Switch# no monitor capture mycap limit
```

monitor capture mycap match

To define an explicit in-line core filter, use the **monitor capture mycap match** command. To remove it, use the **no** form of this command.

```
Switch# [no] monitor capture mycap match {any | mac mac-match-string | ipv4
ipv4-match-string | ipv6 ipv6-match-string}
```

To use a filter for MAC, use the format below

```
Switch# [no] monitor capture mycap match mac {src-mac-addr src-mac-mask | any | host
src-mac-addr} | {dest-mac-addr dest-mac-mask | any | host dest-mac-addr}
```

To use a filter for IPv4/IPv6, use one of the formats below

```
Switch# [no] monitor capture mycap match {ipv4 | ipv6} [src-prefix/length | any | host
src-ip-addr] [dest-prefix/length | any | host dest-ip-addr]
```

```
Switch# [no] monitor capture mycap match {ipv4 | ipv6} proto {tcp | udp}
[src-prefix/length | any | host src-ip-addr] [eq | gt | lt | neq <0-65535>]
[dest-prefix/length | any | host dest-ip-addr] [eq | gt | lt | neq <0-65535>]
```

Syntax Description

any	Specifies “any” packet
mac <i>mac-match-string</i>	Specifies a Layer 2 packet
ipv4 <i>ipv4-match-string</i>	Specifies an IPv4 packet
ipv6 <i>ipv6-match-string</i>	Specifies an IPv6 packet
match <i>name</i>	Specifies a capture point
src-mac-addr	Specifies source MAC address
src-mac-mask	Specifies source MAC mask
host <i>src-mac-addr</i>	Source (or destination) MAC (or IP) address
<i>dest-mac-addr</i>	Specifies a destination MAC address
<i>dest-mac-mask</i>	Specifies a destination MAC mask
host <i>dest-mac-addr</i>	Specifies a source (or destination) MAC (or IP) address
<i>src-prefix/length</i>	Specifies a source prefix / length
host <i>src-ip-addr</i>	Specifies a host source IP address
<i>dest-prefix/length</i>	Specifies a destination prefix / length
host <i>dest-ip-addr</i>	Specifies a source (or destination) MAC (or IP) address
proto { tcp udp }	Specifies the protocol to be used
{ eq gt lt neq } <0-65535>	Specifies Equal, Greater Than, Less than, Not Equal To

Command Default

none

Command Modes

Privileged EXEC mode

Command History

Release	Modification
IOS XE 3.3.0SG/ 15.1(1)SG	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

You can specify the core filter as a class map, access list, or an explicit in-line filter. If the filter has already been specified when you enter this command, it replaces the older one.

The explicit, in-line filter is intended as a simple way to specify a core filter. In certain situations, you must go through the approval process to change a configuration, which could be time-consuming. Although explicit filters simplify this process, be aware that support is more extensive for access list and class maps.

You can capture IPv4, IPv6, MAC, or “any” traffic by specifying the appropriate keywords. Depending on the traffic type, the usage varies. For a MAC, you can specify an address or prefix. For IPv4 or IPv6, you can match on several fields. For source or destination ports, several operators are supported.

Examples

The following example usages show how to set or remove an explicit filter:

```
Switch# monitor capture mycap match any

Switch# monitor capture mycap match mac any any

Switch# monitor capture mycap match mac host 0000.0a01.0102 host 0000.0a01.0103

Switch# monitor capture mycap match ipv4 any any

Switch# monitor capture mycap match ipv4 host 10.1.1.2 host 20.1.1.2

Switch# monitor capture mycap match ipv4 proto udp 10.1.1.0/24 eq 20001 20.1.1.0/24 eq
20002

Switch# monitor capture mycap match ipv4 proto udp 10.1.1.2/24 eq 20001 any

Switch# no monitor capture mycap match
```


monitor capture start

To start or stop a capture point, use the **monitor capture** command.

```
monitor capture name start [capture-filter filter-string] [display [display-filter filter-string]]
[brief | detailed | dump | stop]
```

Syntax Description

<i>name</i>	Specifies a capture point.
start	Starts the Wireshark session and captures live traffic.
capture-filter <i>filter-string</i>	Specifies the capture filter.
display [display-filter <i>filter-string</i>]	Decodes and displays the filter. Optionally, specifies the display filter.
[brief detailed dump]	Specifies the display mode. Default is brief .
stop	Stops the Wireshark session.

Command Default

The default display mode is **brief**.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
IOS XE 3.3.0SG/ 15.1(1)SG	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

These commands start or stop a capture session, assuming all mandatory parameters are specified. We must ensure that resources like CPU and memory are available before starting the session. Because the capture and display filters must observe the Wireshark display filter syntax, ensure that the filters are accurate (for example, specify the filters within double-quotes).

If the packets will be stored and displayed, do not use display filter; in this mode, if a packet is stored, it is displayed as well. If you provide a display filter, it is ignored.

If a capture filter is specified, the capture is limited to 65536 packets. In this release, there is a limitation that the timestamp will be incorrect when we use a capture filter.

Examples

The following example shows how to start or stop a capture session in various modes:

```
Switch# monitor capture mycap int gi 3/1 in match ipv4 any any
Switch# monitor capture mycap file location bootflash:mycap.pcap
Switch# monitor capture mycap limit packets 100 duration 60

Switch# monitor capture mycap start
Switch#
Switch# monitor capture mycap stop
Switch# monitor capture mycap start capture-filter "udp.port == 20001"
Switch# monitor capture mycap stop
```

```
Switch# monitor capture mycap start capture-filter "udp.port == 20001" display
A file by the same capture file name already exists, overwrite?[confirm]
```

```
0.000000    10.1.1.9  -> 20.1.1.2    UDP Source port: 20001 Destination port: 20002
0.000000    10.1.1.10 -> 20.1.1.2    UDP Source port: 20001 Destination port: 20002
0.000000    10.1.1.11 -> 20.1.1.2    UDP Source port: 20001 Destination port: 20002
0.000000    10.1.1.12 -> 20.1.1.2    UDP Source port: 20001 Destination port: 20002
0.000000    10.1.1.13 -> 20.1.1.2    UDP Source port: 20001 Destination port: 20002
0.000000    10.1.1.14 -> 20.1.1.2    UDP Source port: 20001 Destination port: 20002
0.000000    10.1.1.15 -> 20.1.1.2    UDP Source port: 20001 Destination port: 20002
0.000000    10.1.1.16 -> 20.1.1.2    UDP Source port: 20001 Destination port: 20002
0.000000    10.1.1.17 -> 20.1.1.2    UDP Source port: 20001 Destination port: 20002
0.000000    10.1.1.18 -> 20.1.1.2    UDP Source port: 20001 Destination port: 20002
0.000000    10.1.1.19 -> 20.1.1.2    UDP Source port: 20001 Destination port: 20002
0.000000    10.1.1.20 -> 20.1.1.2    UDP Source port: 20001 Destination port: 20002
0.000000    10.1.1.21 -> 20.1.1.2    UDP Source port: 20001 Destination port: 20002
0.000000    10.1.1.22 -> 20.1.1.2    UDP Source port: 20001 Destination port: 20002
0.000000    10.1.1.23 -> 20.1.1.2    UDP Source port: 20001 Destination port: 20002
0.000000    10.1.1.24 -> 20.1.1.2    UDP Source port: 20001 Destination port: 20002
0.000000    10.1.1.25 -> 20.1.1.2    UDP Source port: 20001 Destination port: 20002
0.000000    10.1.1.26 -> 20.1.1.2    UDP Source port: 20001 Destination port: 20002
0.000000    10.1.1.27 -> 20.1.1.2    UDP Source port: 20001 Destination port: 20002
0.000000    10.1.1.28 -> 20.1.1.2    UDP Source port: 20001 Destination port: 20002
0.000000    10.1.1.29 -> 20.1.1.2    UDP Source port: 20001 Destination port: 20002
0.000000    10.1.1.30 -> 20.1.1.2    UDP Source port: 20001 Destination port: 20002
```

```
Switch# monitor capture mycap start capture-filter "udp.port == 20001" display
display-filter "udp.port == 20002"
```

```
%Display-filter cannot be specified when capture is associated to a file. Ignoring
display filter%
```

```
A file by the same capture file name already exists, overwrite?[confirm]
```

```
0.000000    10.1.1.96 -> 20.1.1.2    UDP Source port: 20001 Destination port: 20002
0.000000    10.1.1.97 -> 20.1.1.2    UDP Source port: 20001 Destination port: 20002
0.000000    10.1.1.98 -> 20.1.1.2    UDP Source port: 20001 Destination port: 20002
0.000000    10.1.1.99 -> 20.1.1.2    UDP Source port: 20001 Destination port: 20002
0.000000    10.1.1.100 -> 20.1.1.2    UDP Source port: 20001 Destination port: 20002
0.000000    10.1.1.101 -> 20.1.1.2    UDP Source port: 20001 Destination port: 20002
0.000000    10.1.1.102 -> 20.1.1.2    UDP Source port: 20001 Destination port: 20002
0.000000    10.1.1.103 -> 20.1.1.2    UDP Source port: 20001 Destination port: 20002
0.000000    10.1.1.104 -> 20.1.1.2    UDP Source port: 20001 Destination port: 20002
0.000000    10.1.1.105 -> 20.1.1.2    UDP Source port: 20001 Destination port: 20002
0.000000    10.1.1.106 -> 20.1.1.2    UDP Source port: 20001 Destination port: 20002
0.000000    10.1.1.107 -> 20.1.1.2    UDP Source port: 20001 Destination port: 20002
0.000000    10.1.1.108 -> 20.1.1.2    UDP Source port: 20001 Destination port: 20002
0.000000    10.1.1.109 -> 20.1.1.2    UDP Source port: 20001 Destination port: 20002
```

```
Switch#
```

```
Switch# monitor capture mycap start capture-filter "udp.port == 20001" display
display-filter "udp.port == 20002" detailed
```

```
%Display-filter cannot be specified when capture is associated to a file. Ignoring
display filter%
```

```
A file by the same capture file name already exists, overwrite?[confirm]
```

```
Frame 1: 256 bytes on wire (2048 bits), 256 bytes captured (2048 bits)
```

```
Arrival Time: Dec 31, 1969 17:00:00.000000000 PDT
```

```
Epoch Time: 0.000000000 seconds
```

```
[Time delta from previous captured frame: 0.000000000 seconds]
```

```
[Time delta from previous displayed frame: 0.000000000 seconds]
```

```
[Time since reference or first frame: 0.000000000 seconds]
```

```
Frame Number: 1
```

```
Frame Length: 256 bytes (2048 bits)
```

```
Capture Length: 256 bytes (2048 bits)
```

```
[Frame is marked: False]
```

```

[Frame is ignored: False]
[Protocols in frame: eth:ip:udp:data]
Ethernet II, Src: 00:00:00:00:03:01 (00:00:00:00:03:01), Dst: 54:75:d0:3a:85:3f
(54:75:d0:3a:85:3f)
  Destination: 54:75:d0:3a:85:3f (54:75:d0:3a:85:3f)
    Address: 54:75:d0:3a:85:3f (54:75:d0:3a:85:3f)
      .... 0 .... = IG bit: Individual address (unicast)
      .... 0 .... = LG bit: Globally unique address (factory default)
  Source: 00:00:00:00:03:01 (00:00:00:00:03:01)
    Address: 00:00:00:00:03:01 (00:00:00:00:03:01)
      .... 0 .... = IG bit: Individual address (unicast)
      .... 0 .... = LG bit: Globally unique address (factory default)

```

```

Switch# monitor capture mycap start capture-filter "udp.port == 20001" display dump
A file by the same capture file name already exists, overwrite?[confirm]

```

```

0.000000 10.1.1.6 -> 20.1.1.2 UDP Source port: 20001 Destination port: 20002

0000 54 75 d0 3a 85 3f 00 00 00 00 03 01 08 00 45 00 Tu...?.....E.
0010 00 ee 00 00 00 00 40 11 59 f6 0a 01 01 06 14 01 .....@.Y.....
0020 01 02 4e 21 4e 22 00 da 6e b1 00 01 02 03 04 05 ..N!N".n.....
0030 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 .....
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 ..... !"#$$%
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 &'()*+,-./012345
0060 36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45 6789;:<=>?@ABCDE
0070 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 FGHIJKLMNOPQRSTU
0080 56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 VWXYZ[\]^_`abcde
0090 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 fghijklmnopqrstu
00a0 76 77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85 vwxyz{|}~.....
00b0 86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95 .....
00c0 96 97 98 99 9a 9b 9c 9d 9e 9f a0 a1 a2 a3 a4 a5 .....
00d0 a6 a7 a8 a9 aa ab ac ad ae af b0 b1 b2 b3 b4 b5 .....
00e0 b6 b7 b8 b9 ba bb bc bd be bf c0 c1 c2 c3 c4 c5 .....
00f0 c6 c7 c8 c9 ca cb cc cd ce cf d0 d1 ac 69 6e fd .....in.

```

```

0.000000 10.1.1.7 -> 20.1.1.2 UDP Source port: 20001 Destination port: 20002

```

```

Switch#
Switch# monitor capture mycap start display display-filter "udp.port == 20002"
%Display-filter cannot be specified when capture is associated to a file. Ignoring
display filter%
A file by the same capture file name already exists, overwrite?[confirm]

```

```

0.000000 10.1.1.41 -> 20.1.1.2 UDP Source port: 20001 Destination port: 20002
1.000000 10.1.1.42 -> 20.1.1.2 UDP Source port: 20001 Destination port: 20002
2.000000 10.1.1.43 -> 20.1.1.2 UDP Source port: 20001 Destination port: 20002
3.000000 10.1.1.44 -> 20.1.1.2 UDP Source port: 20001 Destination port: 20002
4.000000 10.1.1.45 -> 20.1.1.2 UDP Source port: 20001 Destination port: 20002
5.000000 10.1.1.46 -> 20.1.1.2 UDP Source port: 20001 Destination port: 20002
5.998993 10.1.1.47 -> 20.1.1.2 UDP Source port: 20001 Destination port: 20002
6.998993 10.1.1.48 -> 20.1.1.2 UDP Source port: 20001 Destination port: 20002
7.998993 10.1.1.49 -> 20.1.1.2 UDP Source port: 20001 Destination port: 20002
8.998993 10.1.1.50 -> 20.1.1.2 UDP Source port: 20001 Destination port: 20002
9.998993 10.1.1.51 -> 20.1.1.2 UDP Source port: 20001 Destination port: 20002
10.998993 10.1.1.52 -> 20.1.1.2 UDP Source port: 20001 Destination port: 20002

```

```

Switch#
Switch# monitor capture mycap start display display-filter "udp.port == 20002" dump
%Display-filter cannot be specified when capture is associated to a file. Ignoring
display filter%
A file by the same capture file name already exists, overwrite?[confirm]

```

```

0.000000 10.1.1.117 -> 20.1.1.2 UDP Source port: 20001 Destination port: 20002

```

```

0000  54 75 d0 3a 85 3f 00 00 00 00 03 01 08 00 45 00  Tu...?.....E.
0010  00 ee 00 00 00 00 40 11 59 87 0a 01 01 75 14 01  .....@.Y....u..
0020  01 02 4e 21 4e 22 00 da 6e 42 00 01 02 03 04 05  ..N!N"...nB.....
0030  06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15  .....
0040  16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  ..... !"#$$%
0050  26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  &'()*+,-./012345
0060  36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45  6789;<=>?@ABCDE
0070  46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55  FGHIJKLMNOPQRSTU
0080  56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65  VWXYZ[\]^_`abcde
0090  66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75  fghijklmnopqrstu
00a0  76 77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85  vwxyz{|}~.....
00b0  86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95  .....
00c0  96 97 98 99 9a 9b 9c 9d 9e 9f a0 a1 a2 a3 a4 a5  .....
00d0  a6 a7 a8 a9 aa ab ac ad ae af b0 b1 b2 b3 b4 b5  .....
00e0  b6 b7 b8 b9 ba bb bc bd be bf c0 c1 c2 c3 c4 c5  .....
00f0  c6 c7 c8 c9 ca cb cc cd ce cf d0 d1 41 0c b4 5d  .....A..]

1.000000  10.1.1.118 -> 20.1.1.2      UDP Source port: 20001  Destination port: 20002

```

```
Switch# no monitor capture mycap file
```

```
Switch# monitor capture mycap start display display-filter "udp.port == 20002" dump
```

```

0.000000  10.1.1.160 -> 20.1.1.2      UDP Source port: 20001  Destination port: 20002

0000  54 75 d0 3a 85 3f 00 00 00 00 03 01 08 00 45 00  Tu...?.....E.
0010  00 ee 00 00 00 00 40 11 59 5c 0a 01 01 a0 14 01  .....@.Y\.....
0020  01 02 4e 21 4e 22 00 da 6e 17 00 01 02 03 04 05  ..N!N"...n.....
0030  06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15  .....
0040  16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  ..... !"#$$%
0050  26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  &'()*+,-./012345
0060  36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45  6789;<=>?@ABCDE
0070  46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55  FGHIJKLMNOPQRSTU
0080  56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65  VWXYZ[\]^_`abcde
0090  66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75  fghijklmnopqrstu
00a0  76 77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85  vwxyz{|}~.....
00b0  86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95  .....
00c0  96 97 98 99 9a 9b 9c 9d 9e 9f a0 a1 a2 a3 a4 a5  .....
00d0  a6 a7 a8 a9 aa ab ac ad ae af b0 b1 b2 b3 b4 b5  .....
00e0  b6 b7 b8 b9 ba bb bc bd be bf c0 c1 c2 c3 c4 c5  .....
00f0  c6 c7 c8 c9 ca cb cc cd ce cf d0 d1 9f 20 8a e5  .....

1.000000  10.1.1.161 -> 20.1.1.2      UDP Source port: 20001  Destination port: 20002

```

```
Switch# monitor capture mycap start display display-filter "udp.port == 20002"
```

```

0.000000  10.1.1.173 -> 20.1.1.2      UDP Source port: 20001  Destination port: 20002
1.000000  10.1.1.174 -> 20.1.1.2      UDP Source port: 20001  Destination port: 20002
2.000000  10.1.1.175 -> 20.1.1.2      UDP Source port: 20001  Destination port: 20002
3.000000  10.1.1.176 -> 20.1.1.2      UDP Source port: 20001  Destination port: 20002
4.000000  10.1.1.177 -> 20.1.1.2      UDP Source port: 20001  Destination port: 20002
5.000000  10.1.1.178 -> 20.1.1.2      UDP Source port: 20001  Destination port: 20002
6.000000  10.1.1.179 -> 20.1.1.2      UDP Source port: 20001  Destination port: 20002
7.000000  10.1.1.180 -> 20.1.1.2      UDP Source port: 20001  Destination port: 20002
8.000000  10.1.1.181 -> 20.1.1.2      UDP Source port: 20001  Destination port: 20002
9.000000  10.1.1.182 -> 20.1.1.2      UDP Source port: 20001  Destination port: 20002
10.000000 10.1.1.183 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
11.000000 10.1.1.184 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
12.000000 10.1.1.185 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002

```

```
Switch# monitor capture mycap start display detailed
```

```
Frame 1: 256 bytes on wire (2048 bits), 256 bytes captured (2048 bits)
Arrival Time: Apr 12, 2012 11:46:54.245974000 PDT
Epoch Time: 1334256414.245974000 seconds
[Time delta from previous captured frame: 0.000000000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 0.000000000 seconds]
Frame Number: 1
Frame Length: 256 bytes (2048 bits)
Capture Length: 256 bytes (2048 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ip:udp:data]
Ethernet II, Src: 00:00:00:00:03:01 (00:00:00:00:03:01), Dst: 54:75:d0:3a:85:3f
(54:75:d0:3a:85:3f)
  Destination: 54:75:d0:3a:85:3f (54:75:d0:3a:85:3f)
    Address: 54:75:d0:3a:85:3f (54:75:d0:3a:85:3f)
      .... 0 .... = IG bit: Individual address (unicast)
      .... 0 .... = LG bit: Globally unique address (factory default)
  Source: 00:00:00:00:03:01 (00:00:00:00:03:01)
    Address: 00:00:00:00:03:01 (00:00:00:00:03:01)
      .... 0 .... = IG bit: Individual address (unicast)
      .... 0 .... = LG bit: Globally unique address (factory default)

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 **no** form of this command.

```
monitor session session {destination interface {FastEthernet interface-number |
GigabitEthernet interface-number} [encapsulation {isl | dot1q}] [ingress [vlan vlan_id]
[learning]]} | {remote vlan vlan_id} | {source { interface {FastEthernet interface-number |
GigabitEthernet interface-number | Port-channel interface-number} } | [vlan vlan_id]
|{remote vlan vlan_id} | {cpu [queue queue_id | acl { input {copy {rx} | error {rx} | forward
{rx} | punt {rx} | rx} } | output {copy {rx} | error {rx} | forward {rx} | punt {rx} | rx} | all
{rx} | control-packet {rx} | esmp {rx} | I2-forward { adj-same-if {rx} | bridge-cpu {rx} |
ip-option {rx} | ipv6-scope-check-fail {rx} | I2-src-index-check-fail {rx} | mcast-rpf-fail
{rx} | non-arpa {rx} | router-cpu {rx} | ttl-expired {rx} | ucast-rpf-fail {rx} | rx} |
I3-forward { forward {rx} | glean {rx} | receive {rx} | rx} mtu-exceeded {rx} |
unknown-port-vlan-mapping {rx} | unknown-sa {rx}}] [, | - | rx | tx | both]} | {filter {ip
access-group [name | id]}{vlan vlan_id [, | - ]} | {packet-type {good | bad}} | {address-type
{unicast | multicast | broadcast} [rx | tx | both]}
```

```
no monitor session session {destination interface {FastEthernet interface-number |
GigabitEthernet interface-number} [encapsulation {isl | dot1q}] [ingress [vlan vlan_id]
[learning]]} | {remote vlan vlan_id} | {source {cpu{both | queue | rx | tx} | interface
{FastEthernet interface-number | GigabitEthernet interface-number | Port-channel
interface-number} } | [vlan vlan_id] |{remote vlan vlan_id} | {cpu [queue queue_id | acl
{input {copy {rx} | error {rx} | forward {rx} | punt {rx} | rx} } | output {copy {rx} | error
{rx} | forward {rx} | punt {rx} | rx} | all {rx} | control-packet {rx} | esmp {rx} | I2-forward
{ adj-same-if {rx} | bridge-cpu {rx} | ip-option {rx} | ipv6-scope-check-fail {rx} |
I2-src-index-check-fail {rx} | mcast-rpf-fail {rx} | non-arpa {rx} | router-cpu {rx} |
ttl-expired {rx} | ucast-rpf-fail {rx} | rx} | I3-forward {forward {rx} | glean {rx} | receive
{rx} | rx} mtu-exceeded {rx} | unknown-port-vlan-mapping {rx} | unknown-sa {rx}}] [, |
- | rx | tx | both]} | {filter {ip access-group [name | id]}{vlan vlan_id [, | - ]} | {packet-type
{good | bad}} | {address-type {unicast | multicast | broadcast} [rx | tx | both]}
```

Syntax Description

<i>session</i>	Number of a SPAN session; valid values are from 1 to 6.
destination	Specifies a SPAN destination.
interface	Specifies an interface.
FastEthernet <i>interface-number</i>	Specifies a Fast Ethernet module and port number; valid values are from 1 to 6.
GigabitEthernet <i>interface-number</i>	Specifies a Gigabit Ethernet module and port number; valid values are from 1 to 6.
encapsulation	(Optional) Specifies the encapsulation type of the destination port.
isl	(Optional) Specifies ISL encapsulation.
dot1q	(Optional) Specifies dot1q encapsulation.
ingress	(Optional) Indicates whether the ingress option is enabled.
vlan <i>vlan_id</i>	(Optional) Specifies the VLAN; valid values are from 1 to 4094.

learning	(Optional) Enables host learning on ingress-enabled destination ports.
remote vlan <i>vlan_id</i>	Specifies an RSPAN source or destination session on a switch.
source	Specifies a SPAN source.
Port-channel <i>interface-number</i>	Specifies a port-channel interface; valid values are from 1 to 64.
cpu	Causes traffic received or sent from the CPU to be copied to the destination of the session.
queue <i>queue_id</i>	(Optional) Specifies that only traffic received on the specific CPU subqueue should be copied to the destination of the session. Valid values are from 1 to 64, or by the following names: all, control-packet, esmp, mtu-exceeded, unknown-port-vlan-mapping, unknown-sa, acl 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, ipv6-scope-check-fail, l2-src-index-check-fail, mcast-rpf-fail, non-arpa, router-cpu, ttl-expired, ucast-rpf-fail, l3-forward, forward, glean, receive.
acl	(Optional) Specifies input and output ACLs; valid values are from 14 to 20.
input	Specifies input ACLs; valid values are from 14 to 16.
error	Specifies the ACL software errors.
log/copy	Specifies packets for ACL logging.
punt	Specifies packets punted due to overflows.
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 exception packets.
bridge-cpu	Specifies packets bridged to CPU.
ip-option	Specifies packets with an IP option.
ipv6-scope-check-fail	Specifies IPv6 packets with scope-check failures.
l2-src-index-check-fail	Specifies IP packets with mismatched SRC MAC and SRC IP addresses.
mcast-rpf-fail	Specifies IPv4/IPv6 multicast RPF failures.
non-arpa	Specifies packets with non-ARPA encapsulation.
router-cpu	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 a low priority.
ucast-rpf-fail	Specifies IPv4/IPv6 Unicast RPF failures.
all	(Optional) all queues.

l3-forward	(Optional) Layer 3 packets.
forward	Specifies special Layer 3 forwards tunnel encapsulation.
glean	Specifies special Layer 3 forwards glean.
receive	Specifies packets addressed to a port.
control-packet	(Optional) Layer 2 control packets.
esmp	(Optional) ESMP packets.
mtu-exceeded	(Optional) Output Layer 3 interface MTU exceeded.
routed	Specifies Layer 3 routed packets.
received	Specifies packets addressed to a port.
rpf-failure	Specifies Multicast RPF failed packets.
unknown-port-vlan-mapping	(Optional) Packets with missing port-VLAN mapping.
unknown-sa	(Optional) Packets with missing source-IP-addresses.
,	(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 access-group	(Optional) Specifies an IP access group filter, either a name or a number.
name	(Optional) Specifies an IP access list name.
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 <i>vlan_id</i>	(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.

Command Default

Received and transmitted traffic, as well as all VLANs, packet types, and address types are monitored on a trunking interface.

Packets are transmitted untagged out the destination port; ingress and learning are disabled.

All packets are permitted and forwarded “as is” on the destination port.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch.
12.1(11b)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 sniffing enhancements was added.
12.1(20)EW	Support for remote SPAN and host 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 Catlyst 4900M 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 first 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. You will also receive an error message if you configure a SPAN session with a source VLAN, and then try to add a source interface to that session. You must first clear any sources for a SPAN session before switching to another type of 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 is 802.1Q. If the encapsulation type is ISL, then no ingress VLAN specification is necessary.

By default, when you enable ingress, no host learning is performed on destination ports. When you enter the **learning** keyword, host learning is performed on the destination port, and traffic to learned hosts is forwarded out 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 **monitor session session source vlan vlan-id** command.

The packet-type filters are supported only in the Rx direction. You can specify both Rx- and Tx-type filters and multiple-type filters at the same time (for example, you can use **good** and **unicast** to only sniff nonerror unicast frames). As with VLAN filters, if you do not specify the type, the session will sniff all packet types.

The **queue** identifier allows sniffing for only traffic that is sent or received on the specified CPU queues. The queues may be identified either by number or by name. The queue names may contain multiple numbered queues for convenience.

Examples

The following example shows how to configure IP access group 100 on a SPAN session:

```
Switch# configure terminal
Switch(config)# monitor session 1 filter ip access-group 100
Switch(config)# end
Switch(config)#
```

The following example shows how to add a source interface to a SPAN session:

```
Switch# configure terminal
Switch(config)# monitor session 1 source interface fa2/3
Switch(config)# end
Switch(config)#
Switch(config)#
Switch(config)#
```

The following example shows how to configure the sources with different directions within a SPAN session:

```
Switch# configure terminal
Switch(config)# monitor session 1 source interface fa2/3 rx
Switch(config)# monitor session 1 source interface fa2/2 tx
Switch(config)# end
```

The following example shows how to remove a source interface from a SPAN session:

```
Switch# configure terminal
Switch(config)# no monitor session 1 source interface fa2/3
Switch(config)# end
```

The following example shows how to limit SPAN traffic to VLANs 100 through 304:

```
Switch# configure terminal
Switch(config)# monitor session 1 filter vlan 100 - 304
Switch(config)# end
```

The following example shows how to configure RSPAN VLAN 20 as the destination:

```
Switch# configure terminal
Switch(config)# monitor session 2 destination remote vlan 20
Switch(config)# end
```

The following example shows how to use queue names and queue number ranges for the CPU as a SPAN source on Supervisor Engine 6-E:

```
Switch# configure terminal
Switch(config)# monitor session 2 source cpu queue control-packet rx
Switch(config)# monitor session 3 source cpu queue 10 rx
Switch(config)# end
```



Note

control-packet is mapped to queue 10.

Related Commands

Command	Description
show monitor	Displays information about the SPAN session.

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.

Command Default

The default settings are as follows:

- Jumbo frames are disabled
- 1500 bytes for all ports

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(13)EW	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 stub-based ports.

The baby giants feature uses the global **system mtu size** command to set the global baby giant MTU. It allows all stub-based port interfaces to support an Ethernet payload size of up to 1552 bytes.

Both the **system mtu** command and the per-interface **mtu** command work on interfaces that can support jumbo frames, but the per-interface **mtu** command takes precedence.

Examples

The following example shows how to specify an MTU of 1800 bytes:

```
Switch(config)# interface GigabitEthernet 1/1
Switch(config-if)# mtu 1800
```

Related Commands

Command	Description
system mtu	Sets the maximum Layer 2 or Layer 3 payload size.

mvr (global configuration)

To enable the multicast VLAN registration (MVR) feature on the switch, use the **mvr** global configuration command without keywords. Use the command with keywords to set the MVR mode for a switch, to configure the MVR IP multicast address, to specify the MVR multicast VLAN, and to set the maximum wait time for a query reply before removing a port from group membership. Use the **no** form of this command to return to the default settings.

mvr [**group** *ip-address* [*count*] | **mode** [**compatible** | **dynamic**] | **querytime** *value* | **vlan** *vlan-id*]

no mvr [**group** *ip-address* | **mode** [**compatible** | **dynamic**] | **querytime** | **vlan** *vlan-id*]

Syntax Description

group <i>ip-address</i>	Statically configures an MVR group IP multicast address on the switch. Use the no form of this command either to remove a statically configured IP multicast address or contiguous addresses, or when no IP address is entered, to remove all statically configured MVR IP multicast addresses.
<i>count</i>	(Optional) Configures multiple contiguous MVR group addresses. The range is 1 to 1500.
mode	(Optional) Specifies the MVR mode of operation. The default is compatible mode.
compatible	Sets MVR mode to disallow dynamic membership joins on source ports.
dynamic	Sets MVR mode to allow dynamic MVR membership on source ports.
querytime <i>value</i>	(Optional) Sets the maximum time to wait for IGMP report memberships on a receiver port. This time applies only to receiver-port leave processing. When an IGMP query is sent from a receiver port, the switch waits for the default or configured MVR querytime for an IGMP group membership report before removing the port from multicast group membership. The value is the response time in units of tenths of a second. The range is 1 to 100; the default is 5 tenths (one-half second). Use the no form of the command to return to the default setting.
vlan <i>vlan-id</i>	(Optional) Specifies the VLAN on which MVR multicast data is to be received. This is also the VLAN to which all the source ports belong. The range is 1 to 4094. The default is VLAN 1.

Command Default

MVR is disabled by default.
The default MVR mode is compatible mode.
No IP multicast addresses are configured on the switch by default.
The default group ip address count is 0.
The default query response time is 5 tenths (one-half) second.
The default multicast VLAN for MVR is VLAN 1.

Command Modes

Global configuration

Command History

Release	Modification
Release IOS XE 3.9.1E	The maximum number of supported MVR groups was increased from 500 to 1500
Release IOS XE 3.5.0E and IOS 15.2(1)E	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

Use the **mvr group** command to statically set all the IP multicast addresses to participate in MVR. Any multicast data sent to a configured multicast address is sent to all the source ports on the switch and to all receiver ports that have registered to receive data on that IP multicast address.

The maximum number of supported MVR groups is 1500.

A hardware entry occurs when there is an IGMP join on a port or when you configure a port to join a group with the **mvr vlan group** interface configuration command.

The **mvr querytime** command applies only to receiver ports.

When operating in compatible mode, MVR does not support IGMP dynamic joins on MVR source ports.

MVR can coexist with IGMP snooping on a switch.

MVR and multicast cannot co-exist on the same switch. If you try to enable MVR while multicast routing or a multicast routing protocol are enabled, your operation is cancelled and you receive an error message. If you enable multicast routing or a multicast routing protocol while MVR is enabled, MVR is disabled and you receive a warning message.

Examples

The following example shows how to enable MVR:

```
Switch(config)# mvr
```

The following example shows how to disable MVR:

```
Switch(config)# no mvr
```

Use the **show mvr** privileged EXEC command to display the current setting for maximum multicast groups.

The following example shows how to configure 228.1.23.4 as an IP multicast address:

```
Switch(config)# mvr group 228.1.23.4
```

The following example shows how to configure ten contiguous IP multicast groups with multicast addresses from 228.1.23.1 to 228.1.23.10:

```
Switch(config)# mvr group 228.1.23.1 10
```

The following example shows how to delete the previously configured ten IP multicast addresses:

```
Switch(config)# no mvr group 228.1.23.1 10
```

The following example shows how to delete all previously configured IP multicast addresses:

```
Switch(config)# no mvr group
```

Use the **show mvr members** privileged EXEC command to display the configured IP multicast group addresses.

The following example shows how to set the maximum query response time as 1 second (10 tenths):

```
Switch(config)# mvr querytime 10
```

The following example shows how to return the maximum query response time to the default setting of one-half second:

```
Switch(config)# no mvr querytime
```

The following example shows how to set VLAN 2 as the multicast VLAN:

```
Switch(config)# mvr vlan 2
```

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

Related Commands	Command	Description
	mvr (interface configuration)	Configures MVR ports.
	show mvr	Displays MVR global parameters or port parameters.
	show mvr interface	Displays the configured MVR interfaces with their type, mode, VLAN, status and Immediate Leave configuration, and can also displays all MVR groups of which the interface is a member.
	show mvr members	Displays all ports that are members of an MVR multicast group; if the group has no members, its status is shown as Inactive.

mvr (interface configuration)

Use the **mvr** interface configuration command to configure a Layer 2 port as a multicast VLAN registration (MVR) receiver or source port, to set the Immediate Leave feature, and to statically assign a port to an IP multicast VLAN and IP address. Use the **no** form of this command to return to the default settings.

```
mvr [immediate | type {receiver | source} | vlan vlan-id {[group ip-address][receiver vlan vlan-id]}]
```

```
no mvr [immediate | type {source | receiver} | vlan vlan-id {[group ip-address][receiver vlan vlan-id]}]
```

Syntax Description		
immediate	(Optional) Enables the Immediate Leave feature of MVR on a port. Use the no mvr immediate command to disable the feature.	
type	(Optional) Configures the port as an MVR receiver port or source port. The default port type is neither source nor receiver. The no mvr type command resets the port as neither source or receiver.	
receiver	Configures the port as a subscriber port that can only receive multicast data. Receiver ports cannot belong to the multicast VLAN.	
source	Configures the port as an uplink port that can send and receive multicast data for the configured multicast groups. All source ports on a switch belong to a single multicast VLAN. Note When you are configuring a trunk port as an MVR receiver port, we recommend that the source port is configured as a network node interface (NNI) and the MVR trunk receiver port is configured as a user node interface (UNI).	
vlan <i>vlan-id</i>	Specifies the mvr VLAN for the system.	
group <i>ip-address</i>	(Optional) Statically configures the specified MVR IP multicast group address for the specified multicast VLAN ID. This is the IP address of the multicast group that the port or VLAN is joining.	
receiver <i>vlan-id</i>	Specifies a receiver VLAN.	

Command Default	
A port is configured as neither receiver nor source.	
The Immediate Leave feature is disabled on all ports.	
No receiver port belongs to any configured multicast group.	

Command Modes	
Interface configuration	

Command History	Release	Modification
	Release IOS XE 3.5.0E and IOS 15.2(1)E	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

Configure a port as a source if it is intended to both send and receive multicast data bound for the configured multicast groups. Multicast data is received on all ports configured as source ports.

Receiver ports on a switch can be in different VLANs, but should not belong to the multicast VLAN.

A port that is not taking part in MVR should not be configured as an MVR receiver port or a source port.

When Immediate Leave is enabled, a receiver port leaves a multicast group more quickly. Without Immediate Leave, when the switch receives an IGMP leave message from a group on a receiver port, it sends out an IGMP MAC-based query on that port and waits for IGMP group membership reports. If no reports are received in a configured time period, the receiver port is removed from multicast group membership. With Immediate Leave, an IGMP MAC-based query is not sent from the receiver port on which the IGMP leave was received. Once the leave message is received, the receiver port is removed from multicast group membership, which expedites leave latency.

The Immediate Leave feature should be enabled only on receiver ports to which a single receiver device is connected.

The **mvr vlan group** command statically configures ports to receive multicast traffic sent to the IP multicast address. A port statically configured as a member of a group remains a member of the group until statically removed. In compatible mode, this command applies only to receiver ports; in dynamic mode, it can also apply to source ports. Receiver ports can also dynamically join multicast groups by using IGMP join messages.

When operating in compatible mode, MVR does not support IGMP dynamic joins on MVR source ports.

Examples

The following example shows how to configure a port as an MVR receiver port:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# mvr type receiver
```

The following example shows how to configure a port as an MVR source port:

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# mvr type source
```

The following example shows how to remove a port as an MVR port:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# no mvr
```

The following example shows how to display configured receiver ports and source ports.

```
Switch# show mvr interface
```

Port	Type	Mode	VLAN	Status	Immediate Leave
Fa0/2	RECEIVER	Trunk	1	ACTIVE/UP	DISABLED
Fa0/4	RECEIVER	Trunk	1	ACTIVE/UP	DISABLED
Fa0/5	RECEIVER	Trunk	1	ACTIVE/UP	DISABLED
Fa0/5	RECEIVER	Trunk	2	ACTIVE/UP	DISABLED
Fa0/10	SOURCE	Access	10	ACTIVE/UP	DISABLED
Fa0/11	SOURCE	Trunk	10	ACTIVE/UP	ENABLED
Fa0/16	RECEIVER	Trunk	2	ACTIVE/UP	DISABLED
Fa0/18	RECEIVER	Trunk	1	ACTIVE/UP	ENABLED
Fa0/18	RECEIVER	Trunk	2	ACTIVE/UP	ENABLED
Fa0/21	SOURCE	Access	10	ACTIVE/UP	DISABLED
Fa0/24	RECEIVER	Access	4	ACTIVE/DOWN	DISABLED
Gi0/1	RECEIVER	Trunk	1	ACTIVE/UP	DISABLED
Gi0/1	RECEIVER	Trunk	2	ACTIVE/UP	DISABLED
Gi0/2	SOURCE	Access	10	ACTIVE/UP	DISABLED

The following example shows how to enable Immediate Leave on a port:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# mvr immediate
```

The following example shows how to disable Immediate Leave on a port:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# no mvr immediate
```

The following example shows how to add a port interface on VLAN 1 as a static member of IP multicast group 228.1.23.4:

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# mvr vlan1 group 230.1.23.4
```

The following example shows how to add a port 5 on VLAN 100 as a static member of IP multicast group 239.1.1.1. In this example, the receiver port is a trunk port:

```
Switch(config)# interface fastethernet0/5
Switch(config-if)# mvr vlan 100 group 239.1.1.1 receiver vlan 201
```

The following example shows how to remove this port from membership:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# no mvr vlan5 group 228.1.23.4
```

The following example shows how to remove this port from all IP multicast groups:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# no mvr vlan5 group
```

The following example shows the result if you try to add a port to a multicast group and the port is not a receiver port:

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# mvr vlan 1 group 230.1.23.4
Interface Gi1/0/2 not configured as a receiver interface
```

The following example shows how to add on port 5 the receiver VLAN 201 with an MVR VLAN of 100.

```
Switch(config)# interface fastethernet0/5
Switch(config-if)# mvr vlan 100 receiver vlan 201
```

The following example shows how to add on port 5 the receiver VLAN 201 as a static member of the IP multicast group 239.1.1.1, with an MVR VLAN of 100:

```
Switch(config)# interface fastethernet0/5
Switch(config-if)# mvr vlan 100 group 239.1.1.1 receiver vlan 201
```

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

Related Commands

Command	Description
mvr (global configuration)	Enables and configures multicast VLAN registration on the switch.
show mvr	Displays MVR global parameters or port parameters.
show mvr interface	Displays the configured MVR interfaces or displays the multicast groups to which a receiver port belongs. Also displays all MVR groups of which the interface is a member.
show mvr members	Displays all receiver ports that are members of an MVR multicast group.

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	<i>name</i>	Specifies the name of the MST region. The name can be any string with a maximum length of 32 characters.
---------------------------	-------------	--

Command Default The MST region name is not set.

Command Modes MST configuration mode

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

Usage Guidelines Two or more Catalyst 4500 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 The following 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.

netflow-lite exporter



Note

NetFlow-lite is supported only on the Catalyst 4948E and Catalyst 4948E-F Ethernet switches.

To define an exporter and to enter NetFlow-lite exporter submode, use the **netflow-lite exporter** command. To delete an exporter, use the **no** form of this command.

```
netflow-lite exporter exporter
```

```
no netflow-lite exporter exporter
```

Syntax Description	<i>exporter</i>	Specifies an exporter.
Command Default	None	
Command Modes	global configuration mode	
Command History	Release	Modification
	15.0(2)SG	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

The exporter's name identifies the exporter. Mandatory parameters for a minimal complete exporter configuration are the destination IP address of the collector, source IP address (on the switch) to use and UDP destination port of the collector. Any unspecified non-mandatory parameters take on default values.

The exporter name can be specified when activating sampling at a data source via the **monitor** command.

The exporter submode also allows you to specify the refresh frequency for the NetFlow templates. Metadata about the NetFlow packet sampling process like sampler configuration parameters and snmp interface table mapping can also be exported periodically to the collector.

Deleting or removing the value of a non-mandatory parameter restores the default.

Examples

The following example shows how to configure an NetFlow exporter:

```
Switch# config terminal
Switch(config)# netflow-lite exporter exporter1
Switch(config-netflow-lite-exporter)# destination 5.5.5.6
Switch(config-netflow-lite-exporter)# source 5.5.5.5
Switch(config-netflow-lite-exporter)# transport udp 8188
Switch(config-netflow-lite-exporter)# ttl 128
Switch(config-netflow-lite-exporter)# cos 7
Switch(config-netflow-lite-exporter)# dscp 32
Switch(config-netflow-lite-exporter)# template data timeout 1
Switch(config-netflow-lite-exporter)# options sampler-table timeout 1
Switch(config-netflow-lite-exporter)# options interface-table timeout 1
```

```
Switch(config-netflow-lite-exporter)# export-protocol netflow-v9
Switch(config-netflow-lite-exporter)# exit
Switch(config)#
```

Display the exporter

```
Switch# show netflow-lite exporter exporter1
```

```
Netflow-lite Exporter exporter1:
  Network Protocol Configuration:
    Destination IP address: 5.5.5.6
    Source IP Address:     5.5.5.5
    VRF label:
    DSCP:                  0x20
    TTL:                   128
    COS:                   7
  Transport Protocol Configuration:
    Transport Protocol:    UDP
    Destination Port:      8188
    Source Port:           61670
  Export Protocol Configuration:
    Export Protocol:       netflow-v9
    Template data timeout: 60
    Options sampler-table timeout: 1800
    Options interface-table timeout: 1800
  Exporter Statistics:
    Packets Exported:     0
```

You can verify your settings with the **show netflow-lite exporter** privileged EXEC command.

Related Commands

Command	Description
export-protocol (netflow-lite exporter submode)	Specifies the export protocol for the NetFlow-lite collector.
netflow-lite exporter	Defines an exporter and to enter NetFlow-lite exporter submode.
destination (netflow-lite exporter submode)	Specifies a destination address in netflow-lite submode.
source (netflow-lite exporter submode)	Specifies a source Layer 3 interface of the NetFlow-lite collector.
transport udp (netflow-lite exporter submode)	Specifies a UDP transport destination port for a NetFlow-lite collector.
ttl (netflow-lite exporter submode)	Specifies a ttl value for the NetFlow-lite collector.
cos (netflow-lite exporter submode)	Specifies a cos value for the NetFlow-lite collector.
dscp (netflow-lite exporter submode)	Specifies a cos value for the NetFlow-lite collector.
template data timeout (netflow-lite exporter submode)	Specifies a template data timeout for the NetFlow-lite collector.
options timeout (netflow-lite exporter submode)	Specifies an options timeout for the NetFlow-lite collector.

netflow-lite monitor



Note

NetFlow-lite is supported only on the Catalyst 4948E and Catalyst 4948E-F Ethernet switches.

To define a monitor instance on an interface and to enter netflow-lite monitor submode, use the **netflow-lite monitor** command. To delete the monitor, use the **no** form of this command.

netflow-lite monitor *sampler-name*

no netflow-lite sampler *sampler-name*

Syntax Description

<i>sampler-name</i>	Specifies a sample.
---------------------	---------------------

Command Default

None

Command Modes

global configuration mode

Command History

Release	Modification
15.0(2)SG	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

Only a single packet sampling instance is supported on a data source. These commands are entered under the physical port interface mode, port channel interface, or config VLAN mode. Monitor is not supported on other interfaces. If the physical port is a member of a port channel, applying the monitor to the port has no effect. You must apply the monitor to the port channel instead.



Note

VLAN sampling is not supported in Cisco IOS Release 15.0(2)SG. It will be supported in a later release.

Mandatory parameters are sampler and exporter. If no exporter is associated with a monitor, no samples are exported. If so, no input packet sampling occurs for that target interface. A warning message displays indicating that the sampler or exporter is invalid if any mandatory parameters are missing.

The packet sampling mechanism tries to achieve random 1-in-N sampling. Internally 2 levels of sampling are done. The accuracy of the first level of sampling depends on the size of the packets arriving at a given interface. To tune the relative accuracy of the algorithm the **average-packet-size** parameter can be used.

The system automatically determines the average packet size at an interface based on observation of input traffic and uses that value in its first level of sampling.

Valid range of packet sizes that can be used by the algorithm is 64 - 9216 bytes. Any number below 64 bytes is taken to mean that automatic determination of average packet size is desired.

Examples

The following example shows how to configure a monitor on a port interface Gigabit 1/3:

```
Switch# config terminal
Switch(config)# int GigabitEthernet1/3
Switch(config-if)# netflow-lite monitor 1
Switch(config-netflow-lite-monitor)# sampler sampler1
Switch(config-netflow-lite-monitor)# average-packet-size 128
Switch(config-netflow-lite-monitor)# exporter exporter1
Switch(config-netflow-lite-monitor)# exit
Switch(config-if)# exit
Switch(config)# exit
Switch# show netflow-lite monitor 1 interface gi1/3
Interface GigabitEthernet1/3:
  Netflow-lite Monitor-1:
    Active:                TRUE
    Sampler:                sampler1
    Exporter:              exporter1
    Average Packet Size:   0
  Statistics:
    Packets exported:      0
    Packets observed:      0
    Packets dropped:       0
    Average Packet Size observed: 64
    Average Packet Size used: 64
```

Similarly, you can configure a monitor on a VLAN in VLAN config mode:

```
Switch# config terminal
Switch(config)# vlan config 2
Switch(config-vlan-config)# netflow-lite monitor 1
Switch(config-netflow-lite-monitor)# average-packet-size 128
Switch(config-netflow-lite-monitor)# exporter exporter1
Switch(config-netflow-lite-monitor)# sampler sampler1
Switch(config-netflow-lite-monitor)# exit
Switch(config-vlan-config)# exit
Switch# show netflow-lite monitor 1 vlan 2
VlanID-2:
  Netflow-lite Monitor-1:
    Active:                TRUE
    Sampler:                sampler1
    Exporter:              exporter1
    Average Packet Size:   0
  Statistics:
    Packets exported:      0
    Packets observed:      0
    Packets dropped:       0
    Average Packet Size observed: 64
    Average Packet Size used: 64
```

You can verify your settings with the **show netflow-lite sampler** privileged EXEC command.

Related Commands

Command	Description
sampler (netflow-lite monitor submode)	Activate sampling on an interface in netflow-lite monitor submode.
average-packet-size (netflow-lite monitor submode)	Specifies the average packet size at the observation point.
exporter (netflow-lite monitor submode)	Assigns an exporter in netflow-lite monitor submode.

netflow-lite sampler



Note

NetFlow-lite is supported only on the Catalyst 4948E and Catalyst 4948E-F Ethernet switches.

To configure packet sampling parameters as a reusable named entity and to enter netflow-lite sampler submode, use the **netflow-lite sampler** command. To delete the sampler, use the **no** form of this command.

netflow-lite sampler *name*

no netflow-lite sampler *name*

Syntax Description	<i>name</i>	Specifies a sampler.
Command Default	None	
Command Modes	global configuration mode	
Command History	Release	Modification
	15.0(2)SG	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

The sampler CLI construct allows the user to configure the rate at which input packets are to be sampled. Packet sampling rate can range from 32 to 2¹⁵ in powers of 2. A sampling rate of 1 is allowed for troubleshooting for up to two 1 Gigabit ports only and is essentially equivalent to rx span. It cannot be configured on 10GE ports because the bandwidth demand on the fpga for export is too high.

Mandatory parameters are packet rate.

You can update a sampler in use at a target interface, but you cannot remove or unconfigure mandatory parameters.

All mandatory parameters must be present to validate a sampler. Any unspecified non-mandatory parameters take on default values.

Examples

The following example shows how to configure packet sampling parameters as a reusable named entity and to display the sampler:

```
Switch# config terminal
Switch(config)# netflow-lite sampler sampler1
Switch(config-netflow-lite-sampler)# packet-rate 32
Switch(config-netflow-lite-sampler)# packet-section size 128
Switch(config-netflow-lite-sampler)# packet-offset 16
Switch(config-netflow-lite-sampler)# exit
Switch(config)# exit
Switch#
```

```
Switch# show netflow-lite sampler sampler1
Netflow-lite Sampler sampler1:
  Id : 1
  Packet Sampling rate: 1 out of 32
  Packet Section Size: 64 bytes
  Packet offset: 16 bytes
```

You can verify your settings with the **show netflow-lite exporter** privileged EXEC command.

Related Commands

Command	Description
packet-offset (netflow-lite sampler submode)	Specifies a starting packet offset in netflow-lite submode.
packet-rate (netflow-lite sampler submode)	Specifies a packet sampling rate in netflow-lite sampler submode.
packet-section size (netflow-lite sampler submode)	Specifies a sampled header size in netflow-lite submode.

nmosp

To configure Network Mobility Services Protocol (NMSP) on the switch, use the **nmosp** 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.

```
nmosp {enable | {notification interval {attachment | location} interval-seconds}}
```

```
no nmosp {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.
<i>interval-seconds</i>	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.

Command Default

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	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

Use the **nmosp** global configuration command to enable the switch to send encrypted NMSP location and attachment notifications to a Cisco Mobility Services Engine (MSE).

Examples

The following example shows how to enable NMSP on a switch and set the location notification time to 10 seconds:

```
Switch(config)# nmosp enable
Switch(config)# nmosp notification interval location 10
Switch(config)#
```

Related Commands

Command	Description
clear nmosp statistics	Clears the NMSP statistic counters.
nmosp attachment suppress	Suppress reporting attachment information from a specified interface.
show nmosp	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.

Command Default Attachment information is reported.

Command Modes Interface configuration mode

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

object-group

To define object groups that you can use to optimize your configuration, use the **object-group** command in the global configuration mode. To remove object groups from the configuration use the **no** form of this command.

**Note**

Object groups for ACLs is supported only on Catalyst 4500-X Series Switches, and Catalyst 4500-E Series Switches (with Supervisor Engines 7-E, 7L-E, and 8-E).

object-group {**network** | **service**} *object-group-name*

no object-group {**network** | **service**} *object-group-name*

Syntax Description	network	Defines network object groups for use in object-group-based ACLs. When you configure the object-group network command, the command mode changes to network group configuration mode. The following options are available in this mode:
		<p>A.B.C.D Network address of the group members</p> <p>description Network object group description</p> <p>execute Execute a shell function</p> <p>exit Exit from object group configuration mode</p> <p>group-object Nested object group</p> <p>host Host address of the object-group member</p> <p>no Negate or set default values of a command</p>
	service	Defines service object groups for use in object-group-based ACLs.
		<p><0-255> An IP protocol number</p> <p>ahp Authentication Header Protocol</p> <p>description Service object group description</p> <p>eigrp Cisco's EIGRP routing protocol</p> <p>esp Encapsulation Security Payload</p> <p>execute Execute a shell function</p> <p>exit Exit from object-group configuration mode</p> <p>gre Cisco's GRE tunneling</p> <p>group-object Nested object group</p> <p>icmp Internet Control Message Protocol</p> <p>igmp Internet Gateway Message Protocol</p> <p>ip Any Internet Protocol</p> <p>ipinip IP in IP tunneling</p> <p>no Negate or set default values of a command</p> <p>nos KA9Q NOS compatible IP over IP tunneling</p> <p>ospf OSPF routing protocol</p> <p>pcp Payload Compression Protocol</p> <p>pim Protocol Independent Multicast</p> <p>tcp Transmission Control Protocol</p> <p>tcp-udp TCP or UDP protocol</p> <p>udp User Datagram Protocol</p>
	<i>object-group-name</i>	Name of the object group (of type service or network). The object group name is a sequence of 1 to 64 characters consisting of letters, digits, underscores (_), dashes (-), or periods (.). The object-group-name must start with a letter.

Command Default This command has no default settings

Command Modes Global configuration mode

Command History	Release	Modification
	3.71E and 15.2(3)E1	This command was introduced.
	3.72E and 15.2(3)E2	Enhancements were made to the no version of the command

Usage Guidelines This command supports only IPv4 addresses.

Commands within the object group configuration mode appear indented when saved or displayed using the **write memory** or **show running-config** commands.

Commands within the group configuration mode (config-network-group or config-service-group) have the same command privilege level as the main command.

The command supports unlimited number of nested object groups; however, we recommend no more than two levels.

The type of child object group must match the type of the parent (for example, if you create a network object group, the child object group that you specify must be another network object group).

The switch ignores all empty object groups. When an ACE uses an empty object-group, that ACE is not expanded, as if there is no such ACE.

When you enter the **no** form of the command to delete an object group, the switch does one of the following:

- If the object group is being used somewhere, the switch removes all the entries of the object group, making this an empty object group.
- If the object group is not being used anywhere, the switch deletes it.

You cannot delete an object group that is being used within an ACL or CPL policy.

If an object group that you are trying to use in an ACE is not previously defined, the switch rejects the command. For example,

```
Switch(config)#ip access-list extend acl-1
```

```
Switch(config-ext-nacl)#permit ip object-group OG-1 any
```

OG-1 doesn't exist, this line is rejected.

Specifics for network groups

<http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/m1/sec-m1-cr-book/sec-cr-m2.html#wp2754379810>

Specifics for service groups

options timeout (netflow-lite exporter submode)



Note

NetFlow-lite is supported only on the Catalyst 4948E and Catalyst 4948E-F Ethernet switches.

To specify an options timeout for the NetFlow-lite collector, use the **options timeout** command. To delete the value, use the **no** form of this command.

```
options {sampler-table | interface-table} timeout seconds
```

```
no options {sampler-table | interface-table} timeout second
```

Syntax Description		
	sampler-table	Specifies timeout value for export of sampler configuration.
	interface-table	Specifies timeout value for export of snmp ifIndex mapping.
	<i>seconds</i>	Specifies a n options timeout for the NetFlow-lite collector.

Command Default 1800 seconds

Command Modes netflow-lite exporter submode

Command History	Release	Modification
	15.0(2)SG	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines Default timeout value is 1800 seconds or 30 minutes. The timeout value configured really depends on the collector and how often it needs the templates to be refreshed.

Examples The following example shows how to specify an options timeout for the NetFlow-lite collector:

```
Switch# config terminal
Switch(config)# netflow-lite exporter exporter1
Switch(config-netflow-lite-exporter)# destination 5.5.5.6
Switch(config-netflow-lite-exporter)# source 5.5.5.5
Switch(config-netflow-lite-exporter)# transport udp 8188
Switch(config-netflow-lite-exporter)# ttl 128
Switch(config-netflow-lite-exporter)# cos 7
Switch(config-netflow-lite-exporter)# dscp 32
Switch(config-netflow-lite-exporter)# template data timeout 1
Switch(config-netflow-lite-exporter)# options sampler-table timeout 1
Switch(config-netflow-lite-exporter)# options interface-table timeout 1
Switch(config-netflow-lite-exporter)# export-protocol netflow-v9
Switch(config-netflow-lite-exporter)# exit
Switch(config)#
```

```

Display the exporter
Switch# show netflow-lite exporter exporter1
Netflow-lite Exporter exporter1:
  Network Protocol Configuration:
    Destination IP address: 5.5.5.6
    Source IP Address:    5.5.5.5
    VRF label:
    DSCP:                 0x20
    TTL:                  128
    COS:                  7
  Transport Protocol Configuration:
    Transport Protocol:   UDP
    Destination Port:     8188
    Source Port:          61670
  Export Protocol Configuration:
    Export Protocol:      netflow-v9
    Template data timeout: 60
    Options sampler-table timeout: 1800
    Options interface-table timeout: 1800
  Exporter Statistics:
    Packets Exported:    0

```

You can verify your settings with the **show netflow-lite exporter** privileged EXEC command.

Related Commands	Command	Description
	cos (netflow-lite exporter submode)	Specifies a cos value for the NetFlow-lite collector.
	source (netflow-lite exporter submode)	Specifies a source Layer 3 interface of the NetFlow-lite collector.
	transport udp (netflow-lite exporter submode)	Specifies a UDP transport destination port for a NetFlow-lite collector.
	ttl (netflow-lite exporter submode)	Specifies a ttl value for the NetFlow-lite collector.
	destination (netflow-lite exporter submode)	Specifies a destination address in netflow-lite submode.
	template data timeout (netflow-lite exporter submode)	Specifies a template data timeout for the NetFlow-lite collector.
	export-protocol (netflow-lite exporter submode)	Specifies the export protocol for the NetFlow-lite collector.
	dscp (netflow-lite exporter submode)	Specifies a cos value for the NetFlow-lite collector.

packet-offset (netflow-lite sampler submode)



Note

NetFlow-lite is supported only on the Catalyst 4948E and Catalyst 4948E-F Ethernet switches.

To specify a starting packet offset in netflow-lite submode, use the **packet-offset** command. To reset to the default, use the **no** form of this command.

```
packet-offset offset
```

```
no packet-offset offset
```

Syntax Description

<i>offset</i>	Specifies the starting packet offset in bytes (maximum of 48).
---------------	--

Command Default

starts at byte 0 of L2 header

Command Modes

netflow-lite exporter submode

Command History

Release	Modification
15.0(2)SG	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

Default packet section offset value is 0. The packet section extracted from the sampled packet start at offset 0 of the packet.

Examples

The following example shows how to specify a starting packet offset:

```
Switch# config terminal
Switch(config)# netflow-lite sampler sampler1
Switch(config-netflow-lite-sampler)# packet-rate 32
Switch(config-netflow-lite-sampler)# packet-section size 128
Switch(config-netflow-lite-sampler)# packet-offset 16
Switch(config-netflow-lite-sampler)# exit
Switch(config)# exit
Switch# show netflow-lite sampler sampler1
Netflow-lite Sampler sampler1:
  Id : 1
  Packet Sampling rate: 1 out of 32
  Packet Section Size: 64 bytes
  Packet offset: 16 bytes
```

You can verify your settings with the **show netflow-lite sampler** privileged EXEC command.

Related Commands.	Command	Description
	packet-section size (netflow-lite sampler submode)	Specifies a sampled header size in netflow-lite submode.
	packet-rate (netflow-lite sampler submode)	Specifies a packet sampling rate in netflow-lite sampler submode

packet-rate (netflow-lite sampler submode)



Note

NetFlow-lite is supported only on the Catalyst 4948E and Catalyst 4948E-F Ethernet switches.

To specify a packet sampling rate in netflow-lite sampler submode, use the **packet rate** command. To delete a packet sampling rate, use the **no** form of this command.

packet rate *n*

no packet rate *n*

Syntax Description

n Specifies the packet sampling rate.

Command Default

None

Command Modes

netflow-lite exporter submode

Command History

Release	Modification
15.0(2)SG	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

Packet sampling rate can range from 32 to 2^{15} in powers of 2. A rate of 1 is allowed for trouble shooting (equivalent to rx span) only for two 1Gigabit Ethernet ports. You cannot configure a rate of 1 on 10 Gigabit Ethernet ports because the bandwidth demand for export is too high.

This is a mandatory parameter. Up to 2 x 1 Gigabit Ethernet ports can be configured with 1-in-1 sampling. The best packet sampling rate that can be configured on any 1 Gigabit or 10 Gigabit Ethernet port is 1-in-32. Packet sampling rates can be configured in powers of 2 (1-in-64, 1-in-128, etc).

Examples

The following example shows how to specify a packet sampling rate in netflow-lite sampler submode:

```
Switch# config terminal
Switch(config)# netflow-lite sampler sampler1
Switch(config-netflow-lite-sampler)# packet-rate 32
Switch(config-netflow-lite-sampler)# packet-section size 128
Switch(config-netflow-lite-sampler)# packet-offset 16
Switch(config-netflow-lite-sampler)# exit
Switch(config)# exit
Switch#

Switch# show netflow-lite sampler sampler1
Netflow-lite Sampler sampler1:
  Id : 1
  Packet Sampling rate: 1 out of 32
  Packet Section Size: 64 bytes
  Packet offset: 16 bytes
```

You can verify your settings with the **show netflow-lite sampler** privileged EXEC command.

Related Commands	Command	Description
	packet-section size (netflow-lite sampler submode)	Specifies a sampled header size in netflow-lite submode.
	packet-offset (netflow-lite sampler submode)	Specifies a starting packet offset in netflow-lite submode.

packet-section size (netflow-lite sampler submode)



Note

NetFlow-lite is supported only on the Catalyst 4948E and Catalyst 4948E-F Ethernet switches.

To specify a sampled header size in netflow-lite submode, use the **packet-section size** command. To store the default, use the **no** form of this command.

packet-section size *bytes*

no packet-section size *bytes*

Syntax Description

bytes Specifies the sampled header size. Size ranges from 16 to 252 bytes in increments of 4 bytes.

Command Default

64 bytes

Command Modes

netflow-lite exporter submode

Command History

Release	Modification
15.0(2)SG	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

Default packet section size is 64 bytes which normally would cover Layer 2, Layer 3, and Layer 4 headers for an input IPv4 packet.

Examples

The following example shows how to specify a sampled header size:

```
Switch# config terminal
Switch(config)# netflow-lite sampler sampler1
Switch(config-netflow-lite-sampler)# packet-rate 32
Switch(config-netflow-lite-sampler)# packet-section size 128
Switch(config-netflow-lite-sampler)# packet-offset 16
Switch(config-netflow-lite-sampler)# exit
Switch(config)# exit
Switch#

Switch# show netflow-lite sampler sampler1
Netflow-lite Sampler sampler1:
  Id : 1
  Packet Sampling rate: 1 out of 32
  Packet Section Size: 64 bytes
  Packet offset: 16 bytes
```

You can verify your settings with the **show netflow-lite sampler** privileged EXEC command.

Related Commands	Command	Description
	packet-rate (netflow-lite sampler submode)	Specifies a packet sampling rate in netflow-lite sampler submode.
	packet-offset (netflow-lite sampler submode)	Specifies a starting packet offset in netflow-lite submode.

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	physical-port
	Specifies learning the address on the port channel.	Specifies learning the address on the physical port within the bundle.

Command Default Aggregation port is enabled.

Command Modes Interface configuration mode

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

Examples The following example shows how to enable physical port address learning within the bundle:

```
Switch(config-if)# pagp learn-method physical-port
Switch(config-if)#
```

The following 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	<i>priority</i> Port priority number; valid values are from 1 to 255.						
Command Default	Port priority is set to 128.						
Command Modes	Interface configuration mode						
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.1(8a)EW</td> <td>This command was introduced on the Catalyst 4500 series switch.</td> </tr> </tbody> </table>	Release	Modification	12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch.		
Release	Modification						
12.1(8a)EW	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	<p>The following example shows how to set the port priority:</p> <pre>Switch(config-if) # pagp port-priority 45 Switch(config-if) #</pre>						
Related Commands	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>pagp learn-method</td> <td>Learns the input interface of the incoming packets.</td> </tr> <tr> <td>show pagp</td> <td>Displays information about the port channel.</td> </tr> </tbody> </table>	Command	Description	pagp learn-method	Learns the input interface of the incoming packets.	show pagp	Displays information about the port channel.
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 reenab 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.
	<i>interface-type</i>	Specifies the interface type.
	<i>interface-number</i>	Specifies the interface number.
	range	Specifies the range of subinterfaces being configured; see the “Usage Guidelines” section.

Command Default Routing updates are sent on the interface.

Command Modes Router configuration mode

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

Usage Guidelines You can use the **passive-interface range** command on the following interfaces: FastEthernet, GigabitEthernet, VLAN, Loopback, Port-channel, 10-GigabitEthernet, and Tunnel. When you use the **passive-interface range** command on a VLAN interface, the interface should be the existing VLAN SVIs. To display the VLAN SVIs, enter the **show running config** command. The VLANs that are not displayed cannot be used in the **passive-interface range** command.

The 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 5/1-20, gigabitethernet4/5-20.
```

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 in OSPF, EIGRP, RIP, and ISIS router mode.

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 provider (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 addresses 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 to all interfaces on network 10.108.0.0 except GigabitEthernet interface 1/1:

```
Switch(config)# interface gigabitethernet 1/1  
Switch(config-if)# router eigrp 109  
Switch(config-router)# network 10.108.0.0  
Switch(config-router)# passive-interface gigabitethernet 1/1  
Switch(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 its link-state protocol data units (PDUs):

```
Switch(config-if)# router isis Finance
Switch(config-router)# passive-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)#
```

The following example sets all interfaces as passive, then activates Ethernet interface 0:

```
Switch(config-if)# router ospf 100
Switch(config-router)# passive-interface default
Switch(config-router)# no passive-interface ethernet0
Switch(config-router)# network 10.108.0.1 0.0.0.255 area 0
Switch(config-router)#
```

The following configuration sets the Ethernet ports 3 through 4 on module 0 and GigabitEthernet ports 4 through 7 on module 1 as passive:

```
Switch(config-if)# router ospf 100
Switch(config-router)# passive-interface range ethernet0/3-4,gigabitethernet1/4-7
Switch(config-router)#
```

permit

To permit an ARP packet based on matches against the DHCP bindings, use the **permit** command. To remove a specified ACE from an access list, use the **no** form of this command.

```
permit {[request] ip {any | host sender-ip | sender-ip sender-ip-mask} mac {any | host sender-mac | sender-mac sender-mac-mask} | response ip {any | host sender-ip | sender-ip sender-ip-mask} [{any | host target-ip | target-ip target-ip-mask}] mac {any | host sender-mac | sender-mac sender-mac-mask} [{any | host target-mac | target-mac target-mac-mask}] [log]
```

```
no permit {[request] ip {any | host sender-ip | sender-ip sender-ip-mask} mac {any | host sender-mac | sender-mac sender-mac-mask} | response ip {any | host sender-ip | sender-ip sender-ip-mask} [{any | host target-ip | target-ip target-ip-mask}] mac {any | host sender-mac | sender-mac sender-mac-mask} [{any | host target-mac | target-mac target-mac-mask}] [log]
```

Syntax Description

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 <i>sender-ip</i>	Specifies that only a specific sender IP address will be accepted.
<i>sender-ip</i> <i>sender-ip-mask</i>	Specifies that a specific range of sender IP addresses will be accepted.
mac	Specifies the sender MAC address.
host <i>sender-mac</i>	Specifies that only a specific sender MAC address will be accepted.
<i>sender-mac</i> <i>sender-mac-mask</i>	Specifies that a specific range of sender MAC addresses will be accepted.
response	Specifies a match for the ARP responses.
ip	Specifies the IP address values for the ARP responses.
host <i>target-ip</i>	(Optional) Specifies that only a specific target IP address will be accepted.
<i>target-ip target-ip-mask</i>	(Optional) Specifies that a specific range of target IP addresses will be accepted.
mac	Specifies the MAC address values for the ARP responses.
host <i>target-mac</i>	(Optional) Specifies that only a specific target MAC address will be accepted.
<i>target-mac</i> <i>target-mac-mask</i>	(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).

Command Default

This command has no default settings.

Command Modes

arp-nacl configuration mode

Command History	Release	Modification
	12.1(19)EW	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 The following example shows a host with a MAC address of 0000.0000.abcd and an IP address of 1.1.1.1. The following example shows how to permit both requests and responses from this host:

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

ARP access list static-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 applies it to a VLAN.

police

To configure the Traffic Policing feature, use the **police** QoS policy-map class configuration command. To remove the Traffic Policing feature from the configuration, use the **no** form of this command.

```
police { bps | kbps | mbps | gbps } [burst-normal] [burst-max] conform-action action exceed-action
action [violate-action action]
```

```
no police { bps | kbps | mbps | gbps } [burst-normal] [burst-max] conform-action action
exceed-action action [violate-action action]
```

Syntax Description	
<i>bps</i>	Average rate, in bits per second. Valid values are 32,000 to 32,000,000,000.
<i>kbps</i>	Average rate, in kilobytes per second. Valid values are 32 to 32,000,000.
<i>mbps</i>	Average rate, in megabits per second. Valid values are 1 to 32,000.
<i>gbps</i>	Average rate, in gigabits per second. Valid values are 1 to 32.
<i>burst-normal</i>	(Optional) Normal burst size, in bytes. Valid values are 64 to 2,596,929,536. Burst value of up to four times the configured rate can be supported.
<i>burst-max</i>	(Optional) Excess burst size, in bytes. Valid values are 64 to 2,596,929,536. 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.
<i>action</i>	Action to take on packets. Specify one of the following keywords: <ul style="list-style-type: none"> • drop—Drops the packet. • set-cos-transmit <i>new-ios</i>—Sets the class of services (CoS) value to a new value and send the packet. The range is 0 to 7. • set-dscp-transmit <i>value</i>—Sets the IP differentiated services code point (DSCP) value and transmits the packet with the new IP DSCP value setting. • set-prec-transmit <i>value</i>—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 (when specifying a single action to be applied to a marked packet)
Policy-map class police configuration mode (when specifying multiple actions to be applied to a marked packet)

Command History

Release	Modification
12.2(40)SG	This command was introduced on Catalyst 4900M and 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 will not be executed for traffic that passes through an interface.

Specifying Multiple Actions

The **police** command allows you to specify multiple policing actions. When specifying multiple policing actions when configuring the **police** command, note the following points:

- You can specify a maximum of four actions at one time.
- You cannot specify contradictory actions such as **conform-action** *transmit* and **conform-action** *drop*.

Using the Police Command with the Traffic Policing Feature

The **police** command can be used with Traffic Policing feature. The Traffic Policing feature works with a token bucket algorithm. Two types of token bucket algorithms are a single-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)/8 bytes
- If the number of bytes in the conform bucket B is greater than or equal to 0, the packet conforms and the conform action 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 0, the exceed action is taken.

Token Bucket Algorithm with Two Token Buckets (Refer to RFC 2697)

The two-token bucket algorithm is used when the **violate-action** is specified in the **police** command CLI.

The conform bucket is initially full (the full size is the number of bytes specified as the normal burst size).

The exceed bucket is initially full (the full exceed bucket size is the number of bytes specified in the maximum burst size).

The tokens for both the conform and exceed token buckets are updated based on the token arrival rate, or committed information rate (CIR).

When a packet of given size (for example, “B” bytes) arrives at specific time (time “T”) the following 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 bits 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 token arrival rate is calculated as follows:

(time between packets <which is equal to $T - T1$ > * policer rate)/8 bytes

- If the number of bytes in the conform bucket - B is greater than or equal to 0, the packet conforms and the conform action is taken on the packet. If the packet conforms, B bytes are removed from the conform bucket and the conform action is taken. The exceed bucket is unaffected in this scenario.
- If the number of bytes in the conform bucket B is less than 0, the excess token bucket is checked for bytes by the packet. If the number of bytes in the exceed bucket B is greater than or equal to 0, the exceed action is taken and B bytes are removed from the exceed token bucket. No bytes are removed from the conform bucket.
- If the number bytes in the exceed bucket B is fewer than 0, the packet violates the rate and the violate action is taken. The action is complete for the packet.

Examples

Token Bucket Algorithm with One Token Bucket

The following example shows how to define a traffic class (using the **class-map** command) and associate the match criteria from the traffic class with the Traffic Policing configuration, which is configured in the service policy (using the **policy-map** command). The **service-policy** command is then used to attach this service policy to the interface.

In this particular example, Traffic Policing is configured with the average rate at 8000 bits per second and the normal burst size at 1000 bytes for all packets leaving Gigabit Ethernet interface 6/1:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# class-map access-match
Switch(config-cmap)# match access-group 1
Switch(config-cmap)# exit
Switch(config)# policy-map police-setting
Switch(config-pmap)# class access-match
Switch(config-pmap-c)# police 8000 1000 conform-action transmit exceed-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet 6/1
Switch(config-if)# service-policy output police-setting
Switch(config-if)# end
```

In this example, the initial token buckets starts full at 1000 bytes. If a 450-byte packet arrives, the packet conforms because enough bytes are available in the conform token bucket. The conform action (send) is taken by the packet and 450 bytes are removed from the conform token bucket (leaving 550 bytes).

If the next packet arrives 0.25 seconds later, 250 bytes are added to the token bucket $((0.25 * 8000)/8)$, leaving 800 bytes in the token bucket. If the next packet is 900 bytes, the packet exceeds and the exceed action (drop) is taken. No bytes are taken from the token bucket.

Token Bucket Algorithm with Two Token Buckets Example (Refer to RFC 2697)

In this particular example, Traffic Policing is configured with the average rate at 8000 bits per second, the normal burst size at 1000 bytes, and the excess burst size at 1000 bytes for all packets leaving Gigabit Ethernet interface 6/1.

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# class-map access-match
Switch(config-cmap)# match access-group 1
Switch(config-cmap)# exit
Switch(config)# policy-map police-setting
Switch(config-pmap)# class access-match
Switch(config-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 police-setting
Switch(config-if)# end
```

In this example, the initial token buckets starts full at 1000 bytes. If a 450-byte packet arrives, the packet conforms because enough bytes are available in the conform token bucket. The conform action (send) is taken by the packet and 450 bytes are removed from the conform token bucket (leaving 550 bytes).

If the next packet arrives 0.25 seconds later, 250 bytes are added to the conform token bucket $((0.25 * 8000)/8)$, leaving 800 bytes in the conform token bucket. If the next packet is 900 bytes, the packet does not conform because only 800 bytes are available in the conform token bucket.

The exceed token bucket, which starts full at 1000 bytes (as specified by the excess burst size) is then checked for available bytes. Because enough bytes are available in the exceed token bucket, the exceed action (set the QoS transmit value of 1) is taken and 900 bytes are taken from the exceed bucket (leaving 100 bytes in the exceed token bucket).

If the next packet arrives 0.40 seconds later, 400 bytes are added to the token buckets $((.40 * 8000)/8)$. 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 $((.20 * 8000)/8)$. 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 multiple ports to specify a service policy and to enter policy-map configuration mode.
	service-policy (policy-map class)	Creates a service policy that is a quality of service (QoS) policy within a policy map.
	show policy-map	Displays information about the policy map.
	show policy-map interface	Displays the statistics and configurations of the input and output policies that are attached to an interface.

police (percent)

To configure traffic policing on the basis of a percentage of bandwidth available on an interface, use the **police** command in QoS policy-map class configuration mode. To remove traffic policing from the configuration, use the **no** form of this command.

police cir percent *percent* [**bc conform-burst-in-msec**] [**pir percent percentage**] [**be peak-burst-inmsec**]

no police cir percent *percent* [**bc conform-burst-in-msec**] [**pir percent percentage**] [**be peak-burst-inmsec**]

Syntax Description

cir	Committed information rate. Indicates that the CIR will be used for policing traffic.
percent	Specifies that a percentage of bandwidth will be used for calculating the CIR.
<i>percent</i>	Specifies the bandwidth percentage. Valid range is a number from 1 to 100.
bc	(Optional) Conform burst (bc) size used by the first token bucket for policing traffic.
<i>conform-burst-in-msec</i>	(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.
<i>percent</i>	(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.
<i>peak-burst-in-msec</i>	(Optional) Specifies the be size in milliseconds. Valid range is a number from 1 to 2000.
<i>action</i>	Action to take on packets. Specify one of the following keywords: <ul style="list-style-type: none"> • drop—Drops the packet. • set-cos-transmit <i>new-ios</i>—Sets the class of services (CoS) value to a new value and send the packet. The range is 0 to 7. • set-dscp-transmit <i>value</i>—Sets the IP differentiated services code point (DSCP) value and transmits the packet with the new IP DSCP value setting. • set-prec-transmit <i>value</i>—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 Catalyst 4900M and Supervisor Engine 6-E..

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 The following example shows how to configure traffic policing using a CIR and a PIR based on a percentage of bandwidth on Gigabit interface 6/2. In this example, a CIR of 20 percent and a PIR of 40 percent have been specified. Additionally, an optional bc value and be value (300 ms and 400 ms, respectively) have been specified.

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# policy-map policy1
Switch(config-pmap)# class-map class1
Switch(config-pmap-c)# police cir percent 20 bc 3 ms pir percent 40 be 4 ms
Switch(config-pmap-c)# exit
Switch(config-pmap-c)# interface gigabitethernet 6/2
Switch(config-if)# service-policy output policy
Switch(config-if)# end
```

police rate

To configure single or dual rate policer, use the **police rate** command in policy-map configuration mode. To remove traffic policing from the configuration, use the **no** form of this command.

Syntax for Bytes Per Second

police rate *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* **ms**] [**peak-rate** *percent* **percentage**] [**pack-burst** *ms* **ms**]

no police rate percent *percentage* [**burst** *ms* **ms**] [**peak-rate** *percent* **percentage**] [**pack-burst** *ms* **ms**]

Syntax Description

<i>units</i>	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 <i>burst-in-bytes</i> bytes	(Optional) Specifies the burst rate, in bytes, will be used for policing traffic. Valid range is from 64 to 2,596,929,536.
peak-rate <i>peak-rate-in-bps</i> 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 <i>peak-burst-in-bytes</i> 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 2,596,929,536.
percent	(Optional) A percentage of interface bandwidth will be used to determine the rate at which traffic is policed.
<i>percentage</i>	(Optional) Bandwidth percentage. Valid range is a number from 1 to 100.
burst <i>ms</i> 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 <i>percentage</i>	(Optional) A percentage of interface bandwidth will be used to determine the PIR. Valid range is a number from 1 to 100.
peak-burst <i>ms</i> 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 4500 series switch using a Supervisor Engine 6-E.

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 The following example shows how to configure policing on a class to limit traffic to an average rate of 1,500,000 bps:

```
Switch(config)# class-map c1
Switch(config-cmap)# match access-group 140
Switch(config-cmap)# exit
Switch(config)# policy-map p1
Switch(config-pmap)# class c1
Switch(config-pmap-c)# police rate 1500000 burst 500000
Switch(config-pmap-c)# exit
```

Related Commands	Command	Description
	policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.
	show policy-map	Displays information about the policy map.

police (two rates)

To configure traffic policing using two rates, the committed information rate (CIR) and the peak information rate (PIR), use the **police** command in policy-map configuration mode. To remove two-rate traffic policing from the configuration, use the **no** form of this command.

```
police cir cir [bc conform-burst] pir pir [be peak-burst] [conform-action action [exceed-action action [violate-action action]]]
```

```
no police cir cir [bc conform-burst] pir pir [be peak-burst] [conform-action action [exceed-action action [violate-action action]]]
```

Syntax Description

cir	Committed information rate (CIR) at which the first token bucket is updated.
<i>cir</i>	Specifies the CIR value in bits per second. The value is a number from 32,000 to 32,000,000,000.
bc	(Optional) Conform burst (bc) size used by the first token bucket for policing.
<i>conform-burst</i>	(Optional) Specifies the bc value in bytes. The value is a number from 64 to 2,596,929,536.
pir	Peak information rate (PIR) at which the second token bucket is updated.
<i>pir</i>	Specifies the PIR value in bits per second. The value is a number from 32,000 to 32,000,000,000.
be	(Optional) Peak burst (be) size used by the second token bucket for policing.
<i>peak-burst</i>	(Optional) Specifies the peak burst (be) size in bytes. The value is a number from 64 to 2,596,929,536.
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.
<i>action</i>	(Optional) Action to take on packets. Specify one of the following keywords: <ul style="list-style-type: none"> • drop—Drops the packet. • set-cos-transmit <i>new-ios</i>—Sets the class of services (CoS) value to a new value and send the packet. The range is 0 to 7. • set-dscp-transmit <i>new-dscp</i>—Sets the IP differentiated services code point (DSCP) value and sends the packet with the new IP DSCP value setting. • set-prec-transmit <i>new-prec</i>—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(40)SG	This command was introduced on the Catalyst 4500 series switch using a Supervisor Engine 6-E.

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 conform burst (Bc) value.
- The Tp token bucket is updated at the PIR value each time a packet arrives at the two-rate policer. The Tp token bucket can contain up to the peak burst (Be) value.

Updating Token Buckets

The following scenario illustrates how the token buckets are updated:

A packet of B bytes arrives at time t. The last packet arrived at time t1. The CIR and the PIR token buckets at time t are represented by Tc(t) and Tp(t), respectively. Using these values and in this scenario, the token buckets are updated as follows:

$$Tc(t) = \min(CIR * (t-t1) + Tc(t1), Bc)$$

$$Tp(t) = \min(PIR * (t-t1) + Tp(t1), Be)$$

Marking Traffic

The two-rate policer marks packets as either conforming, exceeding, or violating a specified rate. The following points (using a packet of B bytes) illustrate how a packet is marked:

- If $B > Tp(t)$, the packet is marked as violating the specified rate.
- If $B > Tc(t)$, the packet is marked as exceeding the specified rate, and the Tp(t) token bucket is updated as $Tp(t) = Tp(t) - B$.

Otherwise, the packet is marked as conforming to the specified rate, and both token buckets—Tc(t) and Tp(t)—are updated as follows:

$$Tp(t) = Tp(t) - B$$

$$Tc(t) = Tc(t) - B$$

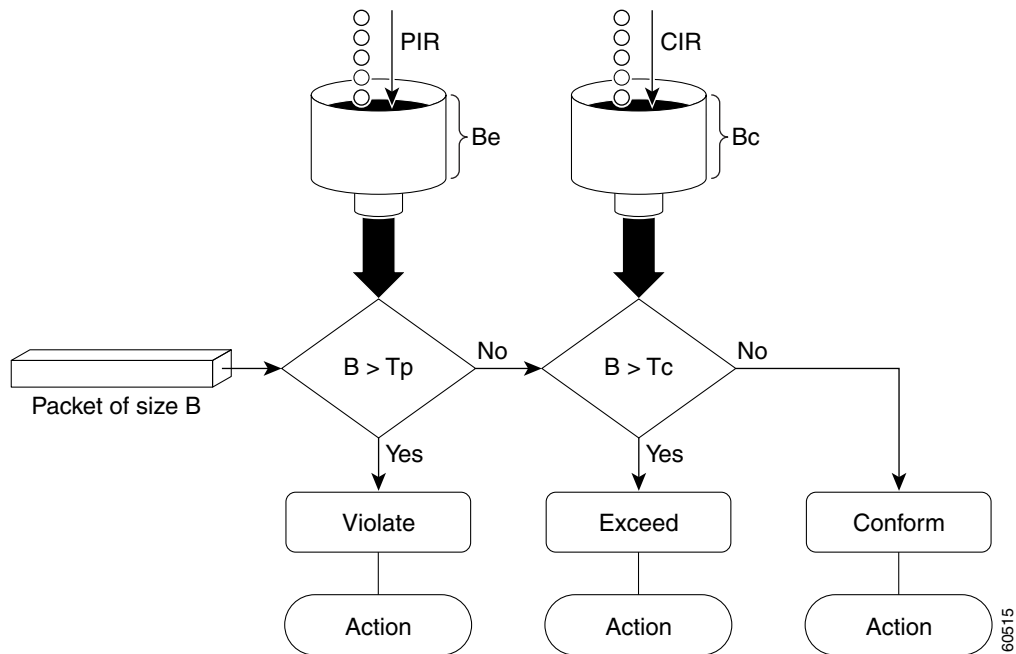
For example, if the CIR is 100 kbps, the PIR is 200 kbps, and a data stream with a rate of 250 kbps arrives at the two-rate policer, the packet would be marked as follows:

- 100 kbps would be marked as conforming to the rate.
- 100 kbps would be marked as exceeding the rate.
- 50 kbps would be marked as violating the rate.

Marking Packets and Assigning Actions 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 Marking Packets and Assigning Actions with the Two-Rate Policer



Examples

The following 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# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# class-map police
Switch(config-cmap)# match access-group 101
Switch(config-cmap)# policy-map policy1
Switch(config-pmap)# class police
Switch(config-pmap-c)# police cir 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 6/1
Switch(config-if)# service-policy output policy1
Switch(config-if)# end
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:

```
Switch# show policy-map interface gigabitethernet 6/1

GigabitEthernet6/1

Service-policy output: policy1

Class-map: police (match all)
 148803 packets, 36605538 bytes
 30 second offered rate 1249000 bps, drop rate 249000 bps
Match: access-group 101
police:
  cir 500000 bps, conform-burst 10000, pir 1000000, peak-burst 100000
  conformed 59538 packets, 14646348 bytes; action: transmit
  exceeded 59538 packets, 14646348 bytes; action: set-prec-transmit 2
  violated 29731 packets, 7313826 bytes; action: drop
  conformed 499000 bps, exceed 500000 bps violate 249000 bps

Class-map: class-default (match-any)
 19 packets, 1990 bytes
 30 seconds offered rate 0 bps, drop rate 0 bps
Match: any
Switch#
```

The two-rate policer marks 500 kbps of traffic as conforming, 500 kbps of traffic as exceeding, and 250 kbps of traffic as violating the specified rate. Packets marked as conforming to the rate will be sent as is, and packets marked as exceeding the rate will be marked with IP Precedence 2 and then sent. Packets marked as violating the rate are dropped.

policy-map

To create or modify a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode, use the **policy-map** global configuration command. To delete an existing policy map and to return to global configuration mode, use the **no** form of this command.

policy-map *policy-map-name*

no policy-map *policy-map-name*

Syntax Description

policy-map-name Name of the policy map.

Command Default

No policy maps are defined.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch.
12.2(40)SG	Extended support to Supervisor Engine 6-E and the Catalyst 4900M 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 2-96.
- **description**—Describes the policy map (up to 200 characters).
- **exit**—Exits policy-map configuration mode and returns you to global configuration mode.
- **no**—Removes a previously defined policy map.

To return to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

You can configure class policies in a policy map only if the classes have match criteria defined for them. To configure the match criteria for a class, use the **class-map** global configuration and **match** class-map configuration commands.

Examples

The following example shows how to configure multiple classes in a policy map called `polycymap2` on a Supervisor Engine 6-E:

```
Switch# configure terminal
Switch(config)# policy-map polycymap2
```

```

Switch(config-pmap) # class class1
Switch(config-pmap-c) # police 10000 20000 exceed-action
Switch(config-pmap-c) # set-dscp-transmit cs3
Switch(config-pmap-c) # set-cos-transmit 3
Switch(config-pmap-c) # exit
Switch(config-pmap) # class class2
Switch(config-pmap-c) # police cir 32000 pir 64000 conform-action transmit exceed-action
Switch(config-pmap-c) # set-dscp-transmit cs3 violate-action drop
Switch(config-pmap-c) # exit
Switch(config-pmap) # class class3
Switch(config-pmap-c) # set dscp cs3
Switch(config-pmap-c) # exit
Switch#

```

The following example shows how to delete the policy map called policymap2:

```

Switch# configure terminal
Switch(config) # no policy-map policymap2
Switch#

```

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

Related Commands

Command	Description
class	Specifies the name of the class whose traffic policy you want to create or change.
class-map	Creates a class map to be used for matching packets to the class whose name you specify and to enter class-map configuration mode.
policy-map	Creates or modifies a policy map that can be attached to 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 an interface belongs to.
show policy-map	Displays information about the policy map.

port-channel load-balance

To set the load-distribution method among the ports in the bundle, use the **port-channel load-balance** command. To reset the load distribution to the default, use the **no** form of this command.

port-channel load-balance *method*

no port-channel load-balance

Syntax Description	<i>method</i> Specifies the load distribution method. See the “Usage Guidelines” section for more information.				
Command Default	Load distribution on the source XOR destination IP address is enabled.				
Command Modes	Global configuration mode				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.1(8a)EW</td> <td>This command was introduced on the Catalyst 4500 series switch.</td> </tr> </tbody> </table>	Release	Modification	12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch.
Release	Modification				
12.1(8a)EW	This command was introduced on the Catalyst 4500 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

The following example shows how to set the load-distribution method to the destination IP address:

```
Switch(config)# port-channel load-balance dst-ip
Switch(config)#
```

The following example shows how to set the load-distribution method to the source XOR destination IP address:

```
Switch(config)# port-channel load-balance src-dst-port
Switch(config)#
```

Related Commands	Command	Description
	interface port-channel	Accesses or creates a port-channel interface.
	show etherchannel	Displays EtherChannel information for a channel.

port-channel standalone-disable

To disable the EtherChannel standalone option in a port channel, use the **port-channel standalone-disable** command in interface configuration mode. To enable this option, use the no form of this command.

port-channel standalone-disable

no port-channel standalone-disable

Syntax Description This command has no arguments or keywords.

Command Default The standalone option is disabled.

Command Modes Interface configuration mode

Command History	Release	Modification
	15.0(2)SG1	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines This command can only be used when the port channel protocol type is Link Aggregation Control Protocol (LACP). It allows you to change the current behavior when a physical port cannot bundle with an LACP EtherChannel.

Examples The following example shows how to enable the EtherChannel standalone option in a port channel:

```
Switch(config-if)# no port-channel standalone-disable
```

Related Commands	Command	Description
	show etherchannel	Displays EtherChannel information for a channel.

port-security mac-address

To configure a secure address on an interface for a specific VLAN or VLAN range, use the **port-security mac-address** command.

port-security mac-address *mac_address*

Syntax Description	<i>mac_address</i>	The MAC-address that needs to be secured.
---------------------------	--------------------	---

Command Modes	VLAN-range interface submenu
----------------------	------------------------------

Command History	Release	Modification
	12.2(25)EWA	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 use the port-security mac-address command to specify different addresses on different VLANs.
-------------------------	--

Examples	The following example shows how to configure the secure address 1.1.1 on interface Gigabit Ethernet 1/1 for VLANs 2-3:
-----------------	--

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# vlan 2-3
Switch(config-if-vlan-range)# port-security mac-address 1.1.1
Switch(config-if-vlan-range)# end
Switch#
```

Related Commands	Command	Description
	port-security mac-address sticky	Configures a sticky address on an interface for a specific VLAN or VLAN range.
	port-security maximum	Configures the maximum number of addresses on an interface for a specific VLAN or VLAN range.

port-security mac-address sticky

To configure a sticky address on an interface for a specific VLAN or VLAN range, use the **port-security mac-address sticky** command.

port-security mac-address sticky *mac_address*

Syntax Description

<i>mac_address</i>	The MAC-address that needs to be secured.
--------------------	---

Command Modes

VLAN-range interface submode

Command History

Release	Modification
12.2(25)EWA	This command was introduced on the Catalyst 4500 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

The following example shows how to configure the sticky address 1.1.1 on interface Gigabit Ethernet 1/1 for VLANs 2-3:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# vlan 2-3
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	<i>max_value</i>	The maximum number of MAC-addresses.
---------------------------	------------------	--------------------------------------

Command Modes	VLAN-range interface submode
----------------------	------------------------------

Command History	Release	Modification
	12.2(25)EWA	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 use 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 The following example shows how to configure a maximum number of addresses (5) on interface Gigabit Ethernet 1/1 for VLANs 2-3:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface g1/1
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)# exit
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	<i>watts</i>	Sets the total capacity of the external DC source in watts; valid values are from 300 to 8500.
---------------------------	--------------	--

Command Default	DC power input is 2500 W.
------------------------	---------------------------

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

Command History	Release	Modification
	12.1(11)EW	This command was introduced on the Catalyst 4500 series switch.
	12.1(13)EW	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 Admin
-------------------------	--

Examples	The following example shows how to set the total capacity of the external DC power source to 5000 W: <pre>Switch(config)# power dc input 5000 Switch(config)#</pre>
-----------------	--

Related Commands	Command	Description
	show power	Displays information about the power status.

power efficient-ethernet auto

To enable EEE, use the **power efficient-ethernet auto** command. To disable EEE, use the **no** form of this command.

power efficient-ethernet auto

no power efficient-ethernet auto

Syntax Description This command has no arguments or keywords.

Command Default EEE is disabled

Command Modes Global configuration mode

Command History	Release	Modification
	Release IOS XE 3.4.0SG and IOS 15.1(2)SG	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines EEE is supported on WS-X4748-UPOE+E and WS-X4748-RJ45-E.

EEE defines support for physical layer devices (PHYs) to operate in Low Power Idle (LPI) mode. When enabled, EEE supports QUIET times during low link utilization allowing both sides of a link to disable portions of each PHY's operating circuitry and save power. This functionality is provided per port and is not enabled by default. To avoid issues with EEE functionality on any port during run-time, Cisco provides the **power efficient-ethernet auto** command to enable or disable EEE.

Because EEE relies on Auto Negotiation pulse to determine whether to activate EEE, the port must initially enable auto negotiation. Furthermore, EEE is the correct action provided the speed is auto 100M, auto 1000M, or auto 100M and 1000M. 10M (either auto or forced mode) does not require EEE for power saving.

Examples The following example shows how to enable EEE:

```
Switch# config t
Switch(config)# interface gigabitethernet 1/1
Switch(config-if)# power efficient-ethernet auto
Switch(config-if)# exit
```

power inline

To set the inline-power state for the inline-power-capable interfaces, use the **power inline** command. To return to the default values, use the **no** form of this command.

```
power inline {auto [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 <i>milliwatt</i>	(Optional) Sets the maximum power that the equipment can consume; valid range is from 2000 to 15400 mW for classic modules. For the WS-X4648-RJ45V-E, the maximum is 20000. For the WS-X4648-RJ45V+E, the maximum is 30000.
never	Disables both the detection and power for the inline-power capable interfaces.
static	Allocates power statically.
consumption <i>milliwatt</i>	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.

Command Default

The default settings are as follows:

- Auto mode for Power over Ethernet is set.
- Maximum mW mode is set to 15400. For the WS-X4648-RJ45V-E, the maximum mW is set to 20000. For the WS-X4648-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)EW	This command was introduced on the Catalyst 4500 series switch.
12.1(19)EW	Support added for static power allocation.
12.1(20)EW	Support added for Power over Ethernet.
12.2(44)SG	Maximum supported wattage increased beyond 15400 for the WS-X4648-RJ45V-E and the WS-X4648-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

The following 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#
```

The following 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#
```

The following 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#
```

The following example shows how to pre-allocate Power over Ethernet to 16500 mW for Gigabit Ethernet interface 2/1 regardless of what is mandated either by the 802.3af class of the discovered device or by any CDP packet that is received from the powered device:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet 2/1
Switch(config-if)# power inline static max 16500
Switch(config-if)# 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.
	<i>milliwatts</i>	Sets the default power allocation in milliwatts; the valid range is from 4000 to 15399. Any non-default value disables automatic adjustment of power allocation.

Command Default Milliwatt mode is set to 15400.

Command Modes Global configuration mode

Command History	Release	Modification
	12.1(11)EW	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 allocated to the port through IEEE/Cisco phone 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 Admin
```

Examples

The following example shows how to set the Power over Ethernet allocation to use 8000 mW, regardless of any CDP packet that is received from the powered device:

```
Switch# configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Switch(config)# power inline consumption default 8000  
Switch(config)# end  
Switch#
```

Related Commands

Command	Description
power inline	Sets the inline-power state for the inline-power-capable interfaces.
show power	Displays information about the power status.

power inline four-pair forced



Note

This command is available only on Supervisor Engine 7-E, Supervisor Engine 7L-E, and Supervisor Engine 8-E.

To automatically enable power on both signal and spare pairs from a switch port, provided the end-device is PoE capable on both signal and spare pairs but does not support the CDP or LLDP extensions required for UPOE, use the **power inline four-pair forced** command.

power inline four-pair forced

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
15.0(2)SG	This command was introduced on the Catalyst 4500 series switch using a Supervisor Engine 7-E and 7L-E.

Usage Guidelines

Although IEEE 802.3at only provides for power up to 30W per port, the WS-X4748-UPOE+E module can provide up to 60W using the spare pair of an RJ45 cable (wires 4,5,7,8) with the signal pair (wires 1,2,3,6). Power on the spare pair is enabled when the switch port and end-device mutually identify themselves as UPOE capable using CDP or LLDP and the end-device requests for power on the spare pair to be enabled. When the spare pair is powered, the end-device can negotiate up to 60W power from the switch using CDP or LLDP.

If the end-device is PoE capable on both signal and spare pairs but does not support the CDP or LLDP extensions required for UPOE, then the following configuration automatically enables power on both signal and spare pairs from the switch port

Examples

The following example shows how to automatically enable power on both signal and spare pairs from switch port gigabit ethernet 2/1:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitEthernet 2/1
Switch(config-if)# power inline four-pair forced
Switch(config-if)# shutdown
Switch(config-if)# no shutdown
Switch(config-if)# end
Switch#
```

Do not enter this command if the end-device is incapable of sourcing inline power on the spare pair or if the end-device supports the CDP or LLDP extensions for UPOE.

power inline logging global

To enable console messages that show when a PoE device has been detected and to show when a PoE device has been removed, use the **power inline logging global** command.

power inline logging global

Syntax Description This command has no arguments or keywords.

Command Default Disabled

Command Modes Global configuration mode

Command History	Release	Modification
	15.0(2)SG2/ XE 3.2.2SG	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines Be aware of the potential for console flooding if this command is used on a switch connected to several PoE devices.

Examples The following example shows how to globally enable PoE status messaging on each interface:

To enable PoE event logging, you use the **logging event poe-status global** command:

```
Switch# conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# power inline logging global
Switch(config)# int gigabitEthernet 5/5
Switch(config-if)# shut
Switch(config-if)#
*Oct 17 12:02:48.407: %ILPOWER-5-IEEE_DISCONNECT: Interface Gi5/5: PD removed
Switch(config-if)# no shut
Switch(config-if)#
*Oct 17 12:02:54.915: %ILPOWER-7-DETECT: Interface Gi5/5: Power Device detected: IEEE PD
```

Related Commands	Command	Description
	logging event link-status global (global configuration)	Changes the default switch-wide global link-status event messaging settings.

power inline police

To configure Power over Ethernet policing on a particular interface, use the **power inline police** command. The **no** form of the command disables PoE policing on an interface.

power inline police [action] [errdisable | log]

no power inline police [action] [errdisable | 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 allocated).
errdisable	(Optional) Enables PoE policing on the interface and places the port in an errdisable 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.

Command Default

PoE policing is disabled.

Command Modes

Interface configuration mode

Command History

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

Usage Guidelines

If a port is in the errdisable 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 errdisable autorecovery so that an errdisabled interface is automatically revived when the errdisable autorecovery timer expires.

Examples

The following example shows how to enable PoE policing and configure a policing action:

```
Switch(config)# int gigabitEthernet 2/1
Switch(config-if)# power inline police
Switch(config-if)# do show power inline police gigabitEthernet 2/1
Available:421(w)  Used:39(w)  Remaining:382(w)
```

Interface	Admin State	Oper State	Admin Police	Oper Police	Cutoff Power	Oper Power
Gi2/1	auto	on	errdisable	ok	17.4	7.6

```
Switch(config-if)# power inline police action log
Available:421(w)  Used:39(w)  Remaining:382(w)
```

Interface	Admin State	Oper State	Admin Police	Oper Police	Cutoff Power	Oper Power
-----	-----	-----	-----	-----	-----	-----
Gi2/1	auto	on	log	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 combined max inputs

To configure the power settings for the chassis specifically for 'Combined Mode Resiliency', use the **power redundancy combined max inputs** command. To return to the default setting, use the **default** form of this command.


Note

This feature only applies in combined mode when both power supply bays contain the 4200 W AC, 6000 W AC, or 9000W power supply.

power redundancy combined max inputs {x | y}

default power redundancy combined max inputs

Syntax Description

x | y

Sets the max input limits.

If 9000W power supplies are installed, the valid input range is 2-5.

Note The maximum number of power-supply inputs with two 9000W power supplies is 6.

If 4200W or 6000W power supplies are installed, the valid input range is 2-3.

Note The maximum number of power-supply inputs with either two 4200W or two 6000W power supplies is 4.

Command Default

Redundant power management mode

Command Modes

Global configuration mode

Command History
Release
Modification

IOS XE 3.4.0SG and 15.1(2)SG This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

Using the combined mode power resiliency feature, you can limit the power usage to a maximum of two or three (configurable) inputs for 4000W and 6000W power supplies. For 9000W power supplies, you can limit the power usage to a maximum of 2 to 5 inputs, since the 9000W is a triple input power supply.

With two 4200 W AC or 6000 W AC power supplies, a maximum of four inputs are available. With two 9000W, a maximum of six inputs are available. This feature allows you to cap the power usage to that of two/three inputs or four/five inputs. If one of the power supplies fails, no loss of power occurs because you have capped its usage to a smaller number of inputs.

If you have max inputs 3 configured with four "good" (220 V) inputs and you limit the user to 5500 W instead of 7600 W and one subunit fails or is powered off, you have three quality inputs providing 5500 W and the chassis is powered at the same rate as it was prior to the failure event:

```
Switch# configuration terminal
```

```

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# power redundancy combined max inputs 3
Switch(config)# end
Switch#
14:32:01: %SYS-5-CONFIG_I: Configured from console by console

```

Here is the output of the **show power** command prior to invoking this feature:

```

Switch# show power
sh power
Power
Supply Model No Type Status Fan Sensor Inline Status
-----
PS1 PWR-C45-4200ACV AC 4200W good good good
PS1-1 110V good
PS1-2 110V good
PS2 PWR-C45-4200ACV AC 4200W good good good
PS2-1 110V good
PS2-2 110V good

Power supplies needed by system : 1
Power supplies currently available : 2

Power Summary
(in Watts) Used Maximum Available
-----
System Power (12V) 140 1360
Inline Power (-50V) 0 1850
Backplane Power (3.3V) 0 40
-----
Total 140 (not to exceed Total Maximum Available = 2100)

```

Here is the output after invoking this feature. The combined mode was indicated before **Power supplies needed = 2** in the output of the **show power** command, combined mode is now indicated by the phrase **Power supplies needed by system: 2 Maximum Inputs = 3**.

```

Switch# show power
sh power
Power
Supply Model No Type Status Fan Sensor Inline Status
-----
PS1 PWR-C45-4200ACV AC 4200W good good good
PS1-1 110V good
PS1-2 110V good
PS2 PWR-C45-4200ACV AC 4200W good good good
PS2-1 110V good
PS2-2 110V good

Power supplies needed by system : 2 Maximum Inputs = 3
Power supplies currently available : 2

Power Summary
(in Watts) Used Maximum Available
-----
System Power (12V) 140 2400
Inline Power (-50V) 0 2000
Backplane Power (3.3V) 0 40
-----
Total 140 (not to exceed Total Maximum Available = 2728)

Switch#

```

Here's another example of combined mode resiliency with 9000W power supply with a maximum of six active inputs, limited to 3 inputs:

```
Switch# show power
Power
Supply Model No Type Status Fan Sensor Inline Status
-----
PS1 PWR-C45-9000ACV AC 9000W good good good
PS1-1 220V good
PS1-2 220V good
PS1-3 220V good
PS2 PWR-C45-9000ACV AC 9000W good good good
PS2-1 220V good
PS2-2 220V good
PS2-3 220V good
```

```
Power supplies needed by system : 2 Maximum Inputs = 3
Power supplies currently available : 2
```

```
Power Summary
(in Watts) Used Maximum Available
-----
System Power (12V) 1323 2646
Inline Power (-50V) 0 6022
Backplane Power (3.3V) 40 67
-----
Total 1363 (not to exceed Total Maximum Available = 7412)
t
```

Examples

The following example shows how to configure the combined mode resiliency feature when a 9000W AC power supply is detected.



Note The power usage is limited to four or five inputs.



Note The maximum inputs part of the command is ignored by all power supplies other than 9000 W AC.

```
Switch# configure terminal
Switch(config)# power redundancy combined max inputs {2 | 5}
```

The following example shows how to configure the combined mode resiliency feature if a 9000W AC power supply is not detected.



Note The power usage is limited to two or three inputs.



Note The maximum inputs part of the command is ignored by all power supplies other than the 4200 W AC or 6000 W AC.

```
Switch# configure terminal
Switch(config)# power redundancy combined max inputs {2 | 3}
```


Related Commands	Command	Description
	show power	Displays information about the power status.

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.

Command Default

Redundant power management mode

Command Modes

Global configuration mode

Command History

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

Usage Guidelines

The two power supplies must be the same type and wattage.



Caution

If you have power supplies with different types or wattages installed in your switch, the switch will not recognize one of the power supplies. A switch set to redundant mode will not have power redundancy. A switch set to combined mode will use only one power supply.

In redundant mode, the power from a single power supply must provide enough power to support the switch configuration.

[Table 2-12](#) lists the maximum available power for chassis and Power over Ethernet for each power supply.

Table 2-12 Available Power for Switch Power Supplies

Power Supply	Redundant Mode (W)	Combined Mode (W)	Sharing Ratio
1000 W AC	Chassis ¹ = 1050 PoE = 0	Chassis = 1667 PoE = 0	2/3
1300 W AC	Chassis (max) = 1050 PoE (max) = 800 Chassis + PoE + Backplane ≤ 1300	Chassis (min) = 767 PoE (max) = 1333 Chassis (max) = 1667 PoE (min) = 533 Chassis + PoE + Backplane ≤ 2200	2/3
1400 W DC	Chassis (min) = 200 Chassis (max) = 1360 PoE (max) ² = (DC Input ³ - [Chassis (min) + Backplane] / 0.75) * 0.96	Chassis = 2267 ⁴ PoE ⁵	Chassis—2/3 PoE—0
1400 W AC	Chassis = 1360 PoE = 0 ⁶	Chassis = 2473 PoE = 0	9/11
2800 W AC	Chassis = 1360 PoE = 1400	Chassis = 2473 PoE = 2333	Chassis ⁷ —9/11 PoE ⁸ —2/3

1. Chassis power includes power for the supervisor engine(s), all line cards, and the fan tray.
2. The efficiency for the 1400 W DC power supply is 0.75, and 0.96 is applied to PoE.
3. DC input can vary for the 1400 W DC power supply and is configurable. F.
4. Not available for PoE.
5. Not available for PoE.
6. No voice power.
7. Data-only.
8. Inline power.

Special Considerations for the 4200 W AC, 6000 W AC, and 9000W Power Supplies

The 4200 W AC and 6000 W AC power supply has two inputs: each can be powered at 110 or 220 V.

The 9000 W AC power supply has three inputs: each can be powered at 110 or 220V.

As with other power supplies, the two power supplies must be of the same type (6000 W AC or 4200 W AC or 9000 W AC). Otherwise, the right power supply is put in err-disable state and the left one is selected. In addition, all the inputs to the chassis must be at the same voltage. In redundant mode, the inputs to the left and right power supplies must be identical. If the left and right power supplies are powered in redundant mode, the power values is based on the power supply with the higher output wattage.



Note

When the system is powered with a 4200 W, 6000 W, or 9000W power supply either in 110 V or 220 V combined mode operation, the available power is determined by the configuration of the system (the type of line cards, the number of line cards, number of ports consuming inline power, etc.) and does not reflect the absolute maximum power.

**Note**

In a matched redundant power supply configuration, if a power supply submodule fails, the other (good) power supply provides power to its full capability.

Table 2-13 illustrates how the 4200 W AC power supply is evaluated in redundant mode.

Table 2-13 Power Output in Redundant Mode for the 4200 W AC Power Supply

Power Supply	Chassis Power	Inline Power
110 V	660	700
110 V+110 V or 220 V	1360	1850
220 V+220 V	1360	3700

In combined mode, all the inputs to the chassis must be at the same voltage.

Table 2-14 illustrates how the 4200 W AC power supply is evaluated in combined mode.

Table 2-14 Combined Mode Output for the 4200 W AC Power Supply

Power Supply	Chassis Power	Inline Power
Both sides (bays) at 110 V	1200	1320
110 V+110 V, other side 110 V	1800	2000
Both sides at 110 V+110 V	2200	3100
Both sides at 220 V	2200	3100
220 V+220 V, other side 220 V	2200	4700
Both sides at 220 V+220 V	2200	6200

Table 2-15 illustrates how the 6000 W AC power supply is evaluated in redundant mode.

Table 2-15 Power Output in Redundant Mode for the 6000 W AC Power Supply

Power Supply	Chassis Power	Inline Power
110 V	850	922
110 V+110 V or 220V	1700	1850
220 V+220 V	2200	4800

In combined mode, all the inputs to the chassis must be at the same voltage.

Table 2-16 illustrates how the 6000 W AC power supply is evaluated in combined mode.

Table 2-16 Combined Mode Output for the 6000 W AC Power Supply

Power Supply	Chassis Power	Inline Power
Both sides (bays) at 110 V	1400	1670
110 V+110 V, other side 110 V	2360	2560

Table 2-16 Combined Mode Output for the 6000 W AC Power Supply

Power Supply	Chassis Power	Inline Power
Both sides at 110 V+110 V	3090	3360
Both sides at 220 V	4000	4360
220 V+220 V, other side 220 V	4000	6600
Both sides at 220 V+220 V	4000	8700

Table 2-17 illustrates how the 9000 W AC power supply is evaluated in redundant mode.

Table 2-17 Power Output in Redundant Mode for the 9000 W AC Power Supply

Power Supply	12V (data) (W)	-50V (PoE) (W)	¹ Total Power (W)
110VAC	960	1000	1100
110VAC + 110 VAC	1460	2000	2200
110VAC + 110 V AC+ 110VAC	1460	2500	3300
220VAC	1460	2500	3000
220VAC + 220VAC	1960	5000	6000
220VAC + 220VAC + 220VAC	1960	7500	9000

1. Power supply output drawings should not exceed the total power.

Table 2-18 illustrates how the 9000 W AC power supply is evaluated in combined mode.

Table 2-18 Power Output in Combined Mode for the 9000 W AC Power Supply

Power Supply	12V (data) (W)	-50V (PoE) (W)	¹ Total Power (W)
Both sides at 110 VAC	1594	1420	1790
Both sides at 110VAC + 110VAC	2627	3320	3610
Both sides at 110VAC + 110VAC + 110VAC	2627	4150	5420
One side at 110VAC + 110VAC + 110VAC, the other at 110VAC + 110VAC	2019	3458	4520
One side at 110VAC + 110VAC + 110VAC, the other at 110VAC	1615	2367	3620
One side at 110VAC + 110VAC, the other at 110VAC	1615	2130	2710
Both sides at 220VAC	2828	4150	4930
Both sides at 220VAC + 220VAC	3762	8300	10140
Both sides at 220VAC + 220VAC + 220VAC	3762	14400	17210

Table 2-18 Power Output in Combined Mode for the 9000 W AC Power Supply

Power Supply	12V (data) (W)	-50V (PoE) (W)	¹ Total Power (W)
One side at 220VAC + 220VAC + 220VAC, the other at 220VAC + 220VAC	2939	11250	13440
One side at 220VAC + 220VAC + 220VAC, the other at 220VAC	2168	8300	9890
One side at 220VAC + 220VAC, the other at 220VAC	2168	6225	7410

1. Power supply output drawings should not exceed the total power.

Examples

The following 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.

Command Default disabled

Command Modes Global configuration mode

Command History	Release	Modification
	12.2(50)SG	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 The following example shows how to enable PPPoE Intermediate Agent on a switch:

```
Switch(config)# pppoe intermediate-agent
```

The following 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.

Command Default

Disabled on all interfaces.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.2(50)SG	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

The following example shows how to enable the PPPoE Intermediate Agent on an interface:

```
Switch(config-if)# pppoe intermediate-agent
```

The following example shows how to disable the PPPoE Intermediate Agent on an interface:

```
Switch(config-if)# no pppoe intermediate-agent
```

Related Commands

Command	Description
pppoe intermediate-agent format-type (interface)	Sets circuit ID or remote ID for an interface.
pppoe intermediate-agent limit rate	Limits the rate of the PPPoE Discovery packets coming on an interface.
pppoe intermediate-agent trust	Sets the trust configuration of an interface.
pppoe intermediate-agent vendor-tag strip	Enables vendor-tag stripping on PPPoE Discovery packets from PPPoE Server (or BRAS).

pppoe intermediate-agent (interface vlan-range)



Note

This command takes effect only if you enable the **pppoe intermediate-agent** global command.

To enable PPPoE Intermediate Agent on an interface VLAN range, use the **pppoe intermediate-agent** global command. To disable the feature, use the **no** form of this command.

pppoe intermediate-agent

no pppoe intermediate-agent

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled on all VLANs on all interfaces

Command Modes

Interface vlan-range configuration mode

Command History

Release	Modification
12.2(50)SG	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

The following example shows how to enable PPPoE Intermediate Agent on a range of VLANs:

```
Switch(config-if)# vlan-range 167-368
Switch(config-if-vlan-range)# pppoe intermediate-agent
```

The following example shows how to disable PPPoE Intermediate Agent on a single VLAN:

```
Switch(config-if)# vlan-range 268
Switch(config-if-vlan-range)# no pppoe intermediate-agent
```

Related Commands

Command	Description
pppoe intermediate-agent (interface)	Enables the PPPoE Intermediate Agent feature on an interface.

pppoe intermediate-agent format-type (global)

To set the access node identifier, generic error message, and identifier string for the switch, use the **pppoe intermediate-agent format-type (global)** command. To disable the feature, use the **no** form of this command:

```
pppoe intermediate-agent format-type access-node-identifier string string
```

```
pppoe intermediate-agent format-type generic-error-message string string
```

```
pppoe intermediate-agent format-type identifier-string string string option {sp|sv|pv|spv}
delimiter {,|.|;|/|#}
```

```
no pppoe intermediate-agent format-type {access-node-identifier | generic-error-message |
identifier-string}
```

Syntax Description

access-node-identifier string <i>string</i>	ASCII string literal value for the access-node-identifier.
generic-error-message string <i>string</i>	ASCII string literal value for the generic-error-message.
identifier-string string <i>string</i>	ASCII string literal value for the identifier-string.
option {sp sv pv spv}	Options: sp = slot + port sv = slot + VLAN pv = port + VLAN spv = slot + port + VLAN
delimiter {, . ; / #}	Delimiter between slot/port/VLAN portions of option .

Command Default

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(50)SG	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 parameters automatically.

The **no** form of **identifier-string** command unsets the option and delimiter.

Use the **generic-error-message** command to set an error message notifying the sender that the PPPoE Discovery packet was too large.

Examples

The following example shows how to set an access-node-identifier:

```
Switch(config)# pppoe intermediate-agent format-type access-node-identifier string  
switch-abc-123
```

The following 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 parameters, use the **no** form of this command.

```
pppoe intermediate-agent format-type { circuit-id | remote-id } string string
```

```
no pppoe intermediate-agent format-type { circuit-id | remote-id } string string
```

Syntax Description

circuit-id string *string* ASCII string literal value for circuit-id.

remote-id string *string* ASCII string literal value for remote-id.

Command Default

No default values for circuit-id and remote-id.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.2(50)SG	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's automatic generated circuit-id value is used.

Examples

The following example shows how to set remote-id for an interface:

```
Switch(config-if)# pppoe intermediate-agent format-type remote-id string user5551983
```

The following example shows how to unset circuit-id for an interface:

```
Switch(config)# no pppoe intermediate-agent format-type circuit-id
```

Related Commands

Command	Description
pppoe intermediate-agent (interface)	Enables the PPPoE Intermediate Agent feature on an interface.
pppoe intermediate-agent (interface vlan-range)	Sets the circuit-id or remote-id for an interface vlan-range.

pppoe intermediate-agent format-type (interface vlan-range)



Note

This command takes effect only if you enable the **pppoe intermediate-agent** interface vlan-range configuration mode command.

To set circuit-id or remote-id for an interface vlan-range, use the **pppoe intermediate-agent format-type** interface vlan-range mode command. To unset the parameters, use the **no** form of this 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 <i>string</i>	ASCII string literal value to be set for circuit-id.
remote-id string <i>string</i>	ASCII string literal value to be set for remote-id.

Command Default

No default values for circuit-id and remote-id.

Command Modes

Interface vlan-range configuration mode

Command History

Release	Modification
12.2(50)SG	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

The following example shows how to set remote-id on an interface VLAN:

```
Switch(config-if)# vlan-range 268
Switch(config-if-vlan-range)#
pppoe intermediate-agent format-type remote-id string user5551983-cabletv
```

The following example shows how to unset circuit-id on an interface vlan-range:

```
Switch(config-if)# vlan-range 167-368
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	<i>number</i>	Specifies the threshold rate of PPPoE Discovery packets received on this interface in packets-per-second.
---------------------------	---------------	---

Command Default This command has no default settings.

Command Modes Interface configuration mode

Command History	Release	Modification
	12.2(50)SG	This command was introduced on the Catalyst 4500 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 The following example shows how to set a rate limit for an interface:

```
Switch(config-if)# pppoe intermediate-agent limit rate 50
```

The following example shows how to disable rate limiting for an interface:

```
Switch(config-if)# no pppoe intermediate-agent limit rate
```

Related Commands	Command	Description
	pppoe intermediate-agent (interface)	Enables the PPPoE Intermediate Agent feature on an interface

pppoe intermediate-agent trust

To set the trust configuration of an interface, use the **pppoe intermediate-agent trust** global command. To unset the trust parameter, use the **no** form of this command.

pppoe intermediate-agent trust

no pppoe intermediate-agent trust

Syntax Description This command has no arguments or keywords.

Command Default All interfaces are untrusted.

Command Modes Interface configuration mode

Command History	Release	Modification
	12.2(50)SG	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 The following example shows how to set an interface as trusted:

```
Switch(config-if)# pppoe intermediate-agent trust
```

The following example shows how to disable the trust configuration for an interface:

```
Switch(config-if)# no pppoe intermediate-agent trust
```

Related Commands	Command	Description
	pppoe intermediate-agent vendor-tag strip	Enables vendor-tag stripping on PPPoE Discovery packets from a PPPoE Server (or BRAS).

pppoe intermediate-agent vendor-tag strip



Note

This command takes effect only if you enable the **pppoe intermediate-agent** interface configuration command and the **pppoe intermediate-agent trust** command.

To enable vendor-tag stripping on PPPoE Discovery packets from PPPoE Server (or BRAS), use the **pppoe intermediate-agent vendor-tag strip** command. To disable this setting, use the **no** form of this command.

pppoe intermediate-agent vendor-tag strip

no pppoe intermediate-agent vendor-tag strip

Syntax Description

This command has no arguments or keywords.

Command Default

vendor-tag stripping is turned off.

Command Modes

Interface configuration mode

Command History

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

The following example shows how to set vendor-tag stripping on an interface:

```
Switch(config-if)# pppoe intermediate-agent vendor-tag strip
```

The following example shows how to disable vendor-tag stripping on an interface:

```
Switch(config-if)# no pppoe intermediate-agent vendor-tag strip
```

Related Commands

Command	Description
pppoe intermediate-agent (interface)	Enables the PPPoE Intermediate Agent feature on an interface.
pppoe intermediate-agent trust	Sets the trust configuration of an interface.

priority

To enable the strict priority queue (low-latency queueing [LLQ]) and to give priority to a class of traffic belonging to a policy map attached to a physical port, use the **priority** policy-map class configuration command. To return to the default setting, use the **no** form of this command.

priority

no priority

Syntax Description

This command has no arguments or keywords.

Command Default

The strict priority queue is disabled.

Command Modes

Policy-map class configuration mode

Command History

Release	Modification
12.2(40)SG	Support introduced on Supervisor Engine 6E and Catalyst 4900M.

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 queueing. Strict-priority queueing enables delay-sensitive data, such as voice, to be sent before packets in other queues are sent. The priority queue is serviced first until it 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 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

The following example shows how to enable the LLQ for the policy map called policy1:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# policy-map policy1
Switch(config-pmap)# class voice
Switch(config-pmap-c)# priority
```

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

Related Commands	Command	Description
	bandwidth	Specifies or modifies the minimum bandwidth 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** | **twoway-community** | **primary** }

private-vlan association *secondary-vlan-list* [{ **add** *secondary-vlan-list* } | { **remove** *secondary-vlan-list* }]

no private-vlan { **isolated** | **community** | **twoway-community** | **primary** }

no private-vlan association

Syntax	Description
isolated	Designates the VLAN as an isolated private VLAN.
community	Designates the VLAN as the community private VLAN.
twoway-community	Designates the VLAN as a host port that belongs to a twoway-community secondary VLAN
primary	Designates the VLAN as the primary private VLAN.
association	Creates an association between a secondary VLAN and a primary VLAN.
<i>secondary-vlan-list</i>	Specifies the number of the secondary VLAN. The list can contain only one isolated VLAN ID; it can also contain multiple community or twoway-community VLAN IDs
add	(Optional) Associates a secondary VLAN to a primary VLAN.
remove	(Optional) Clears the association between a secondary VLAN and a primary VLAN.

Command Default Private VLANs are not configured.

Command Modes VLAN configuration mode

Command History	Release	Modification
	12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW	Support for extended addressing was added.
	12.2(20)EW	Support for community VLAN was added.
	15.0(2)SG	Support for twoway-community was introduced.

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 only by the standard trunking ports and the promiscuous ports that are assigned to the corresponding primary VLAN.

A community VLAN is the VLAN that carries the traffic among the community ports and from the community ports to the promiscuous ports on the corresponding primary VLAN. A community VLAN is not allowed on a private VLAN trunk.

A promiscuous port is a private port that is assigned to a primary VLAN.

A primary VLAN is a VLAN that is used to convey the traffic from the switches to the customer end stations on the private ports.

You can specify only one isolated *vlan-id* value, while multiple community VLANs are allowed. You can only associate isolated and community VLANs to one VLAN. The associated VLAN list may not contain primary VLANs. Similarly, a VLAN that is already associated to a primary VLAN cannot be configured as a primary VLAN.

The **private-vlan** commands do not take effect until you exit the config-VLAN submode.

If you delete either the primary or secondary VLAN, the ports that are associated with the VLAN become inactive.

Refer to the *Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide* for additional configuration guidelines.

Examples

The following example shows how to configure VLAN 202 as a primary VLAN and verify the configuration:

```
Switch# configure terminal
Switch(config)# vlan 202
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# end
Switch# show vlan private-vlan
Primary Secondary Type                Interfaces
-----
202                primary
```

The following example shows how to configure VLAN 303 as a community VLAN and verify the configuration:

```
Switch# configure terminal
Switch(config)# vlan 303
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# end
Switch# show vlan private-vlan

Primary Secondary Type                Interfaces
-----
202                primary
                 303                community
```

The following example shows how to configure VLAN 440 as an isolated VLAN and verify the configuration:

```
Switch# configure terminal
Switch(config)# vlan 440
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# end
Switch# show vlan private-vlan
```

Primary	Secondary	Type	Interfaces
202		primary	
	303	community	
	440	isolated	

The following 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 14
Switch(config-vlan) # private-vlan primary
Switch(config-vlan) # private-vlan association 19
```

The following 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) #
```

The following example shows how to configure VLAN 550 as a twoway-community VLAN and verify the configuration:

```
Switch# configure terminal
Switch(config)# vlan 550
Switch(config-vlan)# private-vlan twoway-community
Switch(config-vlan)# end
Switch# show vlan private-vlan
```

Primary	Secondary	Type	Interfaces
202		primary	
	303	community	
	440	isolated	
	550	twoway-community	

The following example shows how to associate community VLANs 303 through 307 and 309 and isolated VLAN 440 with primary VLAN 202 and verify the configuration:

```
Switch# configure terminal
Switch(config)# vlan 202
Switch(config-vlan) # private-vlan association 303-307,309,440
Switch(config-vlan) # end
Switch# show vlan private-vlan
```

Primary	Secondary	Type	Interfaces
202	303	community	
202	304	community	
202	305	community	
202	306	community	
202	307	community	
202	309	community	

```

202    440    isolated
      308    community

```

**Note**

The secondary VLAN 308 has no associated primary VLAN.

The following 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)#

```

The following example shows how to configure interface FastEthernet 5/1 as a PVLAN host port and verify the configuration:

```

Switch# configure terminal
Switch(config)# interface fastethernet 5/1
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 202 440
Switch(config-if)# end

Switch# show interfaces fastethernet 5/1 switchport
Name: Fa5/1
Switchport: Enabled
Administrative Mode: private-vlan host
Operational Mode: private-vlan host
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Appliance trust: none
Administrative Private Vlan
  Host 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 vlan	Displays VLAN information.
show vlan private-vlan	Displays private VLAN information.

private-vlan mapping

To create a mapping between the primary and the secondary VLANs so that both share the same primary VLAN SVI, use the **private-vlan mapping** command. To remove all PVLAN mappings from an SVI, use the **no** form of this command.

```
private-vlan mapping primary-vlan-id {[secondary-vlan-list | {add secondary-vlan-list} |
{remove secondary-vlan-list}]}
```

```
no private-vlan mapping
```

Syntax Description	
<i>primary-vlan-id</i>	VLAN ID of the primary VLAN of the PVLAN relationship.
<i>secondary-vlan-list</i>	(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.

Command Default All PVLAN mappings are removed.

Command Modes Interface configuration mode

Command History	Release	Modification
	12.1(8a)EW	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

The following example shows how to map the interface of VLAN 20 to the SVI of VLAN 18:

```
Switch(config)# interface vlan 18
Switch(config-if)# private-vlan mapping 18 20
Switch(config-if)#
```

The following example shows how to permit the routing of the secondary VLAN ingress traffic from PVLANS 303 through 307, 309, and 440 and how to verify the configuration:

```
Switch# config 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#
```

The following example shows the displayed message that you will see if the VLAN that you are adding is already mapped to the SVI of VLAN 18. You must delete the mapping from the SVI of VLAN 18 first.

```
Switch(config)# interface vlan 19
Switch(config-if)# private-vlan mapping 19 add 21
Command rejected: The interface for VLAN 21 is already mapped as s secondary.
Switch(config-if)#
```

The following 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 to 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.

Command Default This command has no default settings.

Command Modes MST configuration mode

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

Usage Guidelines If you do not map the VLANs to the same instance as the associated primary VLAN 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 VLAN. The **private-vlan synchronize** command automatically maps all secondary VLANs to the same instance as the associated primary VLANs.

Examples The following 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 CIST instance 1. This example also shows the output if you try to change the mapping for the primary VLAN 2 only:

```
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# instance 1 vlan 2
Switch(config-mst)# exit
These secondary vlans are not mapped to the same instance as their primary:
->3
Switch(config)#
```

Related Commands	Command	Description
	show spanning-tree mst	Displays MST protocol information.

profile

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

profile *profile_name*

Syntax Description	<i>profile_name</i>	Specifies the profile name.
---------------------------	---------------------	-----------------------------

Command Default	This command has no default settings.
------------------------	---------------------------------------

Command Modes	cfg-call-home
----------------------	---------------

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

Usage Guidelines	When you enter the profile <i>profile_name</i> 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

The following example shows how to create and configure a user-defined call-home profile:

```
Switch(config)# call-home
Switch(cfg-call-home)# profile cisco
Switch(cfg-call-home-profile)# destination transport-method http
Switch(cfg-call-home-profile)# destination address http
https://172.17.46.17/its/service/oddce/services/DDCEService
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 "UPDOWN"
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.

profile flow

To enable Media Services Proxy (MSP), use the the **profile flow** command. To return to the default setting, use the **no** form of this command

profile flow

no profile flow

Syntax Description This command has no arguments or keywords.

Command Default This command has no default settings.

Command Modes config

Command History	Release	Modification
	Release IOS XE 3.4.0SG and IOS 15.1(2)SG	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines You must configure the MSP profile flow command to activate the MSP platform Packet parser. This is because the the MSP device handler is tightly coupled with MSP flow parser. Not enabling this CLI means that MSP will not send SIP, H323 notifications to IOS sensor.

Examples The following example shows how to enable MSP:

```
Switch(config)# profile flow
```

qos account layer-all encapsulation

To account for Layer 1 header length of 20 bytes in QoS policing features, use the **qos account layer-all encapsulation** command. To disable the use of additional bytes, use the **no** form of this command.

qos account layer-all encapsulation

no qos account layer-all encapsulation

Syntax Description This command has no arguments or keywords.

Command Default On Supervisor Engine 6-E, Supervisor Engine 6L-E, Catalyst 4900M, Catalyst 4948E, and Catalyst 4948E-F, policers account only for the Layer 2 header length in policing features. In contrast, in rate calculations, shapers account for header length as well as IPG.

Command Modes Global configuration

Command History	Release	Modification
	15.0(2)SG	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines Supervisor Engine 6-E, Supervisor Engine 6L-E, Catalyst 4900M, Catalyst 4948E, and Catalyst 4948E-F use the **qos account layer-all encapsulation** command to account for Layer 1 header of 20 bytes (preamble + IPG) and Layer 2 header in policing features. When this command is configured, policer statistics (in bytes) observed in the output of the **show policy-map interface** command reflect the Layer 1 header length as well (20 bytes per packet).

Examples The following example shows how to shows how to include IPG in policing:

```
Switch)# config t
Switch(config)# qos account layer-all encapsulation
Switch(config)# end
Switch#
```

Related Commands	Command	Description
	show policy-map interface	Displays policer statistics on a specific interface.

qos account layer2 encapsulation

To include additional bytes to be accounted by the QoS features, use the **qos account layer2 encapsulation** command. To disable the use of additional bytes, use the **no** form of this command.

```
qos account layer2 encapsulation {arpa | dot1q | isl | length len}
```

```
no qos account layer2 encapsulation {arpa | dot1q | isl | length len}
```

Syntax Description

arpa	Specifies the account length of the Ethernet ARPA-encapsulated packet (18 bytes).
dot1q	Specifies the account length of the 802.1Q-encapsulated packet (22 bytes).
isl	Specifies the account length of the ISL-encapsulated packet (48 bytes).
length <i>len</i>	Specifies the additional packet length to account for; the valid range is from 0 to 64 bytes.

Command Default

On Supervisor Engine 6E, Supervisor Engine 6L-E, Catalyst 4900M, and Catalyst 4948-E, 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
12.1(19)SG	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

On Supervisor Engine 6E, Supervisor Engine 6L-E, Catalyst 4900M, and Catalyst 4948-E, shaping and sharing always use Ethernet ARPA length to which 20 bytes of IPv6 overhead is always added for policing. However, only Layer 2 length including VLAN tag overhead is considered.



Note

The given length is included when policing all IP packets irrespective of the encapsulation with which it was received. When **qos account layer2 encapsulation isl** is configured, a fixed length of 48 bytes is included when policing all IP packets, not only those IP packets that are received with ISL encapsulation.

Sharing and shaping use the length that is specified in the Layer 2 headers.

Examples

The following example shows how to include an additional 18 bytes when policing IP packets:

```
Switch# config terminal
Switch(config)# qos account layer2 encapsulation length 18
Switch (config)# end
Switch#
```

The following example shows how to disable the consistent accounting of the Layer 2 encapsulation by the QoS features:

```
Switch# config terminal
Switch(config)# no qos account layer2 encapsulation
Switch (config)# end
Switch #
```

Related Commands

Command	Description
show interfaces	Displays traffic on a specific interface.
switchport	Modifies the switching characteristics of a Layer 2 switch interface.
switchport block	Prevents the unknown multicast or unicast packets from being forwarded.

qos trust

To set the trusted state of an interface (for example, whether the packets arriving at an interface are trusted to carry the correct CoS, ToS, and DSCP classifications), use the **qos trust** command. To set an interface to the untrusted state, use the **no** form of this command.

```
qos trust { cos | device cisco-phone | dscp | extend [cos priority] }
```

```
no qos trust { cos | device cisco-phone | dscp | extend [cos priority] }
```

Syntax Description

cos	Specifies that the CoS bits in incoming frames are trusted and derives the internal DSCP value from the CoS bits.
<i>device cisco-phone</i>	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 <i>priority</i>	(Optional) Specifies that the CoS priority value is set to PVID packets; valid values are from 0 to 7.

Command Default

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(8a)EW	This command was introduced on the Catalyst 4500 series switch.
12.1(11)EW	Support for extending trust for voice was added.
12.1(19)EW	Support for trust device Cisco IP phone was added.

Usage Guidelines

You can only configure the trusted state on physical LAN interfaces.

A trusted boundary should not be configured on ports that are part of an EtherChannel (that is, a port channel).

By default, the trust state of an interface when QoS is enabled is untrusted; when QoS is disabled on the interface, the trust state is reset to trust DSCP.

When the interface trust state is **qos trust cos**, the transmit CoS is always the incoming packet CoS (or the default CoS for the interface, if the packet is 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.

Examples

The following example shows how to set the trusted state of an interface to CoS:

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

The following example shows how to set the trusted state of an interface to DSCP:

```
Switch(config-if)# qos trust dscp
Switch(config-if)#
```

The following example shows how to set the PVID CoS level to 6:

```
Switch(config-if)# qos trust extend cos 6
Switch(config-if)#
```

The following 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
queue-limit	Defines per-VLAN QoS for a Layer 2 interface.
show qos interface	Displays QoS information for an interface.

queue-limit

To specify or modify the maximum number of packets the queue can hold for a class policy configured in a policy map, use the **queue-limit** command. To remove the queue packet limit from a class, use the **no** form of this command.

queue-limit *number-of-packets*

no queue-limit *number-of-packets*

Syntax Description

<i>number-of-packets</i>	Number of packets that the queue for this class can accumulate; valid range is 16 to 8184. This number must be a multiple of 8.
--------------------------	---

Command Default

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 linecards.

Command Modes

QoS policy-map class configuration mode

Command History

Release	Modification
12.2(44)SG	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

The class-based queuing (CBQ) command applies only to the Supervisor Engine 6-E and Catalyst Engine 6L-E as part of MQC support on the Catalyst 4500 switch.

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 512K queue entries of which 100 K are set aside as a common sharable 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 criterion for a class accumulate in the queue reserved for the class until they are sent, which occurs when the queue is serviced by the fair queuing process. When the maximum packet threshold you defined for the class is reached, queuing of any further packets to the class queue causes tail drop or, if DBL is configured for the class policy, packet drop to take effect.



Note

The queue-limit command is supported only after you first configure a scheduling action, such as bandwidth, or priority, except when you configure queue-limit in the class-default class of an output QoS policy-map.s

Examples

The following example shows how to configure a policy-map called policy11 to contain policy for a class called acl203. Policy for this class is set so that the queue reserved for it has a maximum packet limit of 40:

```
Switch# configure terminal
Switch (config)# policy-map policy11
Switch (config-pmap)# class acl203
Switch (config-pmap-c)# bandwidth 2000
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-based queuing)	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.

Command Default This command has no default settings.

Command Modes Global configuration mode

Command History	Release	Modification
	12.1(12c)EW	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 reenabling redundancy, the switch returns to default redundancy settings.

Use the **exit** command to exit the redundancy configuration mode.

Examples The following example shows how to enter redundancy mode:

```
Switch(config)# redundancy
Switch(config-red)#
```

The following 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.
main-cpu	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 resets the standby supervisor engine, use the **redundancy config-sync mismatched-commands** command.

If your active and standby supervisors engines are running different versions of Cisco IOS, some of their CLIs will not be compatible. If such commands are already present in the running configuration of the active supervisor engine and the syntax-check for the command fails at the standby supervisor engine while it is booting, you must move the active supervisor engine into the Mismatched Command List (MCL).

redundancy config-sync {ignore | validate} mismatched-commands

Syntax Description	ignore	Ignore the mismatched command list.
	validate	Revalidate the mismatched command list with the modified running-configuration.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.2(31)SGA	This command was introduced on the Catalyst 4500 series switch.
	12.2(44)SG	Updated command name from issu config-sync to redundancy config-sync .

Usage Guidelines The following is a log entry example for mismatched commands:

```
00:06:31: Config Sync: Bulk-sync failure due to Servicing Incompatibility. Please check
full list of mismatched commands via:
  show redundancy config-sync failures mcl
00:06:31: Config Sync: Starting lines from MCL file:
interface GigabitEthernet7/7
 ! <submode> "interface"
- ip address 11.0.0.1 255.0.0.0
 ! </submode> "interface"
```

To display all mismatched commands, use the **show redundancy config-sync failures mcl** command.

To clean the MCL, remove all mismatched commands from the active supervisor engine's running configuration, revalidate the MCL with a modified running configuration using the **redundancy config-sync validate mismatched-commands** command, then reload the standby supervisor engine.

You could also ignore the MCL by entering the **redundancy config-sync ignore mismatched-commands** command and 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 with the exact same image, might cause the C4K_REDUNDANCY-2-*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

The following example shows how to validate removal of entries from the MCL:

```
Switch# redundancy config-sync validate mismatched-commands
Switch#
```

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.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.1(12c)EW	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 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 The following example shows how to switch over manually from the active to the standby supervisor engine:

```
Switch# redundancy force-switchover
Switch#
```

Related Commands	Command	Description
	redundancy	Enters the redundancy configuration mode.
	show redundancy	Displays redundancy facility information.

redundancy reload

To force a reload of one or both supervisor engines, use the **redundancy reload** command.

redundancy reload {peer | shelf}

Syntax Description	peer	Reloads the peer unit.
	shelf	Reboots both supervisor engines.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.1(12c)EW	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 The following example shows how to manually reload one or both supervisor engines:

```
Switch# redundancy reload shelf
Switch#
```

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	<i>mod</i> Target module for the command.
---------------------------	---

Command Default	This command has no default settings.
------------------------	---------------------------------------

Command Modes	Privileged EXEC mode
----------------------	----------------------

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

Usage Guidelines	<p>This command applies only to the Access Gateway Module on Catalyst 4500 series switches.</p> <p>The valid values for <i>mod</i> 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.</p> <p>When you execute the remote login module <i>mod</i> command, the prompt changes to Gateway#</p> <p>The remote login module command is identical to the session module <i>mod</i> and the attach module <i>mod</i> commands.</p>
-------------------------	--

Examples	The following example shows how to remotely log in to the Access Gateway Module:
-----------------	--

```
Switch# remote login module 5
Attaching console to module 5
Type 'exit' at the remote prompt to end the session

Gateway>
```

Related Commands	Command	Description
	attach module	Remotely connects to a specific module.
	session module	Logs in to the standby supervisor engine using a virtual console.

remote-span

To convert a VLAN into an RSPAN VLAN, use the **remote-span** command. To convert an RSPAN VLAN to a VLAN, use the **no** form of this command.

remote-span

no remote-span

Syntax Description This command has no arguments or keywords.

Command Default RSPAN is disabled.

Command Modes VLAN configuration mode

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

Examples The following example shows how to convert a VLAN into an RSPAN VLAN:

```
Switch# config terminal
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] [url]
```

Syntax Description	validation none	(Optional) Specifies that the checksum associated with the contents of the file specified by the URL is not verified.
	url	(Optional) Specifies the file from which the read is performed.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

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

Usage Guidelines If the URL is not provided, the switch tries to read the file from the configured URL.

Examples The following 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 generates a DHCP binding configuration to restore bindings across reboots.
	ip dhcp snooping information option	Enables DHCP option 82 data insertion.
	ip dhcp snooping trust	Enables DHCP snooping on a trusted VLAN.
	ip dhcp snooping vlan	Enables DHCP snooping on a VLAN or a group of VLANs.
	show ip dhcp snooping	Displays the DHCP snooping configuration.
	show ip dhcp snooping binding	Displays the DHCP snooping binding entries.

rep admin vlan

Use the **rep admin vlan** global configuration command to configure a Resilient Ethernet Protocol (REP) administrative VLAN for REP to transmit hardware flood layer (HFL) messages. Use the **no** form of this command to return to the default configuration with VLAN 1 as the administrative VLAN.

rep admin vlan *vlan-id* [**segment** *segment-id*]

no rep admin vlan *vlan-id* [**segment** *segment-id*]

Syntax Description

<i>vlan-id</i>	Configures specified VLAN as the administrative VLAN for the entire domain. The VLAN ID range is from 1 to 4094. The default is VLAN 1; the range to configure is 2 to 4094.
segment <i>segment-id</i>	Configures the administrative VLAN for the specified segment. The segment ID range is from 1 to 1024.

Command Default

The administrative VLAN is VLAN 1.

Command Modes

Global configuration

Command History

Release	Modification
12.2(44)SG	This command was introduced.
3.8.0E and 15.2.(4)E	The segment keyword was introduced.

Usage Guidelines

If the VLAN does not already exist, this command does not create the VLAN.

To avoid the delay introduced by relaying messages in software for link-failure or VLAN-blocking notification during load balancing, REP floods packets at the hardware flood layer (HFL) to a regular multicast address. These messages are flooded to the whole network, not just the REP segment. Switches that do not belong to the segment treat them as data traffic. You can control flooding of these messages by configuring an administrative VLAN for the entire domain or segment-wise.

If no REP administrative VLAN is configured, the default is VLAN 1.

There can be any number of administrative VLANs as long as it is per segment.

The administrative VLAN cannot be the RSPAN VLAN.

Examples

The following example shows how to configure VLAN 100 as the REP administrative VLAN:

```
Switch(config)# rep admin vlan 100
```

The following example shows how to create an administrative VLAN per segment. Here VLAN 2 is configured as the administrative VLAN only for REP segment 2. All remaining segments that are not configured otherwise will, by default, have VLAN 1 as the administrative VLAN.

```
Switch# configure terminal  
Switch (config)# rep admin vlan 2 segment 2  
Switch (config)# end
```

You can verify your settings by entering the **show interface rep detail** privileged EXEC command.

Related Commands

Command	Description
show interfaces rep detail	Displays detailed REP configuration and status for all interfaces or the specified interface, including the administrative VLAN.

rep block port

Use the **rep block port** interface configuration command on the REP primary edge port to configure Resilient Ethernet Protocol (REP) VLAN load balancing. Use the **no** form of this command to return to the default configuration.

```
rep block port {id port-id | neighbor_offset | preferred} vlan {vlan-list | all}
```

```
no rep block port {id port-id | neighbor_offset | preferred}
```

Syntax Description

id <i>port-id</i>	Identify the VLAN blocking alternate port by entering the unique port ID that is automatically generated when REP is enabled. The REP port ID is a 16-character hexadecimal value. You can view the port ID for an interface by entering the show interface interface-id rep detail command.
<i>neighbor_offset</i>	Identify the VLAN blocking alternate port by entering the offset number of a neighbor. The range is -256 to +256; a value of 0 is invalid. The primary edge port has an offset number of 1; positive numbers above 1 identify downstream neighbors of the primary edge port. Negative numbers identify the secondary edge port (offset number -1) and its downstream neighbors.
preferred	Identify the VLAN blocking alternate port as the segment port on which you entered the rep segment segment-id preferred interface configuration command. Note Entering the preferred keyword does not ensure that the preferred port is the alternate port; it gives it preference over other similar ports.
vlan	Identify the VLANs to be blocked.
<i>vlan-list</i>	Enter a VLAN ID from 1 to 4094 or a range or sequence of VLANs (such as 1-3, 22, 41-44) of VLANs to be blocked.
all	Enter to block all VLANs.

Command Default

The default behavior after you enter the **rep preempt segment** privileged EXEC command (for manual preemption) is to block all VLANs at the primary edge port. This behavior remains until you configure the **rep block port** command.

If the primary edge port cannot determine which port is to be the alternate port, the default action is no preemption and no VLAN load balancing.

Command Modes

Interface configuration

Command History

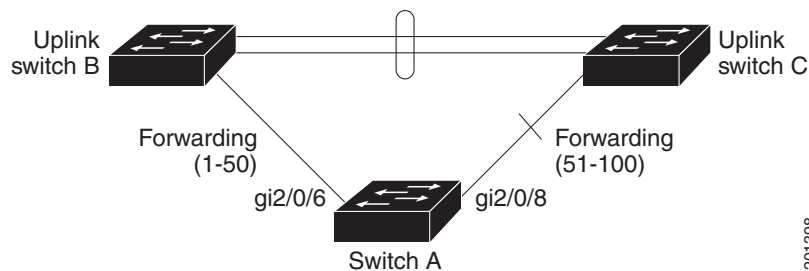
Release	Modification
12.2(44)SG	This command was introduced.

Usage Guidelines

You must enter this command on the REP primary edge port.

When you select an alternate port by entering an offset number, this number identifies the downstream neighbor port of an edge port. The primary edge port has an offset number of 1; positive numbers above 1 identify downstream neighbors of the primary edge port. Negative numbers identify the secondary edge port (offset number -1) and its downstream neighbors. See [Neighbor Offset Numbers in a REP Segment](#) Figure 2-2.

Figure 2-2 Neighbor Offset Numbers in a REP Segment



Note

You would never enter an offset value of 1 because that is the offset number of the primary edge port itself.

If you have configured a preempt delay time by entering the **rep preempt delay seconds** interface configuration command and a link failure and recovery occurs, VLAN load balancing begins after the configured preemption time period elapses without another link failure. The alternate port specified in the load-balancing configuration blocks the configured VLANs and unblocks all other segment ports. If the primary edge port cannot determine the alternate port for VLAN balancing, the default action is no preemption.

Each port in a segment has a unique port ID. The port ID format is similar to the one used by the spanning tree algorithm: a port number (unique on the bridge) associated to a MAC address (unique in the network). To determine the port ID of a port, enter the **show interface interface-id rep detail** privileged EXEC command.

There is no limit to the number of times that you can enter the **rep block port id port-id vlan vlan-list** interface configuration command. You can block an unlimited number, range, or sequence of VLANs.

When you use the **rep block port id port-id vlan vlan-list** interface configuration command on a REP primary edge port to block a VLAN list and then use the same command to block another VLAN list on the same port, the second VLAN list does not replace the first VLAN list but is appended to the first VLAN list.

When you use the **rep block port id port-id vlan vlan-list** interface configuration command on a REP primary edge port to block a VLAN list on one port and then use the same command to block another VLAN list on another port, the original port number and VLAN list are overwritten.

Examples

The following example shows how to configure REP VLAN load balancing on the Switch B primary edge port (Gigabit Ethernet port 1/0/1) and to configure Gigabit Ethernet port 1/1 of Switch A as the alternate port to block VLANs 1 to 100. The alternate port is identified by its port ID, shown in bold in the output of the **show interface rep detail** command for the Switch A port.

```
Switch A# show interface gigabitethernet1/1 rep detail
GigabitEthernet1/1 REP enabled
Segment-id: 2 (Segment)
PortID: 0080001647FB1780
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 007F001647FB1780EEE
Port Role: Open
Blocked Vlan: <empty>
Admin-vlan: 1
Preempt Delay Timer: 35 sec
Load-balancing block port: none
Load-balancing block vlan: none
STCN Propagate to:
PDU/TLV statistics:
LSL PDU rx: 107122, tx: 192493

Switch B# config t
Switch (config)# interface gigabitethernet1/0/1
Switch (config-if)# rep block port id 0080001647FB1780 vlan 1-100
Switch (config-if)# exit
```

The following example shows how to configure VLAN load balancing by using a neighbor offset number and how to verify the configuration by entering the **show interfaces rep detail** privileged EXEC command:

```
Switch# config t
Switch (config)# interface gigabitethernet1/1
Switch (config-if)# rep block port 6 vlan 1-110
Switch (config-if)# end

Switch# show interface GigabitEthernet1/1 rep detail
GigabitEthernet1/1 REP enabled
Segment-id: 2 (Segment)
PortID: 0080001647FB1780
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 007F001647FB17809C3
Port Role: Open
Blocked Vlan: <empty>
Admin-vlan: 3
Preempt Delay Timer: 35 sec
Load-balancing block port: 6
Load-balancing block vlan: 1-110
STCN Propagate to: none
LSL PDU rx: 1466780, tx: 3056637
HFL PDU rx: 2, tx: 0
BPA TLV rx: 1, tx: 2119695
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 757406, tx: 757400
EPA-COMMAND TLV rx: 1, tx: 1
EPA-INFO TLV rx: 178326, tx: 178323
```

Related Commands	Command	Description
	rep preempt delay	Configures a waiting period after a segment port failure and recovery before REP VLAN load balancing is triggered.
	rep preempt segment	Manually starts REP VLAN load balancing on a segment.
	show interfaces rep detail	Displays REP detailed configuration and status for all interfaces or the specified interface, including the administrative VLAN.

rep lsl-age-timer

Use the **rep lsl-age-timer** interface configuration command on a Resilient Ethernet Protocol (REP) port to configure the Link Status Layer (LSL) age timer for the time period that the REP interface remains up without receiving a hello from the REP neighbor. Use the **no** form of this command to return to the default time.

rep lsl-age timer *value*

no rep lsl-age timer

Syntax Description	<i>value</i>	The age-out time in milliseconds. The range is from 120 to 10000 ms in 40-ms increments. The default is 5000 ms (5 seconds).
---------------------------	--------------	--

Command Default	The REP link shuts down if it does not receive a hello message from a neighbor within 5000 ms.
------------------------	--

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

Command History	Release	Modification
	12.2(44)SG	This command was introduced.

Usage Guidelines	The LSL hello timer is set to the age-timer value divided by 3 so that there should be at least two LSL hellos sent during the LSL age-timer period. If no hellos are received within that time, the REP link shuts down.
-------------------------	---

In Cisco IOS Release 12.2(52)SE, the LSL age-timer range changed from 3000 to 10000 ms in 500-ms increments to 120 to 10000 ms in 40-ms increments. If the REP neighbor device is not running Cisco IOS Release 12.2(52)SE or later, you must use the shorter time range because the device does not accept values out of the earlier range.

EtherChannel port channel interfaces do not support LSL age-timer values less than 1000 ms. If you try to configure a value less than 1000 ms on a port channel, you receive an error message and the command is rejected.

Examples	The following example shows how to configure the REP LSL age timer on a REP link to 7000 ms:
-----------------	--

```
Switch(config)# interface GigabitEthernet1/1
Switch(config-if)# rep lsl-age-timer 7000
Switch(config-if)# exit
```

You can verify the configured ageout time by entering the **show interfaces rep detail** privileged EXEC command.

Related Commands	Command	Description
	show interfaces rep [detail]	Displays REP configuration and status for all interfaces or the specified interface, including the configured LSL age-out timer value.

rep preempt delay

Use the **rep preempt delay** interface configuration command on the REP primary edge port to configure a waiting period after a segment port failure and recovery before Resilient Ethernet Protocol (REP) VLAN load balancing is triggered. Use the **no** form of this command to remove the configured delay.

rep preempt delay *seconds*

no rep preempt delay

Syntax Description

seconds Set the number of seconds to delay REP preemption. The range is 15 to 300.

Command Default

No preemption delay is set. If you do not enter the **rep preempt delay** command, the default is manual preemption with no delay.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(44)SG	This command was introduced.

Usage Guidelines

You must enter this command on the REP primary edge port.

You must enter this command and configure a preempt time delay if you want VLAN load balancing to automatically trigger after a link failure and recovery.

If VLAN load balancing is configured, after a segment port failure and recovery, the REP primary edge port starts a delay timer before VLAN load balancing occurs. Note that the timer restarts after each link failure. When the timer expires, the REP primary edge alerts the alternate port to perform VLAN load balancing (configured by using the **rep block port** interface configuration command) and prepares the segment for the new topology. The configured VLAN list is blocked at the alternate port, and all other VLANs are blocked at the primary edge port.

Do not configure VLAN load balancing on an interface that carries Ethernet over multiprotocol label switching (EoMPLS) traffic. VLAN load balancing across the REP ring might cause some of the EoMPLS traffic to not be forwarded.

Examples

The following example shows how to configure REP preemption time delay of 100 seconds on the primary edge port:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# rep preempt delay 100
Switch(config-if)# exit
```

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

Related Commands	Command	Description
	<code>rep block port</code>	Configures VLAN load balancing.
	<code>show interfaces rep [detail]</code>	Displays REP configuration and status for all interfaces or the specified interface.

rep preempt segment

Use the **rep preempt segment** privileged EXEC command to manually start Resilient Ethernet Protocol (REP) VLAN load balancing on a segment.

rep preempt segment *segment-id*

Syntax Description	<i>segment-id</i> ID of the REP segment. The range is from 1 to 1024.
---------------------------	---

Command Default	Manual preemption is the default behavior.
------------------------	--

Command Modes	Privileged EXEC
----------------------	-----------------

Command History	Release	Modification
	12.2(44)SG	This command was introduced.

Usage Guidelines	<p>When you enter the rep preempt segment <i>segment-id</i> command, a confirmation message appears before the command is executed because preemption can cause network disruption.</p> <p>Enter this command on the switch on the segment that has the primary edge port.</p> <p>If you do not configure VLAN load balancing, entering this command results in the default behavior—the primary edge port blocks all VLANs.</p> <p>You configure VLAN load balancing by entering the rep block port {<i>id port-id</i> <i>neighbor_offset</i> preferred} vlan {<i>vlan-list</i> all} interface configuration command on the REP primary edge port before you manually start preemption.</p> <p>There is not a no version of this command.</p>
-------------------------	--

Examples	<p>The following example shows how to manually trigger REP preemption on segment 100 with the confirmation message:</p> <pre>Switch)# rep preempt segment 100 The command will cause a momentary traffic disruption. Do you still want to continue? [confirm]</pre>
-----------------	--

Related Commands	Command	Description
	rep block port	Configures VLAN load balancing.
	show interfaces rep [detail]	Displays REP configuration and status for all interfaces or the specified interface.

rep segment

Use the **rep segment** interface configuration command to enable Resilient Ethernet Protocol (REP) on the interface and to assign a segment ID to it. Use the **no** form of this command to disable REP on the interface.

rep segment *segment-id* [**edge** [**no-neighbor**] [**primary**]] [**preferred**]

no rep segment

Syntax Description

<i>segment-id</i>	Assign a segment ID to the interface. The range is from 1 to 1024.
edge	(Optional) Identify the interface as one of the two REP edge ports. Entering the edge keyword without the primary keyword configures the port as the secondary edge port.
no-neighbor	(Optional) Configure a segment edge with no external REP neighbor.
primary	(Optional) On an edge port, specify that the port is the primary edge port. A segment has only one primary edge port. If you configure two ports in a segment as the primary edge port, for example ports on different switches, the REP selects one of them to serve as the segment primary edge port.
preferred	(Optional) Specify that the port is the preferred alternate port or the preferred port for VLAN load balancing.
Note	Configuring a port as preferred does not guarantee that it becomes the alternate port; it merely gives it a slight edge among equal contenders. The alternate port is usually a previously failed port.

Command Default

REP is disabled on the interface.

When REP is enabled on an interface, the default is for the port to be a regular segment port.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(44)SG	This command was introduced.
15(02)SG	The no-neighbor keyword was added.

Usage Guidelines

REP ports must be Layer 2 trunk ports. A non-ES REP port can be either an IEEE 802.1Q trunk port or an ISL trunk port.

REP ports should not be configured as one of these port types:

- SPAN destination port
- Private VLAN port

- Tunnel port
- Access port

You must configure two edge ports on each REP segment, a primary edge port and a port to act as a secondary edge port. If you configure two ports in a segment as the primary edge port, for example ports on different switches, the configuration is allowed, but the REP selects one of them to serve as the segment primary edge port.

REP is supported on EtherChannels, but not on an individual port that belongs to an EtherChannel.

- REP ports follow these rules:
 - There is no limit to the number of REP ports on a switch; however, only two ports on a switch can belong to the same REP segment.
 - If only one port on a switch is configured in a segment, the port should be an edge port.
 - If two ports on a switch belong to the same segment, they must be both edge ports, both regular segment ports, or one regular port and one edge no-neighbor port. An edge port and regular segment port on a switch cannot belong to the same segment.
 - If two ports on a switch belong to the same segment and one is configured as an edge port and one as a regular segment port (a misconfiguration), the edge port is treated as a regular segment port.

If you configure two ports in a segment as the primary edge port, for example ports on different switches, the REP selects one of them to serve as the segment primary edge port. Enter the **show rep topology** privileged EXEC command on a port in the segment to verify which port is the segment primary edge port.

REP interfaces come up in a blocked state and remain in a blocked state until notified that it is safe to unblock. You need to be aware of this to avoid sudden connection losses.

You should configure REP only in networks with redundancy. Configuring REP in a network without redundancy causes loss of connectivity.

In networks where ports on a neighboring switch do not support REP, you can configure the non-REP facing ports as edge no-neighbor ports. These ports inherit all properties of edge ports and you can configure them as any other edge port, including to send STP or REP topology change notices to the aggregation switch. In this case, the STP topology change notice (TCN) that is sent is a multiple spanning-tree (MST) STP message.

Examples

The following example shows how to enable REP on a regular (nonedge) segment port:

```
Switch (config)# interface gigabitethernet1/0/1
Switch (config-if)# rep segment 100
```

The following example shows how to enable REP on a port and identify the port as the REP primary edge port:

```
Switch (config)# interface gigabitethernet1/1
Switch (config-if)# rep segment 100 edge primary
```

The following example shows how to configure the same configuration when the interface has no external REP neighbor:

```
Switch# configure terminal
Switch (config)# interface gigabitethernet1/1
Switch (config-if)# rep segment 100 edge no-neighbor primary
```

The following example shows how to enable REP on a port and identify the port as the REP secondary edge port:

```
Switch (config)# interface GigabitEthernet1/1  
Switch (config-if)# rep segment 100 edge
```

You can verify your settings by entering the **show interfaces rep** privileged EXEC command. To verify which port in the segment is the primary edge port, enter the **show rep topology** privileged EXEC command.

Related Commands

Command	Description
show interfaces rep [detail]	Displays REP configuration and status for all interfaces or the specified interface.
show rep topology [detail]	Displays information about all ports in the segment, including which one was configured and selected as the primary edge port.

rep stcn

Use the **rep stcn** interface configuration command on a Resilient Ethernet Protocol (REP) edge port to configure the port to send REP segment topology change notifications (STCNs) to another interface, to other segments, or to Spanning Tree Protocol (STP) networks. Use the **no** form of this command to disable the sending of STCNs to the interface, segment, or STP network.

```
rep stcn {interface interface-id | segment id-list | stp}
```

```
no rep stcn {interface | segment | stp}
```

Syntax Description

interface <i>interface-id</i>	Identify a physical interface or port channel to receive STCNs.
segment <i>id-list</i>	Identify one REP segment or list of segments to receive STCNs. The range is 1 to 1024. You can also configure a sequence of segments (for example 3-5, 77, 100).
stp	Send STCNs to an STP network.

Command Default

Transmission of STCNs to other interfaces, segments, or STP networks is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(44)SG	This command was introduced.

Usage Guidelines

Enter this command on a segment edge port.

You use this command to notify other portions of the Layer 2 network of topology changes that occur in the local REP segment. This removes obsolete entries in the Layer 2 forwarding table in other parts of the network, which allows faster network convergence.

Examples

The following example shows how to configure a REP edge port to send STCNs to segments 25 to 50:

```
Switch (config)# interface GigabitEthernet1/1
Switch (config-if)# rep stcn segment 25-50
Switch (config-if)# exit
```

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

Related Commands	Command	Description
	show interfaces rep [detail]	Displays REP configuration and status for all interfaces or the specified interface.

reset

To leave the proposed new VLAN database but remain in VLAN configuration mode and reset the proposed new database to be identical to the VLAN database currently implemented, use the **reset** command.

reset

Syntax Description This command has no arguments or keywords.

Command Default This command has no default settings.

Command Modes VLAN configuration mode

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

Examples The following 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.

Command Default

Revision version is set to 0.

Command Modes

MST configuration mode

Command History

Release	Modification
12.1(12c)EW	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

The following 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.

sampler (netflow-lite monitor submode)



Note

NetFlow-lite is supported only on Catalyst 4948E and Catalyst 4948E-F Ethernet switches.

To activate sampling on an interface in netflow-lite monitor submode, use the **sampler** command. To delete a sampler, use the **no sampler** form of this command.

```
sampler sampler-name
```

```
no sampler sampler-name
```

Syntax Description

<i>sampler-name</i>	Specifies a sampler.
---------------------	----------------------

Command Default

None

Command Modes

netflow-lite exporter submode

Command History

Release	Modification
15.0(2)SG	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

You can enter this command under the physical port interface mode, port channel interface, or config VLAN mode.

Examples

The following example shows how to configure a monitor on a port interface Gigabit 1/3:

```
Switch# config terminal
Switch(config)# int GigabitEthernet1/3
Switch(config-if)# netflow-lite monitor 1
Switch(config-netflow-lite-monitor)# sampler sampler1
Switch(config-netflow-lite-monitor)# average-packet-size 128
Switch(config-netflow-lite-monitor)# exporter exporter1
Switch(config-netflow-lite-monitor)# exit
Switch(config-if)# exit
Switch(config)# exit
Switch# show netflow-lite monitor 1 interface gi1/3
Interface GigabitEthernet1/3:
  Netflow-lite Monitor-1:
    Sampler:                sampler1
    Exporter:                exporter1
    Average Packet Size:    128
  Statistics:
    Packets exported:       0
    Packets observed:       0
    Packets dropped:        0
```


You can verify your settings with the **show netflow-lite sampler** privileged EXEC command.

Related Commands	Command	Description
	average-packet-size (netflow-lite monitor submode)	Specifies the average packet size at the observation point.
	exporter (netflow-lite monitor submode)	Assigns an exporter in netflow-lite monitor 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.
<i>policy-map name</i>	Name of a previously configured policy map.

Command Default

A policy map is not attached to an interface or a VLAN.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(8a)EW	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.

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

The following example shows how to attach a policy map to Fast Ethernet interface 5/20:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 5/20
Switch(config-if)# service-policy input pmap1
Switch(config-if)# end
```

The following example shows how to apply policy map p1 for traffic in VLANs 20 and 400, and policy map p2 for traffic in VLANs 300 through 301:

```
Switch# configure terminal
Switch(config)# interface gigabitEthernet 6/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# vlan-range 20,400
Switch(config-if-vlan-range)# service-policy input p1
Switch(config-if-vlan-range)# exit
Switch(config-if)# vlan-range 300-301
Switch(config-if-vlan-range)# service-policy output p2
Switch(config-if-vlan-range)# end
Switch# show policy-map interface gigabitEthernet 6/1 vlan 20
GigabitEthernet6/1 vlan 20

Service-policy input: p1

Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets
  police: Per-interface
    Conform: 0 bytes Exceed: 0 bytes

Switch# show policy-map interface gigabitEthernet 6/1
GigabitEthernet6/1 vlan 20

Service-policy input: p1

Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets
  police: Per-interface
    Conform: 0 bytes Exceed: 0 bytes

GigabitEthernet6/1 vlan 300

Service-policy output: p2

Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets
  police: Per-interface
    Conform: 0 bytes Exceed: 0 bytes

GigabitEthernet6/1 vlan 301

Service-policy output: p2

Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets
  police: Per-interface
    Conform: 0 bytes Exceed: 0 bytes

GigabitEthernet6/1 vlan 400
```

```

Service-policy input: p1

Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets
  police: Per-interface
    Conform: 0 bytes Exceed: 0 bytes

```

The following example shows how to attach a policy map to a VLAN using a Supervisor Engine 6-E:

```

Switch# configure terminal
Switch(config)#vlan configuration 20
Switch(config-vlan-config)#service-policy out 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

<i>policy-map-name</i>	Name of the policy map.
------------------------	-------------------------

Command Default

No service policies maps are defined.

Command Modes

Policy-map class configuration mode

Command History

Release	Modification
12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch.
12.2(40)SG	Added support for Supervisor Engine 6-E and Catalyst 4900M 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

The following 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#
```

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.
	priority	Enables the strict priority queue (low-latency queueing [LLQ]) and to give priority to a class of traffic belonging to a policy map attached to a physical port.
	random-detect (refer to Cisco IOS documentation)	Enables Weighted Random Early Detection (WRED) or distributed WRED (DWRED).
	shape (class-based queueing)	Enables traffic shaping a class of traffic in 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.
	<i>policy-map-name</i>	Name of a service policy map (created using the policy-map command) to be attached.

Command Default No service policy is specified.

Command Modes Control-plane configuration mode

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

Usage Guidelines In this release, the only policy-map accepted on the control-plane is system-cpp-policy. It is already attached to the control-plane at start up. If not (due to some error conditions), it is recommended to use the **global macro system-cpp** command to attach it to the control-plane. The system-cpp-policy created by the system contains system predefined classes. For these predefined classes, you can change the policing parameters but you should not make any other change to the classes.

You can define your own class-maps and append them to the end of the system-cpp-policy policy-map.

Examples

The following example shows how to configure trusted hosts with source addresses 10.1.1.1 and 10.1.1.2 to forward Telnet packets to the control plane without constraint, while allowing all remaining Telnet packets to be policed at the specified rate:

```
Switch(config)# access-list 140 deny tcp host 10.1.1.1 any eq telnet
! Allow 10.1.1.2 trusted host traffic.
Switch(config)# access-list 140 deny tcp host 10.1.1.2 any eq telnet
! Rate limit all other Telnet traffic.
Switch(config)# access-list 140 permit tcp any any eq telnet
! Define class-map "telnet-class."
Switch(config)# class-map telnet-class
Switch(config-cmap)# match access-group 140
Switch(config-cmap)# exit
Switch(config)# policy-map control-plane-policy
Switch(config-pmap)# class telnet-class
Switch(config-pmap-c)# police 80000 conform transmit exceed drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
! Define aggregate control plane service for the active Route Processor.
```

```
Switch(config)# control-plane
Switch(config-cp)# service-policy input control-plane-policy
Switch(config-cp)# exit
```

Related Commands	Command	Description
	control-plane	Enters control-plane configuration mode.
	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 either of a class or of 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

<i>mod</i>	Target module for the command.
------------	--------------------------------

Command Default

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.2(31)SG	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 session is also terminated. Virtual console session is also automatically terminated when the standby is rebooted. After the standby boots up, you need to create another virtual console session.

The following limitations apply to the standby virtual console:

- All commands on the virtual console run to completion. It does not provide the auto-more feature; it behaves as if the **terminal length 0** command has been executed. It is also non-interactive. Therefore, a running command cannot be interrupted or aborted by any key sequence on the active supervisor engine. If a command produces considerable output, the virtual console displays it on the supervisor screen.
- The virtual console is non-interactive. Because the virtual console does not detect the interactive nature of a command, any command that requires user interaction causes the virtual console to wait until the RPC timer aborts the command.
- The virtual console timer is set to 60 seconds. The virtual console returns to its prompt after 60 seconds. During this time, you cannot abort the command from the keyboard. You must wait for the timer to expire before you continue.
- You cannot use virtual console to view debug and syslog messages that are being displayed on the standby supervisor engine. The virtual console only displays the output of commands that are executed from the virtual console. Other information that is displayed on the real standby console does not appear on the virtual console.

Examples

To log in to the standby supervisor engine using a virtual console, do the following:

```
Switch# session module 2
Connecting to standby virtual console
Type "exit" or "quit" to end this session
```

```
Switch-standby-console# exit
Switch#
```

If the standby console is not enabled, the following message appears:

```
Switch-standby-console#
Standby console disabled.
Valid commands are: exit, logout
```

Related Commands

Command	Description
attach module	Remotely connects to a specific module.
remote login module	Remotely connects to a specific module.

set

To mark IP traffic by setting a class of service (CoS), a Differentiated Services Code Point (DSCP), or IP-precedence in the packet, use the **set** policy-map class configuration command. To remove the traffic classification, use the **no** form of this command.

```
set { cos new-cos | [ip] { dscp new-dscp | precedence new-precedence } | qos group value }
```

```
no set cos new-cos | ip { dscp new-dscp | precedence new-precedence } | qos group value }
```

Syntax Description

cos <i>new-cos</i>	New CoS value assigned to the classified traffic. The range is 0 to 7.
ip dscp <i>new-dscp</i>	New DSCP value assigned to the classified traffic. The range is 0 to 63. You also can enter a mnemonic name for a commonly used value. The specified value sets the type of service (ToS) traffic class byte in the IPv4/IPv6 packet header.
ip precedence <i>new-precedence</i>	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 <i>value</i>	Internal QoS group assigned to a classified packet on ingress to an interface.

Command Default

No marking is enabled on packets.

Command Modes

Policy-map class configuration mode

Command History

Release	Modification
12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch.
12.2(40)SG	Added support for Supervisor Engine 6-E and Catalyst 4900M 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 as entering the **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

The following example shows how to create a policy map called p1 with CoS values assigned to different traffic types. Class maps for voice and video-data have already been created.

```
Switch# configure terminal
Switch(config)# policy-map p1
Switch(config-pmap)# class voice
Switch(config-pmap-c)# set cos 1
Switch(config-pmap)# exit
Switch(config-pmap)# class video-data
Switch(config-pmap-c)# set cos 2
Switch(config-pmap)# exit
Switch#
```

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

Related Commands

Command	Description
class	Specifies the name of the class whose traffic policy you want to create or change.
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.
show policy-map	Displays information about the policy map.
trust	Defines a trust state for traffic classified through the class policy-map configuration command.

set cos

To set the Layer 2 class of service (CoS) value of a packet, use the **set cos** command in policy-map class configuration mode. To remove a specific CoS value setting, use the **no** form of this command.

```
set cos {cos-value | from-field [table table-map-name]}
```

```
no set cos {cos-value | from-field [table table-map-name]}
```

Syntax Description	
<i>cos-value</i>	Specific IEEE 802.1Q CoS value from 0 to 7.
<i>from-field</i>	Specific 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: <ul style="list-style-type: none"> • 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.
<i>table-map-name</i>	(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(40)SG	This command was introduced on Supervisor Engine 6E and Catalyst 4900M.

Usage Guidelines The **set cos** command can be used in an ingress as well as an egress policy map attached to an interface or VLAN.

You can use this command to specify the “from-field” packet-marking category to be used for mapping and setting the CoS value. The “from-field” packet-marking categories are as follows:

- Precedence
- Differentiated services code point (DSCP)
- Cost of Service (CoS)
- Quality of Service (QoS) group

If you specify a “from-field” category but do not specify the **table** keyword and the applicable *table-map-name* argument, the default action will be to copy the value associated with the “from-field” category as the CoS value. For 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

The following 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# configure terminal
Switch(config)# policy-map cos-set
Switch(config-pmap)# class voice
Switch(config-pmap-c)# set cos 1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class video-data
Switch(config-pmap-c)# set cos 2
Switch(config-pmap-c)# end
Switch#
```

The following 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.

The following 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-pmap)# class class-default
Switch(config-pmap-c)# set cos precedence 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.

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.
<i>dscp-value</i>	A number from 0 to 63 that sets the DSCP value. A mnemonic name for commonly used values can also be used.
<i>from-field</i>	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: <ul style="list-style-type: none"> • cos • qos-group • dscp • precedence
table	(Optional) Used in conjunction with the <i>from-field</i> argument. Indicates that the values set in a specified table map will be used to set the DSCP value.
<i>table-map-name</i>	(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(8a)EW	This command was introduced on the Catalyst 4500 series switch.
12.2(40)SG	Added support for from-field on Supervisor Engine 6-E and Catalyst 4900M.

Usage Guidelines

Once the DSCP bit is set, other quality of service (QoS) features can then operate on the bit settings.

DSCP and Precedence Values Are Mutually Exclusive

The **set dscp** command cannot be used with the **set precedence** command to mark the *same* packet. The two values, DSCP and precedence, are mutually exclusive. A packet can have one value or the other, but not both.

You can use this command to specify the “from-field” packet-marking category to be used for mapping and setting the DSCP value. The “from-field” packet-marking categories are as follows:

- Class of service (CoS)
- QoS group
- Precedence
- Differentiated services code point (DSCP)

If you specify a “from-field” category but do not specify the **table** keyword and the applicable *table-map-name* argument, the default action will be to copy the value associated with the “from-field” category as the DSCP value. For instance, if you configure the **set dscp cos** command, the CoS value will be copied and used as the DSCP value.

**Note**

The CoS field is a three-bit field, and the DSCP field is a six-bit field. If you configure the **set dscp cos** command, only the three bits of the CoS field will be used.

If you configure the **set dscp qos-group** command, the QoS group value will be copied and used as the DSCP value.

The valid value range for the DSCP is a number from 0 to 63. The valid value range for the QoS group is a number from 0 to 63.

Set DSCP Values in IPv6 Environments

When this command is used in IPv6 environments, the default match occurs on both IP and IPv6 packets. However, the actual packets set by this function are only those which meet the match criteria of the class-map containing this function.

Set DSCP 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 **ip** keyword in the **match** command for classification. Without the **ip** keyword, the match occurs on both IPv4 and IPv6 packets.

Examples**Packet-marking Values and Table Map**

In the following example, the policy map called policy1 is created to 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.

The following 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)# 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 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

<i>precedence-value</i>	A number from 0 to 7 that sets the precedence bit in the packet header.
<i>from-field</i>	Specific packet-marking category to be used to set the precedence value of the packet. If you are using a table map for mapping and converting packet-marking values, this argument value establishes the “map from” packet-marking category. Packet-marking category keywords are as follows: <ul style="list-style-type: none"> • 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.
<i>table-map-name</i>	(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(8a)EW	This command was introduced on the Catalyst 4500 series switch.
12.2(40)SG	Added support for from-field on Supervisor Engine 6-E and Catalyst 4900M.

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.

You can use this command to specify the “from-field” packet-marking category to be used for mapping and setting the precedence value. The “from-field” packet-marking categories are as follows:

- CoS
- QoS group
- DSCP
- Precedence

If you specify a “from-field” category but do not specify the **table** keyword and the applicable *table-map-name* 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 CoS value will be copied and used as the precedence value.

You can do the same for the QoS group-marking category. That is, you can configure the **set precedence qos-group** command, and the QoS group value will be copied and used as the precedence value.

The valid value range for the precedence value is a number from 0 to 7. The valid value range for the QoS group is a number from 0 to 63. Therefore, when configuring the **set precedence qos-group** command the three least 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 IPv6 Packets Only

To set the precedence values for IPv6 packets only, the **match protocol ipv6** command must also be used in the class-map that classified packets for this action. Without the **match protocol ipv6** command, the class-map may classify both IPv6 and IPv4 packets, (depending on other match criteria) and the **set precedence** command will act upon both types of packets.

Setting Precedence Values for IPv4 Packets Only

To set the precedence values for IPv4 packets only, use a command involving the **ip** keyword like the **match ip precedence** or **match ip dscp** command or include the **match protocol ip** command along with the others in the class map. Without the additional **ip** keyword, the class-map may match both IPv6 and IPv4 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-cos is created to use the values defined in a table map named table-map1. The table map named table-map1 was created earlier with the **table-map** (value mapping) command. For more information about the **table-map** (value mapping) command, see the **table-map** (value mapping) command page.

The following example shows how the precedence value is set according to the CoS value defined in table-map1.

```
Switch# configure terminal
Switch(config)# policy-map policy-cos
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 (ID) that can be used later to classify packets, use the **set qos-group** command in policy-map class configuration mode. To remove the group ID, use the **no** form of this command.

```
set qos-group group-id
```

```
no set qos-group group-id
```

Syntax Description

<i>group-id</i>	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(40)SG	This command was introduced on the Catalyst 4500 series switch using a Supervisor Engine 6-E and Catalyst 4900M 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

The following example shows how to set the qos-group to 5:

```
Switch# 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#
```

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 {rate} [**bps** | **kbps** | **mbps** | **gbps**]

shape average percent {percent_value}

no shape average

Syntax Description

<i>rate</i>	Specifies an average rate for traffic shaping; the range is 16000 to 10000000000. Post-fix notation (k, m, and g) is optional and a decimal point is allowed.
bps	(Optional) Specifies a rate in bits per seconds.
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.
<i>percent_value</i>	(Optional) Specifies a percentage of the bandwidth used for traffic shaping; valid values are from 1 to 100 percent.

Command Default

Average-rate traffic shaping is disabled.

Command Modes

Policy-map class configuration mode

Command History

Release	Modification
12.2(40)SG	This command was introduced on 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

The following 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. Post-fix notation (k, m, and g) is optional and a decimal point is allowed.
percent	(Optional) Specifies a percent of bandwidth for traffic shaping.

Command Default

Default is no traffic shaping.

Command Modes

Interface transmit queue configuration mode

Command History

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

Usage Guidelines

This command is not supported on Supervisor Engine 6-E, Supervisor Engine 6L-E, Catalyst 4900M, Catalyst 4948E, and Catalyst 4948E-F.

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 the Catalyst 4500 Supervisor Engine V (WS-X4516) and the Catalyst 4500 Supervisor Engine V-10GE (WS-X4516-10GE), the shaped traffic rate may not be achieved 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 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 24-port modules and the 48-port modules are multiplexed through a Stub ASIC. Some examples of ports multiplexed through a Stub ASIC are as follows:

- 10/100 ports on the WS-X4148-RJ45 module
- 10/100/1000 ports on the WS-X4124-GB-RJ45 module
- 10/100/1000 ports on the WS-X4448-GB-RJ45 module

Examples

The following 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)#
```

shell trigger

Use the **shell trigger** global configuration command to create a user defined trigger. Use the **no** form of this command to delete the trigger.

shell trigger *identifier description*

no shell trigger *identifier description*

Syntax Description

<i>identifier</i>	Specifies the event trigger identifier. The identifier should have no spaces or hyphens between words.
<i>description</i>	Specifies the event trigger description text.

Command Default

There are system-defined event triggers:

- CISCO_PHONE_EVENT
- CISCO_SWITCH_EVENT
- CISCO_ROUTER_EVENT
- CISCO_WIRELESS_AP_EVENT
- CISCO_WIRELESS_LIGHTWEIGHT_AP_EVENT
- DMP
- IPVSC

Command Modes

Global configuration

Command History

Release	Modification
12.2(50)SE	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

Use this command to create user-defined event triggers in conjunction with the **macro auto execute** global configuration command.

To support dynamic device discovery when using 802.1X authentication, configure the RADIUS authentication server to support the Cisco attribute-value (AV) pair: **auto-smart-port=event trigger**.

This command is mainly used for 802.1X authentication based triggers provided 802.1X or MAB is supported, enabling you to map new platform strings or device IDs to their respective macros or functions.

Examples

The following example shows how to create a user-defined event trigger called RADIUS_MAB_EVENT:

```
Switch# configure terminal
Switch(config)# shell trigger RADIUS_MAB_EVENT MAC_AuthBypass Event
```

```
Switch(config)# end
```

Related Commands	Command	Description
	macro auto global processing	Enables Auto Smartports on a switch.
	macro auto processing	Enable Auto SmartPorts macros on a specific interface.
	show shell	Displays information about event triggers and macros.
	macro auto device	Simplifies changing the parameters for a built-in functions for a device type.
	macro auto execute (builtin function)	Changes built-in function default values or to map user-defined triggers to built-in functions, and to pass the parameter values.
	macro auto execute (user-defined function)	Maps a trigger to a user-defined function.
	macro auto execute (remotely-defined function)	Maps a trigger to a remotely defined functions.
	macro auto processing	Enables Auto SmartPorts macros on a specific interface.
	macro auto sticky	Specifies not to remove configurations applied by ASP across link flaps and device removal.

show access-group mode interface

To display the ACL configuration on a Layer 2 interface, use the **show access-group mode interface** command.

show access-group mode interface [*interface interface-number*]

Syntax Description	<i>interface</i>	(Optional) Interface type; valid values are ethernet , fastethernet , gigabitethernet , tengigabitethernet , and port-channel .
	<i>interface-number</i>	(Optional) Interface number.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.1(19)EW	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 The following example shows how to display the ACL configuration on the Fast Ethernet interface 6/1:

```
Switch# show access-group mode interface fa6/1
Interface FastEthernet6/1:
  Access group mode is: 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		
<i>interface</i>	(Optional) Interface type; possible valid values are ethernet , fastethernet , gigabitethernet , tengigabitethernet , pos , ge-wan , and atm .	
<i>interface-number</i>	(Optional) Module and port number; see the “Usage Guidelines” section for valid values.	
null <i>interface-number</i>	(Optional) Specifies the null interface; the valid value is 0 .	
port-channel <i>number</i>	(Optional) Specifies the channel interface; valid values are a maximum of 64 values ranging from 1 to 256.	
vlan <i>vlan-id</i>	(Optional) Specifies the VLAN; valid values are from 1 to 4094.	
detail	(Optional) Displays the information about the protocol detail and timer.	
internal	(Optional) Displays the information about the internal data structure.	
summary	(Optional) Displays a summary of CEF-adjacency information.	

Command Default 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 10/100BASE-T 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

The following example shows how to display adjacency information:

```
Switch# show adjacency
Protocol Interface          Address
IP       FastEthernet2/3      172.20.52.1(3045)
IP       FastEthernet2/3      172.20.52.22(11)
Switch#
```

The following example shows how to display a summary of adjacency information:

```
Switch# show adjacency summary
Adjacency Table has 2 adjacencies
  Interface          Adjacency Count
  FastEthernet2/3      2
Switch#
```

The following example shows how to display protocol detail and timer information:

```
Switch# show adjacency detail
Protocol Interface          Address
IP       FastEthernet2/3      172.20.52.1(3045)
                                0 packets, 0 bytes
                                000000000FF920000380000000000000
                                00000000000000000000000000000000
                                00605C865B2800D0BB0F980B0800
                                ARP          03:58:12
IP       FastEthernet2/3      172.20.52.22(11)
                                0 packets, 0 bytes
                                000000000FF920000380000000000000
                                00000000000000000000000000000000
                                00801C93804000D0BB0F980B0800
                                ARP          03:58:06
Switch#
```

The following example shows how to display adjacency information for a specific interface:

```
Switch# show adjacency fastethernet2/3
Protocol Interface          Address
IP       FastEthernet2/3      172.20.52.1(3045)
IP       FastEthernet2/3      172.20.52.22(11)
Switch#
```

Related Commands

Command	Description
debug adjacency	Displays information about the adjacency debugging.

show ancp multicast

To display multicast streams activated by Access Node Control Protocol (ANCP), use the **show ancp multicast** command.

```
show ancp multicast [group groupaddr] [source sourceaddr] | [ interface interfacename ]
```

Syntax Description	
group <i>groupaddr</i>	(Optional) Specifies a multicast group address.
source <i>sourceaddr</i>	(Optional) Specifies a multicast source address.
interface <i>interfacename</i>	(Optional) Specifies a multicast flowing on a specific interface.

Command Default Displays all the multicast streams activated with ANCP.

Command Modes Privileged EXEC

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 multicast streams activated by ANCP:

```
ANCP-Client# show ancp mul
ANCP Multicast Streams
ClientID VLAN Interface Joined on
Group 235.3.2.1
0x01060004000A0703 10 Fa7/3 18:27:35 UTC Sat Sep 13 2008
0x0106000400140703 20 Fa7/3 18:27:35 UTC Sat Sep 13 2008
0x01060004000A0704 10 Fa7/4 18:25:43 UTC Sat Sep 13 2008
0x0106000400140704 20 Fa7/4 18:25:43 UTC Sat Sep 13 2008
Group 238.1.2.3
0x01060004000A0703 10 Fa7/3 18:27:37 UTC Sat Sep 13 2008
0x0106000400140703 20 Fa7/3 18:27:35 UTC Sat Sep 13 2008
0x01060004000A0704 10 Fa7/4 18:25:43 UTC Sat Sep 13 2008
0x0106000400140704 20 Fa7/4 18:25:43 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.

Command Default This command has no default settings.

Command Modes EXEC

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

Examples The following example shows how to display the ARP ACL information for a switch:

```
Switch# show arp access-list
ARP access list rose
  permit ip 10.101.1.1 0.0.0.255 mac any
  permit ip 20.3.1.0 0.0.0.255 mac any
```

Related Commands	Command	Description
	access-group mode	Specifies the override modes (for example, VACL overrides 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 | registrations | sessions [session-id session-id] [handle handle] [interface interface] [mac mac] [method method] [interface interface [details | policy]]
```

Syntax Description

interface <i>interface</i>	Displays all of the Auth Manager details associated with the specified interface.
registrations	Displays details of all methods registered with the Auth Manager.
sessions	Displays details of the current Auth Manager sessions (for example, client devices). If you do not enter any optional specifiers, all current active sessions are displayed. You can enter the specifiers singly or in combination to display a specific session (or group of sessions).
session-id <i>session-id</i>	(Optional) Specifies an Auth Manager session.
handle <i>handle</i>	(Optional) Specifies the particular handle for which Auth Manager information is displayed. Range is 1 to 4294967295.
mac <i>mac</i>	(Optional) Displays Auth Manager session information for a specified MAC address.
method <i>method</i>	(Optional) Displays all clients authorized by a specified authentication method. Valid values are as follows: <ul style="list-style-type: none"> • dot1x • mab • webauth
interface <i>interface</i> details	(Optional) Displays detailed information.
interface <i>interface</i> policy	(Optional) Displays policies applied on the interface.

Command Default

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
12.2(50)SG	This command was introduced.

Usage Guidelines

[Table 2-19](#) 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 “Authz Failed” are displayed. “No methods” is displayed if no method has provided a result.

Table 2-19 *show authentication Command Output*

Field	Description
Idle	The session has been initialized and no methods have run yet.
Running	A method is running for this session.
No methods	No method has provided a result for this session.
Authc Success	A method has resulted in authentication success for this session.
Authc Failed	A method has resulted in authentication fail for this session.
Authz Success	All features have been successfully applied for this session.
Authz Failed	A feature has failed to be applied for this session.

Table 2-20 lists the possible values for the state of methods. For a session in terminal state, “Authc Success,” “Authc Failed,” or “Failed over” are displayed (the latter indicates a method ran and failed over to the next method which did not provide a result. “Not run” is displayed in the case of sessions that are synchronized on standby.

Table 2-20 *State Method Values*

Method State	State Level	Description
Not run	Terminal	The method has not run for this session.
Running	Intermediate	The method is running for this session.
Failed over	Terminal	The method has failed and the next method is expected to provide a result.
Authc Success	Terminal	The method has provided a successful authentication result for the session.
Authc Failed	Terminal	The method has provided a failed authentication result for the session.

Examples

The following example shows how to display authentication methods registered with Auth Manager:

```
Switch# show authentication registrations
Auth Methods registered with the Auth Manager:
Handle Priority Name
3 0 dot1x
2 1 mab
1 2 webauth
Switch#
```

The following example shows how to display Auth Manager details for a specific interface:

```
Switch# show authentication interface gigabitethernet1/23
Client list:
MAC Address Domain Status Handle Interface
000e.84af.59bd DATA Authz Success 0xE0000000 GigabitEthernet1/0/23
```

```

Available methods list:
Handle Priority Name
3 0 dot1x
Runnable methods list:
Handle Priority Name
3 0 dot1x
Switch#

```

The following example shows how to display all Auth Manager sessions on the switch:

```

Switch# show authentication sessions
Interface MAC Address Method Domain Status Session ID
Gi3/45 (unknown) N/A DATA Authz Failed 0908140400000007003651EC
Gi3/46 (unknown) N/A DATA Authz Success 09081404000000080057C274

```

The following example shows how to display all Auth Manager sessions on an interface:

```

Switch# show authentication sessions int gi 3/46
      Interface: GigabitEthernet3/46
      MAC Address: Unknown
      IP Address: Unknown
      Status: Authz Success
      Domain: DATA
      Oper host mode: multi-host
      Oper control dir: both
      Authorized By: Guest Vlan
      Vlan Policy: 4094
      Session timeout: N/A
      Idle timeout: N/A
      Common Session ID: 09081404000000080057C274
      Acct Session ID: 0x0000000A
      Handle: 0xCC000008

```

```

Runnable methods list:
Method State
dot1x Failed over

```

The following example shows how to display Auth Manager session for a specified MAC address:

```

Switch# show authentication sessions mac 000e.84af.59bd
Interface: GigabitEthernet1/23
MAC Address: 000e.84af.59bd
Status: Authz Success
Domain: DATA
Oper host mode: single-host
Authorized By: Authentication Server
Vlan Policy: 10
Handle: 0xE0000000
Runnable methods list:
Method State
dot1x Authc Success
Switch#

```

The following example shows how to display all clients authorized via a specified auth method:

```

Switch# show authentication sessions method mab
No Auth Manager contexts match supplied criteria
Switch# show authentication sessions method dot1x
MAC Address Domain Status Handle Interface
000e.84af.59bd DATA Authz Success 0xE0000000 GigabitEthernet1/23
Switch#

```

The following example displays the policies applied on interface e0/0:

```
AUTH# show authentication sessions interface e0/0 policy
```

```

  Interface: Ethernet0/0
  MAC Address: aabb.cc01.ff00
  IPv6 Address: Unknown
  IPv4 Address: Unknown
  User-Name: gupn
  Status: Authorized
  Domain: DATA
  Security Policy: Should Secure
  Security Status: Unsecure
  Oper host mode: multi-host
  Oper control dir: both
  Session timeout: N/A
  Common Session ID: 0D0102330000000D0003329A
  Acct Session ID: Unknown
  Handle: 0x6F000002
  Current Policy: POLICY_Et0/0

```

Local Policies:

```

  Template: SVC_1 (priority 10)
  Idle timeout: 500 sec
  TAG: blue
  URL Redirect: www.a.com
  URL Redirect ACL: a

```

```

  Template: SVC_3 (priority 20)
  Idle timeout: 300 sec
  TAG: red
  URL_Redirect: www.b.com
  URL-Redirect ACL: b

```

Server Policies:

```
Idle timeout: 800 sec
```

Resultant policies:

```

  Idle timeout: 500 sec
  TAG: blue
  URL Redirect: www.a.com
  URL Redirect ACL: a
  TAG: red

```

Method status list:

```

  Method      State
  dot1x      Authc Success

```

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.

Command	Description
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.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

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

Examples The following 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      : 30.0.0.3
Config File Fetched : Undetermined
```

The first IP address in the display indicates the server that is used for the automatic installation. The second IP address indicates the TFTP server that provided the configuration file.

show auto qos

To display the automatic quality of service (auto-QoS) configuration that is applied, use the **show auto qos** user EXEC command.

```
show auto qos [interface interface-id] [{begin | exclude | include} expression]
```

Syntax Description

interface <i>interface-id</i>	(Optional) Displays auto-QoS information for the specified interface or for all interfaces. Valid interfaces include physical ports.
begin	(Optional) Begins with the line that matches the expression.
exclude	(Optional) Excludes lines that match the expression.
include	(Optional) Includes lines that match the specified expression.
<i>expression</i>	(Optional) Expression in the output to use as a reference point.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.1(19)EW	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

The following example shows output from the **show auto qos** command when auto-QoS is enabled:

```
Switch# show auto qos
GigabitEthernet1/2
auto qos voip cisco-phone
Switch#
```

Related Commands

Command	Description
auto qos voip	Automatically configures quality of service (auto-QoS) for Voice over IP (VoIP) within a QoS domain.

show auto security

To display the auto security (configuration), use the **show auto security** command.

show auto security [configuration]

Syntax Description	configuration Displays the CLIs that are applied with AS.				
Command Default	This command has no default settings.				
Command Modes	Privileged EXEC mode				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>3.6.0E</td> <td>This command was introduced on the Catalyst 4500 series switch.</td> </tr> </tbody> </table>	Release	Modification	3.6.0E	This command was introduced on the Catalyst 4500 series switch.
Release	Modification				
3.6.0E	This command was introduced on the Catalyst 4500 series switch.				

Examples

The following example shows the output of the **show auto security** command when AS is disabled globally:

```
Switch# show auto security
Auto Secure is Disabled globally

AutoSecure is Enabled on below interface(s):
-----
none
Switch#
```

The following example shows how to enable auto security on an uplink port:

```
Switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# int g1/0/15
Switch(config-if)# auto security-port uplink
Switch(config-if)# end
Switch# sh auto security
Auto Secure is Enabled globally

AutoSecure is Enabled on below interface(s):
-----
GigabitEthernet1/0/2
GigabitEthernet1/0/3
GigabitEthernet1/0/15
```

The following example shows how to enable auto security on an access port:

```
Switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# int g1/0/18
Switch(config-if)# auto security-port host
Switch(config-if)# end
Switch#
Apr 5 22:16:41.725: %SYS-5-CONFIG_I: Configured from console by console$ auto security
```

```
Switch# show auto security
Auto Secure is Enabled globally

AutoSecure is Enabled on below interface(s):
-----
GigabitEthernet1/0/2
GigabitEthernet1/0/3
GigabitEthernet1/0/15
GigabitEthernet1/0/18
```

The following example shows how to display the CLIs that are applied with AS:

```
Switch# show auto security configuration
%AutoSecure provides a single CLI config 'auto secure'
to enable Base-line security Features like
DHCP snooping, ARP inspection and Port-Security

Auto Secure CLIs applied globally:
-----
ip dhcp snooping
ip dhcp snooping vlan 2-1005
no ip dhcp snooping information option
ip arp inspection vlan 2-1005

Auto Secure CLIs applied on Access Port:
-----
switchport port-security maximum 2
switchport port-security maximum 1 vlan access
switchport port-security maximum 1 vlan voice
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity
switchport port-security
ip arp inspection limit rate 100
ip dhcp snooping limit rate 100

Auto Secure CLIs applied on Trunk Port:
-----
ip dhcp snooping trust
ip arp inspection trust
switchport port-security maximum 100
switchport port-security violation restrict
switchport port-security
```

show bootflash:

To display information about the bootflash: file system, use the **show bootflash:** command.

show bootflash: [all | chips | fileys]

Syntax Description	all	(Optional) Displays all possible Flash information.
	chips	(Optional) Displays Flash chip information.
	fileys	(Optional) Displays file system information.

Command Default This command has no default settings.

Command Modes EXEC

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

Examples The following example shows how to display file system status information:

```
Switch> show bootflash: fileys

----- 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
  File System Offset = 40000     Length           = F40000
  MONLIB Offset     = 100        Length           = C628
  Bad Sector Map Offset = 3FFF8   Length           = 8
  Squeeze Log Offset = F80000    Length           = 40000
  Squeeze Buffer Offset = FC0000   Length           = 40000
  Num Spare Sectors = 0
    Spares:
STATUS INFO:
  Writable
  NO File Open for Write
  Complete Stats
  No Unrecovered Errors
  No Squeeze in progress
USAGE INFO:
  Bytes Used      = 917CE8   Bytes Available = 628318
  Bad Sectors     = 0        Spared Sectors  = 0
  OK Files        = 2        Bytes           = 917BE8
  Deleted Files   = 0        Bytes           = 0
  Files w/Errors  = 0        Bytes           = 0
Switch>
```

The following example shows how to display system image information:

```
Switch> show bootflash:
-# - ED --type-- --crc--- -seek-- nlen -length- -----date/time----- name
1  .. image      8C5A393A 237E3C   14 2063804 Aug 23 1999 16:18:45 c4-boot-mz
2  .. image      D86EE0AD 957CE8    9 7470636 Sep 20 1999 13:48:49 rp.halley
Switch>
```

The following example shows how to display all bootflash information:

```
Switch> show bootflash: all
-# - ED --type-- --crc--- -seek-- nlen -length- -----date/time----- name
1  .. image      8C5A393A 237E3C   14 2063804 Aug 23 1999 16:18:45 c4-boot-
mz
2  .. image      D86EE0AD 957CE8    9 7470636 Sep 20 1999 13:48:49 rp.halley

6456088 bytes available (9534696 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
  File System Offset = 40000     Length = F40000
  MONLIB Offset     = 100       Length = C628
  Bad Sector Map Offset = 3FFF8   Length = 8
  Squeeze Log Offset = F80000   Length = 40000
  Squeeze Buffer Offset = FC0000  Length = 40000
  Num Spare Sectors = 0
  Spares:
STATUS INFO:
  Writable
  NO File Open for Write
  Complete Stats
  No Unrecovered Errors
  No Squeeze in progress
USAGE INFO:
  Bytes Used      = 917CE8   Bytes Available = 628318
  Bad Sectors    = 0        Spared Sectors  = 0
  OK Files       = 2        Bytes = 917BE8
  Deleted Files  = 0        Bytes = 0
  Files w/Errors = 0        Bytes = 0
Switch>
```

show bootvar

To display BOOT environment variable information, use the **show bootvar** command.

show bootvar

Syntax Description This command has no arguments or keywords.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

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

Examples The following example shows how to display BOOT environment variable information:

```
Switch# show bootvar
BOOT variable = sup:1;
CONFIG_FILE variable does not exist
BOOTLDR variable does not exist
Configuration register is 0x0
Switch#
```

show cable-diagnostics tdr

To display the test results for the TDR cable diagnostics, use the **show cable-diagnostics tdr** command.

```
show cable-diagnostics tdr {interface {interface interface-number}}
```



Note

This command will be deprecated in future Cisco IOS releases; use the **diagnostic start** command instead.

Syntax Description

interface *interface* Interface type; valid values are **fastethernet** and **gigabitethernet**.
interface-number Module and port number.

Command Default

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 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

The following example shows how to display information about the TDR test:

```
Switch# show cable-diagnostics tdr interface gi4/13
Interface Speed Local pair Cable length Remote channel Status
Gi4/13    0Mbps   1-2      102 +-2m   Unknown      Fault
          3-6      100 +-2m   Unknown      Fault
          4-5      102 +-2m   Unknown      Fault
          7-8      102 +-2m   Unknown      Fault
Switch#
```


Table 2-21 describes the fields in the **show cable-diagnostics tdr** command output.

Table 2-21 *show cable-diagnostics tdr Command Output Fields*

Field	Description
Interface	Interface tested.
Speed	Current line speed.
Pair	Local 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: <ul style="list-style-type: none"> Terminated—The link is up. Fault—Cable fault (open or short)

Related Commands

Command	Description
test cable-diagnostics tdr	Tests the condition of copper cables on 48-port 10/100/1000 BASE-T modules.

show call-home

To display the configured CallHome information, use the **show call-home** command in privileged EXEC mode.

```
show call-home [alert-group | detail | mail-server | profile {all | name} | statistics]
```

Syntax Description	
alert-group	(Optional) Displays the available alert group.
detail	(Optional) Displays the CallHome configuration in detail.
mail-server	(Optional) Displays the CallHome mail server-related information.
profile all	(Optional) Displays configuration information for all existing profiles.
profile name	(Optional) Displays configuration information for a specific destination profile.
statistics	(Optional) Displays the CallHome statistics.

Command Default This command has no default settings.

Command Modes Privileged EXEC (#)

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:

```
Switch# show call-home
Current call home settings:
  call home feature : disable
  call home message's from address: switch@example.com
  call home message's reply-to address: support@example.com

  vrf for call-home messages: Not yet set up

  contact person's email address: technical@example.com

  contact person's phone number: +1-408-555-1234
  street address: 1234 Picaboo Street, Any city, Any state, 12345
  customer ID: ExampleCorp
  contract ID: X123456789
  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

Switch#

```

Configured CallHome Information in Detail

```

Switch# show call-home detail
Current call home settings:
  call home feature : disable
  call home message's from address: switch@example.com
  call home message's reply-to address: support@example.com

  vrf for call-home messages: Not yet set up

  contact person's email address: technical@example.com

  contact person's phone number: +1-408-555-1234
  street address: 1234 Picaboo Street, Any city, Any state, 12345
  customer ID: ExampleCorp
  contract ID: X123456789
  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 status: ACTIVE
  Preferred Message Format: long-text
  Message Size Limit: 3145728 Bytes
  Transport Method: email
  Email address(es): noc@example.com
  HTTP address(es): 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(es): callhome@cisco.com
HTTP address(es): https://tools.cisco.com/its/service/oddce/services/DDCEService

```

Periodic configuration info message is scheduled every 1 day of the month at 09:27

Periodic inventory info message is scheduled every 1 day of the month at 09: 12

Alert-group	Severity
-----	-----
diagnostic	minor
environment	warning
inventory	normal

Syslog-Pattern	Severity
-----	-----
.*	major

Switch#

Available Call Home Alert Groups

Switch# **show call-home alert-group**

Available alert groups:

Keyword	State	Description
-----	-----	-----
configuration	Disable	configuration info
diagnostic	Disable	diagnostic info
environment	Disable	environmental info
inventory	Enable	inventory info
syslog	Disable	syslog info

Switch#

E-Mail Server Status Information

Switch# **show call-home mail-server status**

Please wait. Checking for mail server status ...

Translating "smtp.example.com"

```

Mail-server[1]: Address: smtp.example.com Priority: 1 [Not Available]
Mail-server[2]: Address: 192.168.0.1 Priority: 2 [Not Available]

```

Switch#

Information for All Destination Profiles (Predefined and User-Defined)

Switch# **show call-home profile all**

```

Profile Name: campus-noc
Profile status: ACTIVE
Preferred Message Format: long-text
Message Size Limit: 3145728 Bytes
Transport Method: email
Email address(es): noc@example.com
HTTP address(es): 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(es): callhome@cisco.com
  HTTP address(es): https://tools.cisco.com/its/service/oddce/services/DDCEService

Periodic configuration info message is scheduled every 1 day of the month at 09:27

Periodic inventory info message is scheduled every 1 day of the month at 09:12

Alert-group          Severity
-----
diagnostic           minor
environment          warning
inventory            normal

Syslog-Pattern      Severity
-----
.*                  major

Switch#

```

Information for a User-Defined Destination Profile

```

Switch# show call-home profile CiscoTAC-1
Profile Name: CiscoTAC-1
  Profile status: INACTIVE
  Preferred Message Format: xml
  Message Size Limit: 3145728 Bytes
  Transport Method: email
  Email address(es): callhome@cisco.com
  HTTP address(es): https://tools.cisco.com/its/service/oddce/services/DDCEService

Periodic configuration info message is scheduled every 11 day of the month at 11:25

Periodic inventory info message is scheduled every 11 day of the month at 11:10

Alert-group          Severity
-----
diagnostic           minor
environment          warning
inventory            normal

Syslog-Pattern      Severity
-----
.*                  major

```

Call Home Statistics

```

Switch# show call-home statistics
Message Types      Total      Email      HTTP
-----
Total Success     0          0          0
  Config          0          0          0
  Diagnostic      0          0          0
  Environment     0          0          0
  Inventory       0          0          0
  SysLog         0          0          0
  Test           0          0          0
  Request        0          0          0
  Send-CLI       0          0          0

```

show call-home

```

Total In-Queue 0          0          0
  Config      0          0          0
  Diagnostic  0          0          0
  Environment 0          0          0
  Inventory   0          0          0
  SysLog      0          0          0
  Test        0          0          0
  Request     0          0          0
  Send-CLI    0          0          0

Total Failed  0          0          0
  Config      0          0          0
  Diagnostic  0          0          0
  Environment 0          0          0
  Inventory   0          0          0
  SysLog      0          0          0
  Test        0          0          0
  Request     0          0          0
  Send-CLI    0          0          0

Total Ratelimit
  -dropped  0          0          0
  Config    0          0          0
  Diagnostic 0          0          0
  Environment 0        0          0
  Inventory  0          0          0
  SysLog     0          0          0
  Test       0          0          0
  Request    0          0          0
  Send-CLI   0          0          0

```

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	
<i>type</i>	(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 .
<i>number</i>	(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.

Command Default 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 The following 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          157        R           7206VXR   Fas 0/0/0
lab-as5300-1     Eth 0          163        R           AS5300    Fas 0
lab-as5300-2     Eth 0          159        R           AS5300    Eth 0
lab-as5300-3     Eth 0          122        R           AS5300    Eth 0
lab-as5300-4     Eth 0          132        R           AS5300    Fas 0/0
lab-3621         Eth 0          140        R S         3631-telcoFas 0/0
008024 2758E0    Eth 0          132        T           CAT3000   1/2
Switch#
```

Table 2-22 describes the fields that are shown in the example.

Table 2-22 *show cdp neighbors Field Descriptions*

Field	Definition
Device ID	Configured ID (name), MAC address, or serial number of the neighbor device.
Local Intrfce	(Local Interface) The protocol that is used by the connectivity media.
Holdtme	(Holdtime) Remaining amount of time, in seconds, that the current device holds the CDP advertisement from a transmitting router before discarding it.
Capability	Capability code that is discovered on the device. This device type is listed in the CDP Neighbors table. Possible values are as follows: R—Router T—Transparent bridge B—Source-routing bridge S—Switch H—Host I—IGMP device r—Repeater P—Phone
Platform	Product number of the device.
Port ID	Protocol and port number of the device.

The following 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 7206VXR, Capabilities: Router
Interface: Ethernet0, Port ID (outgoing port): FastEthernet0/0/0
Holdtime : 123 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) 5800 Software (C5800-P4-M), Version 12.1(2)
Copyright (c) 1986-2002 by Cisco Systems, Inc.

advertisement version: 2
Duplex: half

-----
Device ID: lab-as5300-1
Entry address(es):
  IP address: 172.19.169.87
.
.
.
Switch#
```


Table 2-23 describes the fields that are shown in the example.

Table 2-23 *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 in IP, IPX, AppleTalk, DECnet, or CLNS protocol conventions.
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, a source-routing bridge, a switch, a host, an IGMP device, or a repeater.
Interface	Protocol and port number of the port on the current device.
Holdtime	Remaining amount of time, in seconds, that the current device holds the CDP advertisement from a transmitting router before discarding it.
Version:	Software version running on the neighbor device.
advertisement version:	Version of CDP that is being used for CDP advertisements.
Duplex:	Duplex state of connection between the current device and the neighbor device.

Related Commands

Command	Description
show cdp (refer to Cisco IOS documentation)	Displays global CDP information, including timer and hold-time information.
show cdp entry (refer to Cisco IOS documentation)	Displays information about a specific neighboring device discovered using Cisco Discovery Protocol (CDP).
show cdp interface (refer to Cisco IOS documentation)	Displays information about the interfaces on which Cisco Discovery Protocol (CDP) is enabled.
show cdp traffic (refer to Cisco IOS documentation)	Displays traffic information from the CDP table.

show class-map

To display class map information, use the **show class-map** command.

show class-map *class_name*

Syntax Description	<i>class_name</i> Name of the class map.
---------------------------	--

Command Default	This command has no default settings.
------------------------	---------------------------------------

Command Modes	Privileged EXEC mode
----------------------	----------------------

Command History	Release	Modification
	12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch.
	12.2(25)SG	Displays results from the full-flow option.

Examples The following example shows how to display class map information for all class maps:

```
Switch# show class-map
Class Map match-any class-default (id 0)
  Match any
Class Map match-any class-simple (id 2)
  Match any
Class Map match-all ipp5 (id 1)
  Match ip precedence 5
Class Map match-all agg-2 (id 3)
Switch#
```

The following example shows how to display class map information for a specific class map:

```
Switch# show class-map ipp5
Class Map match-all ipp5 (id 1)
  Match ip precedence 5
Switch#
```

Assume there are two active flows as shown below on Fast Ethernet interface 6/1:

SrcIp	DstIp	IpProt	SrcL4Port	DstL4Port
192.168.10.10	192.168.20.20	20	6789	81
192.168.10.10	192.168.20.20	20	6789	21

With following configuration, each flow will be policed to a 1000000 bps with an allowed 9000-byte burst value.



Note

If you use the **match flow ip source-address|destination-address** command, these two flows are consolidated into one flow and they have the same source and destination address.

```

Switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# class-map c1
Switch(config-cmap)# match flow ip source-address ip destination-address ip protocol 14
source-port 14 destination-port
Switch(config-cmap)# exit
Switch(config)# policy-map p1
Switch(config-pmap)# class c1
Switch(config-pmap-c)# police 1000000 9000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastEthernet 6/1
Switch(config-if)# service-policy input p1
Switch(config-if)# end
Switch# write memory
Switch# show policy-map interface
FastEthernet6/1

class-map c1
  match flow ip source-address ip destination-address ip protocol 14 source-port 14
  destination-port
  !
  policy-map p1
    class c1
      police 1000000 bps 9000 byte conform-action transmit exceed-action drop
  !
interface FastEthernet 6/1
  service-policy input p1

Switch# show class-map c1
Class Map match-all c1 (id 2)
  Match flow ip source-address ip destination-address ip protocol 14 source-port 14
  destination-port
Switch#

```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to the class whose name you specify and to be used enter class-map configuration mode.
show policy-map	Displays information about the policy map.
show policy-map interface	Displays the statistics and configurations of the input and output policies that are attached to an interface.

show device-sensor cache

To display Device Sensor cache entries, use the **show device-sensor cache** command in privileged EXEC mode.

show device-sensor cache {mac *mac-address* | all}

Syntax Description	mac	mac-address
	Specifies the MAC address of the device for which the sensor cache entries are to be displayed.	
	all	Displays sensor cache entries for all devices.

Command Default There are no defaults for this command.

Command Modes Privileged EXEC

Command History	Release	Modification
	IOS XE 3.4.0SG and IOS 15.1(2)SG	Command introduced on the Catalyst 4500 Series switch.

Usage Guidelines Use the **show device-sensor cache** command to display a list of TLV fields or options received from a particular device or from all devices.

Examples The following is sample output from the **show device-sensor cache mac *mac-address*** command:

```
Router# show device-sensor cache mac 0024.14dc.df4d

Device: 0024.14dc.df4d on port GigabitEthernet1/0/24
-----
Proto  Type:Name                               Len Value
cdp    26:power-available-type                 16 00 1A 00 10 00 00 00 01 00 00 00 00 FF FF FF FF
cdp    22:mgmt-address-type                    17 00 16 00 11 00 00 00 01 01 01 CC 00 04 09 1B 65
      0E
cdp    11:duplex-type                          5 00 0B 00 05 01
cdp    9:vtp-mgmt-domain-type                  4 00 09 00 04
cdp    4:capabilities-type                     8 00 04 00 08 00 00 00 28
cdp    1:device-name                           14 00 01 00 0E 73 75 70 70 6C 69 63 61 6E 74
lldp   0:end-of-lldpdu                         2 00 00
lldp   8:management-address                    14 10 0C 05 01 09 1B 65 0E 03 00 00 00 01 00
lldp   7:system-capabilities                   6 0E 04 00 14 00 04
lldp   4:port-description                      23 08 15 47 69 67 61 62 69 74 45 74 68 65 72 6E 65
      74 31 2F 30 2F 32 34
lldp   5:system-name                          12 0A 0A 73 75 70 70 6C 69 63 61 6E 74
dhcp   82:relay-agent-info                     20 52 12 01 06 00 04 00 18 01 18 02 08 00 06 00 24
      14 DC DF 80
dhcp   12:host-name                          12 0C 0A 73 75 70 70 6C 69 63 61 6E 74
dhcp   61:client-identifier                   32 3D 1E 00 63 69 73 63 6F 2D 30 30 32 34 2E 31 34
      64 63 2E 64 66 34 64 2D 47 69 31 2F 30 2F 32 34
```

```
dhcp      57:max-message-size          4 39 02 04 80
```

The following is sample output from the **show device-sensor cache all** command:

```
Router# show device-sensor cache all
```

```
Device: 001c.0f74.8480 on port GigabitEthernet2/1
```

```
-----
Proto  Type:Name                Len  Value
dhcp   52:option-overload       3   34 01 03
dhcp   60:class-identifier      11  3C 09 64 6F 63 73 69 73 31 2E 30
dhcp   55:parameter-request-list 8   37 06 01 42 06 03 43 96
dhcp   61:client-identifier     27  3D 19 00 63 69 73 63 6F 2D 30 30 31 63 2E 30 66
                                37 34 2E 38 34 38 30 2D 56 6C 31
dhcp   57:max-message-size      4   39 02 04 80
```

```
Device: 000f.f7a7.234f on port GigabitEthernet2/1
```

```
-----
Proto  Type:Name                Len  Value
cdp    22:mgmt-address-type     8   00 16 00 08 00 00 00 00
cdp    19:cos-type              5   00 13 00 05 00
cdp    18:trust-type            5   00 12 00 05 00
cdp    11:duplex-type           5   00 0B 00 05 01
cdp    10:native-vlan-type      6   00 0A 00 06 00 01
cdp    9:vtp-mgmt-domain-type   9   00 09 00 09 63 69 73 63 6F
```

The following table describes the significant fields shown in the display:

Field	Description
Device	MAC address of the device and the interface which it is connected to.
Proto	Protocol from which the endpoint device data is being gleaned.
Type	Type of TLV.
Name	Name of the TLV.
Len	Length of the TLV.
Value	Value of the TLV.

Related Commands

Command	Description
debug device-sensor	Enables debugging for Device Sensor.
device-sensor accounting	Adds the Device Sensor protocol data to accounting records and generates additional accounting events when new sensor data is detected.
device-sensor filter-list	Creates a CDP or LLDP filter containing a list of options that can be included or excluded in the Device Sensor output.
device-sensor filter-list dhcp	Creates a DHCP filter containing a list of options that can be included or excluded in the Device Sensor output.
show device-sensor cache	Displays Device Sensor cache entries.

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.

Command Default This command has no default settings.

Command Modes EXEC

Command History	Release	Modification
	12.2(20)EWA	This command was introduced on the Catalyst 4500 series switch.

Examples The following example shows how to display the test suite, monitoring interval, and test attributes for all the modules of the chassis:

```
Switch# show diagnostic content module all
```

```
module 1:
```

```
Diagnostics test suite attributes:
```

```

  B/* - Basic ondemand test / NA
  P/V/* - Per port test / Per device test / NA
  D/N/* - Disruptive test / Non-disruptive test / NA
  S/* - Only applicable to standby unit / NA
  X/* - Not a health monitoring test / NA
  F/* - Fixed monitoring interval test / NA
  E/* - Always enabled monitoring test / NA
  A/I - Monitoring is active / Monitoring is inactive
  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-bootup -----> **D***I**   not configured
  2) packet-memory-bootup -----> **D***I**   not configured
  3) packet-memory-ongoing -----> **N***I*o   not configured

```

```
module 6:
```

```
Diagnostics test suite attributes:
  B/* - Basic ondemand test / NA
  P/V/* - Per port test / Per device test / NA
  D/N/* - Disruptive test / Non-disruptive test / NA
  S/* - Only applicable to standby unit / NA
  X/* - Not a health monitoring test / NA
  F/* - Fixed monitoring interval test / NA
  E/* - Always enabled monitoring test / NA
  A/I - Monitoring is active / Monitoring is inactive
  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) linecard-online-diag -----> **D***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**]

Syntax Description

<i>slot-num</i>	(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.
<i>test-id</i>	(Optional) Specifies a single test ID.
<i>test-id-range</i>	(Optional) Specifies a range of test IDs.
all	(Optional) Displays the diagnostics for all tests.
detail	(Optional) Displays the complete test results.

Command Default

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)EW	This command was introduced on the Catalyst 4500 series switch.

Examples

The following 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 4:

  Overall diagnostic result: PASS
  Diagnostic level at card bootup: minimal

  Test results: (. = Pass, F = Fail, U = Untested)

    1) linecard-online-diag -----> .
```



```

module 5:

Overall diagnostic result: PASS
Diagnostic level at card bootup: minimal

Test results: (. = Pass, F = Fail, U = Untested)

1) linecard-online-diag -----> .

```

```

module 6:

Overall diagnostic result: PASS
Diagnostic level at card bootup: minimal

Test results: (. = Pass, F = Fail, U = Untested)

1) linecard-online-diag -----> .

```

The following example shows how to display the online diagnostics for module 1:

```

Switch# show diagnostic result module 1 detail

Current bootup diagnostic level: minimal

module 1:

Overall diagnostic result: PASS
Diagnostic level at card bootup: minimal

Test results: (. = Pass, F = Fail, U = Untested)

-----

1) supervisor-bootup -----> .

Error code -----> 0 (DIAG_SUCCESS)
Total run count -----> 0
Last test execution time -----> n/a
First test failure time -----> n/a
Last test failure time -----> n/a
Last test pass time -----> n/a
Total failure count -----> 0
Consecutive failure count -----> 0

Power-On-Self-Test Results for ACTIVE Supervisor

Power-on-self-test for Module 1: WS-X4014
Port/Test Status: (. = Pass, F = Fail)
Reset Reason: PowerUp Software/User

Port Traffic: L2 Serdes Loopback ...
0: . 1: . 2: . 3: . 4: . 5: . 6: . 7: . 8: . 9: . 10: . 11: .
12: . 13: . 14: . 15: . 16: . 17: . 18: . 19: . 20: . 21: . 22: . 23: .
24: . 25: . 26: . 27: . 28: . 29: . 30: . 31: .

Port Traffic: L2 Asic Loopback ...
0: . 1: . 2: . 3: . 4: . 5: . 6: . 7: . 8: . 9: . 10: . 11: .

```

```
12: . 13: . 14: . 15: . 16: . 17: . 18: . 19: . 20: . 21: . 22: . 23: .
24: . 25: . 26: . 27: . 28: . 29: . 30: . 31: .
```

Port Traffic: L3 Asic Loopback ...

```
0: . 1: . 2: . 3: . 4: . 5: . 6: . 7: . 8: . 9: . 10: . 11: .
12: . 13: . 14: . 15: . 16: . 17: . 18: . 19: . 20: . 21: . 22: . 23: .
24: . 25: . 26: . 27: . 28: . 29: . 30: . 31: . au: .
```

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) packet-memory-bootup -----> .

    Error code -----> 0 (DIAG_SUCCESS)
    Total run count -----> 0
    Last test execution time -----> n/a
    First test failure time -----> n/a
    Last test failure time -----> n/a
    Last test pass time -----> n/a
    Total failure count -----> 0
    Consecutive failure count -----> 0
packet buffers on free list: 64557 bad: 0 used for ongoing tests: 979

Number of errors found: 0
Cells with hard errors (failed two or more tests): 0
Cells with soft errors (failed one test, includes hard): 0
Suspect bad cells (uses a block that tested bad): 0
total buffers: 65536
bad buffers: 0 (0.0%)
good buffers: 65536 (100.0%)
Bootup test results:1
No errors.
```

```
3) packet-memory-ongoing -----> U

    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
packet buffers on free list: 64557 bad: 0 used for ongoing tests: 979
```

Packet memory errors: 0 0

```

Current alert level: green
Per 5 seconds in the last minute:
  0 0 0 0 0 0 0 0 0 0
  0 0
Per minute in the last hour:
  0 0 0 0 0 0 0 0 0 0
  0 0 0 0 0 0 0 0 0 0
  0 0 0 0 0 0 0 0 0 0
  0 0 0 0 0 0 0 0 0 0
  0 0 0 0 0 0 0 0 0 0
  0 0 0 0 0 0 0 0 0 0
Per hour in the last day:
  0 0 0 0 0 0 0 0 0 0
  0 0 0 0 0 0 0 0 0 0
  0 0 0 0
Per day in the last 30 days:
  0 0 0 0 0 0 0 0 0 0
  0 0 0 0 0 0 0 0 0 0
  0 0 0 0 0 0 0 0 0 0
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 0 0
  0 0 0 0 0 0 0 0 0 0
Potential false positives: 0 0
Ignored because of rx errors: 0 0
Ignored because of cdm fifo overrun: 0 0
Ignored because of oir: 0 0
Ignored because isl frames received: 0 0
Ignored during boot: 0 0
Ignored after writing hw stats: 0 0
Ignored on high gigaport: 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	
<i>N</i>	(Optional) Specifies the module number.
all	(Optional) Specifies all modules.
test <i>test-id</i>	(Optional) Specifies the number for the tdr test on the platform.
detail	(Optional) Specifies the display of detailed information for analysis. This option is recommended.

Command Default Non-detailed results.

Command Modes EXEC mode

Command History	Release	Modification
	12.2(25)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

The following example shows how to display the results of the bootup packet memory tests:

```
Switch# show diagnostic result module 6 detail
module 6:

Overall diagnostic result:PASS

Test results:(. = Pass, F = Fail, U = Untested)

-----

1) linecard-online-diag -----> .

Error code -----> 0 (DIAG_SUCCESS)
Total run count -----> 1
Last test execution time -----> Jan 21 2001 19:48:30
First test failure time -----> n/a
Last test failure time -----> n/a
Last test pass time -----> Jan 21 2001 19:48:30
Total failure count -----> 0
Consecutive failure count -----> 0
```

```

Slot Ports Card Type                               Diag Status   Diag Details
-----
 6    48  10/100/1000BaseT (RJ45)V, Cisco/IEEE  Passed        None

```

Detailed Status

```

-----
. = Pass                U = Unknown
L = Loopback failure   S = Stub failure
I = Ilc failure        P = Port failure
E = SEEPROM failure    G = GBIC 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-tdr:

```

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
-----
      .  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U

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
-----
      U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U

```

```

Error code -----> 0 (DIAG_SUCCESS)
Total run count -----> 1
Last test execution time -----> Jan 22 2001 03:01:54
First test failure time -----> n/a
Last test failure time -----> n/a
Last test pass time -----> Jan 22 2001 03:01:54
Total failure count -----> 0
Consecutive failure count -----> 0

```

Detailed Status

```

-----
TDR test is in progress on interface Gi6/1

```

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 the test passed, failed, or was not run.

show diagnostic result module *N* test 2 [detail]

Syntax Description	<i>N</i>	Specifies the module number.
	detail	(Optional) Specifies the display of detailed information for analysis.

Command Default Non-detailed results.

Command Modes EXEC mode

Command History	Release	Modification
	12.2(18)EW	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 The following example shows how to display the results of the bootup packet memory tests:

```
Switch# show diagnostic result module 1 test 2

Test results: (. = Pass, F = Fail, U = Untested)

    2) packet-memory-bootup -----> .
```

The following example shows how to display detailed results from the bootup packet memory tests:

```
Switch# show diagnostic result module 2 test 2 detail

Test results: (. = Pass, F = Fail, U = Untested)

-----> .

    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
packet buffers on free list: 64557 bad: 0 used for ongoing tests: 979
```

```
Number of errors found: 0
Cells with hard errors (failed two or more tests): 0
Cells with soft errors (failed one test, includes hard): 0
Suspect bad cells (uses a block that tested bad): 0
total buffers: 65536
bad buffers: 0 (0.0%)
good buffers: 65536 (100.0%)
Bootup test results:
No errors.
```

Related Commands

Command	Description
diagnostic monitor action	Directs the action of the switch when it detects a packet memory failure.
show diagnostic result module test 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 3 [detail]

Syntax Description	<i>N</i>	Module number.
	detail	(Optional) Specifies the display of detailed information for analysis.

Command Default Non-detailed results.

Command Modes EXEC mode

Command History	Release	Modification
	12.2(18)EW	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 The following example shows how to display the results from the ongoing packet memory tests:

```
Switch# show diagnostic result module 1 test 3

Test results: (. = Pass, F = Fail, U = Untested)

    3) packet-memory-ongoing -----> .
```

The following example shows how to display the detailed results from the ongoing packet memory tests:

```
Switch# show diagnostic result module 1 test 3 detail

Test results: (. = Pass, F = Fail, U = Untested)

-----> .

    3) packet-memory-ongoing -----> .

        Error code -----> 0 (DIAG_SUCCESS)
        Total 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
packet buffers on free list: 64557 bad: 0 used for ongoing tests: 979
```



```

Packet memory errors: 0 0
Current alert level: green
Per 5 seconds in the last minute:
 0 0 0 0 0 0 0 0 0 0
 0 0
Per minute in the last hour:
 0 0 0 0 0 0 0 0 0 0
 0 0 0 0 0 0 0 0 0 0
 0 0 0 0 0 0 0 0 0 0
 0 0 0 0 0 0 0 0 0 0
 0 0 0 0 0 0 0 0 0 0
 0 0 0 0 0 0 0 0 0 0
Per hour in the last day:
 0 0 0 0 0 0 0 0 0 0
 0 0 0 0 0 0 0 0 0 0
 0 0 0 0
Per day in the last 30 days:
 0 0 0 0 0 0 0 0 0 0
 0 0 0 0 0 0 0 0 0 0
 0 0 0 0 0 0 0 0 0 0
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 0 0
 0 0 0 0 0 0 0 0 0 0
Potential false positives: 0 0
  Ignored because of rx errors: 0 0
  Ignored because of cdm fifo overrun: 0 0
  Ignored because of oir: 0 0
  Ignored because isl frames received: 0 0
  Ignored during boot: 0 0
  Ignored after writing hw stats: 0 0
  Ignored on high gigaport: 0
Ongoing diag action mode: Normal
Last 1000 Memory Test Failures: v
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 status for the entire switch or for a specified interface, use the **show dot1x** command.

```
show dot1x [interface interface-id] | [statistics [interface interface-id]] | [all]
```

Syntax Description	
interface <i>interface-id</i>	(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.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.1(12c)EW	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 to honor the Session-Timeout value) was added.
	12.2(31)SG	Support for port direction control and critical recovery was added.

Usage Guidelines If you do not specify an interface, the global parameters and a summary are displayed. If you specify an interface, the details for that interface are displayed.

If you enter the **statistics** keyword without the **interface** option, the statistics are displayed for all interfaces. If you enter the **statistics** keyword with the **interface** option, the statistics are displayed for the specified interface.

Expressions are case sensitive. For example, if you enter **exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

The **show dot1x** command displays the currently assigned reauthentication timer and time remaining before reauthentication, if reauthentication is enabled.

Examples

The following example shows how to display the output from the **show dot1x** command:

```
Switch# show dot1x
Sysauthcontrol = Disabled
Dot1x Protocol Version = 2
Dot1x Oper Controlled Directions = Both
Dot1x Admin Controlled Directions = Both
Critical Recovery Delay = 500
Critical EAP = Enabled
Switch#
```

The following example shows how to display the 802.1X statistics for a specific port:

```
Switch# show dot1x interface fastethernet6/1
Dot1x Info for FastEthernet6/1
-----
PAE = AUTHENTICATOR
PortControl = AUTO
ControlDirection = Both
HostMode = MULTI_DOMAIN
ReAuthentication = Disabled
QuietPeriod = 60
ServerTimeout = 10
SuppTimeout = 30
ReAuthPeriod = 3600 (Locally configured)
ReAuthMax = 2
MaxReq = 2
TxPeriod = 30
RateLimitPeriod = 0

Dot1x Authenticator Client List
-----
Domain = DATA
Supplicant = 0000.0000.ab01
    Auth SM State = AUTHENTICATED
    Auth BEND SM Stat = IDLE

Port Status = AUTHORIZED
Authentication Method = Dot1x
Authorized By = Authentication Server
Vlan Policy = 12

Domain = VOICE
Supplicant = 0060.b057.4687
    Auth SM State = AUTHENTICATED
    Auth BEND SM Stat = IDLE
Port Status = AUTHORIZED
Authentication Method = Dot1x
Authorized By = Authentication Server

Switch#
```

**Note**

[Table 2-24](#) 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 2-24 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.
MultiHosts	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 2-25](#) describes the fields in the display.

```
Switch# show dot1x statistics interface gigabitethernet1/1

PortStatistics Parameters for Dot1x
-----
TxReqId = 0      TxReq = 0      TxTotal = 0
RxStart = 0      RxLogoff = 0   RxRespId = 0   RxResp = 0
RxInvalid = 0    RxLenErr = 0   RxTotal= 0
RxVersion = 0    LastRxSrcMac 0000.0000.0000
Switch#
```

Table 2-25 show dot1x statistics Field Descriptions

Field	Description
TxReq/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 is critically authorized partway through an EAP exchange.
	dot1x critical recovery delay	Sets the time interval between port reinitializations.
	dot1x critical vlan	Assigns a critically authenticated port to a specific VLAN.
	dot1x guest-vlan	Enables a guest VLAN on a per-port basis.
	dot1x max-reauth-req	Sets the maximum number of times that the switch will retransmit an EAP-Request/Identity frame to the client before restarting the authentication process.
	dot1x port-control	Enables manual control of the authorization state on a port.
	mac-address-table notification	Enables MAC address notification on a switch.

show eigrp plugins

To display general information including the versions of the Enhanced Interior Gateway Routing Protocol (EIGRP) protocol features that are currently running, use the **show eigrp plugins** command in user EXEC or privileged EXEC mode.

```
show eigrp plugins [plugin-name] [detailed]
```

Syntax Description

<i>plugin-name</i>	(Optional) Name of an EIGRP plugin to display.
detailed	(Optional) Displays detailed information about EIGRP features.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.2(5)E2	Support for EVN/vNets is introduced.

Usage Guidelines

Use the **show eigrp plugins** command in user EXEC or privileged EXEC mode to determine if a particular EIGRP feature is available in your Cisco IOS image. This command displays a summary of information about EIGRP service families and address families.

This command is useful when contacting Cisco technical support.

Examples

The following example shows how to display EIGRP plugin information:

```
Sup7e#show eigrp plugins
EIGRP feature plugins::
  eigrp-release      : 20.00.00 : Portable EIGRP Release
                    : 1.01.18 : Source Component Release(rel20)
  parser             : 2.02.00 : EIGRP Parser Support
  igrp2              : 2.00.00 : Reliable Transport/Dual Database
  eigrp-nsf          : 2.01.00 : Platform Support
  Spatial Reuse Prot : 1.01.00 : Platform Support
  bfd                : 2.00.00 : BFD Platform Support
  EVN/vNets          : 1.00.00 : Easy Virtual Network (EVN/vNets)
  ipv4-af            : 2.01.01 : Routing Protocol Support
  ipv4-sf            : 1.02.00 : Service Distribution Support
  ipv6-af            : 2.01.01 : Routing Protocol Support
  ipv6-sf            : 2.01.00 : Service Distribution Support
  vNets-parse        : 1.00.00 : EIGRP vNets Parse Support
  snmp-agent         : 2.00.00 : SNMP/SNMPv2 Agent Support
```

[Table 26](#) describes the significant fields shown in the display.

Table 26 *show eigrp plugins Field Descriptions*

Field	Description
eigrp release	Displays the portable EIGRP release version.
igrp2	Displays the reliable transport and dual database version.
bfd	Displays the EIGRP-BFD feature version.
EVN/vNets	Displays the EVN/vNets version.
ipv4-af	Displays the EIGRP IPv4 routing protocol feature version.
ipv4-sf	Displays the EIGRP IPv4 service distribution feature version.
ipv6-af	Displays the EIGRP IPv6 routing protocol feature version.
ipv6-sf	Displays the EIGRP IPv6 service distribution feature version.
snmp-agent	Displays the EIGRP SNMP and SNMPv2 Agent Support version.

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.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch.
12.1(12c)EW	Support for the ability to display generic environment information with the show environment command was added.

Examples

The following example shows how to display information about the environment alarms, operational status, and current temperature readings for the chassis:

```
Switch# show environment
no alarm

Chassis Temperature           = 32 degrees Celsius
Chassis Over Temperature Threshold = 75 degrees Celsius
Chassis Critical Temperature Threshold = 95 degrees Celsius

Power Supply Model No      Type      Fan Status      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           --        --     --     --     --
```


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

The following example shows how to display information about the environment alarms:

```
Switch# show environment alarm
no alarm
Switch#
```

The following example shows how to display information about the power supplies, chassis type, and fan trays:

```
Switch# show environment status
Power                               Fan
Supply Model No                    Type      Status    Sensor
-----
PS1   PWR-C45-1400AC                 AC 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                --        --        --        --        --
```

Power supplies needed by system : 1

Chassis Type : WS-C4507R

Supervisor Led Color : Green

Fantray : good

Power consumed by Fantray : 50 Watts

Switch#

The following example shows how to display information about the chassis:

```
Switch# show environment status chassis
Chassis Type :WS-C4507R
Switch#
```

The following example shows how to display information about the fan tray:

```
Switch# show environment status fantray
Fantray : good
Power consumed by Fantray : 50 Watts
Switch#
```

The following example shows how to display information about the power supply:

```
Switch# show environment status powersupply
Power
Supply Model No          Type          Status      Fan
-----
PS1     WS-X4008              AC 400W      good        good
PS2     WS-X4008              AC 400W      good        good
PS3     none                  --           --          --
Switch#
```

The following example shows how to display information about the supervisor engine:

```
Switch# show environment status supervisor
Supervisor Led Color :Green
Switch#
```

The following example shows how to display information about the temperature of the chassis:

```
Switch# show environment temperature
Chassis Temperature                = 32 degrees Celsius
Chassis Over Temperature Threshold = 75 degrees Celsius
Chassis Critical Temperature Threshold = 95 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.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch.
	12.1(19)EW	Display includes the status of storm control.

Usage Guidelines A displayed `gbic-invalid` error reason refers to an invalid small form-factor pluggable (SFP) module. The error-disable reasons in the command output are listed in alphabetical order. The mode column shows how error disable is configured for each feature.

You can configure error-disabled detection in these modes:

- port mode—The entire physical port is error disabled if a violation occurs.
- vlan mode—The VLAN is error disabled if a violation occurs.
- port/vlan mode—The entire physical port is error disabled on some ports and per-VLAN error disabled on other ports.

Examples This is an example of output from the **show errdisable detect** command:

```
Switch> show errdisable detect
ErrDisable Reason    Detection    Mode
-----
arp-inspection       Enabled     port
bpduguard            Enabled     vlan
channel-misconfig    Enabled     port
community-limit     Enabled     port
dhcp-rate-limit      Enabled     port
dtp-flap             Enabled     port
gbic-invalid         Enabled     port
inline-power         Enabled     port
invalid-policy       Enabled     port
l2ptguard           Enabled     port
link-flap            Enabled     port
loopback             Enabled     port
lsgroup              Enabled     port
pagp-flap           Enabled     port
```

show errdisable detect

psecure-violation	Enabled	port/vlan
security-violatio	Enabled	port
sfp-config-mismat	Enabled	port
storm-control	Enabled	port
udld	Enabled	port
vmps	Enabled	port

Related Commands

Command	Description
errdisable detect cause	Enables error-disabled detection for a specific cause or all causes.
show errdisable recovery	Displays error-disabled recovery timer information.
show interfaces status	Displays interface status or a list of interfaces in error-disabled state.

show errdisable recovery

Use the **show errdisable recovery** user EXEC command to display the error-disabled recovery timer information.

show errdisable recovery

Syntax Description This command has no arguments or keywords.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch.
	12.1(19)EW	Display includes the status of storm control.

Usage Guidelines A *gbic-invalid error-disable* reason refers to an invalid small form-factor pluggable (SFP) module interface.

Examples This is an example of output from the **show errdisable recovery** command:

```
Switch> show errdisable recovery
ErrDisable Reason      Timer Status
-----
udld                   Disabled
bpduguard              Disabled
security-violatio     Disabled
channel-misconfig     Disabled
vmps                   Disabled
pagg-flap              Disabled
dtp-flap               Disabled
link-flap              Enabled
l2ptguard              Disabled
psecure-violation     Disabled
gbic-invalid           Disabled
dhcp-rate-limit       Disabled
unicast-flood         Disabled
storm-control         Disabled
arp-inspection        Disabled
loopback               Disabled
Timer interval:300 seconds

Interfaces that will be enabled at the next timeout:

Interface      Errdisable reason      Time left(sec)
-----
Gi1/0/2        link-flap                279
```

**Note**

Though visible in the output, the unicast-flood field is not valid.

Related Commands

Command	Description
errdisable recovery	Configures the recover mechanism variables.
show errdisable detect	Displays error-disabled detection status.
show interfaces status	Displays 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	
<i>channel-group</i>	(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.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch.
	12.1(13)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 Passive 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 in the only port channel in the channel group).

Examples The following example shows how to display port-channel information for a specific group:

```
Switch# show etherchannel 1 port-channel
      Port-channels in the group:
      -----
Port-channel: Po1
-----
Age of the Port-channel   = 02h:35m:26s
Logical slot/port        = 10/1           Number of ports in agport = 0
GC                       = 0x00000000    HotStandBy port = null
Passive port list        = Fa5/4 Fa5/5
Port state                = Port-channel L3-Ag Ag-Not-Inuse
```

```
Ports in the Port-channel:
Index  Load  Port
-----
Switch#
```

The following example shows how to display load-balancing information:

```
Switch# show etherchannel load-balance
Source XOR Destination mac address
Switch#
```

The following example shows how to display a summary of information for a specific group:

```
Switch# show etherchannel 1 brief
Group state = L3
Ports: 2 Maxports = 8
port-channels: 1 Max port-channels = 1
Switch#
```

The following example shows how to display detailed information for a specific group:

```
Switch# show etherchannel 1 detail
Group state = L3
Ports: 2 Maxports = 8
Port-channels: 1 Max Port-channels = 1
                Ports in the group:
                -----
Port: Fa5/4
-----

Port state      = EC-Enbld Down Not-in-Bndl Usr-Config
Channel group = 1          Mode = Desirable      Gcchange = 0
Port-channel   = null      GC   = 0x00000000      Psudo-agport = Po1
Port indx      = 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.
Timers: H - Hello timer is running.        Q - Quit timer is running.
        S - Switching timer is running.    I - Interface timer is running.

Local information:

Port      Flags State  Timers  Hello  Partner  PAgP    Learning  Group
Fa5/4    d    U1/S1    1s     0      0        128     Any       0

Age of the port in the current state: 02h:33m:14s
Port: Fa5/5
-----

Port state      = EC-Enbld Down Not-in-Bndl Usr-Config
Channel group = 1          Mode = Desirable      Gcchange = 0
Port-channel   = null      GC   = 0x00000000      Psudo-agport = Po1
Port indx      = 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.
Timers: H - Hello timer is running.        Q - Quit timer is running.
        S - Switching timer is running.    I - Interface timer is running.

Local information:

Port      Flags State  Timers  Hello  Partner  PAgP    Learning  Group
Fa5/5    d    U1/S1    1s     0      0        128     Any       0
```



```

Age of the port in the current state: 02h:33m:17s
Port-channels in the group:
-----

Port-channel: Po1
-----
Age of the Port-channel = 02h:33m:52s
Logical slot/port = 10/1          Number of ports in agport = 0
GC = 0x00000000          HotStandBy port = null
Passive port list = Fa5/4 Fa5/5
Port state = Port-channel L3-Ag Ag-Not-Inuse

Ports in the Port-channel:

Index  Load  Port
-----
Switch#

```

The following example shows how to display a one-line summary per channel group:

```

Switch# show etherchannel summary
Flags: D - down          P - bundled in port-channel
       I - stand-alone  s - suspended
       H - Hot-standby (LACP only)
       R - Layer3       S - Layer2
       U - in use       f - failed to allocate aggregator

       M - not in use, minimum links not met
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port

Number of channel-groups in use: 2
Number of aggregators:          2

```

```

Group  Port-channel  Protocol  Ports
-----+-----+-----+-----
1      Po1(SD)         LACP      Gi1/23(H) Gi1/24(H)
Switch#

```

The following example shows how to display EtherChannel port information for all ports and all groups:

```

Switch# show etherchannel port
Channel-group listing:
-----

Group: 1
-----

Ports in the group:
-----

Port: Fa5/4
-----
Port state = EC-Enbld Down Not-in-Bndl Usr-Config
Channel group = 1          Mode = Desirable      Gcchange = 0
Port-channel = null       GC = 0x00000000      Psudo-agport = Po1
Port indx = 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.
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

```

show etherchannel

```

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: 02h:40m:35s
Port: Fa5/5
-----

Port state      = EC-Enbld Down Not-in-Bndl Usr-Config
Channel group = 1           Mode = Desirable   Gchange = 0
Port-channel   = null      GC   = 0x00000000   Pseudo-agport = Po1
Port indx      = 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.
Timers: H - Hello timer is running.         Q - Quit timer is running.
      S - Switching timer is running.       I - Interface timer is running.

<...output truncated...>

```

Switch#

The following example shows how to display the protocol enabled:

```

Switch# show etherchannel protocol
          Channel-group listing:
          -----

Group: 12
-----
Protocol: PAgP

Group: 24
-----
Protocol: - (Mode ON)
Switch#

```

Related Commands

Command	Description
channel-group	Assigns and configures an EtherChannel interface to an EtherChannel group.
interface port-channel	Accesses or creates a port-channel interface.

show fabric domain

To display your fabric domain configuration, use the **show fabric domain** command.

show fabric domain

Command Default Default domain and default context.

Command Modes Privileged EXEC

Command History	Release	Modification
	3.9.01E	This command was introduced on the Catalyst 4500-E series switch using a Supervisor Engines 8-E and 8L-E.

Usage Guidelines Use the command to display a summary of the fabric domain.

Examples This is sample output for the show fabric domain command, for an edge device.

```
device#show fabric domain
Fabric Domain : "default"
Role : Edge
Control-Plane Service: Disabled
Number of "Control-Plane" node(s): 2
IP Address          Auth-key
-----
192.168.1.4         example-key1
192.168.1.5         example-key2

Number of "Border" node(s): 1
IP Address
-----
192.168.1.6

Number of context(s): 2
Codes: * - Not Configured

Name                ID      Host-pools
-----
default             0      *
example-context     10     1
```

show fabric context

To display your fabric domain configuration, use the **show fabric domain** command.

show fabric context [default | name]

Syntax Description	default	The default context
	name	Specifies a context in the fabric domain

Command Default Default context

Command Modes Privileged EXEC

Command History	Release	Modification
	3.9.01E	This command was introduced on the Catalyst 4500-E series switch using a Supervisor Engines 8-E and 8L-E.

Usage Guidelines Use the command to display a summary of the context configuration in your fabric domain.

Examples This is sample output for the **show fabric context** command:

```
device#show fabric context
Fabric-domain: default
Number of context(s): 2
  Name                ID          Host-pools
  -----
default              0          *
example-context      10         1

* - Not Configured
```

show fabric host-pool

To display your fabric domain configuration, use the **show fabric domain** command.

show fabric host-pool *name*

Syntax Description	<i>name</i>	The name of the host-pool
Command Default	None	
Command Modes	Privileged EXEC	
Command History	Release	Modification
	3.9.01E	This command was introduced on the Catalyst 4500-E series switch using a Supervisor Engines 8-E and 8L-E.

Usage Guidelines Use the command to display a summary of the specified host-pool configuration.

Examples This is sample output for the **show fabric host-pool** command:

```
device# show fabric host-pool
Fabric Domain : "default"
context: default
  Number of host-pools : 0
  name                 vlan   prefix                gateway              use-dhcp
  -----
context: example-context
  Number of host-pools : 1
  name                 vlan   prefix                gateway              use-dhcp
  -----
VOICE_DOMAIN          10    192.168.1.0/24        192.168.1.254        209.65.201.6
```

show flowcontrol

To display the per-interface status 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.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.1(8a)EW	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 Table 2-27 describes the fields in the **show flowcontrol** command output.

Table 2-27 show flowcontrol Command Output

Field	Description
Port	Module and port number.
Send-Flowcontrol-Admin	Flow-control administration. Possible settings: on indicates the local port sends flow control to the far end; off indicates the local port does not send flow control to the far end; desired indicates the local end sends flow control to the far end if the far end supports it.
Send-Flowcontrol-Oper	Flow-control operation. Possible setting: 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 setting: 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

The following 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
-----
Tel1/1    off    off         on      off         0        0
Tel1/2    off    off         on      off         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
Gi3/1     off    off         desired off        0        0
Gi3/2     off    off         desired off        0        0
Gi3/3     off    off         desired off        0        0
Gi3/4     off    off         desired off        0        0
Gi3/5     off    off         desired off        0        0
Gi3/6     off    off         desired off        0        0
Switch#
```

The following 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#
```

The following example shows how to display the flow control status on Gigabit Ethernet interface 3/4:

```
Switch# show flowcontrol interface gigabitethernet3/4
Port      Send FlowControl  Receive FlowControl  RxPause  TxPause
         admin   oper         admin   oper
-----
Gi3/4     off    off         on      on         0        0
Switch#
```

The following 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
-----
Tel1/1    off    off         on      off         0        0
Switch#
```

Related Commands

Command	Description
channel-group	Configures a Gigabit Ethernet interface to send or receive pause frames.
show interfaces status	Displays the interface status or a list of interfaces in error-disabled state.

show hw-module port-group

To display how the X2 holes on a module are grouped, use the **show hw-module port-group** command.

show hw-module module *number* port-group

Syntax Description	module	Specifies a line module.
	<i>number</i>	Specifies a slot or module number.
	port-group	Specifies a port-group on a switch.

Command Default X2 mode.

Command Modes Global configuration mode

Command History	Release	Modification
	12.2(40)SG	Support for WS-X4606-10GE-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, 10-Gigabit ports are named TenGigabit and 1-Gigabit ports are named Gigabit. Starting with Cisco IOS Release 12.2(40)SG, to avoid having ports named TenGigabit1/1 and Gigabit1/1, the 10-Gigabit and 1-Gigabit port numbers are independent. The WS-X4606-10GE-E module with six X2 ports are named TenGigabit<slot-num>/<1-6>, and the SFP ports are named Gigabit<slot-num>/<7-18>.

On Supervisor Engine 6-E, Supervisor Engine 6L-E, Catalyst 4900M, Catalyst 4948E, and Catalyst 4948E-F, the ports are connected to the switching engine through a stub ASIC. This stub ASIC imposes some limitations on the ports: Gigabit and 10-Gigabit ports cannot be mixed on a single stub ASIC; they must either be all 10-Gigabit (X2), or all Gigabit (TwinGig converter and SFP). The faceplates of X2 modules show this stub-port grouping, either with an actual physical grouping, or a box drawn around a grouping.

Examples The following example shows to determine how the X2 holes on a module are grouped on a WS-X4606-10GE-E:

```
Switch# show hw-module module 1 port-group
Module  Port-group  Active      Inactive
-----
1       1              Tel1/1-3   Gi1/7-12
1       2              Tel1/4-6   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 system max-port-num-mode

To display the current mode in which a system is running as well as a message informing you that linecards beyond the 5th slot are unsupported, use the **show hw-module system max-port-num-mode** command.

show hw-module system max-port-num-mode

Command Default none

Command Modes Privileged EXEC mode

Command History	Release	Modification
	Release IOS XE 3.5.0E and IOS 15.2(1)E	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines The CLI shall be visible only on a 10-slot chassis or if 10-slot chassis is present in VSS.

Examples The following example shows the output of the **show hw-module system max-port-num-mode** command on the standalone switch:

```
Switch# show hw-module system max-port-num-mode
Active max-port-num-mode configuration is 2
In this mode, Line cards inserted in last 3 slots (8,9 and 10) will not be active
```

The following example shows the output of the **show hw-module system max-port-num-mode** command in switch virtual mode:

```
Switch1# show hw-module system max-port-num-mode
Executing the command on VSS member switch role = VSS Active, id = 1
Active max-port-num-mode configuration is 1 (Default)
Executing the command on VSS member switch role = VSS Standby, id = 2
Active max-port-num-mode configuration is 2
In this mode, Line cards inserted in last 3 slots (8,9 and 10) will not be active
```

show hw-module uplink

To display the current uplink mode, use the **show hw-module uplink** command.

show hw-module uplink

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.

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

The following example shows the output displaying the current (active) uplinks:

```
Switch# show hw-module uplink
Active uplink configuration is TenGigabitEthernet
```

The following 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)
A 'redundancy reload shelf' or power-cycle of chassis is required to
apply the new configuration
```

The following 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 W-C4510R 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 [mod] | interface int_name | supervisor | power-supply
  number | fan-tray }
```

Syntax Description

all	Displays information for all IDPROMs.
chassis	Displays information for the chassis IDPROMs.
module	Displays information for the module IDPROMs.
<i>mod</i>	(Optional) Specifies the module name.
interface <i>int_name</i>	Displays information for the GBIC or SFP IDPROMs.
supervisor	Displays information for the supervisor engine IDPROMs.
power-supply <i>number</i>	Displays information for the power supply IDPROMs.
fan-tray	Displays information for the fan tray IDPROMs.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.1(8a)EW	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 interface keyword was added.
12.2(18)EW	Enhanced the show idprom interface output to include the hexadecimal display of the GBIC/SFP SEEPROM 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 lines for Calibration type and Rx (receive) power measurement may not be displayed for all GBICs.

Examples

The following example shows how to display IDPROM information for module 4:

```
Switch# show idprom module 4
Module 4 Idprom:
Common Block Signature = 0xABAB
Common Block Version = 1
Common Block Length = 144
Common Block Checksum = 4199
Idprom Size = 256
Block Count = 2
FRU Major Type = 0x4201
FRU Minor Type = 303
OEM String = Cisco Systems, Inc.
Product Number = WS-X4306
Serial Number = 00000135
Part Number = <tb>
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
Linecard Block Signature = 0x4201
Linecard Block Version = 1
Linecard Block Length = 24
Linecard Block Checksum = 658
Feature Bits = 0x0000000000000000
Card Feature Index = 50
MAC Base = 0010.7bab.9830
MAC Count = 6
Switch#
```

The following example shows how to display IDPROM information for the GBICs on the Gigabit Ethernet interface 1/2:

```
Switch# show idprom interface gigabitethernet1/2
GBIC Serial EEPROM Contents:
Common Block:
Identifier           = GBIC [0x1]
Extended Id         = Not specified/compliant with defined MOD_DEF [0x0]
Connector           = SC connector [0x1]
Transceiver
Speed               = Not available [0x0]
Media               = Not available [0x0]
Technology          = Not available [0x0]
Link Length         = Not available [0x0]
GE Comp Codes       = Not available [0x0]
SONET Comp Codes    = Not available [0x0]
Encoding            = 8B10B [0x1]
BR, Nominal         = 1300000000 MHz
Length(9u) in km    = GBIC does not support single mode fibre, or the length
                    must be determined from the transceiver technology.
Length(9u)          = > 25.4 km
Length(50u)         = GBIC does not support 50 micron multi-mode fibre, or the
                    length must be determined from the transceiver technology.
Length(62.5u)       = GBIC does not support 62.5 micron multi-mode fibre, or
                    the length must be determined from transceiver technology.
Length(Copper)      = GBIC does not support copper cables, or the length must
                    be determined from the transceiver technology.
Vendor name         = CISCO-FINISAR
Vendor OUI          = 36965
Vendor Part No.     = FTR-0119-CSC
Vendor Part Rev.    = B
Wavelength          = Not available
```

```

CC_BASE                = 0x1A

Extended ID Fields
Options                = Loss of Signal implemented TX_FAULT signal implemented TX_DISABLE is
implemented and disables the serial output [0x1A]
BR, max               = Unspecified
BR, min               = Unspecified
Vendor Serial No.    = K1273DH
Date code            = 030409
Diag monitoring      = Implemented
Calibration type     = Internal
Rx pwr measurement  = Optical Modulation Amplitude (OMA)
Address change       = Required
CC_EXT               = 0xB2

Vendor Specific ID Fields:
20944D30 29 00 02 80 22 33 38 3D C7 67 83 E8 DF 65 6A AF )..."38=Gg^Ch_ej/
20944D40 1A 80 ED 00 00 00 00 00 00 00 00 00 38 23 3C 1B .....8#<.

                SEEPROM contents (hex) size 128:
0x0000 01 00 01 00 00 00 00 00 00 00 01 0D 00 00 FF .....
0x0010 00 00 00 00 43 49 53 43 4F 2D 46 49 4E 49 53 41 ...CISCO-FINISA
0x0020 52 20 20 20 00 00 90 65 46 54 52 2D 30 31 31 39 R ..^PeFTR-0119
0x0030 2D 43 53 43 20 20 20 20 42 20 20 00 00 00 1A -CSC B ....
0x0040 00 1A 00 00 4B 31 32 37 33 44 48 20 20 20 20 20 ...K1273DH
0x0050 20 20 20 20 30 33 30 34 30 39 20 20 64 00 00 B2 030409 d..2
0x0060 29 00 02 80 22 33 38 3D C7 67 83 E8 DF 65 6A AF )..^@"38=Gg^C._ej.
0x0070 1A 80 ED 00 00 00 00 00 00 00 00 00 38 23 3C 1B .^@m.....8#<.

Switch#

```

The following example shows how to display IDPROM information for the 10-Gigabit Ethernet interface 1/1:

```

Switch# show idprom interface tengigabitethernet1/1
X2 Serial EEPROM Contents:
Non-Volatile Register (NVR) Fields
X2 MSA Version supported           :0xA
NVR Size in bytes                 :0x100
Number of bytes used              :0xD0
Basic Field Address               :0xB
Customer Field Address            :0x77
Vendor Field Address              :0xA7
Extended Vendor Field Address     :0x100
Reserved                          :0x0
Transceiver type                  :0x2 =X2
Optical connector type            :0x1 =SC
Bit encoding                      :0x1 =NRZ
Normal BitRate in multiple of 1M b/s :0x2848
Protocol Type                     :0x1 =10GgE

Standards Compliance Codes :
10GbE Code Byte 0                :0x2 =10GBASE-LR
10GbE Code Byte 1                :0x0
SONET/SDH Code Byte 0            :0x0
SONET/SDH Code Byte 1            :0x0
SONET/SDH Code Byte 2            :0x0
SONET/SDH Code Byte 3            :0x0
10GFC Code Byte 0                :0x0
10GFC Code Byte 1                :0x0
10GFC Code Byte 2                :0x0
10GFC Code Byte 3                :0x0
Transmission range in 10m       :0x3E8
Fibre Type :

```

```

Fibre Type Byte 0          :0x40 =NDSF only
Fibre Type Byte 1          :0x0 =Unspecified

Centre Optical Wavelength in 0.01nm steps - Channel 0 :0x1 0xFF 0xB8
Centre Optical Wavelength in 0.01nm steps - Channel 1 :0x0 0x0 0x0
Centre Optical Wavelength in 0.01nm steps - Channel 2 :0x0 0x0 0x0
Centre Optical Wavelength in 0.01nm steps - Channel 3 :0x0 0x0 0x0
Package Identifier OUI     :0xC09820
Transceiver Vendor OUI     :0x3400800
Transceiver vendor name    :CISCO-OPNEXT,INC
Part number provided by transceiver vendor              :TRT5021EN-SMC-W
Revision level of part number provided by vendor       :00
Vendor serial number      :ONJ08290041
Vendor manufacturing date code :2004072000

Reserved1 : 00 02 02 20 D1 00 00
Basic Field Checksum :0x10

Customer Writable Area :
0x00: 58 32 2D 31 30 47 42 2D 4C 52 20 20 20 20 20 20
0x10: 20 20 20 20 20 4F 4E 4A 30 38 32 39 30 30 34 31
0x20: 31 30 2D 32 30 33 36 2D 30 31 20 20 41 30 31 20

Vendor Specific :
0x00: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x10: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x30: 00 00 00 00 11 E2 69 A9 2F 95 C6 EE D2 DA B3 FD
0x40: 9A 34 4A 24 CB 00 00 00 00 00 00 00 00 00 EF FC
0x50: F4 AC 1A D7 11 08 01 36 00
Switch#

```

The following example shows how to display IDPROM information for the supervisor engine:

```

Switch# show idprom supervisor
Supervisor Idprom:
Common Block Signature = 0xABAB
Common Block Version = 1
Common Block Length = 144
Common Block Checksum = 4153
Idprom Size = 256
Block Count = 2
FRU Major Type = 0x4101
FRU Minor Type = 333
OEM String = Cisco Systems, Inc.
Product Number = WS-X4014
Serial Number = JAB05320CCE
Part Number = 73-6854-04
Part Revision = 05
Manufacturing Deviation String = 0
Hardware Revision = 0.4
Manufacturing Bits = 0x0000
Engineering Bits = 0x0000
Snmp OID = 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 = 24
Supervisor Block Checksum = 548
Feature Bits = 0x0000000000000000
Card Feature Index = 95
MAC Base = 0007.0ee5.2a44
MAC Count = 2

```

Switch#

The following example shows how to display IDPROM information for the chassis:

```
Switch# show idprom chassis
Chassis Idprom:
  Common Block Signature = 0xABAB
  Common Block Version = 1
  Common Block Length = 144
  Common Block Checksum = 4285
  Idprom Size = 256
  Block Count = 2
  FRU Major Type = 0x4001
  FRU Minor Type = 24
  OEM String = Cisco Systems, Inc.
  Product Number = WS-C4507R
  Serial Number = FOX04473737
  Part Number = 73-4289-02
  Part Revision = 02
  Manufacturing Deviation String = 0x00
  Hardware Revision = 0.2
  Manufacturing Bits = 0x0000
  Engineering Bits = 0x0000
  Snmp OID = 0.0.0.0.0.0.0
  Chassis Block Signature = 0x4001
  Chassis Block Version = 1
  Chassis Block Length = 22
  Chassis Block Checksum = 421
  Feature Bits = 0x0000000000000000
  MAC Base = 0004.dd42.2600
  MAC Count = 1024
Switch#
```

The following example shows how to display IDPROM information for power supply 1:

```
Switch# show idprom power-supply 1
Power Supply 0 Idprom:
  Common Block Signature = 0xABAB
  Common Block Version = 1
  Common Block Length = 144
  Common Block Checksum = 10207
  Idprom Size = 256
  Block Count = 1
  FRU Major Type = 0xAB01
  FRU Minor Type = 8224
  OEM String = Cisco Systems, Inc.
  Product Number = WS-CAC-1440W
  Serial Number = ACP05180002
  Part Number = 34-XXXX-01
  Part Revision = A0
  Manufacturing Deviation String =
  Hardware Revision = 1.1
  Manufacturing Bits = 0x0000
  Engineering Bits = 0x3031
  Snmp OID = 9.12.3.65535.65535.65535.65535.65535
  Power Consumption = -1
  RMA Failure Code = 255 255 255 255
  Power Supply Block Signature = 0xFFFF
  PowerSupply Block Version = 255
  PowerSupply Block Length = 255
  PowerSupply Block Checksum = 65535
  Feature Bits = 0x00000000FFFFFFF
  Current @ 110V = -1
  Current @ 220V = -1
```



```
StackMIB OID = 65535  
Switch#
```

The following 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 = 19781  
Idprom Size = 256  
Block Count = 1  
FRU Major Type = 0x4002  
FRU Minor Type = 0  
OEM String = "Cisco Systems"  
Product Number = WS-X4502-fan  
Serial Number =  
Part Number =  
Part Revision =  
Manufacturing Deviation String =  
Hardware Revision = 0.1  
Manufacturing Bits = 0xFFFF  
Engineering Bits = 0xFFFF  
Snmp OID = 65535.65535.65535.65535.65535.65535.65535.65535  
Power Consumption = -1  
RMA Failure Code = 255 255 255 255  
Switch#
```

show interfaces

To display traffic on a specific interface, use the **show interfaces** command.

```
show interfaces [{fastethernet mod/interface-number} | {gigabitethernet
  mod/interface-number} | {tengigabitethernet mod/interface-number} | {null
  interface-number} | vlan vlan_id] | status}]
```

Syntax Description		
fastethernet <i>mod/interface-number</i>	(Optional)	Specifies the Fast Ethernet module and interface.
gigabitethernet <i>mod/interface-number</i>	(Optional)	Specifies the Gigabit Ethernet module and interface.
tengigabitethernet <i>mod/interface-number</i>	(Optional)	Specifies the 10-Gigabit Ethernet module and interface.
null <i>interface-number</i>	(Optional)	Specifies the null interface; the valid value is 0.
vlan <i>vlan_id</i>	(Optional)	Specifies the VLAN; valid values are from 1 to 4094.
status	(Optional)	Displays status information.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.1(8a)EW	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 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.
	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 switched 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 auto-MDIX configuration on their copper media ports include: WS-X4124-RJ45, WS-X4148-RJ with hardware revision 3.0 or later, and WS-X4232-GB-RJ with hardware revision 3.0 or later.

Examples

The following example shows how to display traffic for Gigabit Ethernet interface 2/5:

```
Switch# show interfaces gigabitethernet2/5
GigabitEthernet9/5 is up, line protocol is up (connected) (vlan-err-dis)
Hardware is C4k 1000Mb 802.3, address is 0001.64f8.3fa5 (bia 0001.64f8.3fa5)
Internet address is 172.20.20.20/24
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 1000Mb/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
L2 Switched: ucast: 8199 pkt, 1362060 bytes - mcast: 6980 pkt, 371952 bytes
L3 in Switched: ucast: 0 pkt, 0 bytes - mcast: 0 pkt, 0 bytes mcast
L3 out Switched: ucast: 0 pkt, 0 bytes - mcast: 0 pkt, 0 bytes
300114 packets input, 27301436 bytes, 0 no buffer
Received 43458 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 input packets with dribble condition detected
15181 packets output, 1955836 bytes, 0 underruns
0 output errors, 0 collisions, 3 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
Switch#
```

The following example shows how to display traffic for 10-Gigabit Ethernet interface 1/1:

```
Switch# show interfaces tengigabitethernet1/1
Name: Tengigabitethernet1/1
Switchport: Enabled
Administrative Mode: private-vlan promiscuous trunk
Operational Mode: private-vlan promiscuous (suspended member of bundle Po1)
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: none
Trunking Native Mode VLAN: none
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: 202 (VLAN0202) 303 (VLAN0303) 304 (VLAN0304)
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk
Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: 802.1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Administrative private-vlan mapping trunk: New 202 (VLAN0202) 303 (VLAN0303) 304
(VLAN0304) 204 (VLAN0204) 305 (VLAN0305) 306 (VLAN0306)
```

```
Operational private-vlan: 202 (VLAN0202) 303 (VLAN0303) 304 (VLAN0304)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Switch#
```

The following 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 EXEC** command. This field is applicable and appears only on the **show interfaces** command output for 10/100/1000BaseT RJ-45 copper ports on supported linecards including WS-X4124-RJ45, WS-X4148-RJ with hardware revision 3.0 or later, and WS-X4232-GB-RJ with hardware revision 3.0 or later.

```
FastEthernet6/3 is up, line protocol is up (connected)
  Hardware is Fast Ethernet Port, address is 0003.6ba8.ee68 (bia 0003.6ba8.ee68)
  MTU 1500 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, 100Mb/s, link type is auto, media type is 10/100BaseTX
  input flow-control is unsupported output flow-control is unsupported
Auto-MDIX on (operational: on)
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 multicasts)
    0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 input packets with dribble condition detected
  157082 packets output, 13418032 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 babbles, 0 late collision, 0 deferred
    1 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
Switch#
```

The following 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                    notconnect  1          auto     1000 1000-XWDM-RXONLY
Switch#
```

The following 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
Te1/1                    connected  1          full     10G 10GBase-LR
Te1/2                    connected  1          full     10G 10GBase-LR
Switch#
```

show interfaces (virtual switch)

To display traffic that is seen by a specific interface, use the **show interfaces** command in EXEC mode.

```
show interfaces [interface iswitch-num/mod/port]
```

Syntax Description	
<i>interface</i>	(Optional) Specifies interface type
<i>switch-num</i>	Specifies port number.
<i>/mod</i>	Specifies module number
<i>/port</i>	Specifies port number

Command Default This command has no defaults settings.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	Cisco IOS XE 3.4.0SG and 15.1(2)SG	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines Statistics are collected on a per-VLAN basis for Layer 2-switched packets and Layer 3-switched packets. Statistics are available for both unicast and multicast traffic. The Layer 3-switched packet counts are available for both ingress and egress directions. The per-VLAN statistics are updated every 5 seconds.

In some cases, you might see a difference in the duplex mode that is displayed between the **show interfaces (virtual switch)** command and the **show running-config switch (virtual switch)** command. In this case, the duplex mode that is displayed in the **show interfaces (virtual switch)** command is the actual duplex mode that the interface is running. The **show interfaces (virtual switch)** command shows the operating mode for an interface, while the **show running-config switch (virtual switch)** command shows the configured mode for an interface.

If you do not specify an interface, the information for all interfaces is displayed.

The output of the **show interfaces GigabitEthernet** command displays an extra 4 bytes for every packet that is sent or received. The extra 4 bytes are the Ethernet frame CRC in the input and output byte statistics.

Examples

The following example shows how to display traffic for a specific interface:

```
Router# show interfaces GigabitEthernet switch 1/3/3
GigabitEthernet1/3/3 is up, line protocol is up (connected)
  Hardware is C6k 1000Mb 802.3, address is 000f.2305.49c0 (bia 000f.2305.49c0)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation 802.1Q Virtual LAN, Vlan ID 1., loopback not set
  Keepalive set (10 sec)
  Full-duplex, 1000Mb/s, media type is LH
  input flow-control is off, output flow-control is on
  Clock mode is auto
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:19, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  L2 Switched: ucast: 360 pkt, 23040 bytes - mcast: 0 pkt, 0 bytes
  L3 in Switched: ucast: 0 pkt, 0 bytes - mcast: 0 pkt, 0 bytes mcast
  L3 out Switched: ucast: 0 pkt, 0 bytes mcast: 0 pkt, 0 bytes
    437 packets input, 48503 bytes, 0 no buffer
    Received 76 broadcasts (0 IP multicast)
    0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 0 multicast, 0 pause input
    0 input packets with dribble condition detected
    86 packets output, 25910 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 PAUSE output
    0 output buffer failures, 0 output buffers swapped out
Router#
```

Related Commands

Command	Description
interface (virtual switch)	Selects an interface to configure and enters the interface configuration mode.

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 <i>mod</i>	(Optional) Limits the display to interfaces on a specific module.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch.
	12.1(19)EW	Support for storm control.
	12.2(18)EW	Support for the display of total suppression 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 The following 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#
```

The following 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#
```

The following example shows how to display the trunk counters for a specific module:

```
Switch# show interfaces counters trunk module 1

Port          TrunkFramesTx  TrunkFramesRx  WrongEncap
Gi1/1         0              0              0
Gi1/2         0              0              0
Switch#
```

The following 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          BcastSuppLevel  TotalSuppressionDiscards
Fa5/35        10.00%          6278550
Switch#
```

Related Commands

Command	Description
show interfaces (virtual switch)	Displays the interface capabilities for an interface or for all the interfaces on a switch.

show interfaces counters (virtual switch)

To display the traffic that the physical interface sees, use the **show interfaces counters** command in EXEC mode.

```
show interfaces [interface switch-num/mod/port] counters [errors | etherchannel | protocol status | storm-control]
```

Syntax Description	
<i>interface</i>	(Optional) Specifies the interface type.
<i>switch-num</i>	Specifies the switch number; valid values are 1 and 2.
<i>/mod</i>	Specifies the module number.
<i>/port</i>	Specifies the port number.
errors	(Optional) Displays the interface error counters.
etherchannel	(Optional) Displays information about the EtherChannel interface.
protocol status	(Optional) Displays information about the current status of the enabled protocols.
storm-control	(Optional) Displays the discard count and the level settings for each mode.

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.

Usage Guidelines The **show interfaces counters** command displays the number of all of the packets arriving and includes the number of packets that may be dropped by the interface due to the storm-control settings. To display the total number of dropped packets, you can enter the **show interfaces counters storm-control** command.

The **show interfaces counters storm-control** command displays the discard count and the level settings for each mode. The discard count is a total of all three modes.

If you do not enter any keywords, all counters for all modules are displayed.

If you do not specify an interface, the information for all interfaces is displayed.

When you enter the **show interfaces interface counters etherchannel** command, follow these guidelines:

- If interface specifies a physical port, the command displays the message "Etherchannel not enabled on this interface."
- If interface is omitted, the command displays the counters for all port channels (in the system) and for their associated physical ports.

- If interface specifies a port channel, the command displays the counters for the port channel and all of the physical ports that are associated with it. In addition, when you enter the command specifying the primary aggregator in a Link Aggregation Control Protocol (LACP) port channel with multiple aggregators, the output includes the statistics for all of the aggregators in the port channels and for the ports that are associated with them.

Examples

The following example shows how to display the error counters for a specific:

```
Router# show interfaces gigabitethernet 2/4/47 counters errors
Port          Align-Err  FCS-Err   Xmit-Err   Rcv-Err  UnderSize  OutDiscards
Gi2/4/47      0          0         0          0        0          0
Port          Single-Col Multi-Col  Late-Col   Excess-Col Carri-Sen   Runts   s
Gi2/4/47      0          0         0          0        0          0    0
Port          SQETest-Err Deferred-Tx IntMacTx-Err IntMacRx-Err Symbol-Err
Gi2/4/47      0          0         0          0        0          0
Router#
```

The following example shows how to display traffic that is seen by a specific interface:

```
Router# show interfaces gigabitethernet 1/2/5 counters
Port          InOctets   InUcastPkts  InMcastPkts  InBcastPkts
Gi1/2/5       0          0            0            0
Port          OutOctets  OutUcastPkts  OutMcastPkts  OutBcastPkts
Gi1/2/5       0          0            0            0
Router#
```

The following example shows how to display the counters for all port channels (in the system) and their associated physical ports:

```
Router# show interfaces counters etherchannel
Port          InOctets   InUcastPkts  InMcastPkts  InBcastPkts
Po1           0          0            0            0
Po3           0          0            0            0
Po10          16341138343  77612803    12212915    14110863
Gi1/4/1       15628478622  77612818    7525970     14110865
Gi1/4/2       712662881   0            4686951     5
Po20          33887345029  88483183    11506653    14101212
Gi2/4/1       33326378013  88491521    7177393     14101663
Gi2/4/2       562904837   0            4330030     6
Port          OutOctets  OutUcastPkts  OutMcastPkts  OutBcastPkts
Po1           0          0            0            0
Po3           0          0            0            0
Po10          33889238079  14101204    99999327    0
Gi1/4/1       33326354634  14101205    95669326    0
Gi1/4/2       562904707   7            4330029     0
Po20          16338422056  14353951    89573339    0
Gi2/4/1       15628501864  14232410    85017290    0
Gi2/4/2       712663011   121541      4565416     0
Router#
```

The following example shows how to display the counters for all port channels (in the system) and their associated physical ports in Cisco IOS Release 12.2(50)SY and later releases:

```
Router# show interfaces counters etherchannel
Port          InOctets   InUcastPkts  InMcastPkts  InBcastPkts
Po1           0          0            0            0
Po3           0          0            0            0
Po10          16341138343  77612803    12212915    14110863
Gi1/4/1       15628478622  77612818    7525970     14110865
Gi1/4/2       712662881   0            4686951     5
Po20          33887345029  88483183    11506653    14101212
Gi2/4/1       33326378013  88491521    7177393     14101663
```

```

Gi2/4/2          562904837          0          4330030          6
Router#

```

The following example shows how to display the protocols enabled for a specific interface:

```

Router# show interfaces gigabitethernet 1/2/5 counters protocol status
Protocols allocated:
  GigabitEthernet1/2/5: Other, IP
Router#

```

The following example shows how to display the discard count and the level settings for each mode for a specific interface:

```

Router# show interfaces gigabitethernet 1/2/5 counters storm-control
Port          UcastSupp %      McastSupp %      BcastSupp %      TotalSuppDiscards
Gi1/2/5          100.0            100.0            100.0            0
Router#

```

Related Commands

Command	Description
clear counters	Clears the interface counters.

show interfaces description

To display a description and status of an interface, use the **show interfaces description** command.

show interfaces [*interface*] **description**

Syntax Description	<i>interface</i> (Optional) Type of interface.
---------------------------	--

Command Default	This command has no default settings.
------------------------	---------------------------------------

Command Modes	Privileged EXEC mode
----------------------	----------------------

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

Examples The following example shows how to display information for all interfaces:

```
Switch# show interfaces description
Interface Status      Protocol Description
PO0/0      admin down         down    First interface
PO0/1      admin down         down
Gi1/1      up                 up      GigE 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 <i>mod_num</i> (Optional) Limits the display to interfaces on a module.				
Command Default	This command has no default settings.				
Command Modes	Privileged EXEC mode				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.2(18)EW</td> <td>This command was introduced on the Catalyst 4500 series switch.</td> </tr> </tbody> </table>	Release	Modification	12.2(18)EW	This command was introduced on the Catalyst 4500 series switch.
Release	Modification				
12.2(18)EW	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 The following example shows how to display active link-level information:

```
Switch# show interfaces link

Port      Name                Down Time
Gi1/1     Gi1/1                00:00:00
Gi1/2     Gi1/2                00:00:00
Gi3/1     Gi3/1                00:00:00
Gi3/2     Gi3/2                00:00:00
Fa4/1     Fa4/1                00:00:00
Fa4/2     Fa4/2                00:00:00
Fa4/3     Fa4/3                00:00:00
Fa4/4     Fa4/4                00:00:00
```

The following example shows how to display inactive link-level information:

```
Switch# show interfaces link

Port      Name                Down Time
Gi3/4     Gi3/4                1 minute 28 secs
Gi3/5     Gi3/5                1 minute 28 secs
Gi3/6     Gi3/6                1 minute 28 secs
Gi4/1     Gi4/1                1 minute 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 <i>mod</i> (Optional) Limits the display to interfaces on a specific module.
---------------------------	--

Command Default	This command has no default settings.
------------------------	---------------------------------------

Command Modes	EXEC
----------------------	------

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

Examples The following 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     Gi1/1          1500
Gi1/2     Gi1/2          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.
---------------------------	---

Command Default	This command has no default settings.
------------------------	---------------------------------------

Command Modes	Privileged EXEC mode
----------------------	----------------------

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

Usage Guidelines	This command displays SVI information only.
-------------------------	---

Examples	<p>The following example shows how to display PVLAN mapping information:</p> <pre>Switch# show interfaces private-vlan mapping Interface Secondary VLAN Type ----- vlan2 301 isolated vlan2 302 isolated Switch#</pre>
-----------------	--

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 <i>module</i>	(Optional) Displays interfaces on a specific module.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch.
	12.2(40)SG	Support for WS-X4606-10GE-E Twin Gigabit converter introduced.
	12.2(52)SG	Support for per-VLAN error-disable was introduced by adding Err-Disabled VLAN 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-dis* in the VLAN column.

Examples The following example shows how to display the status of all interfaces:

```
Switch# show interfaces status
```

```
Port      Name              Status      Vlan      Duplex  Speed  Type
Te1/1    Te1/1             connected   1         full    10G    10GBase-LR
Te1/2    Te1/2             connected   vl-err-dis full    10G    10GBase-LR
Switch#
```

The following 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
----      -
Fa9/4    Fa9/4             notconnect   link-flap
Fa9/5    Fa9/5             err-disabled  psecure_violation  3-5
Fa9/6    Fa9/6             connected   psecure_violation  10,15
Switch#
```


The following example shows how to display the Gigabit Ethernet interfaces on a WS-X4606-10GE-E switch using the TwinGig Converter:

```
Switch# show interfaces status module 1
Port Name Status Vlan Duplex Speed Type
Tel/1 inactive 1 full 10G No X2
Tel/2 inactive 1 full 10G No X2
Tel/3 inactive 1 full 10G No X2
Tel/4 notconnect 1 full 10G No X2
Tel/5 notconnect 1 full 10G No X2
Tel/6 notconnect 1 full 10G No X2
Gi1/7 notconnect 1 full 1000 No Gbic
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
Switch#
```

Related Commands

Command	Description
errdisable detect cause	Enables error-disable detection.
hw-module port-group	Selects either Gigabit Ethernet or Ten Gigabit Ethernet interfaces on your 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	
<i>interface-id</i>	(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.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch.
	12.1(19)EW	Support for per-interface display.
	12.2(18)EW	Support for displaying the status of native VLAN tagging in the command output.
	15.1.0 SG	Support for PVLAN modes over EtherChannel. Modes include: private-vlan host, private-vlan promiscuous, private-vlan trunk secondary, and private-vlan trunk promiscuous.

Examples The following example shows how to display switch-port information using the **begin** output modifier:

```
Switch# show interfaces switchport | include VLAN
Name: Fa5/6
Access Mode VLAN: 200 (VLAN0200)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: ALL
Switch#
```

The following example shows how to display switch-port information for module 1:

```
Switch# show interfaces switchport module 1
Name:Gi1/1
Switchport:Enabled
Administrative Mode:dynamic auto
Operational Mode:down
Administrative Trunking Encapsulation:negotiate
Negotiation of Trunking:On
Access Mode VLAN:1 (default)
Trunking Native Mode VLAN:1 (default)
Administrative private-vlan host-association:none
Administrative private-vlan mapping:none
Operational private-vlan:none
Trunking VLANs Enabled:ALL
```

```

Pruning VLANs Enabled:2-1001

Name:Gi1/2
Switchport:Enabled
Administrative Mode:dynamic auto
Operational Mode:down
Administrative Trunking Encapsulation:negotiate
Negotiation of Trunking:On
Access Mode VLAN:1 (default)
Trunking Native Mode VLAN:1 (default)
Administrative private-vlan host-association:none
Administrative private-vlan mapping:none
Operational private-vlan:none
Trunking VLANs Enabled:ALL
Pruning VLANs Enabled:2-1001
Switch#

```

The following example shows how to display the status of native VLAN tagging on the port:

```

Switch# show interfaces f3/1 switchport
show interface f3/1 switchport
Name: Fa3/1
Switchport: Enabled
Administrative Mode: private-vlan promiscuous
Operational Mode: private-vlan trunk secondary
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: 1
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: 1
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings:
    10 (VLAN0010) 100 (VLAN0100)
Operational private-vlan:
    10 (VLAN0010) 100 (VLAN0100)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
Switch#

```

Related Commands

Command	Description
show interfaces (virtual switch)	Displays the interface capabilities for an interface or for all the interfaces on a switch.
show interfaces 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

<i>int_name</i>	(Optional) Interface name.
detail	(Optional) Displays the calibrated values and the A2D readouts if the readout 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.

Command Default

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	This command was introduced on the Catalyst 4500 series switch.
12.2(18)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, reenter the command to confirm.

Examples

The following 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 alarm.
NA or N/A: not applicable, Tx: transmit, Rx: receive.
mA: milliamperes, dBm: decibels (milliwatts).

      Temperature  Voltage  Current  Optical  Optical
      (Celsius)   (Volts) (mA)     Tx Power Rx Power
      -----
Gi1/1    48.1      3.30    0.0      8.1 ++   N/A
Gi1/2    33.0      3.30    1.8     -10.0   -36.9
Gi2/1    43.7      5.03    50.6 +   -16.7 --  N/A
Gi2/2    39.2      5.02    25.7     0.8     N/A

Switch#
```



Note The value for the Optical Tx Power (in dBm) equals ten times log (Tx Power in mW). If the Tx Power value is 3 mW, then the Optical Tx Power value equals $10 * \log(3)$, which equals $10 * .477$ or 4.77 dBm. The Optical Rx Power value behaves similarly. If the Tx Power or the Rx Power is zero, then its dBm value is undefined and is shown as N/A (not applicable).

The following example shows how to display detailed diagnostic monitoring data, including calibrated values, alarm and warning thresholds, A2D readouts, and alarm and warning flags. The A2D readouts are reported separately in parentheses only if they differ from the calibrated values:

```
Switch# show interfaces transceiver detail
mA: milliamperes, dBm: decibels (milliwatts), NA or N/A: not applicable.
++ : high alarm, + : high warning, - : low warning, -- : low alarm.
A2D readouts (if they differ), are reported in parentheses.
The threshold values are calibrated.
```

Port	Temperature (Celsius)	High Alarm Threshold (Celsius)	High Warn Threshold (Celsius)	Low Warn Threshold (Celsius)	Low Alarm Threshold (Celsius)
Gi1/1	48.1	100.0	100.0	0.0	0.0
Gi1/2	34.9	100.0	100.0	0.0	0.0
Gi2/1	43.5	70.0	60.0	5.0	0.0
Gi2/2	39.1	70.0	60.0	5.0	0.0

Port	Voltage (Volts)	High Alarm Threshold (Volts)	High Warn Threshold (Volts)	Low Warn Threshold (Volts)	Low Alarm Threshold (Volts)
Gi1/1	3.30	6.50	6.50	N/A	N/A
Gi1/2	3.30	6.50	6.50	N/A	N/A
Gi2/1	5.03	5.50	5.25	4.75	4.50
Gi2/2	5.02	5.50	5.25	4.75	4.50

Port	Current (milliamperes)	High Alarm Threshold (mA)	High Warn Threshold (mA)	Low Warn Threshold (mA)	Low Alarm Threshold (mA)
Gi1/1	0.0	130.0	130.0	N/A	N/A
Gi1/2	1.7	130.0	130.0	N/A	N/A
Gi2/1	50.6 +	60.0	40.0	10.0	5.0
Gi2/2	25.8	60.0	40.0	10.0	5.0

Port	Optical Transmit Power (dBm)		High Alarm Threshold (dBm)	High Warn Threshold (dBm)	Low Warn Threshold (dBm)	Low Alarm Threshold (dBm)
Gi1/1	8.1	++	8.1	8.1	N/A	N/A
Gi1/2	-9.8		8.1	8.1	N/A	N/A
Gi2/1	-16.7 (-13.0)	--	3.4	3.2	-0.3	-0.5
Gi2/2	0.8 (5.1)		3.4	3.2	-0.3	-0.5

Port	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
Gi1/2	-30.9		8.1	8.1	N/A	N/A
Gi2/1	N/A (-28.5)		5.9	-6.7	-28.5	-28.5
Gi2/2	N/A (-19.5)		5.9	-6.7	-28.5	-28.5

Switch#

The following example shows how to display the monitoring data for the interfaces that have transceivers installed on module 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.
 NA or N/A: not applicable, Tx: transmit, Rx: receive.
 mA: milliamperes, dBm: decibels (milliwatts).

Port	Temperature (Celsius)	Voltage (Volts)	Current (mA)	Optical Tx Power (dBm)	Optical Rx Power (dBm)
Gi2/1	43.7	5.03	50.6 +	-16.7 --	N/A
Gi2/2	39.2	5.02	25.7	0.8	N/A

Switch#

The following 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), NA or N/A: not applicable.
 ++ : high alarm, + : high warning, - : low warning, -- : low alarm.
 A2D readouts (if they differ), are reported in parentheses.
 The threshold values are calibrated.

Port	Temperature (Celsius)	High Alarm Threshold (Celsius)	High Warn Threshold (Celsius)	Low Warn Threshold (Celsius)	Low Alarm Threshold (Celsius)
Gi2/1	43.5	70.0	60.0	5.0	0.0
Gi2/2	39.1	70.0	60.0	5.0	0.0

Port	Voltage (Volts)	High Alarm Threshold (Volts)	High Warn Threshold (Volts)	Low Warn Threshold (Volts)	Low Alarm Threshold (Volts)
Gi2/1	5.03	5.50	5.25	4.75	4.50
Gi2/2	5.02	5.50	5.25	4.75	4.50

Port	Current (milliamperes)		High Alarm Threshold (mA)	High Warn Threshold (mA)	Low Warn Threshold (mA)	Low Alarm Threshold (mA)
Gi2/1	50.6	+	60.0	40.0	10.0	5.0
Gi2/2	25.8		60.0	40.0	10.0	5.0

Port	Optical Transmit Power (dBm)		High Alarm Threshold (dBm)	High Warn Threshold (dBm)	Low Warn Threshold (dBm)	Low Alarm Threshold (dBm)
Gi2/1	-16.7 (-13.0)	--	3.4	3.2	-0.3	-0.5
Gi2/2	0.8 (5.1)		3.4	3.2	-0.3	-0.5

Port	Optical Receive 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	-6.7	-28.5	-28.5
Gi2/2	N/A (-19.5)		5.9	-6.7	-28.5	-28.5

Switch#

The following example shows how to display the monitoring data for the transceivers on interface Gi1/2:

```
Switch# show interfaces g1/2 transceiver
ITU Channel 23 (1558.98 nm),
Transceiver is externally calibrated.
If device is externally calibrated, only calibrated values are printed.
++ : high alarm, + : high warning, - : low warning, -- : low alarm.
NA or N/A: not applicable, Tx: transmit, Rx: receive.
mA: milliamperes, dBm: decibels (milliwatts).
```

Port	Temperature (Celsius)	Voltage (Volts)	Current (mA)	Optical Tx Power (dBm)	Optical Rx Power (dBm)
Gi2/1	43.7	5.03	50.6 +	-16.7 --	N/A

Switch#

The following example shows how to display detailed the monitoring data for the transceivers on interface Gi1/2:

```
Switch# show interfaces g1/2 transceiver detail
ITU Channel 23 (1558.98 nm),
Transceiver is externally calibrated.
mA: milliamperes, dBm: decibels (milliwatts), NA or N/A: not applicable.
++ : high alarm, + : high warning, - : low warning, -- : low alarm.
A2D readouts (if they differ), are reported in parentheses.
The threshold values are calibrated.
```

Port	Temperature (Celsius)	High Alarm Threshold (Celsius)	High Warn Threshold (Celsius)	Low Warn Threshold (Celsius)	Low Alarm Threshold (Celsius)
Gi2/1	43.5	70.0	60.0	5.0	0.0

Port	Voltage (Volts)	High Alarm Threshold (Volts)	High Warn Threshold (Volts)	Low Warn Threshold (Volts)	Low Alarm Threshold (Volts)
Gi2/1	5.03	5.50	5.25	4.75	4.50

show interfaces transceiver

```

          High Alarm High Warn Low Warn Low Alarm
          Threshold Threshold Threshold Threshold
Port      Current      (mA)      (mA)      (mA)      (mA)
-----
Gi2/1     50.6          +      60.0      40.0      10.0      5.0

          High Alarm High Warn Low Warn Low Alarm
          Threshold Threshold Threshold Threshold
Port      Optical      (dBm)      (dBm)      (dBm)      (dBm)
          Transmit Power
-----
Gi2/1     -16.7 (-13.0) --      3.4        3.2        -0.3       -0.5

          High Alarm High Warn Low Warn Low Alarm
          Threshold Threshold Threshold Threshold
Port      Optical      (dBm)      (dBm)      (dBm)      (dBm)
          Receive Power
-----
Gi2/1     N/A (-28.5)      5.9        -6.7       -28.5      -28.5
Switch#

```

Related Commands

Command	Description
show idprom	Displays the IDPROMs for the chassis.
show interfaces status	Displays the interface status or a list of interfaces in error-disabled state.

show interfaces trunk

To display port and module interface-trunk information, use the **show interfaces trunk** command.

```
show interfaces trunk [module mod]
```

Syntax Description	module <i>mod</i> (Optional) Limits the display to interfaces on the specified module; valid values are from 1 to 6.				
Command Default	This command has no default settings.				
Command Modes	Privileged EXEC mode				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.1(8a)EW</td> <td>This command was introduced on the Catalyst 4500 series switch.</td> </tr> </tbody> </table>	Release	Modification	12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch.
Release	Modification				
12.1(8a)EW	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 The following 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	routed	negotiate	routed	1
Fa5/2	routed	negotiate	routed	1
Fa5/3	routed	negotiate	routed	1
Fa5/4	routed	negotiate	routed	1
Fa5/5	routed	negotiate	routed	1
Fa5/6	off	negotiate	not-trunking	10
Fa5/7	off	negotiate	not-trunking	10
Fa5/8	off	negotiate	not-trunking	1
Fa5/9	desirable	n-isl	trunking	1
Fa5/10	desirable	negotiate	not-trunking	1
Fa5/11	routed	negotiate	routed	1
Fa5/12	routed	negotiate	routed	1
...				
Fa5/48	routed	negotiate	routed	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	200
Fa5/9	1-1005

■ **show interfaces trunk**

```

Fa5/10    none
Fa5/11    none
Fa5/12    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     1-6,10,20,50,100,152,200,300,303-305,349-351,400,500,521,524,570,801-8
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     1-6,10,20,50,100,152,200,300,303-305,349-351,400,500,521,524,570,801-8
02,850,917,999,1002-1005
Fa5/10    none
Fa5/11    none

Fa5/48    none
Switch#

```

The following example shows how to display trunking information for active trunking ports:

```

Switch# show interfaces trunk

Port      Mode           Encapsulation  Status        Native vlan
Fa5/9     desirable     n-isl          trunking     1

Port      Vlans allowed on trunk
Fa5/9     1-1005

Port      Vlans allowed and active in management domain
Fa5/9     1-6,10,20,50,100,152,200,300,303-305,349-351,400,500,521,524,570,801-8
02,850,917,999,1002-1005

Port      Vlans in spanning tree forwarding state and not pruned
Fa5/9     1-6,10,20,50,100,152,200,300,303-305,349-351,400,500,521,524,570,801-8
02,850,917,999,1002-1005
Switch#

```

show ip arp inspection

To show the status of dynamic ARP inspection for a specific range of VLANs, use the **show ip arp inspection** command.

```
show ip arp inspection {[statistics] vlan vlan-range | interfaces [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 <i>vlan-range</i>	(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.	
interfaces <i>interface-name</i>	(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.	

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

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

Examples The following 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	31753	102407	102407	0

Vlan	DHCP Permits	ACL Permits	Source MAC Failures
3	31753	0	0

Vlan	Dest MAC Failures	IP Validation Failures
3	0	0

```
Switch#
```

The following example shows how to display the statistics of packets that have been processed by DAI for all active VLANs:

```
Switch# show ip arp inspection statistics
```

Vlan	Forwarded	Dropped	DHCP Drops	ACL Drops
1	0	0	0	0
2	0	0	0	0
3	68322	220356	220356	0
4	0	0	0	0
100	0	0	0	0
101	0	0	0	0
1006	0	0	0	0
1007	0	0	0	0

Vlan	DHCP Permits	ACL Permits	Source MAC Failures
1	0	0	0
2	0	0	0
3	68322	0	0
4	0	0	0
100	0	0	0
101	0	0	0
1006	0	0	0
1007	0	0	0

Vlan	Dest MAC Failures	IP Validation Failures
1	0	0
2	0	0
3	0	0
4	0	0
100	0	0
101	0	0
1006	0	0
1007	0	0

```
Switch#
```

The following example shows how to display the configuration and operating state of DAI for VLAN 1:

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

```
Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
```

Vlan	Configuration	Operation	ACL Match	Static ACL
1	Enabled	Active		

Vlan	ACL Logging	DHCP Logging
1	Deny	Deny

```
Switch#
```

The following example shows how to display the trust state of Fast Ethernet interface 6/1:

```
Switch# show ip arp inspection interfaces fastEthernet 6/1
```

Interface	Trust State	Rate (pps)	Burst Interval
Fa6/1	Untrusted	20	5

```
Switch#
```

The following 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
Gi3/1              Untrusted        15
Gi3/2              Untrusted        15
Fa3/3              Trusted          None
Fa3/4              Untrusted        15
Fa3/5              Untrusted        15
Fa3/6              Untrusted        15
Fa3/7              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.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

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

Examples The following example shows how to display the current contents of the log buffer before and after the buffers are cleared:

```
Switch# show ip arp inspection log
Total Log Buffer Size : 10
Syslog rate : 0 entries per 10 seconds.
```

Interface	Vlan	Sender MAC	Sender IP	Num of Pkts
Fa6/3	1	0002.0002.0002	1.1.1.2	1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3	1	0002.0002.0002	1.1.1.3	1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3	1	0002.0002.0002	1.1.1.4	1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3	1	0002.0002.0002	1.1.1.5	1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3	1	0002.0002.0002	1.1.1.6	1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3	1	0002.0002.0002	1.1.1.7	1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3	1	0002.0002.0002	1.1.1.8	1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3	1	0002.0002.0002	1.1.1.9	1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3	1	0002.0002.0002	1.1.1.10	1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3	1	0002.0002.0002	1.1.1.11	1(12:02:52 UTC Fri Apr 25 2003)
--	--	--	--	5(12:02:52 UTC Fri Apr 25 2003)

```
Switch#
```

The following example shows how to clear the buffer with the **clear ip arp inspection log** command:

```
Switch# clear ip arp inspection log
Switch# show ip arp inspection log
Total Log Buffer Size : 10
Syslog rate : 0 entries per 10 seconds.
No entries in log buffer.
Switch#
```

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

show ip cef vlan

To view IP CEF VLAN interface status and configuration information and display the prefixes for a specific interface, use the **show ip cef vlan** command.

```
show ip cef vlan vlan_num [detail]
```

Syntax Description	
<i>vlan_num</i>	Number of the VLAN.
detail	(Optional) Displays detailed information.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

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

Examples The following example shows how to display the prefixes for a specific VLAN:

```
Switch# show ip cef vlan 1003
Prefix          Next Hop          Interface
0.0.0.0/0      172.20.52.1      FastEthernet3/3
0.0.0.0/32     receive
10.7.0.0/16    172.20.52.1      FastEthernet3/3
10.16.18.0/23  172.20.52.1      FastEthernet3/3
Switch#
```

The following example shows how to display detailed IP CEF information for a specific VLAN:

```
Switch# show ip cef vlan 1003 detail
IP Distributed CEF with switching (Table Version 2364), flags=0x0
 1383 routes, 0 reresolve, 0 unresolved (0 old, 0 new)
 1383 leaves, 201 nodes, 380532 bytes, 2372 inserts, 989 invalidations
 0 load sharing elements, 0 bytes, 0 references
 universal per-destination load sharing algorithm, id 9B6C9823
 3 CEF resets, 0 revisions of existing leaves
 refcounts: 54276 leaf, 51712 node

Adjacency Table has 5 adjacencies
Switch#
```


show ip dhcp snooping

To display the DHCP snooping configuration, use the **show ip dhcp snooping** command.

show ip dhcp snooping

Syntax Description This command has no arguments or keywords.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.1(12c)EW	This command was introduced on the Catalyst 4500 series switch.
	12.2(25)EWA	Support for option 82 on untrusted ports was added.

Examples The following 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:
500,555
DHCP snooping is operational on following VLANs:
500,555
DHCP snooping is configured on the following L3 Interfaces:
Insertion of option 82 is enabled
circuit-id default format: vlan-mod-port
remote-id: switch123 (string)
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)
-----
FastEthernet5/1 yes 100
Custom circuit-ids:
VLAN 555: customer-555
FastEthernet2/1 no unlimited
Custom circuit-ids:
VLAN 500: customer-500
Switch#
```

show ip dhcp snooping binding

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.

To display the DHCP snooping binding entries, use the **show ip dhcp snooping binding** command.

```
show ip dhcp snooping binding [ip-address] [mac-address] [vlan vlan_num]
[interface interface_num]
```

Syntax Description

<i>ip-address</i>	(Optional) IP address for the binding entries.
<i>mac-address</i>	(Optional) MAC address for the binding entries.
vlan <i>vlan_num</i>	(Optional) Specifies a VLAN.
interface <i>interface_num</i>	(Optional) Specifies an interface.

Command Default

If no argument is specified, the switch will display the entire DHCP snooping binding table.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.1(12c)EW	This command was introduced on the Catalyst 4500 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 *last_vlan* argument to specify the end of the VLAN range.

Examples

The following 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
-----
0000.0100.0201  10.0.0.1        1600             dhcp-snooping     100   FastEthernet3/1
Switch#
```

The following example shows how to display an IP address for DHCP snooping binding entries:

```
Switch# show ip dhcp snooping binding 172.100.101.102
```

MacAddress	IP Address	Lease (seconds)	Type	VLAN	Interface
0000.0100.0201	172.100.101.102	1600	dhcp-snooping	100	FastEthernet3/1

```
Switch#
```

The following example shows how to display the MAC address for the DHCP snooping binding entries:

```
Switch# show ip dhcp snooping binding 55.5.5.2 0002.b33f.3d5f
```

MacAddress	IpAddress	Lease(sec)	Type	VLAN	Interface
00:02:B3:3F:3D:5F	55.5.5.2	492	dhcp-snooping	99	FastEthernet6/36

The following example shows how to display the DHCP snooping binding entries' MAC address for a specific VLAN:

```
Switch# show ip dhcp snooping binding 55.5.5.2 0002.b33f.3d5f vlan 99
```

MacAddress	IpAddress	Lease(sec)	Type	VLAN	Interface
00:02:B3:3F:3D:5F	55.5.5.2	479	dhcp-snooping	99	FastEthernet6/36

The following example shows how to display the dynamic DHCP snooping binding entries:

```
Switch# show ip dhcp snooping binding dynamic
```

MacAddress	IP Address	Lease (seconds)	Type	VLAN	Interface
0000.0100.0201	10.0.0.1	1600	dhcp-snooping	100	FastEthernet3/1

The following example shows how to display the DHCP snooping binding entries on VLAN 100:

```
Switch# show ip dhcp snooping binding vlan 100'
```

MacAddress	IP Address	Lease (seconds)	Type	VLAN	Interface
0000.0100.0201	10.0.0.1	1600	dhcp-snooping	100	FastEthernet3/1

The following example shows how to display the DHCP snooping binding entries on Ethernet interface 0/1:

```
Switch# show ip dhcp snooping binding interface fastethernet3/1
```

MacAddress	IP Address	Lease (seconds)	Type	VLAN	Interface
0000.0100.0201	10.0.0.1	1600	dhcp-snooping	100	FastEthernet3/1

Table 2-28 describes the fields in the `show ip dhcp snooping` command output.

Table 2-28 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.
---------------------------	--

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.1(12c)EW	This command was introduced on the Catalyst 4500 series switch.
	12.1(19)EW	Added support of state and statistics information.

Examples The following 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#
```

The following example shows how to view additional operating statistics:

```
Switch# show ip dhcp snooping database detail
Agent URL : tftp://10.1.1.1/directory/file
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : 7 (00:00:07)
Abort Timer Expiry : Not Running

Last Succeeded Time : None
Last Failed Time : 17:14:25 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 <i>slot/port</i>	(Optional) Specifies the Fast Ethernet interface and the number of the slot and port.	
gigabitethernet <i>slot/port</i>	(Optional) Specifies the Gigabit Ethernet interface and the number of the slot and port; valid values are from 1 to 9.	
tengigabitethernet <i>slot/port</i>	(Optional) Specifies the 10-Gigabit Ethernet interface and the number of the slot and port; valid values are from 1 to 2.	
null <i>interface-number</i>	(Optional) Specifies the null interface and the number of the interface; the only valid value is 0 .	
vlan <i>vlan_id</i>	(Optional) Specifies the VLAN and the number of the VLAN; valid values are from 1 to 4094.	

Command Default If you do not specify a VLAN, information for VLAN 1 is shown.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.1(8a)EW	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 The following example shows how to view IGMP information for VLAN 200:

```
Switch# show ip igmp interface vlan 200
IGMP snooping is globally enabled
IGMP snooping is 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
	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 switch 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	<i>profile number</i> (Optional) IGMP profile number to be displayed; valid ranges are from 1 to 4294967295.
---------------------------	--

Command Default	This command has no default settings.
------------------------	---------------------------------------

Command Modes	Privileged EXEC mode
----------------------	----------------------

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

Usage Guidelines	If no profile number is entered, all IGMP profiles are displayed.
-------------------------	---

Examples	The following 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#
```

The following example shows how to display all IGMP profiles:

```
Switch# show ip igmp profile
IGMP Profile 3
  range 230.9.9.0 230.9.9.0
IGMP Profile 4
  permit
  range 229.9.9.0 229.255.255.255
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 members sorted 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.

Command Default This command has no default settings.

Command Modes EXEC

Command History	Release	Modification
	12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch.
	12.1(19)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

The following example shows how to display the global snooping information on the switch:

```
Switch# show ip igmp snooping
Global IGMP Snooping configuration:
-----
IGMP snooping           : Enabled
IGMPv3 snooping        : Enabled
Report suppression     : Enabled
TCN solicit query      : Disabled
TCN flood query count   : 2

Vlan 1:
-----
IGMP snooping           : Enabled
IGMPv2 immediate leave  : Disabled
Explicit host tracking   : Enabled
Multicast router learning mode : pim-dvmrp
CGMP interoperability mode : IGMP_ONLY

Vlan 2:
-----
IGMP snooping           : Enabled
IGMPv2 immediate leave  : Disabled
Explicit host tracking   : Enabled
Multicast router learning mode : pim-dvmrp
CGMP interoperability mode : IGMP_ONLY
Switch>
```

The following 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
Explicit host tracking   : Enabled
Multicast router learning mode : pim-dvmrp
CGMP interoperability mode : IGMP_ONLY
Switch>
```

The following 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>
```

The following 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>
```

The following 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>
```

The following 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
2         224.2.2.2       v3       Fa6/2
Switch>
```

The following 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         229.2.3.4      v3         fa2/1 fa2/3
1         224.2.2.2      v3         Fa6/2
Switch>
```

The following example shows how to display the group's host types and ports in VLAN 10:

```
Switch# show ip igmp snooping group vlan 10 226.6.6.7
Vlan      Group          Version  Ports
-----
10        226.6.6.7      v3       Fa7/13, Fa7/14
Switch>
```

The following 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
-----
2.0.0.1       00:03:04    00:03:48    2          0
2.0.0.2       00:03:04    00:02:07    2          0
Switch>
```

The following 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 10 226.6.6.7 hosts
IGMPv3 host information for group 226.6.6.7
Timers: Expired hosts are deleted on next IGMP General Query

Host (MAC/IP)  Filter mode  Expires  Uptime  # Sources
-----
175.1.0.29     INCLUDE     stopped  00:00:51  2
175.2.0.30     INCLUDE     stopped  00:04:14  2
Switch>
```

The following example shows how to display summary information for a v3 group:

```
Switch# show ip igmp snooping group vlan 10 226.6.6.7 summary
Group Address (Vlan 10)      : 226.6.6.7
Host type                    : v3
Member Ports                 : Fa7/13, Fa7/14
Filter mode                  : INCLUDE
Expires                      : stopped
Sources                      : 2
Reporters (Include/Exclude)  : 2/0
Switch>
```

The following example shows how to display multicast router information for VLAN 1:

```
Switch# show ip igmp snooping mrouter vlan 1
vlan          ports
-----+-----
1             Gi1/1,Gi2/1,Fa3/48,Router
Switch#
```

The following example shows how to display the total number of group addresses learned by the system globally:

```
Switch# show ip igmp snooping group count
Total number of groups: 54
Switch>
```

The following example shows how to display the total number of group addresses learned on VLAN 5:

```
Switch# show ip igmp snooping group vlan 5 count
Total number of groups: 30
Switch>
```

Related Commands

Command	Description
ip igmp snooping	Enable IGMP snooping.
ip igmp snooping vlan immediate-leave	Enable IGMP immediate-leave processing.
ip igmp snooping vlan mrouter	Configures a Layer 2 interface as a multicast router interface for a VLAN.
ip igmp snooping vlan static	Configures a Layer 2 interface as a member of a group.
show ip igmp interface	Displays the information about the IGMP-interface status and configuration.

Command	Description
<code>show ip igmp snooping mrouter</code>	Displays information on the dynamically learned and manually configured multicast switch interfaces.
<code>show mac-address-table multicast</code>	Displays information about the multicast MAC address table.

show ip igmp snooping membership

To display host membership information, use the **show ip igmp snooping membership** command.

```
show ip igmp snooping membership [interface interface_num] [vlan vlan_id]
[reporter a.b.c.d] [source a.b.c.d group a.b.c.d]
```

Syntax Description

interface <i>interface_num</i>	(Optional) Displays IP address and version information of an interface.
vlan <i>vlan_id</i>	(Optional) Displays VLAN members sorted by group IP address of a VLAN; valid values are from 1 to 1001 and from 1006 to 4094.
reporter <i>a.b.c.d</i>	(Optional) Displays membership information for a specified reporter.
source <i>a.b.c.d</i>	(Optional) Specifies a reporter, source, or group IP address.
group <i>a.b.c.d</i>	(Optional) Displays all members of a channel (source, group), sorted by interface or VLAN.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.1(20)EW	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

The following example shows how to display host membership for the Gigabit Ethernet interface 4/1:

```
Switch# show ip igmp snooping membership interface gigabitethernet4/1
#channels: 5
#hosts : 1
Source/Group Interface Reporter Uptime Last-Join Last-Leave

40.40.40.2/224.10.10.10 Gi4/1 20.20.20.20 00:23:37 00:06:50 00:20:30
40.40.40.4/224.10.10.10Gi4/1 20.20.20.20 00:39:42 00:09:17 -
Switch#
```

The following 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
#channels: 5
#hosts : 1
Source/Group Interface Reporter Uptime Last-Join Last-Leave

40.40.40.2/224.10.10.10 Gi4/1 20.20.20.20 00:23:37 00:06:50 00:20:30
Switch#
```


The following 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-Join/
-----
40.0.0.1/224.1.1.1          Fa7/37    0002.4ba0.a4f6 00:00:04 00:00:04 /
                               -
40.0.0.2/224.1.1.1          Fa7/37    0002.fd80.f770 00:00:17 00:00:17 /
                               -
40.0.0.3/224.1.1.1          Fa7/36    20.20.20.20    00:00:04 00:00:04 /
                               -
40.0.0.4/224.1.1.1          Fa7/35    20.20.20.210   00:00:17 00:00:17 /
                               -
40.0.0.5/224.1.1.1          Fa7/37    0002.fd80.f770 00:00:17 00:00:17 /
                               -

Switch# clear ip igmp snooping membership vlan 20
Switch#
```

Related Commands	Command	Description
	clear ip igmp snooping membership	Clears the explicit host tracking database.
	ip igmp snooping vlan explicit-tracking	Enables per-VLAN explicit host tracking.
	show ip igmp snooping	Displays information on dynamically learned and manually configured VLAN switch interfaces.

show ip igmp snooping mrouter

To display information on the dynamically learned and manually configured multicast switch interfaces, use the **show ip igmp snooping mrouter** command.

```
show ip igmp snooping mrouter [vlan vlan-id]
```

Syntax Description	vlan <i>vlan-id</i> (Optional) Specifies a VLAN; valid values are from 1 to 1001 and from 1006 to 4094.
---------------------------	--

Command Default	This command has no default settings.
------------------------	---------------------------------------

Command Modes	Privileged EXEC mode
----------------------	----------------------

Command History	Release	Modification
	12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch.
	12.1(19)EW	Added support for extended VLAN addresses.

Usage Guidelines	<p>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.</p> <p>You can display IGMP snooping information for the VLAN interfaces by entering the show ip igmp interface vlan <i>vlan-num</i> command.</p>
-------------------------	--

Examples	The following 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,Fa3/48,Switch
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	<i>vlan_num</i> Number of the VLAN; valid values are from 1 to 1001 and from 1006 to 4094.
---------------------------	--

Command Default	This command has no default settings.
------------------------	---------------------------------------

Command Modes	Privileged EXEC mode
----------------------	----------------------

Command History	Release	Modification
	12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch.
12.1(12c)EW	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	The following example shows how to display snooping information for a specific VLAN:
-----------------	--

```
Switch# show ip igmp snooping vlan 2
vlan 2
-----
IGMP snooping is globally enabled
IGMP snooping TCN solicit query is globally enabled
IGMP snooping global TCN flood query count is 2
IGMP snooping is enabled on this Vlan
IGMP snooping immediate-leave is disabled on this Vlan
IGMP snooping mrouter learn mode is pim-dvmrp on this Vlan
IGMP snooping is running in IGMP_ONLY mode on this Vlan
Switch#
```

Related Commands	Command	Description
	ip igmp snooping	Enable IGMP snooping.
	ip igmp snooping vlan immediate-leave	Enable IGMP immediate-leave processing.
	ip igmp snooping vlan mrouter	Statically configures a Layer 2 interface as a multicast router interface for a VLAN.
	ip igmp snooping vlan static	Configures a Layer 2 interface as a member of a group.
	show ip igmp interface	Displays the information about the IGMP-interface status and configuration.
	show ip igmp snooping mrouter	Displays information on the dynamically learned and manually configured multicast switch interfaces.
	show mac-address-table multicast	Displays information about the multicast MAC address table.

show ip interface

To display the usability status of interfaces that are configured for IP, use the **show ip interface** command.

```
show ip interface [type number]
```

Syntax Description

<i>type</i>	(Optional) Interface type.
<i>number</i>	(Optional) Interface number.

Command Default

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

The following example shows how to display the usability status for a specific VLAN:

```
Switch# show ip interface vlan 1
Vlan1 is up, line protocol is up
  Internet address is 10.6.58.4/24
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
```

```

Local Proxy ARP is disabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachable 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 disabled
Network address translation is disabled
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
Netflow Data Export (hardware) is enabled
Switch#

```

Table 2-29 describes the fields that are shown in the example.

Table 2-29 *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 2-29 *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 unreachable	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	NDE hardware flow status on the interface.

show ip mfib

To display all 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 accelerate fast switching but that are not necessarily in the upper-layer 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.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch.
	12.2(40)SG	Support for command introduced on the Supervisor Engine 6-E and Catalyst 4900M chassis.

Usage Guidelines In the Supervisor Engine 6-E, Supervisor Engine 6L-E, Catalyst 4900M, Catalyst 4948E, and Catalyst 4948E-F, 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 switch 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 route should be signaled to a protocol process.

A route can also have a set of flags associated with one or more interfaces. For an (S,G) route, the flags on interface 1 indicate how the ingress packets should be treated and whether packets matching the route should be forwarded onto interface 1. These per-interface flags are associated with the MFIB routes:

- Accepting (A)—Set on the RPF interface when a packet that arrives on the interface and that is marked as Accepting (A) is forwarded to all Forwarding (F) interfaces.
- Forwarding (F)—Used with the A flag as described above. The set of forwarding interfaces together form a multicast olist or output interface list.
- Signaling (S)—Set on an interface when a multicast routing protocol process in Cisco IOS needs to be notified of ingress packets on that interface.
- Not Platform (NP) fast-switched—Used with the F flag. A forwarding interface is also marked as Not Platform fast-switched whenever that output interface cannot be fast-switched by the platform hardware and requires software forwarding.

Examples

The following example shows how to display all active MFIB routes:

```
Switch# show ip mfib
IP Multicast Forwarding Information Base
Entry Flags: C - Directly Connected, S - Signal,
             IC - Internal Copy
Interface Flags: A - Accept, F - Forward, NS - Signal,
                NP - Not platform switched
Packets: Fast/Partial/Slow Bytes: Fast/Partial/Slow:
(171.69.10.13, 224.0.1.40), flags (IC)
  Packets: 2292/2292/0, Bytes: 518803/0/518803
  Vlan7 (A)
  Vlan100 (F NS)
  Vlan105 (F NS)
(*, 224.0.1.60), flags ()
  Packets: 2292/0/0, Bytes: 518803/0/0
  Vlan7 (A NS)
(*, 224.0.1.75), flags ()
  Vlan7 (A NS)
(10.34.2.92, 239.192.128.80), flags ()
  Packets: 24579/100/0, 2113788/15000/0 bytes
  Vlan7 (F NS)
  Vlan100 (A)
(*, 239.193.100.70), flags ()
  Packets: 1/0/0, 1500/0/0 bytes
  Vlan7 (A)
Switch#
```

Related Commands

Command	Description
clear ip mfib counters	Clears the global MFIB counters 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.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

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

Examples The following example shows how to display all currently active fast-drop entries and whether fast drop is enabled.

```
Switch# show ip mfib fastdrop
MFIB fastdrop 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 ) 00:02:30
(1.2.3.4, 225.6.7.8, Vlan3) 00:01:50
Switch#
```

Related Commands	Command	Description
	clear ip mfib fastdrop	Clears all the MFIB fast-drop entries.

show ip mroute

To display IP multicast routing table information, use the **show ip mroute** command.

```
show ip mroute [interface_type slot/port | host_name | host_address [source] | active [kbps | interface_type num] | count | pruned | static | summary]
```

Syntax Description	
<i>interface_type slot/port</i>	(Optional) Interface type and number of the slot and port; valid values for <i>interface type</i> are fastethernet , gigabitethernet , tengigabitethernet , null , and vlan .
<i>host_name</i>	(Optional) Name or IP address as defined in the DNS hosts table.
<i>host_address source</i>	(Optional) IP address or name of a multicast source.
active	(Optional) Displays the rate that active sources are sending to multicast groups.
<i>kbps interface_type num</i>	(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.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch.
	12.2(25)EW	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 “S” 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

The following example shows how to display all the entries in the IP multicast routing table:

```
Switch# show ip mroute

IP Multicast Routing Table
Flags:D - Dense, S - Sparse, s - SSM Group, C - Connected, L - Local,
      P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
      J - Join SPT, M - MSDP created entry, X - Proxy Join Timer Running
      A - Advertised via MSDP, U - URD, I - Received Source Specific Host
      Report
Outgoing interface flags:H - Hardware switched
Timers:Uptime/Expires
Interface state:Interface, Next-Hop or VCD, State/Mode

(*, 230.13.13.1), 00:16:41/00:00:00, RP 10.15.1.20, flags:SJC
  Incoming interface:GigabitEthernet4/8, RPF nbr 10.15.1.20
  Outgoing interface list:

GigabitEthernet4/9, Forward/Sparse-Dense, 00:16:41/00:00:00, H

(*, 230.13.13.2), 00:16:41/00:00:00, RP 10.15.1.20, flags:SJC

  Incoming interface:GigabitEthernet4/8, RPF nbr 10.15.1.20, RPF-MFD
  Outgoing interface list:
    GigabitEthernet4/9, Forward/Sparse-Dense, 00:16:41/00:00:00, H

(10.20.1.15, 230.13.13.1), 00:14:31/00:01:40, flags:CJT

  Incoming interface:GigabitEthernet4/8, RPF nbr 10.15.1.20, RPF-MFD
  Outgoing interface list:
    GigabitEthernet4/9, Forward/Sparse-Dense, 00:14:31/00:00:00, H
(132.206.72.28, 224.2.136.89), 00:14:31/00:01:40, flags:CJT
  Incoming interface:GigabitEthernet4/8, RPF nbr 10.15.1.20, RPF-MFD

  Outgoing interface list:Null
Switch#
```

The following 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 mroute 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: 1 pps/4 kbps(1sec), 4 kbps(last 1 secs), 4 kbps(life avg)

Group: 224.2.201.241, ACM 97
  Source: 130.129.52.160 (webcast3-e1.acm97.interop.net)
  Rate: 9 pps/93 kbps(1sec), 145 kbps(last 20 secs), 85 kbps(life avg)

Group: 224.2.207.215, ACM 97
  Source: 130.129.52.160 (webcast3-e1.acm97.interop.net)
  Rate: 3 pps/31 kbps(1sec), 63 kbps(last 19 secs), 65 kbps(life avg)
Switch#
```

The following example shows how to display route and packet count information:

```
Switch# show ip mroute count
IP Multicast Statistics
56 routes using 28552 bytes of memory
13 groups, 3.30 average sources per group
Forwarding Counts:Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second

Other counts:Total/RPF failed/Other drops(OIF-null, rate-limit etc)

Group:224.2.136.89, Source count:1, Group pkt count:29051
Source:132.206.72.28/32, Forwarding:29051/-278/1186/0, Other:85724/8/56665
Switch#
```

The following example shows how to display summary information:

```
Switch# show ip mroute summary
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, s - SSM Group, C - Connected, L - Local,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT, M - MSDP created entry, X - Proxy Join Timer Running
       A - Advertised via MSDP, U - URD, I - Received Source Specific Host
       Report
Outgoing interface flags: H - Hardware switched
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

Switch#
```

Table 2-30 describes the fields shown in the output.

Table 2-30 *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.
s - 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	Switch is a member of the multicast group.
P - Pruned	Route has been pruned. This information is retained in case a downstream member wants to join the source.
R - Rp-bit set	Status of the (S,G) entry; is the (S,G) entry pointing toward the RP. The R - Rp-bit set is typically a 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 2-30 *show ip mroute Field Descriptions (continued)*

Field	Description
J - Join SPT	<p>For (*, G) entries, indicates that the rate of traffic flowing down the shared tree is exceeding the SPT-Threshold set for the group. (The default SPT-Threshold setting is 0 kbps.) When the J - Join SPT flag is set, the next (S,G) packet received down the shared tree triggers an (S,G) join in the direction of the source causing the switch to join the source tree.</p> <p>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.</p> <p>The switch measures the traffic rate on the shared tree and compares the measured rate to the group's SPT-Threshold once every second. 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. The flag is cleared when the next packet arrives on the shared tree and a new measurement interval is started.</p> <p>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.</p>
Outgoing interface flag:	Information about the outgoing entry.
H - Hardware switched	Entry is hardware switched.
Timer:	Uptime/Expires.
Interface state:	Interface, Next-Hop or VCD, State/Mode.
(*, 224.0.255.1) (198.92.37.100/32, 224.0.255.1)	<p>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.</p> <p>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 (S,G) entries.</p>
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 2-30 *show ip mroute Field Descriptions (continued)*

Field	Description
RP	Address of the RP switch. For switches and access servers operating in sparse mode, this address is always 0.0.0.0.
flags:	Information about the entry.
Incoming interface	Expected interface for a multicast packet from the source. If the packet is not received on this interface, it is discarded.
RPF neighbor	IP address of the upstream switch to the source. “Tunneling” indicates that this switch is sending data to the RP encapsulated in Register packets. The hexadecimal number in parentheses indicates to which RP it is registering. Each bit indicates a different RP if multiple RPs per group are used.
DVMRP or Mroute	Status of whether the RPF information is obtained from the DVMRP routing table or the static mroutes configuration.
Outgoing interface list	Interfaces through which packets are forwarded. When the ip pim nbma-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.
Forward/Dense	Status of the packets; indicates if they are they forwarded on the interface if there are no restrictions due to access lists or the TTL threshold. Following the slash (/), mode in which the interface is operating (dense or sparse).
Forward/Sparse	Sparse mode interface is in forward mode.
time/time (uptime/expiration time)	Per interface, how long (in hours, minutes, and seconds) the entry has been in the IP multicast routing table. Following the slash (/), how 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	
<i>ip-address</i>	(Optional) Binding IP address.
<i>mac-address</i>	(Optional) Binding MAC address.
dhcp-snooping	(Optional) DHCP-snooping type binding.
static	(Optional) Statically configured binding.
vlan <i>vlan-id</i>	(Optional) VLAN number.
interface <i>interface-name</i>	(Optional) Binding interface.

Command Default Displays both static and DHCP snooping bindings.

Command Modes Privileged EXEC mode

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

Usage Guidelines The optional parameters filter the display output result.

Examples The following example shows how to display the IP source bindings:

```
Switch# show ip source binding
MacAddress      IpAddress      Lease(sec)  Type           VLAN  Interface
-----
00:00:00:0A:00:0B  11.0.0.1      infinite    static         10    FastEthernet6/10

Switch#
```

The following example shows how to display the static IP binding entry of IP address 11.0.01:

```
Switch# show ip source binding 11.0.0.1 0000.000A.000B static vlan 10 interface Fa6/10
show ip source binding 11.0.0.1 0000.000A.000B static vlan 10 interface Fa6/10
MacAddress      IpAddress      Lease(sec)  Type           VLAN  Interface
-----
00:00:00:0A:00:0B  11.0.0.1      infinite    static         10    FastEthernet6/10

Switch#
```

Related Commands	Command	Description
	ip source binding	Adds or deletes a static IP source binding entry.

show ip verify source

To display the IP source guard configuration and filters on a particular interface, use the **show ip verify source** command.

show ip verify source [**interface** *interface_num*]

Syntax Description	interface <i>interface_num</i> (Optional) Specifies an interface.				
Command Default	This command has no default settings.				
Command Modes	Privileged EXEC mode				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.1(19)EW</td> <td>This command was introduced on the Catalyst 4500 series switch.</td> </tr> </tbody> </table>	Release	Modification	12.1(19)EW	This command was introduced on the Catalyst 4500 series switch.
Release	Modification				
12.1(19)EW	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 fa6/2** command and DHCP snooping is enabled on VLANs 10–20, interface fa6/1 has IP source filter mode that is configured as IP, and there is an existing IP address binding 10.0.0.1 on VLAN 10:

Interface	Filter-type	Filter-mode	IP-address	Mac-address	Vlan
fa6/2	ip	inactive-trust-port			

- This output appears when you enter the **show ip verify source interface fa6/3** command and the interface fa6/3 does not have a VLAN enabled for DHCP snooping:

Interface	Filter-type	Filter-mode	IP-address	Mac-address	Vlan
fa6/3	ip	inactive-no-snooping-vlan			

- This output appears when you enter the **show ip verify source interface fa6/4** command and the interface fa6/4 has an IP source filter mode that is configured as IP MAC and the existing IP MAC that binds 10.0.0.2/aaaa.bbbb.cccc on VLAN 10 and 11.0.0.1/aaaa.bbbb.cccd on VLAN 11:

Interface	Filter-type	Filter-mode	IP-address	Mac-address	Vlan
fa6/4	ip-mac	active	10.0.0.2	aaaa.bbbb.cccc	10
fa6/4	ip-mac	active	11.0.0.1	aaaa.bbbb.cccd	11
fa6/4	ip-mac	active	deny-all	deny-all	12-20

- This output appears when you enter the **show ip verify source interface fa6/5** command and the interface fa6/5 has IP source filter mode that is configured as IP MAC and existing IP MAC binding 10.0.0.3/aaaa.bbbb.cccc on VLAN 10, but port security is not enabled on fa6/5:

Interface	Filter-type	Filter-mode	IP-address	Mac-address	Vlan
fa6/5	ip-mac	active	10.0.0.3	permit-all	10
fa6/5	ip-mac	active	deny-all	permit-all	11-20



Note Enable port security first because the DHCP security MAC filter cannot apply to the port or VLAN.

- This output appears when you enter the **show ip verify source interface fa6/6** command and the interface fa6/6 does not have IP source filter mode that is configured:

DHCP security is not configured on the interface fa6/6.

The following 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	10.0.0.1		10
fa6/1	ip	active	deny-all		11-20
fa6/2	ip	inactive-trust-port			
Fa6/3	ip trk	active	40.1.1.24		10
Fa6/3	ip trk	active	40.1.1.20		10
Fa6/3	ip trk	active	40.1.1.21		10
fa6/4	ip-mac	active	10.0.0.2	aaaa.bbbb.cccc	10
fa6/4	ip-mac	active	11.0.0.1	aaaa.bbbb.cccd	11
fa6/4	ip-mac	active	deny-all	deny-all	12-20
fa6/5	ip-mac	active	10.0.0.3	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 ip wccp

To display the Web Cache Communication Protocol (WCCP) global configuration and statistics, use the **show ip wccp** command in user EXEC or privileged EXEC mode.

show ip wccp [*service-number* [**view** | **detail**] | **interfaces** [**cef** | **counts** | **detail**] | **web-cache**]

Syntax Description

service-number	(Optional) Identification number of the web cache service group being controlled by the cache. The number can be from 0 to 254. For web caches using Cisco cache engines, the reverse proxy service is indicated by a value of 99.
interfaces	(Optional) WCCP redirect interfaces.
cef	(Optional) CEF interface statistics, including the number of input, output, dynamic, static, and multicast services.
counts	(Optional) WCCP interface count statistics, including the number of CEF and process-switched output and input packets redirected.
detail	(Optional) WCCP interface configuration statistics, including the number of input, output, dynamic, static, and multicast services.
web-cache	(Optional) Statistics for the web cache service.
view	(Optional) Other members of a particular service group, have or have not been detected.
detail	(Optional) Information about the router and all web caches.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.0(2)SG	This command was introduced on Catalyst 4900M, Catalyst 4948E, Supervisor Engine 6-E, and Supervisor Engine 6L-E.

Usage Guidelines

Use the **clear ip wccp** command to reset the counter for the “Packets Redirected” information.

Use the **show ip wccp service-number** command to get the “Total Packets S/W Redirected” count. The “Total Packets S/W Redirected” count is the number of packets redirected in software.

Use the **show ip wccp service-number detail** command to get the “Packets Redirected” count. The “Packets Redirected” count is the number of packets redirected in software.

Use the **show ip wccp web-cache detail** command to get an indication of which traffic is redirected to which cache engine.

Use the **show ip wccp** command to show the configured WCCP services and a summary of their current state.

For cache-engine clusters using Cisco cache engines, the reverse proxy *service-number* is indicated by a value of 99.

All the packet statistics correspond to packets switched in software.

Examples

This section contains examples and field descriptions for the following forms of this command:

- **show ip wccp service-number**
- **show ip wccp service-number view**
- **show ip wccp service-number detail**
- **show ip wccp interfaces**
- **show ip wccp web-cache**
- **show ip wccp web-cache detail**
- **show ip wccp**

show ip wccp service-number

The following is sample output from the **show ip wccp service-number** command:

```
Switch# show ip wccp 90

Global WCCP information:
  Router information:
    Router Identifier:          100.1.1.16
    Protocol Version:          2.0

  Service Identifier: 90
    Number of Service Group Clients: 1
    Number of Service Group Routers: 1
    Total Packets s/w Redirected: 0
    Process:                    0
    CEF:                         0
    Redirect Access-list:       -none-
    Total Packets Denied Redirect: 0
    Total Packets Unassigned: 0
    Group Access-list:         -none-
    Total Messages Denied to Group: 0
    Total Authentication failures: 0
    Total Bypassed Packets Received: 0
```

[Table 31](#) describes the significant fields shown in the display.

Table 31 *show ip wccp service-number* **Field Descriptions**

Field	Description
Router information	A list of routers detected by the current router.
Protocol Version	The version of WCCP being used by the router in the service group.
Service Identifier	Indicates which service is detailed.
Number of Service Group Clients:	The number of clients that are visible to the router and other clients in the service group.
Number of Service Group Routers	The number of routers in the service group.
Total Packets s/w Redirected	Total number of packets s/w redirected by the router.
Redirect Access-list	The name or number of the access list that determines which packets will be redirected.
Total Packets Denied Redirect	Total number of packets that were not redirected because they did not match the access list.

Table 31 *show ip wccp service-number Field Descriptions (continued)*

Field	Description
Total Packets Unassigned	Number of packets that were not redirected because they were not assigned to any cache engine. Packets may not be assigned during initial discovery of cache engines or when a cache is dropped from a cluster.
Group Access-list	Indicates which cache engine is allowed to connect to the router.
Total Messages Denied to Group	Indicates the number of packets denied by the <i>group-list</i> access list.
Total Authentication failures	The number of instances where a password did not match.
Total Bypassed Packets Received	The number of packets that have been bypassed. Process, fast, and Cisco Express Forwarding (CEF) are switching paths within Cisco IOS software.

show ip wccp service-number view

The following is sample output from the **show ip wccp service-number view** command for service group 1:

```
Switch# show ip wccp 1 view

WCCP Router Informed of:
 10.168.88.10
 10.168.88.20

WCCP Cache Engines Visible
 10.168.88.11
 10.168.88.12

WCCP Cache Engines Not Visible:
 -none-
```

**Note**

The number of maximum service groups that can be configured is 256.

If any web cache is displayed under the WCCP Cache Engines Not Visible field, the router needs to be reconfigured to map the web cache that is not visible to it.

[Table 32](#) describes the significant fields shown in the display.

Table 32 *show ip wccp service-number view Field Descriptions*

Field	Description
WCCP Router Informed of	A list of routers detected by the current router.
WCCP Clients Visible	A list of clients that are visible to the router and other clients in the service group.
WCCP Clients Not Visible	A list of clients in the service group that are not visible to the router and other clients in the service group.

show ip wccp service-number detail

The following example displays WCCP client information and WCCP router statistics that include the type of services:

```
Switch# show ip wccp 91 detail

WCCP Client information:
  WCCP Client ID:      10.10.10.2
  Protocol Version:    2.0
  State:               Usable
  Redirection:         L2
  Packet Return:       GRE
  Packets Redirected:  0
  Connect Time:        00:05:23
  Assignment:          MASK

Mask  SrcAddr  DstAddr  SrcPort  DstPort
----  -
0000: 0x00000000 0x00000001 0x0000  0x0000

Value SrcAddr  DstAddr  SrcPort  DstPort  CE-IP
----  -
0000: 0x00000000 0x00000000 0x0000  0x0000  0x0A0A0A02 (10.10.10.2)
0001: 0x00000000 0x00000001 0x0000  0x0000  0x0A0A0A02 (10.10.10.2)
```

show ip wccp interfaces

The following is sample output from the **show ip wccp interfaces** command:

```
Switch# show ip wccp interfaces

WCCP interface configuration:
  FastEthernet10/4
    Output services: 2
    Input services:  3
    Mcast services:  1
    Exclude In:      FALSE
```

[Table 33](#) describes the significant fields shown in the display.

Table 33 *show ip wccp interfaces Field Descriptions*

Field	Description
Output services	Indicates the number of output services configured on the interface.
Input services	Indicates the number of input services configured on the interface.
Mcast services	Indicates the number of multicast services configured on the interface.
Exclude In	Displays whether traffic on the interface is excluded from redirection.

show ip wccp web-cache

The following is sample output from the **show ip wccp web-cache** command:

```
Switch# show ip wccp web-cache

Global WCCP information:
  Router information:
```

```

Router Identifier:          10.10.11.10
Protocol Version:         2.0

Service Identifier: web-cache
Number of Service Group Clients: 1
Number of Service Group Routers: 1
Total Packets Redirected: 0
  Process:                 0
  CEF:                     0
  Platform:                0
Redirect access-list:     no_linux
Total Packets Denied Redirect: 0
Total Packets Unassigned: 0
Group access-list:       -none-
Total Messages Denied to Group: 0
Total Authentication failures: 0
Total Bypassed Packets Received: 0

```

Table 34 describes the significant fields shown in the display.

Table 34 *show ip wccp web-cache Field Descriptions*

Field	Description
Protocol Version	Indicates that WCCPv2 is enabled.
Service Identifier	Indicates which service is detailed.
Number of Service Group Clients	Number of clients using the router as their home router.
Number of Service Group Routers	The number of routers in the service group.
Total Packets s/w Redirected	Total number of packets s/w redirected by the router.
Redirect access-list	The name or number of the access list that determines which packets will be redirected.
Total Packets Denied Redirect	Total number of packets that were not redirected because they did not match the access list.
Total Packets Unassigned	Number of packets that were not redirected because they were not assigned to any cache engine. Packets may not be assigned during initial discovery of cache engines or when a cache is dropped from a cluster.
Group access-list	Indicates which cache engine is allowed to connect to the router.
Total Messages Denied to Group	Indicates the number of packets denied by the <i>group-list</i> access list.
Total Authentication failures	The number of instances where a password did not match.

show ip wccp web-cache detail

The following example displays web cache engine information and WCCP router statistics for the web cache service:

```
Switch# show ip wccp web-cache detail
```

```

WCCP Client information:
  WCCP Client ID:      10.10.10.2
  Protocol Version:    2.0
  State:               Usable
  Redirection:         L2
  Packet Return:       GRE

```



```

Packets Redirected:    0
Connect Time:         00:23:19
Assignment:           MASK

Mask  SrcAddr  DstAddr  SrcPort  DstPort
----  -
0000: 0x00000000 0x00000001 0x0000  0x0000

Value SrcAddr  DstAddr  SrcPort  DstPort  CE-IP
----  -
0000: 0x00000000 0x00000000 0x0000  0x0000  0x0A0A0A02 (10.10.10.2)
0001: 0x00000000 0x00000001 0x0000  0x0000  0x0A0A0A02 (10.10.10.2)

```

Table 35 describes the significant fields shown in the display.

Table 35 *show ip wccp web-cache detail Field Descriptions*

Field	Description
WCCP Client Information	The header for the area that contains fields for information on clients.
WCCP Client ID	The IP address of the cache engine in the service group.
Protocol Version	The version of WCCP being used by the cache engine in the service group.
State	Indicates whether the cache engine is operating properly and can be contacted by a router and other cache engines in the service group.
Packets Redirected	The number of packets that have been redirected to the cache engine.
Connect Time	The amount of time the cache engine has been connected to the router.

show ip wccp

```
Switch# show ip wccp
```

```

Global WCCP information:
  Router information:
    Router Identifier:          10.10.11.10
    Protocol Version:          2.0

  Service Identifier: web-cache
    Number of Service Group Clients: 1
    Number of Service Group Routers: 1
    Total Packets s/w Redirected: 0
    Process:                    0
    CEF:                         0
    Redirect access-list:       -none-
    Total Packets Denied Redirect: 0
    Total Packets Unassigned: 0
    Group access-list:          -none-
    Total Messages Denied to Group: 0
    Total Authentication failures: 0
    Total Bypassed Packets Received: 0

  Service Identifier: 91
    Number of Service Group Clients: 1
    Number of Service Group Routers: 1

```

show ip wccp

```

Total Packets s/w Redirected:      0
  Process:                         0
  CEF:                             0
Redirect access-list:             -none-
Total Packets Denied Redirect:    0
Total Packets Unassigned:         0
Group access-list:                -none-
Total Messages Denied to Group:   0
Total Authentication failures:    0
Total Bypassed Packets Received:  0

```

Related Commands

Command	Description
clear ip wccp	Clears the counter for packets redirected using WCCP.
ip wccp	Enables support of the WCCP service for participation in a service group.
ip wccp redirect	Enables packet redirection on an outbound or inbound interface using WCCP.

show ipc

To display IPC information, use the **show ipc** command.

show ipc { nodes | ports | queue | status }

Syntax Description	nodes	Displays the participating nodes.
	ports	Displays the local IPC ports.
	queue	Displays the contents of the IPC retransmission queue.
	status	Displays the status of the local IPC server.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

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

Examples The following example shows how to display the participating nodes:

```
Switch# show ipc nodes
There are 3 nodes in this IPC realm.
  ID      Type      Name                               Last Sent  Last Heard
  10000   Local      IPC Master                         0          0
  2010000 Local      GALIOS IPC:Card 1                  0          0
  2020000 Ethernet  GALIOS IPC:Card 2                  12         26
Switch#
```

The following example shows how to display the local IPC ports:

```
Switch# show ipc ports
There are 11 ports defined.
Port ID      Type      Name                               (current/peak/total)
  10000.1    unicast   IPC Master:Zone
  10000.2    unicast   IPC Master:Echo
  10000.3    unicast   IPC Master:Control
  10000.4    unicast   Remote TTY Server Port
  10000.5    unicast   GALIOS RF :Active
  index = 0  seat_id = 0x2020000  last sent = 0  heard = 1635  0/1/1635
  10000.6    unicast   GALIOS RED:Active
  index = 0  seat_id = 0x2020000  last sent = 0  heard = 2  0/1/2
  2020000.3  unicast   GALIOS IPC:Card 2:Control
  2020000.4  unicast   GALIOS RFS :Standby
  2020000.5  unicast   Slave: Remote TTY Client Port
  2020000.6  unicast   GALIOS RF :Standby
  2020000.7  unicast   GALIOS RED:Standby
```

```
RPC packets: current/peak/total
                                           0/1/17
Switch#
```

The following example shows how to display the contents of the IPC retransmission queue:

```
Switch# show ipc queue
There are 0 IPC messages waiting for acknowledgement 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 currently on the IPC inboundQ.
There are 0 messages currently in use by the system.
Switch#
```

The following 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.

6000 IPC message headers in cache
3363 messages in, 1680 out, 1660 delivered to local port,
1686 acknowledgements received, 1675 sent,
0 NACKS received, 0 sent,
0 messages dropped on input, 0 messages dropped on output
0 no local port, 0 destination unknown, 0 no transport
0 missing callback or queue, 0 duplicate ACKs, 0 retries,
0 message timeouts.
0 ipc_output failures, 0 mtu failures,
0 msg alloc failed, 0 emer msg alloc failed, 0 no origs for RPC replies
0 pak alloc failed, 0 memd alloc failed
0 no hwq, 1 failed opens, 0 hardware errors
No regular dropping of IPC output packets for test purposes
Switch#
```

show ipv6 dhcp-ldra

To display configuration details and statistics for a Lightweight DHCPv6 Relay Agent (LDRA), use the **show ipv6 dhcp-ldra** command in user EXEC or privileged EXEC mode.

```
show ipv6 ldra [statistics]
```

Syntax Description

statistics	(Optional) Displays LDRA-related statistics.
-------------------	--

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS Release 15.2(5)E2	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

Use this command to view the number and type of DHCPv6 packets received or processed, the number and type of DHCPv6 messages dropped, error counters, and the interface state (client-facing trusted interface, server-facing interface, and so on).

You can also view LDRA configuration details, such as the type of LDRA configuration and the interface or VLAN where the LDRA is configured.

Examples

The following sample output displays LDRA configuration details. The fields in the example below are self-explanatory.

```
Device # show ipv6 dhcp-ldra

DHCPv6 LDRA is Enabled.
DHCPv6 LDRA policy: client-facing-disable
    Target: none
DHCPv6 LDRA policy: client-facing-trusted
    Target: vlan 5
DHCPv6 LDRA policy: client-facing-untrusted
    Target: none
DHCPv6 LDRA policy: server-facing
    Target: Gi1/0/7
```

The following sample output displays LDRA configuration details after initiating a DHCP session. The fields in the example below are self-explanatory.

```
Device # show ipv6 dhcp-ldra statistics

DHCPv6 LDRA client facing statistics.

Messages received          2
Messages sent              2
Messages discarded         0
```

show ipv6 dhcp-ldra

```

Messages                               Received
SOLICIT                                1
REQUEST                                 1

Messages                               Sent
RELAY-FORWARD                           2

```

DHCPv6 LDRA server facing statistics.

```

Messages received                       2
Messages sent                           2
Messages discarded                       0

Messages                               Received
RELAY-REPLY                             2

Messages                               Sent
ADVERTISE                                1
REPLY                                     1

```

Related Commands

Command	Description
ipv6 dhcp-ldra	Enables LDRA functionality on an access node.
ipv6 dhcp ldra attach-policy (VLAN)	Enables LDRA functionality on a VLAN.
ipv6 dhcp-ldra attach-policy	Enables LDRA functionality on an interface.

show ipv6 snooping counters

To display the number of packets dropped per port due to RA Guard, use the **show ipv6 snooping counters interface** command.

show ipv6 snooping counters interface

Syntax Description	<i>interface</i>	Specifies the interface.
---------------------------	------------------	--------------------------

Command Default	None
------------------------	------

Command Modes	Interface mode
----------------------	----------------

Command History	Release	Modification
	12.2(54)SG	The show ipv6 first-hop counters command was introduced on the Catalyst 4500 series switch.
	15.0(2)SG, XE 3.3.0SG	Same behavior, new syntax; show ipv6 snooping counters

Examples

This example provides a sample output for the **show ipv6 snooping counters** command on interface Gi2/49:

```
Switch# show ipv6 snooping counters int gi 2/48
Received messages on Gi2/48:
Protocol      Protocol message
ICMPv6        RS          RA          NS          NA          REDIR       CPS          CPA
              0           0           0           0           0           0           0

Bridged messages from Gi2/48:
Protocol      Protocol message
ICMPv6        RS          RA          NS          NA          REDIR       CPS          CPA
              0           0           0           0           0           0           0

Dropped messages on Gi2/48:
Feature/Message RS          RA          NS          NA          REDIR       CPS          CPA

Dropped reasons on Gi2/48:
Switch#
```



Note

Only RA (Router Advertisement) and REDIR (Router Redirected packets) counters are supported in Cisco IOS Release 12.2(54)SG.

Related Commands	Command	Description
	ipm access control	Configures access control.

show ipv6 mld snooping

To display IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping configuration of the switch or the VLAN, use the **show ipv6 mld snooping** command.

```
show ipv6 mld snooping [vlan vlan-id]
```

Syntax Description	vlan <i>vlan-id</i> (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(40)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 : Enabled
MLDv2 snooping (minimal) : Enabled
Listener message suppression : Enabled
TCN solicit query : Disabled
TCN flood query count : 2
Robustness variable : 3
Last listener query count : 2
Last listener query interval : 1000

Vlan 100:
-----
MLD snooping : Disabled
MLDv1 immediate leave : Disabled
Explicit host tracking : Enabled
Multicast router learning mode : pim-dvmrp
Robustness variable : 3
Last listener query count : 2
Last listener query interval : 1000
```

This is an example of output from the **show ipv6 mld snooping** command. It displays snooping characteristics for all VLANs on the switch.

```
Switch> show ipv6 mld snooping
Global MLD Snooping configuration:
-----
```



```

MLD snooping : Enabled
MLDv2 snooping (minimal) : Enabled
Listener message suppression : Enabled
TCN solicit query : Disabled
TCN flood query count : 2
Robustness variable : 3
Last listener query count : 2
Last listener query interval : 1000

Vlan 1:
-----
MLD snooping : Disabled
MLDv1 immediate leave : Disabled
Explicit host tracking : Enabled
Multicast router learning mode : pim-dvmrp
Robustness variable : 1
Last listener query count : 2
Last listener query interval : 1000

<output truncated>

Vlan 951:
-----
MLD snooping : Disabled
MLDv1 immediate leave : Disabled
Explicit host tracking : Enabled
Multicast router learning mode : pim-dvmrp
Robustness variable : 3
Last listener query count : 2
Last listener query interval : 1000

```

Related Commands

Command	Description
ipv6 mld snooping	Enables IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping globally or on the specified VLAN.

show ipv6 mld snooping mrouter

To display dynamically learned and manually configured IP version 6 (IPv6) Multicast Listener Discovery (MLD) switch ports for the switch or a VLAN, use the **show ipv6 mld snooping mrouter** command.

```
show ipv6 mld snooping mrouter [vlan vlan-id]
```

Syntax Description	vlan <i>vlan-id</i> (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(40)SG	This command was introduced on Catalyst 4500.

Usage Guidelines	Use this command to display MLD snooping switch ports for the switch or for a specific VLAN. VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in MLD snooping.
-------------------------	--

Examples	This is an example of output from the show ipv6 mld snooping mrouter command. It displays snooping characteristics for all VLANs on the switch that are participating in MLD snooping.
-----------------	---

```
Switch> show ipv6 mld snooping mrouter
Vlan    ports
----    -
    2    Gi1/0/11(dynamic)
    72    Gi1/0/11(dynamic)
   200    Gi1/0/11(dynamic)
```

This is an example of output from the **show ipv6 mld snooping mrouter vlan** command. It shows multicast switch ports for a specific VLAN.

```
Switch> show ipv6 mld snooping mrouter vlan 100
Vlan    ports
----    -
    2    Gi1/0/11(dynamic)
```

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 <i>vlan-id</i> (Optional) Specifies a VLAN; the range is 1 to 1001 and 1006 to 4094.				
Command Modes	User EXEC mode				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.2(40)SG</td> <td>This command was introduced on the Catalyst 4500.</td> </tr> </tbody> </table>	Release	Modification	12.2(40)SG	This command was introduced on the Catalyst 4500.
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 switches but has only one MLD querier. The querier can be a Layer 3 switch.

The **show ipv6 mld snooping querier** command output also shows the VLAN and interface on which the querier was detected. If the querier is the switch, the output shows the *Port* field as *Router*. If the querier is a router, the output shows the port number on which the querier is learned in the *Port* field.

The output of the **show ipv6 mld snoop 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 VLAN values, such as the snooping robustness variable on the particular VLAN. This querier information is used only on the MASQ message that is sent by the switch. It does not override the user-configured robustness variable that is used for aging out a member that does not respond to query messages.

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

Examples

This is an example of output from the **show ipv6 mld snooping querier** command:

```
Switch> show ipv6 mld snooping querier
Vlan      IP Address                MLD Version Port
-----
2         FE80::201:C9FF:FE40:6000 v1      Gi3/0/1
```

This is an example of output from the **show ipv6 mld snooping querier vlan** command:

```
Switch> show ipv6 mld snooping querier vlan 2
IP address : FE80::201:C9FF:FE40:6000
MLD version : v1
Port : Gi3/0/1
Max response time : 1000s
```

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.
	<i>client_id</i>	(Optional) Identifies the client registered to the ISSU infrastructure. To obtain a list of client IDs, use the show issu clients command.

Command Default 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 (clientid=2082):

```
Switch# show issu capability types 2082
Client_ID = 2082, Entity_ID = 1 :
    Cap_Type = 0
Switch#
```

The following example shows how to display the ISSU capabilities entries for the IP host ISSU client (clientid=2082):

```
Switch# show issu capability entries 2082
Client_ID = 2082, Entity_ID = 1 :
    Cap_Entry = 1 :
        Cap_Type = 0
Switch#
```

The following example shows how to display the ISSU capabilities groups for the IP host ISSU client (clientid=2082):

```
Switch# show issu capability groups 2082
Client_ID = 2082, Entity_ID = 1 :
  Cap_Group = 1 :
    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	<i>peer_uid</i>	(Optional) Displays a list of clients registered to ISSU infrastructure at the peer supervisor engine.
---------------------------	-----------------	--

Command Default	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(31)SGA	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 = 2, Client_Name = ISSU Proto client, Entity_Count = 1
Client_ID = 3, Client_Name = ISSU RF, Entity_Count = 1
Client_ID = 4, Client_Name = ISSU CF client, Entity_Count = 1
Client_ID = 5, Client_Name = ISSU Network RF client, Entity_Count = 1
Client_ID = 7, Client_Name = ISSU CONFIG SYNC, Entity_Count = 1
Client_ID = 8, Client_Name = ISSU ifIndex sync, Entity_Count = 1
Client_ID = 9, Client_Name = ISSU IPC client, Entity_Count = 1
Client_ID = 10, Client_Name = ISSU IPC Server client, Entity_Count = 1
Client_ID = 11, Client_Name = ISSU Red Mode Client, Entity_Count = 1
Client_ID = 100, Client_Name = ISSU rfs client, Entity_Count = 1
Client_ID = 110, Client_Name = ISSU ifs client, Entity_Count = 1
Client_ID = 200, Client_Name = ISSU Event Manager client, Entity_Count = 1
Client_ID = 2002, Client_Name = CEF Push ISSU client, Entity_Count = 1
Client_ID = 2003, Client_Name = ISSU XDR client, Entity_Count = 1
Client_ID = 2004, Client_Name = ISSU SNMP client, Entity_Count = 1
Client_ID = 2010, Client_Name = ARP HA, Entity_Count = 1
Client_ID = 2012, Client_Name = ISSU HSRP Client, Entity_Count = 1
Client_ID = 2021, Client_Name = XDR Int Priority ISSU client, Entity_Count = 1
Client_ID = 2022, Client_Name = XDR Proc Priority ISSU client, Entity_Count = 1
Client_ID = 2023, Client_Name = FIB HWIDB ISSU client, Entity_Count = 1
Client_ID = 2024, Client_Name = FIB IDB ISSU client, Entity_Count = 1
Client_ID = 2025, Client_Name = FIB HW subblock ISSU client, Entity_Count = 1
Client_ID = 2026, Client_Name = FIB SW subblock ISSU client, Entity_Count = 1
Client_ID = 2027, Client_Name = Adjacency ISSU client, Entity_Count = 1
Client_ID = 2028, Client_Name = FIB IPV4 ISSU client, Entity_Count = 1
```

```

Client_ID = 2054, Client_Name = ISSU process client, Entity_Count = 1
Client_ID = 2058, Client_Name = ISIS ISSU RTR client, Entity_Count = 1
Client_ID = 2059, Client_Name = ISIS ISSU UPD client, Entity_Count = 1
Client_ID = 2067, Client_Name = ISSU PM Client, Entity_Count = 1
Client_ID = 2068, Client_Name = ISSU PAGP_SWITCH Client, Entity_Count = 1
Client_ID = 2070, Client_Name = ISSU Port Security client, Entity_Count = 1
Client_ID = 2071, Client_Name = ISSU Switch VLAN client, Entity_Count = 1
Client_ID = 2072, Client_Name = ISSU dot1x client, Entity_Count = 1
Client_ID = 2073, Client_Name = ISSU STP, Entity_Count = 1
Client_ID = 2077, Client_Name = ISSU STP MSTP, Entity_Count = 1
Client_ID = 2078, Client_Name = ISSU STP IEEE, Entity_Count = 1
Client_ID = 2079, Client_Name = ISSU STP RSTP, Entity_Count = 1
Client_ID = 2081, Client_Name = ISSU DHCP Snooping client, Entity_Count = 1
Client_ID = 2082, Client_Name = ISSU IP Host client, Entity_Count = 1
Client_ID = 2083, Client_Name = ISSU Inline Power client, Entity_Count = 1
Client_ID = 2084, Client_Name = ISSU IGMP Snooping client, Entity_Count = 1
Client_ID = 4001, Client_Name = ISSU C4K Chassis client, Entity_Count = 1
Client_ID = 4002, Client_Name = ISSU C4K Port client, Entity_Count = 1
Client_ID = 4003, Client_Name = ISSU C4K Rkios client, Entity_Count = 1
Client_ID = 4004, Client_Name = ISSU C4K HostMan client, Entity_Count = 1
Client_ID = 4005, Client_Name = ISSU C4k GaliosRedundancy client, Entity_Count = 1

```

Base Clients:

```

Client_Name = ISSU Proto client
Client_Name = ISSU RF
Client_Name = ISSU CF client
Client_Name = ISSU Network RF client
Client_Name = ISSU CONFIG SYNC
Client_Name = ISSU ifIndex sync
Client_Name = ISSU IPC client
Client_Name = ISSU IPC Server client
Client_Name = ISSU Red Mode Client
Client_Name = ISSU rfs client
Client_Name = ISSU ifs client
Client_Name = ISSU Event Manager client
Client_Name = CEF Push ISSU client
Client_Name = ISSU XDR client
Client_Name = ARP HA
Client_Name = XDR Int Priority ISSU client
Client_Name = XDR Proc Priority ISSU client
Client_Name = FIB HWIDB ISSU client
Client_Name = FIB IDB ISSU client
Client_Name = FIB HW subblock ISSU client
Client_Name = FIB SW subblock ISSU client
Client_Name = Adjacency ISSU client
Client_Name = FIB IPV4 ISSU client
Client_Name = ISSU process client
Client_Name = ISSU PM Client
Client_Name = ISSU C4K Chassis client
Client_Name = ISSU C4K Port client
Client_Name = ISSU C4K Rkios client
Client_Name = ISSU C4K HostMan client
Client_Name = ISSU C4k GaliosRedundancy client

```

Related Commands

Command	Description
show issu capability	Displays the ISSU capability for a client.
show issu entities	Displays the ISSU entity 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 | xml }
```

Syntax Description

negotiated	Displays negotiated compatibility matrix information.
stored	Displays stored compatibility matrix information.
xml	Displays negotiated compatibility matrix information in XML format.

Command Default

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 impact.
- **Base-Level Compatible**—One or more of the optional HA-aware subsystems are not compatible. Although an in-service upgrade or downgrade between these versions will succeed, some subsystems will not be able to maintain their state during the switchover. Prior to attempting an in-service upgrade or downgrade, the impact of this on operation and service of the switch must be considered carefully.

- **Incompatible**—A set of core system infrastructure must be able to execute in a stateful manner for SSO to function correctly. If any of these “required” features or subsystems is not compatible in two different Cisco IOS images, the two versions of the Cisco IOS images are declared “Incompatible”. This means that an in-service upgrade or downgrade between these versions is not possible. The systems operates in RPR mode during the period when the versions of Cisco IOS at the active and standby supervisor engines differ.

Examples

This example displays negotiated compatibility matrix information:

```
Switch# show issu comp-matrix negotiated
```

```
CardType: WS-C4507R(112), Uid: 2, Image Ver: 12.2(31)SGA
Image Name: cat4500-ENTSERVICES-M
```

Cid	Eid	Sid	pSid	pUid	Compatibility
2	1	262151	3	1	COMPATIBLE
3	1	262160	5	1	COMPATIBLE
4	1	262163	9	1	COMPATIBLE
5	1	262186	25	1	COMPATIBLE
7	1	262156	10	1	COMPATIBLE
8	1	262148	7	1	COMPATIBLE
9	1	262155	1	1	COMPATIBLE
10	1	262158	2	1	COMPATIBLE
11	1	262172	6	1	COMPATIBLE
100	1	262166	13	1	COMPATIBLE
110	113	262159	14	1	COMPATIBLE
200	1	262167	24	1	COMPATIBLE
2002	1	-	-	-	UNAVAILABLE
2003	1	262185	23	1	COMPATIBLE
2004	1	262175	16	1	COMPATIBLE
2008	1	262147	26	1	COMPATIBLE
2008	1	262168	27	1	COMPATIBLE
2010	1	262171	32	1	COMPATIBLE
2012	1	262180	31	1	COMPATIBLE
2021	1	262170	41	1	COMPATIBLE
2022	1	262152	42	1	COMPATIBLE
2023	1	-	-	-	UNAVAILABLE
2024	1	-	-	-	UNAVAILABLE
2025	1	-	-	-	UNAVAILABLE
2026	1	-	-	-	UNAVAILABLE
2027	1	-	-	-	UNAVAILABLE
2028	1	-	-	-	UNAVAILABLE
2054	1	262169	8	1	COMPATIBLE
2058	1	262154	29	1	COMPATIBLE
2059	1	262179	30	1	COMPATIBLE
2067	1	262153	12	1	COMPATIBLE
2068	1	196638	40	1	COMPATIBLE
2070	1	262145	21	1	COMPATIBLE
2071	1	262178	11	1	COMPATIBLE
2072	1	262162	28	1	COMPATIBLE
2073	1	262177	33	1	COMPATIBLE
2077	1	262165	35	1	COMPATIBLE
2078	1	196637	34	1	COMPATIBLE
2079	1	262176	36	1	COMPATIBLE
2081	1	262150	37	1	COMPATIBLE
2082	1	262161	39	1	COMPATIBLE
2083	1	262184	20	1	COMPATIBLE
2084	1	262183	38	1	COMPATIBLE
4001	101	262181	17	1	COMPATIBLE
4002	201	262164	18	1	COMPATIBLE

```

4003 301 262182 19 1 COMPATIBLE
4004 401 262146 22 1 COMPATIBLE
4005 1 262149 4 1 COMPATIBLE

```

Message group summary:

Cid	Eid	GrpId	Sid	pSid	pUid	Nego Result
2	1	1	262151	3	1	Y
3	1	1	262160	5	1	Y
4	1	1	262163	9	1	Y
5	1	1	262186	25	1	Y
7	1	1	262156	10	1	Y
8	1	1	262148	7	1	Y
9	1	1	262155	1	1	Y
10	1	1	262158	2	1	Y
11	1	1	262172	6	1	Y
100	1	1	262166	13	1	Y
110	113	115	262159	14	1	Y
200	1	1	262167	24	1	Y
2002	1	2	-	-	-	N - did not negotiate
2003	1	1	262185	23	1	Y
2004	1	1	262175	16	1	Y
2008	1	1	262147	26	1	Y
2008	1	2	262168	27	1	Y
2010	1	1	262171	32	1	Y
2012	1	1	262180	31	1	Y
2021	1	1	262170	41	1	Y
2022	1	1	262152	42	1	Y
2023	1	1	-	-	-	N - did not negotiate
2024	1	1	-	-	-	N - did not negotiate
2025	1	1	-	-	-	N - did not negotiate
2026	1	1	-	-	-	N - did not negotiate
2027	1	1	-	-	-	N - did not negotiate
2028	1	1	-	-	-	N - did not negotiate
2054	1	1	262169	8	1	Y
2058	1	1	262154	29	1	Y
2059	1	1	262179	30	1	Y
2067	1	1	262153	12	1	Y
2068	1	1	196638	40	1	Y
2070	1	1	262145	21	1	Y
2071	1	1	262178	11	1	Y
2072	1	1	262162	28	1	Y
2073	1	1	262177	33	1	Y
2077	1	1	262165	35	1	Y
2078	1	1	196637	34	1	Y
2079	1	1	262176	36	1	Y
2081	1	1	262150	37	1	Y
2082	1	1	262161	39	1	Y
2083	1	1	262184	20	1	Y
2084	1	1	262183	38	1	Y
4001	101	1	262181	17	1	Y
4002	201	1	262164	18	1	Y
4003	301	1	262182	19	1	Y
4004	401	1	262146	22	1	Y
4005	1	1	262149	4	1	Y

List of Clients:

Cid	Client Name	Base/Non-Base
2	ISSU Proto client	Base
3	ISSU RF	Base
4	ISSU CF client	Base
5	ISSU Network RF client	Base
7	ISSU CONFIG SYNC	Base

```

8      ISSU ifIndex sync      Base
9      ISSU IPC client        Base
10     ISSU IPC Server client Base
11     ISSU Red Mode Client   Base
100    ISSU rfs client        Base
110    ISSU ifs client        Base
200    ISSU Event Manager clientBase
2002   CEF Push ISSU client   Base
2003   ISSU XDR client        Base
2004   ISSU SNMP client       Non-Base
2008   ISSU Tableid Client    Base
2010   ARP HA                 Base
2012   ISSU HSRP Client       Non-Base
2021   XDR Int Priority ISSU cliBase
2022   XDR Proc Priority ISSU clBase
2023   FIB HWIDB ISSU client   Base
2024   FIB IDB ISSU client    Base
2025   FIB HW subblock ISSU clieBase
2026   FIB SW subblock ISSU clieBase
2027   Adjacency ISSU client   Base
2028   FIB IPV4 ISSU client    Base
2054   ISSU process client     Base
2058   ISIS ISSU RTR client    Non-Base
2059   ISIS ISSU UPD client    Non-Base
2067   ISSU PM Client         Base
2068   ISSU PAGP_SWITCH Client Non-Base
2070   ISSU Port Security clientNon-Base
2071   ISSU Switch VLAN client Non-Base
2072   ISSU dot1x client       Non-Base
2073   ISSU STP                Non-Base
2077   ISSU STP MSTP          Non-Base
2078   ISSU STP IEEE           Non-Base
2079   ISSU STP RSTP          Non-Base
2081   ISSU DHCP Snooping clientNon-Base
2082   ISSU IP Host client     Non-Base
2083   ISSU Inline Power client Non-Base
2084   ISSU IGMP Snooping clientNon-Base
4001   ISSU C4K Chassis client Base
4002   ISSU C4K Port client    Base
4003   ISSU C4K Rkios client   Base
4004   ISSU C4K HostMan client Base
4005   ISSU C4k GaliosRedundancyBase

```

This example displays stored compatibility matrix information:

```
Switch> show issu comp-matrix stored
```

```
Number of Matrices in Table = 1
```

```
(1) Matrix for cat4500-ENTSERVICES-M(112) - cat4500-ENTSERVICES-M(112)
```

```
=====
```

```
Start Flag (0xDEADBABE)
```

```

My Image ver: 12.2(31)SGA
Peer Version   Compatibility
-----
12.2(31)SGA           Comp(3)

```

Related Commands	Command	Description
	show issu clients	Displays the ISSU clients.
	show issu sessions	Displays ISSU session information for a specified client.

show issu endpoints

To display the ISSU endpoint information, use the **show issu endpoints** command.

show issu endpoints

Syntax Description This command has no arguments or keywords

Command Default 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 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
My_Unique_ID = 1/0x1, Client_Count = 46

This endpoint communicates with 1 peer endpoints :
Peer_Unique_ID    CAP    VER    XFORM    ERP    Compatibility
                2/0x2    1      1      1      1      Same

Shared Negotiation Session Info :
Nego_Session_ID = 15
Nego_Session_Name = shared nego session
Transport_Mtu = 4096
Ses_In_Use = 2
Switch#
```

Related Commands	Command	Description
	show issu clients	Displays the ISSU clients.

show issu entities

To display the ISSU entity information, use the **show issu entities** command.

```
show issu entities [client_id]
```

Syntax Description	<i>client_id</i> (Optional) ISSU client ID.
---------------------------	---

Command Default	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 2072
Client_ID = 2072 :
  Entity_ID = 1, Entity_Name = ISSU dot1x entity :
    MsgType MsgGroup CapType CapEntry CapGroup
    Count   Count   Count   count   Count
    28      1       1       1       1
Switch#
```

Related Commands	Command	Description
	show issu clients	Displays the ISSU clients.

show issu fsm



Note

This command is not intended for end-users.

To display the ISSU finite state machine (FSM) information corresponding to an ISSU session, use the **show issu fsm** command.

```
show issu fsm [session_id]
```

Syntax Description

<i>session_id</i>	(Optional) Provides detailed information about the FSM for the specified session.
-------------------	---

Command Default

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.

Examples

The following example displays and verifies the ISSU state after LOADVERSION:

```
Switch# show issu fsm 26
Session_ID = 26 :
  FSM_Name      Curr_State      Old_State      Error_Reason
  FSM_L1        TRANS          A_VER         none
  FSM_L2_HELLO  EXIT           RCVD          none
  FSM_L2_A_CAP  A_EXIT        A_RSP         none
  FSM_L2_P_CAP  P_INIT        unknown       none
  FSM_L2_A_VER  A_EXIT        A_RES_RSP     none
  FSM_L2_P_VER  P_INIT        unknown       none
  FSM_L2_TRANS  COMP          COMP          none
Current FSM is FSM_L2_TRANS
Session is compatible
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.

Command Default If client ID is not specified, displays message groups or message types information for all clients registered to the ISSU infrastructure.

Command Modes User EXEC mode

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

Usage Guidelines Messages are sync-data (also known as checkpoint data) sent between two endpoints. When an ISSU-aware client establishes its session with a peer, an ISSU negotiation takes place. The ISSU infrastructure uses the registered information to negotiate the capabilities and the message version to be used during the session.

Examples The following example shows how to display the message groups for Client_id 2082:

```
Switch#show issu message groups 2082
Client_ID = 2082, Entity_ID = 1 :
  Message_Group = 1 :
    Message_Type = 1, Version_Range = 1 ~ 2
    Message_Type = 2, Version_Range = 1 ~ 2
Switch#
```

The following example shows how to display the message types for Client_id 2082:

```
Switch#show issu message types 2082
Client_ID = 2082, Entity_ID = 1 :
  Message_Type = 1, Version_Range = 1 ~ 2
    Message_Ver = 1, Message_Mtu = 12
    Message_Ver = 2, Message_Mtu = 8
  Message_Type = 2, Version_Range = 1 ~ 2
    Message_Ver = 1, Message_Mtu = 32
    Message_Ver = 2, Message_Mtu = 28
Switch#
```

■ show issu message

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.

Command Default Displays negotiated capability or version information for all ISSU sessions.

Command Modes User EXEC mode

Command History	Release	Modification
	12.2(31)SGA	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 26
Session_ID = 26 :
  Cap_Type = 0,      Cap_Result = 1      No cap value assigned

Switch# show issu negotiated version 26
Session_ID = 26 :
  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.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.2(31)SGA	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 = Not in progress
      Configured Rollback Time = 45:00
Switch#
```

Related Commands	Command	Description
	issu acceptversion	Halts the rollback timer and ensures that the new Cisco IOS software image is not automatically stopped during the ISSU process.
	issu runversion	Forces a change from the active supervisor engine to the standby supervisor engine and causes the newly active supervisor engine to run the new image specified in the issu loadversion command.

show issu sessions

To display ISSU session information for a specified client, use the **show issu sessions** command.

```
show issu sessions [client_id]
```

Syntax Description	<i>client_id</i> (Optional) Specifies the ISSU client ID.
---------------------------	---

Command Default	Displays session 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 Session is bidirectional and a reliable connection is established between two endpoints. Sync-data 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 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 rollback-timer status:

```
Switch#show issu sessions 2072
Client_ID = 2072, Entity_ID = 1 :

*** Session_ID = 26, Session_Name = dot1x :

    Peer   Peer   Negotiate   Negotiated   Cap      Msg      Session
  UniqueID Sid   Role        Result       GroupID  GroupID  Signature
    2       26   PRIMARY    COMPATIBLE   1        1        0
                                (no policy)

Negotiation Session Info for This Message Session:
  Nego_Session_ID = 26
  Nego_Session_Name = dot1x
  Transport_Mtu = 17884
Switch#
```

Related Commands	Command	Description
	show issu clients	Displays the ISSU clients.

show issu state

To display the ISSU state and current booted image name during the ISSU process, use the **show issu state** command.

```
show issu state [slot_number] [detail]
```

Syntax Description	
<i>slot_number</i>	(Optional) Specifies the slot number whose ISSU state needs to be displayed (1 or 2).
detail	(Optional) Provides detailed information about the state of the active and standby supervisor engines.

Command Default The command displays the ISSU state and current booted image name of both the active and standby supervisor engines.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.2(31)SGA	This command was introduced on the Catalyst 4500 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 LOADVERSION:

```
Switch# show issu state detail
      Slot = 1
      RP State = Active
      ISSU State = Load Version
      Boot Variable = bootflash:old_image,12
      Operating Mode = Stateful Switchover
      Primary Version = bootflash:old_image
      Secondary Version = bootflash:new_image
      Current Version = bootflash:old_image

      Slot = 2
      RP State = Standby
      ISSU State = Load Version
      Boot Variable = bootflash:new_image,12;bootflash:old_image,12
      Operating Mode = Stateful Switchover
      Primary Version = bootflash:old_image
      Secondary Version = bootflash:new_image
      Current Version = bootflash:new_image

Switch#
```

Related Commands	Command	Description
	issu abortversion	Cancels the ISSU upgrade or the downgrade process in progress and restores the switch to its state before the start of the process.
	issu acceptversion	Halts the rollback timer and ensures that the new Cisco IOS software image is not automatically stopped during the ISSU process.
	issu commitversion	Loads the new Cisco IOS software image into the new standby supervisor engine.
	issu loadversion	Starts the ISSU process.
	issu runversion	Forces a change from the active supervisor engine to the standby supervisor engine and causes the newly active supervisor engine to run the new image specified.

show l2protocol-tunnel

To display information about the Layer 2 protocol tunnel ports, use the **show l2protocol-tunnel** command. This command displays information for the interfaces with protocol tunneling enabled.

```
show l2protocol-tunnel [interface interface-id] [[summary] | {begin | exclude | include}
expression]
```

Syntax Description

interface <i>interface-id</i>	(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 <i>expression</i> .
exclude	(Optional) Displays information that excludes lines that match the <i>expression</i> .
include	(Optional) Displays the lines that match the specified <i>expression</i> .
<i>expression</i>	(Optional) Expression in the output to use as a reference point.

Command Modes

User EXEC mode

Command History

Release	Modification
12.2(18)EW	This command was first introduced on the Catalyst 4500 series switch.
12.2(25)EW	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 l2protocol-tunnel** command:

```
Switch> show l2protocol-tunnel
COS for Encapsulated Packets: 5

Port      Protocol Shutdown Drop      Encapsulation Decapsulation Drop
          Threshold Threshold Counter      Counter      Counter
-----
Fa0/10    ---          ----          ----          ----          ----
          stp          ----          ----  9847          1866          0
          vtp          ----          ----   77           12            0
          pagp         ----          ----  859           860           0
          lacp         ----          ----    0            0             0
          udld         ----          ----  219           211           0
Fa0/11    cdp          1100          ----  2356          2350          0
          stp          1100          ----  116           13            0
          vtp          1100          ----    3            67            0
          pagp         ----          900 856          5848          0
          lacp         ----          900 0           0             0
          udld         ----          900 0           0             0
Fa0/12    cdp          ----          ----  2356          0             0
          stp          ----          ---- 11787          0             0
          vtp          ----          ----   81            0             0
          pagp         ----          ----    0            0             0
          lacp         ----          ----  849           0             0
          udld         ----          ----    0            0             0
Fa0/13    cdp          ----          ----  2356          0             0
          stp          ----          ---- 11788          0             0
          vtp          ----          ----   81            0             0
          pagp         ----          ----    0            0             0
          lacp         ----          ----  849           0             0
          udld         ----          ----    0            0             0

Switch#
```

This is an example of output from the **show l2protocol-tunnel summary** command:

```
Switch> show l2protocol-tunnel summary
COS for Encapsulated Packets: 5

Port      Protocol      Shutdown Drop      Status
          Threshold Threshold
          (cdp/stp/vtp) (cdp/stp/vtp)
          (pagp/lacp/udld) (pagp/lacp/udld)
-----
Fa0/10    --- stp vtp ----/----/---- ----/----/---- up
          pagp lacp udld ----/----/---- ----/----/----
Fa0/11    cdp stp vtp 1100/1100/1100 ----/----/---- up
          pagp lacp udld ----/----/---- 900/ 900/ 900
Fa0/12    cdp stp vtp ----/----/---- ----/----/---- up
          pagp lacp udld ----/----/---- ----/----/----
Fa0/13    cdp stp vtp ----/----/---- ----/----/---- up
          pagp lacp udld ----/----/---- ----/----/----
Fa0/14    cdp stp vtp ----/----/---- ----/----/---- down
          pagp ---- udld ----/----/---- ----/----/----
Fa0/15    cdp stp vtp ----/----/---- ----/----/---- down
          pagp ---- udld ----/----/---- ----/----/----
Fa0/16    cdp stp vtp ----/----/---- ----/----/---- down
          pagp lacp udld ----/----/---- ----/----/----
Fa0/17    cdp stp vtp ----/----/---- ----/----/---- down
          pagp lacp udld ----/----/---- ----/----/----

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	
<i>channel-group</i>	(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.
sys-id	Displays the LACP system identification.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

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

Usage Guidelines If you do not specify a *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 **sys-id** keyword.

Examples The following example shows how to display LACP statistical information for a specific channel group:

```
Switch# show lacp 1 counters
          LACPDU          Marker          LACPDU
Port      Sent  Recv      Sent  Recv      Pkts  Err
-----
Channel group: 1
  Fa4/1    8    15         0    0         3    0
  Fa4/2   14   18         0    0         3    0
  Fa4/3   14   18         0    0         0
  Fa4/4   13   18         0    0         0
Switch#
```

The output displays the following information:

- The LACPDU Sent and Recv columns display the LACPDU sent and received on each specific interface.
- The LACPDU Pkts and Err columns display the marker protocol packets.

The following example shows how to display internal information for the interfaces belonging to a specific channel:

```
Switch# show lacp 1 internal
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

```

Port	Flags	State	LACPDUs Interval	LACP Port Priority	Admin Key	Oper Key	Port Number	Port State
Fa4/1	saC	bndl	30s	32768	100	100	0xc1	0x75
Fa4/2	saC	bndl	30s	32768	100	100	0xc2	0x75
Fa4/3	saC	bndl	30s	32768	100	100	0xc3	0x75
Fa4/4	saC	bndl	30s	32768	100	100	0xc4	0x75

```
Switch#
```

Table 2-36 lists the output field definitions.

Table 2-36 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: <ul style="list-style-type: none"> <i>bndl</i>—Port is attached to an aggregator and bundled with other ports. <i>susp</i>—Port is in a suspended state; it is not attached to any aggregator. <i>indep</i>—Port is in an independent state (not bundled but able to switch data traffic. In this case, LACP is not running on the partner port). <i>hot-sby</i>—Port is in a hot-standby state. <i>down</i>—Port is down.
LACPDUs Interval	Interval setting.
LACP Port Priority	Port priority setting.
Admin Key	Administrative key.
Oper Key	Operator key.
Port Number	Port number.
Port State	State variables for the port encoded as individual bits within a single octet with the following meaning [1]: <ul style="list-style-type: none"> bit0: <i>LACP_Activity</i> bit1: <i>LACP_Timeout</i> bit2: <i>Aggregation</i> bit3: <i>Synchronization</i> bit4: <i>Collecting</i> bit5: <i>Distributing</i> bit6: <i>Defaulted</i> bit7: <i>Expired</i>

The following example shows how to display LACP neighbors information for a specific port channel:

```
Switch# show lacp 1 neighbor
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

Port      Partner                               Partner
System ID System ID                               Port Number  Age    Flags
Fa4/1     8000,00b0.c23e.d84e                    0x81         29s   P
Fa4/2     8000,00b0.c23e.d84e                    0x82         0s    P
Fa4/3     8000,00b0.c23e.d84e                    0x83         0s    P
Fa4/4     8000,00b0.c23e.d84e                    0x84         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 braces.

The following example shows how to display the LACP 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 license

To display information about the software license, use the **show license** command.

.show license [**agent** [**counters** | **session**] [**all** | **detail** [*feature-name*] | **feature** | **file** | **statistics** | **status** | **udi** | **right-to-use** | **summary** | **permanent** | **in-use** | **image levels** | **evaluation** | **expiring**]

Syntax Description

agent	Shows information about the software license agent.
all	Shows information about all licenses in the system.
detail <i>feature-name</i>	Shows detailed information about a specified licensed feature or about all licenses.
feature	Shows a list of licensed features available in an image
file	Shows license entries stored in the license file.
statistics	Shows license statistics information.
status	Shows information about supported license types and license operations, and provides device status.
udi	Shows all the unique device identifier (UDI) values that can be licensed in a system
right-to-use	Shows all PRTU licenses.
summary	Shows a brief summary of all licenses.
permanent	Show all available permanent licenses
in-use	Show all available in-use licenses
image levels	Shows license image levels
evaluation	Shows all evaluation licenses.
expiring	Shows all available expiring licenses.

Command Default

License-related information is not displayed

Command Modes

Privileged EXEC mode

Command History

Release	Modification
IOS XE 3.1.0	Support for show license introduced on the Catalyst 4500 series switches.
IOS XE 3.4.2	Keyword right-to-use introduced on the Catalyst 4500 series switches

Usage Guidelines

Use this command to display license information and to help with troubleshooting issues related to Cisco IOS software licenses. It displays all the licenses in the system.

This command also displays those features that are available but not licensed to execute (i.e., multiple license can be active but not in use (execute) simultaneously). Only one type license can be used at a given time. Output is grouped according to how the features are stored in license storage (i.e., where license information is stored on the device).

Examples).

These are examples of output from the `show license agent` command:

```
Switch# show license agent counters
License Agent Counters
Request Messages Received:0: Messages with Errors:0
Request Operations Received:0: Operations with Errors:0
Notification Messages Sent:1: Transmission Errors:0

Switch# show license agent session
License Agent Sessions: 0 open, maximum is 9

Switch# show license ?
agent show license agent
all Displays All The License(s).
call-home Show license call-home information
detail Displays Details Of A Given License.
evaluation Displays Evaluation License(s)
expiring Displays Expiring License(s).
feature Displays License Enabled Features.
file Displays All The License File(s).
handle show license handle
image show license image level
in-use Displays License That Are In-Use.
permanent Displays Permanent License(s)
right-to-use show permanent right-to-use licenses
statistics Displays License Statistics.
status Displays License Status.
summary Displays Brief Summary Of All License(s).
udi Displays UDI Value
```

This is an example of output from the `show license detail` command:

```
Switch# show license detail
Index: 1 Feature: entservices Version: 1.0
License Type: Evaluation
Evaluation total period: 8 weeks 4 days
Evaluation period left: 8 weeks 3 days
License State: Active, Not in Use, EULA accepted
License Count: Non-Counted
License Priority: Low
Store Index: 0
Store Name: Dynamic Evaluation License Storage
Index: 2 Feature: entservices Version: 1.0
License Type: PermanentRightToUse
License State: Inactive
License Count: Non-Counted
Store Index: 1
Store Name: Dynamic Evaluation License Storage
Index: 3 Feature: ipbase Version: 1.0
License Type: PermanentRightToUse
License State: Active, Not in Use, EULA accepted
License Count: Non-Counted
Store Index: 3
Store Name: Dynamic Evaluation License Storage
Index: 4 Feature: ipbase Version: 1.0
License Type: Evaluation
Evaluation total period: 8 weeks 4 days
Evaluation period left: 8 weeks 3 days
License State: Inactive
License Count: Non-Counted
License Priority: Low
Store Index: 2
Store Name: Dynamic Evaluation License Storage
```

This is an example of output from the **show license detail entservices** command:

```
Switch# show license detail entservices
Feature: entservices Period Left: 8 weeks 3 days
Index: 1 Feature: entservices Version: 1.0
License Type: Evaluation
Evaluation total period: 8 weeks 4 days
Evaluation period left: 8 weeks 3 days
License State: Active, Not in Use, EULA accepted
License Count: Non-Counted
License Priority: Low
Store Index: 0
Store Name: Dynamic Evaluation License Storage
Index: 2 Feature: entservices Version: 1.0
License Type: PermanentRightToUse
License State: Inactive
License Count: Non-Counted
Store Index: 1
Store Name: Dynamic Evaluation License Storage
```

This is an example of output from the **show license feature** command:

```
Switch# show license feature
Feature name Enforcement Evaluation Clear Allowed Enabled Right...
-----
entservices true true true false true
ipbase true true true true true
lanbase false false true false false
internal_service true false true false false
```

This is an example of output from the **show license file** command:

```
Switch# show license file
License Store: Primary License Storage
License Index: 1
License: 11 ipbase 1.0 LONG NORMAL STANDALONE EXCL INFINITE_KEYS INFINITE_KEYS NEVER NEVER
NiL SLM_CODE CL_ND_LCK NiL *1DELA9XDSFSJXAH400 NiL NiL NiL 5_MINS WS-C4507R+EFOX1327G52D
xLt5Q1e2VJi03pzp3GSE3PrvxwyfO,SLjP0SXuZ0q0f4QTYxc1pSQY51xj31fh7ZfTD6AskNyeUYT8sCUesi9IVKB8
5wsZSX1HZiXwOd9RHp3mjmhxFDnS0e6UxjgXgqvV:$AQEBIf8B///kh4dluXv+U+xjUPlzoc3++jpv9d8He4jOuba
fbkmmOtaOYAoB3inJLnLlyv50VCuRqwInXo3s+nsLU7rOtdOxoIxyZao3LYmUJ+MFzsqlhKoJv1PyEvQ8H21MNUjVb
hoN0gyIWsyiJaM8AQIkVBQFzhr10GYo1VzdzfJfEPQIx6tZ++/Vtc/q3SF/5Ko8XCY=
Comment:
Hash: Z+EY3ce1csQ1VpRGc5NNy5ypmds=
License Store: Dynamic License Storage
License Store: Primary License Storage
License Store: Dynamic License Storage
License Index: 0
License: 11 entservices 1.0 LONG TRIAL DISABLED 1440 DISABLED STANDALONE ADD INFINITE_KEYS
INFINITE_KEYS NEVER NEVER NiL SLM_CODE DEMO NiL NiL Ni NiL NiL 5_MINS NiL
BGf3gQnLuroDmnMjMwWVa2ukR8kP2JZyinkpmOXpa32jwPuSbmHvcSRiSSaqBngV8$AQEBIQAB///FTlc+Qu1Xlg2
Z+yB2StUHHymf2w5PEw+cYg/hTOKYCI+oXi0jwBZ2iLrYTKYwxSSRqwInXo3s+nsLU7rOtdOxoIxyZao3LYmUJ+MFz
sqlhKoJv1PyEvQ8H21MNUjVbhoN0gyIWsyiJaM8AQIkVBQFzhr10GYo1VzdzfJfEPQIx6tZ++/Vtc/q3SF/5Ko8XCY
=
Comment:
Hash: Rm09Kumi8BFKq0wCAx2CcUDE6rg=
License Index: 1
License: 12 entservices 1.0 LONG TRIAL DISABLED DISABLED DISABLED STANDALONE ADD
INFINITE_KEYS INFINITE_KEYS 1 JAN 2006 1 JAN 2035 NiL NiL SLM_CODE DEMO NiL NiL Ni NiL NiL
5_MINS NOTLOCKEDNOTLOCKEDHBL
11nG2zXePlBt,ifk7ZReL80LqzvzgrUCelWrBp41FC3jOKer6ZMT7XC4834W3Ev7fm1eXoWaK58t:oDeH5RI1V3dVE
2VpAnYb7WiKDz9En8PfrI7vewayNbschEXBD9:tfPfir6GaALUFwsLxcqYzHuL2$AQEBIf8B///mCS09+7kn+8zTC
3WX1YS9if+g0e8AjRRu1Jq3Kye4y8wv4c+Y9FHJ7Ro/mw7ERwqRqwInXo3s+nsLU7rOtdOxoIxyZao3LYmUJ+MFzsq
lhKoJv1PyEvQ8H21MNUjVbhoN0gyIWsyiJaM8AQIkVBQFzhr10GYo1VzdzfJfEPQIx6tZ++/Vtc/q3SF/5Ko8XCY=
Comment:
Hash: 9w09jAFGBzi2w6XQC1jLOBe2p+Y=
```



```

License Index: 2
License: 11 ipbase 1.0 LONG TRIAL DISABLED 1440 DISABLED STANDALONE ADD INFINITE_KEYS
INFINITE_KEYS NEVER NEVER NiL SLM_CODE DEMO NiL NiL Ni NiL NiL 5_MINS NiL
YXNJUtpFJiC2Rpd1t1SJNVQBCpQUBNT59tdkJJTgKwmLTKj:vmp,sVkmiiRYLFMHQfj$AQEBIf8B//kagzg0R7bT5rn
6dVYVPUFmxBlUslGgbkInHYo55DJzHE/Bqnlf9keNdSyzPbUhsRqWInXo3snsLU7rOtdOxoIxYZAo3LYmUJ+MFzsq
lhKoJv1PyEvQ8H21MNUjVbhoN0gyIwSyiJam8AQIkVBQFzhr10GYo1VzdzfJfEPQIx6tZ++/Vtc/q3SF/5Ko8XCy=
Comment:
Hash: H6zsXVLv9TF1mTffGm0tK4VHJ2Q=
License Index: 3
License: 12 ipbase 1.0 LONG TRIAL DISABLED DISABLED DISABLED STANDALONE ADD INFINITE_KEYS
INFINITE_KEYS 1 JAN 2006 1 JAN 2035 NiL NiL SLM_CODE DEMO NiL NiL Ni NiL NiL 5_MINS
NOTLOCKEDNOTLOCKEDHBL
Zh0GdIANT1XwW6LJgQ95LB0aCazzbsjSOL4HUaqcySLcOvcLq,d04oTgS8pJbHIO3BaD0tgELHog9egQWj9bCJ3,sm
2jRaJkgkhYKO9BrbwYLOA,m03Qe2E,TPJou8fms:LtvrfctzLbujmB0XcB68MPLm$AQEBIf8B//+08JwRWipzFjtWl
AIctclx+D6NlhKMyqS1hJoxCM1Txgw8BpmG5QQY5nCiE14CPvVKRqWInXo3s+nsLU7rOtdOxoIxYZAo3LYmUJ+MFzsq
lhKoJv1PyEvQ8H21MNUjVbhoN0gyIwSyiJam8AQIkVBQFzhr10GYo1VzdzfJfEPQIx6tZ++/Vtc/q3SF/5Ko8XCy=
Comment:
Hash: S3Ks+G07ueugA9hMFPkXGTF12So=

```

This is an example of output from the **show license statistics** command:

```

Switch# show license statistics
Administrative statistics
Install success count: 4
Install failure count: 1
Install duplicate count: 0
Comment add count: 0
Comment delete count: 0
Clear count: 0
Save count: 0
Save cred count: 0
Client status Request success count 1 Request failure count 0 Release count 0 Global
Notify count 1

```

This is an example of output from the **show license status** command:

```

Switch# show license status
License Type Supported
permanent Non-expiring node locked license
extension Expiring node locked license
evaluation Expiring non node locked license
License Operation Supported install Install license clear Clear license annotate Comment
license save Save license revoke Revoke license call-home License call-home Call-home
Operation Supported show pak Display license pak via call-home install Install license via
call-home revoke Revoke license via call-home resend Fetch license via call-home Device
status Device Credential type: IMAGE Device Credential Verification: PASS Rehost Type:
DC_OR_IC

```

When you enter the **show license udi** command on WS-C4507R+E, this output appears:

```

Switch# show license udi
Device# PID SN UDI
-----
*0 WS-C4507R+E FOX1327G52D WS-C4507R+E:FOX1327G52D

```



Note The **show license udi** command output shows details on the current switch.

Displays all the Right to use licenses present on the device and their status. It contains license details: license state, licenses currently in use, and whether the EULA is accepted by the user.

```

Switch# show license right-to-use
License Store: Built-In License Storage
StoreIndex: 1 Feature: ipservices Version: 1.0

```

```

License Type: PermanentRightToUse
License State: Active, Not in Use, EULA accepted
  Period used: 1 hour 50 minutes
License Priority: High
License Count: Non-Counted

```

This is an example of the **show license summary** command:

```

Switch# show license summary
Index 0 Feature: entservices
Period left: 8 weeks 3 days
License Type: Evaluation
License State: Active, Not in Use, EULA accepted
License Count: Non-Counted
License Priority: Low
Index 1 Feature: ipbase
Period left: Life time
License Type: Permanent
License State: Active, In Use
License Count: Non-Counted
License Priority: Medium
Index 2 Feature: lanbase
Period left: 0 seconds
Index 3 Feature: internal_service
Period left: 0 seconds

```

This is an example of the **show license evaluation** command:

```

Switch# show license evaluation
License Store: Primary License Storage
License Store: Dynamic License Storage
StoreIndex: 0 Feature: entservices Version: 1.0
License Type: Evaluation
Evaluation total period: 8 weeks 4 days
Evaluation period left: 8 weeks 3 days
License State: Active, Not in Use, EULA accepted
License Count: Non-Counted
License Priority: Low
StoreIndex: 2 Feature: ipbase Version: 1.0
License Type: Evaluation
Evaluation total period: 8 weeks 4 days
Evaluation period left: 8 weeks 4 days
License State: Inactive
License Count: Non-Counted
License Priority: None

```

This is an example of the **show license image levels** command:

```

Switch# show license image levels
Module name Image level Priority Configured Valid license
-----
WS-X45-SUP7-E entservices 1 NO entservices
ipbase 2 NO ipbase
lanbase 3 NO lanbase

Module Name Role Current Level Reboot Level
-----
WS-X45-SUP7-E Active ipbase ipbase

```

This is an example of the **show license expiring** command

```

Switch# show license expiring
License Store: Primary License Storage
License Store: Dynamic License Storage
StoreIndex: 0 Feature: entservices Version: 1.0

```

```
License Type: Evaluation
Evaluation total period: 8 weeks 4 days
Evaluation period left: 8 weeks 3 days
License State: Active, Not in Use, EULA accepted
License Count: Non-Counted
License Priority: Low
StoreIndex: 2 Feature: ipbase Version: 1.0
License Type: Evaluation
Evaluation total period: 8 weeks 4 days
Evaluation period left: 8 weeks 4 days
License State: Inactive
License Count: Non-Counted
License Priority: None
Switch#
```

This is an example of the **show license in-use** command

```
Switch# show license in-use
License Store: Primary License Storage
StoreIndex: 1 Feature: ipbase Version: 1.0
License Type: Permanent
License State: Active, In Use
License Count: Non-Counted
License Priority: Medium
License Store: Dynamic License Storage
```

show link state group

To display link state group information, use the **show link state group** command in user EXEC or privileged EXEC mode.

show link state group detail

Syntax Description	detail	Displays detailed information about the group.
--------------------	--------	--

Command Default	None
-----------------	------

Command Modes	User EXEC (>) Privileged EXEC (#)
---------------	--------------------------------------

Command History	Release	Modification
	15.1(1)S	This command was introduced.

Examples The following example displays the link-state group information:

```
Switch# enable
Switch# show link state group 1
Link State Group: 1 Status: Enabled, Down
Router> show link state group detail
(Up):Interface up (Dwn):Interface Down (Dis):Interface disabled
Link State Group: 1 Status: Enabled, Down
Upstream Interfaces : Gi3/5(Dwn) Gi3/6(Dwn)
Downstream Interfaces : Gi3/1(Dis) Gi3/2(Dis) Gi3/3(Dis) Gi3/4(Dis)
Link State Group: 2 Status: Enabled, Down
Upstream Interfaces : Gi3/15(Dwn) Gi3/16(Dwn) Gi3/17(Dwn)
Downstream Interfaces : Gi3/11(Dis) Gi3/12(Dis) Gi3/13(Dis) Gi3/14(Dis)
(Up):Interface up (Dwn):Interface Down (Dis):Interface disabled
```

Related Commands	Command	Description
	link state track	Configures the link state group and enables link state tracking.
	link state group	Configures the link state group and interface, as either an upstream or downstream interface in the group.

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 <i>interface</i>	Interface type; possible valid value is gigabitethernet .
<i>interface-number</i>	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(50)SG	This command was introduced.

Usage Guidelines

[Table 2-37](#) lists the fields in the **show mab** command.

Table 2-37 *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	Authorization status

[Table 2-38](#) lists the possible values for the state of the MAB state machine.

Table 2-38 *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 2-38 MAB State Machine Values (continued)

Authorizing	Intermediate	The state of the session during MAC-based authorization
Terminate	Terminal	The state of the session once a result has been obtained. For a session in terminal state, “TERMINATE” displays.

Table 2-39 lists the possible displayed values for the MAB authorization status.

Table 2-39 MAB Authorization 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 GigaEthernet1/3
-----
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 GigaEthernet1/3
-----
Mac-Auth-Bypass = Enabled
Inactivity Timeout = None
MAB Client List
-----
Client MAC = 000f.23c4.a401
MAB SM state = TERMINATE
Auth Status = AUTHORIZED
```

The following example shows how to display MAB information for a specific interface:

```
Switch# show mab interface GigaEthernet1/3
MAB details for GigaEthernet1/3
-----
Mac-Auth-Bypass = Enabled
Inactivity Timeout = None
```

The following example shows how to display detailed MAB information for a specific interface:

```
Switch# show mab interface gigabitethernet1/1 detail
MAB details for GigaEthernet1/1
-----
Mac-Auth-Bypass = Enabled
Inactivity Timeout = None
MAB Client List
-----
Client MAC = 000f.23c4.a401
MAB SM state = TERMINATE
Auth Status = AUTHORIZED
Switch#
```

Related Commands

Command	Description
mab	Enables and configures MAC authorization 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	<i>interface</i>	(Optional) Specifies the interface type; valid values are ethernet , fastethernet , gigabitethernet , tengigabitethernet , pos , atm , port-channel , and ge-wan .
	<i>interface-number</i>	(Optional) Specifies the port number.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.1(19)EW	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 The following example shows how to display the ACL configuration on interface fast 6/1:

```
Switch# show mac access-group interface fast 6/1
Interface FastEthernet6/1:
  Inbound access-list is simple-mac-acl
  Outbound access-list is not set
```

Related Commands	Command	Description
	access-group mode	Specifies the override modes (for example, VACL overrides PACL) and the non-override modes (for example, merge or strict mode).

show mac-address-table address

To display MAC address table information for a specific MAC address, use the **show mac-address-table address** command.

```
show mac-address-table address mac_addr [interface type slot/port | protocol protocol | vlan
vlan_id]
```

Syntax Description		
<i>mac_addr</i>		48-bit MAC address; the valid format is H.H.H.
interface <i>type slot/port</i>	(Optional)	Displays information for a specific interface; valid values for <i>type</i> are fastethernet , gigabitethernet , and tengigabitethernet .
protocol <i>protocol</i>	(Optional)	Specifies a protocol. See the “Usage Guidelines” section for more information.
vlan <i>vlan_id</i>	(Optional)	Displays entries for the specific VLAN only; valid values are from 1 to 4094.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.1(8a)EW	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 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 protocols.
- **assigned** specifies the assigned protocol entries.
- **other** specifies the other protocol entries.

Examples

The following example shows how to display MAC address table information for a specific MAC address:

```
Switch# show mac-address-table address 0030.94fc.0dff
Unicast Entries
  vlan  mac address      type          protocols          port
-----+-----+-----+-----+-----
    1   0030.94fc.0dff    static ip, ipx, assigned, other  Switch
Fa6/1   0030.94fc.0dff    static ip, ipx, assigned, other  Switch
Fa6/2   0030.94fc.0dff    static ip, ipx, assigned, other  Switch
Switch#
```

Related Commands

Command	Description
show mac-address-table aging-time	Displays MAC address table aging information.
show mac-address-table count	Displays the number of entries currently in the MAC address table.
show mac-address-table dynamic	Displays the dynamic MAC address table entries only.
show mac-address-table interface	Displays the MAC address table information for a specific interface.
show mac-address-table multicast	Displays information about the multicast MAC address table.
show mac-address-table protocol	Displays the MAC address table information that is based on the protocol.
show mac-address-table static	Displays the static MAC address table entries only.
show mac-address-table vlan	Displays information about the MAC address table for a specific VLAN.

show mac-address-table aging-time

To display the MAC address aging time, use the **show mac-address-table aging-time** command.

```
show mac-address-table aging-time [vlan vlan_id]
```

Syntax Description	vlan <i>vlan_id</i> (Optional) Specifies a VLAN; valid values are from 1 to 4094.
---------------------------	--

Command Default	This command has no default settings.
------------------------	---------------------------------------

Command Modes	Privileged EXEC mode
----------------------	----------------------

Command History	Release	Modification
	12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW	Support for extended addressing was added.

Examples The following example shows how to display the currently configured aging time for all VLANs:

```
Switch# show mac-address-table aging-time
Vlan    Aging Time
----    -
100     300
200     1000

Switch#
```

The following example shows how to display the currently configured aging time for a specific VLAN:

```
Switch# show mac-address-table aging-time vlan 100
Vlan    Aging Time
----    -
100     300

Switch#
```

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 <i>vlan_id</i> (Optional) Specifies a VLAN; valid values are from 1 to 4094.
---------------------------	--

Command Default	This command has no default settings.
------------------------	---------------------------------------

Command Modes	Privileged EXEC mode
----------------------	----------------------

Command History	Release	Modification
	12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW	Added support for extended VLAN addresses.

Examples	The following example shows how to display the entry count for a specific VLAN:
-----------------	---

```
Switch# show mac-address-table count vlan 1
MAC Entries for Vlan 1:
Dynamic Unicast Address Count:          0
Static Unicast Address (User-defined) Count: 0
Static Unicast Address (System-defined) Count: 1
Total Unicast MAC Addresses In Use:      1
Total Unicast MAC Addresses Available:    32768
Multicast MAC Address Count:             1
Total Multicast MAC Addresses Available:  16384
Switch#
```

Related Commands	Command	Description
	show mac-address-table address	Displays the information about the MAC-address table.
	show mac-address-table aging-time	Displays MAC address table aging information.
	show mac-address-table dynamic	Displays the dynamic MAC address table entries only.
	show mac-address-table interface	Displays the MAC address table information for a specific interface.
	show mac-address-table multicast	Displays information about the multicast MAC address table.
	show mac-address-table protocol	Displays the MAC address table information that is based on the protocol.

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 <i>mac_addr</i>	(Optional) Specifies a 48-bit MAC address; the valid format is H.H.H.
interface <i>type slot/port</i>	(Optional) Specifies an interface to match; valid values for <i>type</i> are fastethernet , gigabitethernet , and tengigabitethernet .
protocol <i>protocol</i>	(Optional) Specifies a protocol. See the “Usage Guidelines” section for more information.
vlan <i>vlan_id</i>	(Optional) Displays entries for a specific VLAN; valid values are from 1 to 4094.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.1(8a)EW	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 The keyword definitions for the *protocol* argument are as follows:

- **assigned** specifies assigned protocol entries.
- **ip** specifies IP protocol.
- **ipx** specifies IPX protocols.
- **other** specifies other protocol entries.

The **show mac-address-table dynamic** command output for an EtherChannel interface changes the port number designation (such as, 5/7) to a port group number (such as, Po80).

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

The following example shows how to display all the dynamic MAC address entries:

```
Switch# show mac-address-table dynamic
Unicast Entries
vlan  mac address      type      protocols      port
-----+-----+-----+-----+-----
  1    0000.0000.0201    dynamic  ip              FastEthernet6/15
  1    0000.0000.0202    dynamic  ip              FastEthernet6/15
  1    0000.0000.0203    dynamic  ip,assigned     FastEthernet6/15
  1    0000.0000.0204    dynamic  ip,assigned     FastEthernet6/15
  1    0000.0000.0205    dynamic  ip,assigned     FastEthernet6/15
  2    0000.0000.0101    dynamic  ip              FastEthernet6/16
  2    0000.0000.0102    dynamic  ip              FastEthernet6/16
  2    0000.0000.0103    dynamic  ip,assigned     FastEthernet6/16
  2    0000.0000.0104    dynamic  ip,assigned     FastEthernet6/16
  2    0000.0000.0105    dynamic  ip,assigned     FastEthernet6/16
Switch#
```

The following 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
Unicast Entries
vlan  mac address      type      protocols      port
-----+-----+-----+-----+-----
  1    0000.0000.0203    dynamic  ip,assigned     FastEthernet6/15
  1    0000.0000.0204    dynamic  ip,assigned     FastEthernet6/15
  1    0000.0000.0205    dynamic  ip,assigned     FastEthernet6/15
  2    0000.0000.0103    dynamic  ip,assigned     FastEthernet6/16
  2    0000.0000.0104    dynamic  ip,assigned     FastEthernet6/16
  2    0000.0000.0105    dynamic  ip,assigned     FastEthernet6/16
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	<i>type</i>	Interface type; valid values are ethernet , fastethernet , gigabitethernet , and tengigabitethernet .
	<i>slot/port</i>	Number of the slot and port.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.1(8a)EW	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 used by the routed ports, the routed port name is displayed in the “vlan” column not the internal VLAN number.

Examples The following example shows how to display MAC address table information for a specific interface:

```
Switch# show mac-address-table interface fastethernet6/16
Unicast Entries
  vlan  mac address      type      protocols      port
-----+-----+-----+-----+-----
   2    0000.0000.0101    dynamic  other          FastEthernet6/16
   2    0000.0000.0102    dynamic  other          FastEthernet6/16
   2    0000.0000.0103    dynamic  other          FastEthernet6/16
   2    0000.0000.0104    dynamic  other          FastEthernet6/16
   2    0000.0000.0105    dynamic  other          FastEthernet6/16
   2    0000.0000.0106    dynamic  other          FastEthernet6/16

Multicast Entries
  vlan  mac address      type      ports
-----+-----+-----+-----
   2    ffff.ffff.ffff    system  Fa6/16
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 learning

To display the status of MAC address learning for all VLANs or a specified VLAN, use the **show mac address-table learning** user EXEC command.

```
show mac address-table learning [vlan vlan-id] [ | { begin | exclude | include } expression]
```

Syntax Description		
vlan <i>vlan-id</i>	(Optional)	Displays information for a specific VLAN. The range is 1 to 4094.
 begin	(Optional)	Displays the line that matches the <i>expression</i> .
 exclude	(Optional)	Displays excluded lines that match the <i>expression</i> .
 include	(Optional)	Displays included lines that match the specified <i>expression</i> .
<i>expression</i>	(Optional)	Specifies the expression in the output as a reference point.

Command Default MAC address learning is enabled on all VLANs.

Command Modes User EXEC

Command History	Release	Modification
	12.2(54)SG	This command was modified to support the learning disable feature on the Catalyst 4500 series switch.

Usage Guidelines

To display configured VLANs, and whether MAC address learning is enabled or disabled, use the **show mac address-table learning** command without keywords. .

To display the learning status on an individual VLAN, use the command with a specific VLAN ID.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain output do not appear, but the lines that contain Output appear.

Examples The following example shows that MAC address learning is disabled on VLAN 200:

```
Switch> show mac address-table learning
VLAN      Learning Status
-----      -
1          yes
100        yes
200        no
```

Related Commands	Command	Description
	mac-address-table learning vlan	Enables or disables MAC address learning on a VLAN.

show mac-address-table multicast

To display information about the multicast MAC address table, use the **show mac-address-table multicast** command.

```
show mac-address-table multicast [count | {igmp-snooping [count]} | {user [count]} |
    {vlan vlan_num}]
```

Syntax Description	Parameter	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 addresses.
	vlan vlan_num	(Optional) Displays information for a specific VLAN only; valid values are from 1 to 4094.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.1(8a)EW	This command was introduced on the Catalyst 4500 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 The following 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 ffff.ffff.ffff system Switch,Fa6/15
Switch#
```

The following 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 Address Count: 141
Total Multicast MAC Addresses Available: 16384
Switch#
```

Related Commands	Command	Description
	<code>show mac-address-table address</code>	Displays the information about the MAC-address table.
	<code>show mac-address-table aging-time</code>	Displays MAC address table aging information.
	<code>show mac-address-table count</code>	Displays the number of entries currently in the MAC address table.
	<code>show mac-address-table dynamic</code>	Displays the dynamic MAC address table entries only.
	<code>show mac-address-table interface</code>	Displays the MAC address table information for a specific interface.
	<code>show mac-address-table protocol</code>	Displays the MAC address table information that is based on the protocol.
	<code>show mac-address-table static</code>	Displays the static MAC address table entries only.
	<code>show mac-address-table vlan</code>	Displays information about the MAC address table for a specific VLAN.

show mac-address-table notification

To display the MAC address table notification status and history, use the **show mac-address-table notification** command.

```
show mac-address-table notification [change] [interface interface-id] | [mac-move] |
[threshold] | [learn-fail]
```

Syntax Description		
change	(Optional)	Displays the MAC address change notification status.
interface	(Optional)	Displays MAC change information for an interfaces.
<i>interface-id</i>	(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.
learn-fail	(Optional)	Displays general information of hardware MAC learning failure notifications.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.2(31)SG	This command was introduced on the Catalyst 4500 series switch.
	12.2(52)SG	Support for learn-fail keyword, Supervisor Engine 6-E, and Catalyst 4900M 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 The following example shows how to display all the MAC address notification information:

```
Switch# show mac-address-table notification change
MAC Notification Feature is Enabled on the switch
Interval between Notification Traps : 1 secs
Number of MAC Addresses Added : 5
Number of MAC Addresses Removed : 1
Number of Notifications sent to NMS : 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 478433, Despatch Timestamp 478433
MAC Changed Message :
Operation: Added   Vlan: 1      MAC Addr: 1234.5678.9ab0 Dot1dBasePort: 323
History Index 2, Entry Timestamp 481834, Despatch Timestamp 481834
MAC Changed Message :
Operation: Added   Vlan: 1      MAC Addr: 1234.5678.9ab1 Dot1dBasePort: 323
Operation: Added   Vlan: 1      MAC Addr: 1234.5678.9ab2 Dot1dBasePort: 323
Operation: Added   Vlan: 1      MAC Addr: 1234.5678.9ab3 Dot1dBasePort: 323
Operation: Added   Vlan: 1      MAC Addr: 1234.5678.9ab4 Dot1dBasePort: 323
History Index 3, Entry Timestamp 484334, Despatch Timestamp 484334
MAC Changed Message :
Operation: Deleted Vlan: 1      MAC Addr: 1234.5678.9ab0 Dot1dBasePort: 323
Switch#

```

The following 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#

```

The following example shows how to display the MAC address move status:

```

Switch# show mac-address-table notification mac-move
MAC Move Notification: Enabled
Switch#

```

The following 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#

```

The following example shows how to display general information of MAC learning failure notifications:

```

Switch# show mac address-table notification learn-fail
Status   limit      Interval
-----+-----+-----
disabled 2000       120

```

Related Commands

Command	Description
clear mac-address-table	Clears the address entries from the Layer 2 MAC address table.
mac-address-table notification	Enables MAC address notification on a switch.
snmp-server enable traps	Enables SNMP notifications (traps or informs).
snmp trap mac-notification change	Enables SNMP MAC address 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	Parameter	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.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

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

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 The following 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  0050.3e8d.6400    static  assigned  --    Switch
 100  0050.3e8d.6400    static  assigned  --    Switch
   5  0050.3e8d.6400    static  assigned  --    Switch
4092  0000.0000.0000    dynamic  assigned  --    Switch
   1  0050.3e8d.6400    static  assigned  --    Switch
   4  0050.3e8d.6400    static  assigned  --    Switch
4092  0050.f0ac.3058    static  assigned  --    Switch
4092  0050.f0ac.3059    dynamic  assigned  --    Switch
   1  0010.7b3b.0978    dynamic  assigned  --    Fa5/9
Switch#
```


The following example shows the other output for the previous example:

```
Switch# show mac-address-table protocol other
Unicast Entries
  vlan  mac address  type      protocols  port
-----+-----+-----+-----+-----
   1    0000.0000.0201  dynamic  other      FastEthernet6/15
   1    0000.0000.0202  dynamic  other      FastEthernet6/15
   1    0000.0000.0203  dynamic  other      FastEthernet6/15
   1    0000.0000.0204  dynamic  other      FastEthernet6/15
   1    0030.94fc.0dff   static   ip,ipx,assigned,other  Switch
   2    0000.0000.0101  dynamic  other      FastEthernet6/16
   2    0000.0000.0102  dynamic  other      FastEthernet6/16
   2    0000.0000.0103  dynamic  other      FastEthernet6/16
   2    0000.0000.0104  dynamic  other      FastEthernet6/16
Fa6/1  0030.94fc.0dff   static   ip,ipx,assigned,other  Switch
Fa6/2  0030.94fc.0dff   static   ip,ipx,assigned,other  Switch

Multicast Entries
  vlan  mac address  type      ports
-----+-----+-----+-----
   1    ffff.ffff.ffff  system   Switch, Fa6/15
   2    ffff.ffff.ffff  system   Fa6/16
1002   ffff.ffff.ffff  system
1003   ffff.ffff.ffff  system
1004   ffff.ffff.ffff  system
1005   ffff.ffff.ffff  system
Fa6/1  ffff.ffff.ffff  system   Switch, Fa6/1
Fa6/2  ffff.ffff.ffff  system   Switch, Fa6/2
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.
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 <i>type</i> 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.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.1(8a)EW	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

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 protocols.
- **other** specifies the other protocol entries.

Examples

The following example shows how to display all the static MAC address entries:

```
Switch# show mac-address-table static
Unicast Entries
  vlan  mac address      type      protocols      port
-----+-----+-----+-----+-----
    1    0030.94fc.0dff     static ip,ipx,assigned,other Switch
Fa6/1    0030.94fc.0dff     static ip,ipx,assigned,other Switch
Fa6/2    0030.94fc.0dff     static ip,ipx,assigned,other Switch

Multicast Entries
  vlan  mac address      type      ports
-----+-----+-----+-----
    1    ffff.ffff.ffff     system Switch,Fa6/15
    2    ffff.ffff.ffff     system Fa6/16
1002    ffff.ffff.ffff     system
1003    ffff.ffff.ffff     system
1004    ffff.ffff.ffff     system
1005    ffff.ffff.ffff     system
Fa6/1    ffff.ffff.ffff     system Switch,Fa6/1
Fa6/2    ffff.ffff.ffff     system Switch,Fa6/2
.
.
Switch#
```

The following 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
Unicast Entries
  vlan  mac address      type      protocols      port
-----+-----+-----+-----+-----
    1    0030.94fc.0dff     static ip,ipx,assigned,other Switch
Fa6/1    0030.94fc.0dff     static ip,ipx,assigned,other Switch
Fa6/2    0030.94fc.0dff     static ip,ipx,assigned,other Switch

Multicast Entries
  vlan  mac address      type      ports
-----+-----+-----+-----
    1    ffff.ffff.ffff     system Switch,Fa6/15
    2    ffff.ffff.ffff     system Fa6/16
1002    ffff.ffff.ffff     system
1003    ffff.ffff.ffff     system
1004    ffff.ffff.ffff     system
1005    ffff.ffff.ffff     system
Fa6/1    ffff.ffff.ffff     system Switch,Fa6/1
Fa6/2    ffff.ffff.ffff     system Switch,Fa6/2
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 <i>vlan_id</i>	(Optional) Displays the entries for a specific VLAN; valid values are from 1 to 4094.	
protocol <i>protocol</i>	(Optional) Specifies a protocol. See the “Usage Guidelines” section for more information.	

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.1(8a)EW	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

The following 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    0000.0000.0201    dynamic  ip              FastEthernet6/15
  1    0000.0000.0202    dynamic  ip              FastEthernet6/15
  1    0000.0000.0203    dynamic  other           FastEthernet6/15
  1    0000.0000.0204    dynamic  other           FastEthernet6/15
  1    0030.94fc.0dff     static   ip,ipx,assigned,other  Switch

Multicast Entries
vlan  mac address      type      ports
-----+-----+-----+-----
  1    ffff.ffff.ffff     system   Switch,Fa6/15
Switch#
```

The following 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    0000.0000.0203    dynamic  other           FastEthernet6/15
  1    0000.0000.0204    dynamic  other           FastEthernet6/15
  1    0030.94fc.0dff     static   ip,ipx,assigned,other  Switch

Multicast Entries
vlan  mac address      type      ports
-----+-----+-----+-----
  1    ffff.ffff.ffff     system   Switch,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 macro auto mac-address-group

Use the **show macro auto mac-address-group** command to display the configuration of MAC address group.

show macro auto mac-address-group

Syntax Description

No keywords

Command History

Release	Modification
12.2(54)SG	This command was introduced on the Catalyst 4500 series switch.

Examples

The following example shows how to display the configuration of the MAC address group:

```
Switch# show macro auto address-group
MAC Address Group Configuration:

Group Name                OUI                MAC ADDRESS
-----
testGroup                 2222.2222.2222
                           1111.1111.1111
```

show macro auto device

Use the **show macro auto device** global configuration command to display the default information for a device, including builtin function name and the parameters that can be provided for the commands when executing the builtin function.

```
show macro auto device device_id
```

Syntax Description	<i>device_id</i>	Specifies the device ID.
---------------------------	------------------	--------------------------

Command Default	None
------------------------	------

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

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

Usage Guidelines	This command displays the default values as well as the currently used values if configured.
-------------------------	--

Examples	The following example shows how to display the default information for the device access-point:
-----------------	---

```
Switch# show macro auto device access-point
Device:access-point
Default Macro:CISCO_AP_AUTO_SMARTPORT
Current Macro:CISCO_AP_AUTO_SMARTPORT
Configurable Parameters:NATIVE_VLAN
Defaults Parameters:NATIVE_VLAN=1
Current Parameters:NATIVE_VLAN=1
```

Related Commands	Command	Description
	show macro auto event manager	Refer to the Command Reference in the IOS library
	show macro auto interface	Display Auto SmartPorts status and the functions applied on an interface.

show macro auto interface

Use the **show macro auto interface** command to display Auto SmartPorts status and the functions applied on an interface.

show macro auto interface *interface_id*

Syntax Description	<i>interface_id</i>	Specifies an interface ID.
---------------------------	---------------------	----------------------------

Command Default	None
------------------------	------

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

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

Examples The following example shows how to display Auto SmartPorts status and the applied macros:

```
Switch# show macro auto int gi3/8
Global Auto Smart Port Status
Auto Smart Ports Enabled
Fallback : CDP Disabled, LLDP Disabled
Interface      Auto Smart Port  Fallback      Macro Description(s)
-----
Gi3/8          TRUE                       None          CISCO_PHONE_EVENT
```

Related Commands	Command	Description
	show macro auto device	Displays the default information for a device, including builtin function name and the parameters that can be provided for the commands when executing the builtin function.

show macro auto monitor clients

To display the clients using the device classifier facility on the switch, use the **show macro auto monitor clients** user EXEC command.

show macro auto monitor clients

Syntax Description This command has no arguments or keywords.

Command Default User EXEC
Privileged EXEC

Command History	Release	Modification
	Release IOS XE 3.3.0 SG (15.1(1)SG)	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines Device classifier (DC) is enabled by default when you enable a client application (for example, Auto Smartports) that uses its functionality. Use the **show macro auto monitor clients** command to display the clients that are using the DC feature on the switch.

As long as any clients are using the DC, you cannot disable it by using the **no macro auto monitor** command. If you attempt to disable the DC while a client is using it, an error message appears.

Examples The following example shows how to use the **show macro auto monitor clients** privileged EXEC command to view the clients using the DC on the switch:

```
Switch# show macro auto monitor clients
Client Name
=====
Auto Smart Ports
```

The following example shows the error message that appears when you attempt to disable DC while a client is using it:

```
Switch(config)# no macro auto monitor
These subsystems should be disabled before disabling Device classifier
Auto Smart Ports

% Error - device classifier is not disabled
```

Related Commands	Command	Description
	macro auto device	Configures macro default parameter values.
	macro auto execute (built-in function)	Configures mapping from an event trigger to a built-in macro.
	macro auto global processing	Enables Auto Smartports on a switch.

Command	Description
macro auto mac-address-group	Configures MAC address groups.
macro auto sticky	Configures macro persistence.
shell trigger	Creates event triggers.
show macro auto monitor type	Displays all the device types recognized by the device classifier.
show shell triggers	Displays information about event triggers and macros.

show macro auto monitor device

To display the devices connected to a switch and their associated properties, use the **show macro auto monitor device** user EXEC command.

```
show macro auto monitor device [detail | filter string | interface interface_id | mac-address
                               mac_address]
```

Syntax Description		
detail		Displays detailed device classifier information.
filter <i>string</i>		Displays information for devices that match the filter.
interface <i>interface_id</i>		Displays information about devices attached to the specified interface.
mac <i>mac_address</i>		Displays device information for the specified endpoint.

Command Modes	
	User EXEC
	Privileged EXEC

Command History	Release	Modification
	Release IOS XE 3.3.0 SG (15.1(1)SG)	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines	
	Use this command to display the devices connected to a switch. Use the show macro auto device privileged EXEC command to display the configurable parameters for a device.

Examples	
	The following example shows how to use the show macro auto monitor device privileged EXEC command with no optional keywords to view the devices connected to the switch:

```
Switch# show macro auto monitor device
MAC_Address          Port_Id          Profile Name
=====
000a.b8c6.1e07      Gi1/0/2         Cisco-Device
001f.9e90.1250      Gi1/0/4         Cisco-AP-Aironet-1130
=====
```

The following example shows how to use the **show macro auto monitor device** privileged EXEC command with the optional **mac-address** keyword to view summary information about the connected device with the specified MAC address:

```
Switch# show macro auto monitor device mac-address 001f.9e90.1250
MAC_Address          Port_Id          Profile Name
=====
001f.9e90.1250      Gi1/0/4         Cisco-AP-Aironet-1130
=====
```

The following example shows how to use the **show macro auto monitor device** privileged EXEC command with the optional **mac-address** and **detail** keywords to view detailed information about the connected device with the specified MAC address:

```
Switch# show macro auto monitor device mac-address 001f.9e90.1250 detail
MAC_Address      Port_Id      Certainty Parent      ProfileType  Profile Name
Device_Name
=====
001f.9e90.1250   Gi1/0/4     40         2           Built-in     Cisco-AP-Aironet-1130
cisco AIR-LAP1131AG-E-K9
=====
```

The following example shows how to use the **show macro auto monitor device** privileged EXEC command with the optional **interface** keyword to view summary information about the device connected to the specified interface:

```
Switch# show macro auto monitor device interface gi 1/0/2
MAC_Address      Port_Id      Profile Name
=====
000a.b8c6.1e07   Gi1/0/2     Cisco-Device
=====
```

The following example shows how to use the **show macro auto monitor device** privileged EXEC command with the optional **interface** and **detail** keywords to view detailed information about the device connected to the specified interface:

```
Switch# show macro auto monitor device interface gi 1/0/2 detail
MAC_Address      Port_Id      Certainty Parent      ProfileType  Profile Name
Device_Name
=====
000a.b8c6.1e07   Gi1/0/2     10         0           Default     Cisco-Device   cisco
WS-C2960-48TT-L
=====
```

Related Commands

Command	Description
macro auto device	Configures macro default parameter values.
macro auto execute (built-in function)	Configures mapping from an event trigger to a built-in macro.
macro auto global processing	Enables Auto Smartports on a switch.
macro auto mac-address-group	Configures MAC address groups.
macro auto sticky	Configures macro persistence.
shell trigger	Creates event triggers.
show macro auto monitor clients	Displays all the device types recognized by the device classifier.
show macro auto monitor type	Displays all the device types recognized by the device classifier.
show shell triggers	Displays information about event triggers and macros.

show macro auto monitor type

To display all the device types recognized by the device classifier, use the **show macro auto monitor type** user EXEC command.

show macro auto monitor type [**table** [*built-in* | *default*] | **string** *filter_string*]

Syntax Description	table	Displays device classification in a table.
	<i>built-in</i>	Displays device classification information from the built-in device table.
	<i>default</i>	Displays device classification information from the default device table.
	filter <i>string</i>	Displays information for devices that match the filter.

Command Modes	User EXEC Privileged EXEC
---------------	------------------------------

Command History	Release	Modification
	Release IOS XE 3.3.0 SG (15.1(1)SG)	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines This command displays all the device types recognized by the device classification engine. The number of available device types is the number of profiles stored on the switch. Because the number of profiles can be very large, you can use the **filter** keyword to limit the command output.

Examples The following example shows how to use the **show macro auto monitor type** privileged EXEC command with no optional keywords to view the devices recognized by the device classifier:

```
Switch# show macro auto monitor type table
Valid      Type      Profile Name      min Conf  ID
-----
Valid      Default   Apple-Device      10        0
Valid      Default   Aruba-Device      10        1
Valid      Default   Avaya-Device      10        2
Valid      Default   Avaya-IP-Phone    20        3
Valid      Default   BlackBerry         20        4
Valid      Default   Cisco-Device       10        5
Valid      Default   Cisco-IP-Phone    20        6
Valid      Default   Cisco-IP-Phone-7902 70        7
Valid      Default   Cisco-IP-Phone-7905 70        8
Valid      Default   Cisco-IP-Phone-7906 70        9
Valid      Default   Cisco-IP-Phone-7910 70       10
Valid      Default   Cisco-IP-Phone-7911 70       11
Valid      Default   Cisco-IP-Phone-7912 70       12
Valid      Default   Cisco-IP-Phone-7940 70       13
Valid      Default   Cisco-IP-Phone-7941 70       14
Valid      Default   Cisco-IP-Phone-7942 70       15
```

Valid	Default	Cisco-IP-Phone-7945	70	16
Valid	Default	Cisco-IP-Phone-7945G	70	17
Valid	Default	Cisco-IP-Phone-7960	70	18
Valid	Default	Cisco-IP-Phone-7961	70	19
Valid	Default	Cisco-IP-Phone-7962	70	20
Valid	Default	Cisco-IP-Phone-7965	70	21
Valid	Default	Cisco-IP-Phone-7970	70	22
Valid	Default	Cisco-IP-Phone-7971	70	23
Valid	Default	Cisco-IP-Phone-7975	70	24
Valid	Default	Cisco-IP-Phone-7985	70	25
Valid	Default	Cisco-IP-Phone-9971	70	26
Valid	Default	Cisco-WLC-2100-Series	40	27
Valid	Default	DLink-Device	10	28
Valid	Default	Enterasys-Device	10	29
Valid	Default	HP-Device	10	30
Valid	Default	HP-JetDirect-Printer	30	31
Valid	Default	Lexmark-Device	10	32
Valid	Default	Lexmark-Printer-E260dn	30	33
Valid	Default	Microsoft-Device	10	34
Valid	Default	Netgear-Device	10	35
Valid	Default	NintendoWII	10	36
Valid	Default	Nortel-Device	10	37
Valid	Default	Nortel-IP-Phone-2000-Series	20	38
Valid	Default	SonyPS3	10	39
Valid	Default	XBOX360	20	40
Valid	Default	Xerox-Device	10	41
Valid	Default	Xerox-Printer-Phaser3250	30	42
Valid	Default	Aruba-AP	20	43
Valid	Default	Cisco-Access-Point	10	44
Valid	Default	Cisco-IP-Conference-Station-7935	70	45
Valid	Default	Cisco-IP-Conference-Station-7936	70	46
Valid	Default	Cisco-IP-Conference-Station-7937	70	47
Valid	Default	DLink-DAP-1522	20	48
Valid	Default	Cisco-AP-Aironet-1130	30	49
Valid	Default	Cisco-AP-Aironet-1240	30	50
Valid	Default	Cisco-AP-Aironet-1250	30	51
Valid	Default	Cisco-AIR-LAP	25	52
Valid	Default	Cisco-AIR-LAP-1130	30	53
Valid	Default	Cisco-AIR-LAP-1240	50	54
Valid	Default	Cisco-AIR-LAP-1250	50	55
Valid	Default	Cisco-AIR-AP	25	56
Valid	Default	Cisco-AIR-AP-1130	30	57
Valid	Default	Cisco-AIR-AP-1240	50	58
Valid	Default	Cisco-AIR-AP-1250	50	59
Invalid	Default	Sun-Workstation	10	60
Valid	Default	Linksys-Device	20	61
Valid	Default	LinksysWAP54G-Device	30	62
Valid	Default	HTC-Device	10	63
Valid	Default	MotorolaMobile-Device	10	64
Valid	Default	VMWare-Device	10	65
Valid	Default	ISE-Appliance	10	66
Valid	Built-in	Cisco-Device	10	0
Valid	Built-in	Cisco-Router	10	1
Valid	Built-in	Router	10	2
Valid	Built-in	Cisco-IP-Camera	10	3
Valid	Built-in	Cisco-IP-Camera-2xxx	30	4
Valid	Built-in	Cisco-IP-Camera-2421	50	5
Valid	Built-in	Cisco-IP-Camera-2500	50	6
Valid	Built-in	Cisco-IP-Camera-2520	50	7
Valid	Built-in	Cisco-IP-Camera-2530	50	8
Valid	Built-in	Cisco-IP-Camera-4xxx	50	9
Valid	Built-in	Cisco-Transparent-Bridge	8	10
Valid	Built-in	Transparent-Bridge	8	11
Valid	Built-in	Cisco-Source-Bridge	10	12

show macro auto monitor type

Valid	Built-in	Cisco-Switch	10	13
Valid	Built-in	Cisco-IP-Phone	20	14
Valid	Built-in	IP-Phone	20	15
Valid	Built-in	Cisco-DMP	10	16
Valid	Built-in	Cisco-DMP-4305G	70	17
Valid	Built-in	Cisco-DMP-4310G	70	18
Valid	Built-in	Cisco-DMP-4400G	70	19
Valid	Built-in	Cisco-WLC-2100-Series	40	20
Valid	Built-in	Cisco-Access-Point	10	21
Valid	Built-in	Cisco-AIR-LAP	30	22
Valid	Built-in	Cisco-AIR-AP	30	23
Valid	Built-in	Linksys-Device	20	24

Related Commands

Command	Description
macro auto device	Configures macro default parameter values.
macro auto execute (built-in function)	Configures mapping from an event trigger to a built-in macro.
macro auto global processing	Enables Auto Smartports on a switch.
macro auto mac-address-group	Configures MAC address groups.
macro auto sticky	Configures macro persistence.
shell trigger	Creates event triggers.
show macro auto monitor clients	Displays all the device types recognized by the device classifier.
show macro auto monitor device	Displays all the device types recognized by the device classifier.

show module

To display information about the module, use the **show module** command.

show module [*mod* | **all**]

Syntax Description	
<i>mod</i>	(Optional) Number of the module; valid values vary from chassis to chassis.
all	(Optional) Displays information for all modules.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch.
	12.2(25)EW	Enhanced the output of the show idprom interface 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 The following example shows how to display information for all the modules.

The following 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 "PwrDeny."

```
Switch# show module all
Mod  Ports Card Type                               Model                Serial No.
-----+-----+-----+-----+-----+-----+-----
 1      2 1000BaseX (GBIC) Supervisor (active)  WS-X4014             JAB054109GH
 2      6 1000BaseX (GBIC)                               WS-X4306             00000110
 3     18 1000BaseX (GBIC)                               WS-X4418             JAB025104WK
 5      0 Not enough power for module                    WS-X4148-FX-MT      0000000000
 6     48 10/100BaseTX (RJ45)                            WS-X4148             JAB023402RP
```

```

M MAC addresses                Hw  Fw          Sw          Status
-----+-----+-----+-----+-----+-----
1 005c.9d1a.f9d0 to 005c.9d1a.f9df 0.5 12.1(11br)EW 12.1(20020313:00 Ok
2 0010.7bab.9920 to 0010.7bab.9925 0.2                               Ok
3 0050.7356.2b36 to 0050.7356.2b47 1.0                               Ok
5 0001.64fe.a930 to 0001.64fe.a95f 0.0                               PwrDeny

6 0050.0f10.28b0 to 0050.0f10.28df 1.0                               Ok
Switch#

```

The following example shows how to display information for a specific module:

```

Switch# show module mod2
Mod Ports Card Type                               Model                               Serial No.
-----+-----+-----+-----+-----+-----
2    2 Catalyst 4000 supervisor 2 (Active)      WS-X6K-SUP2-2GE                      SAD04450LF1
Mod MAC addresses                Hw  Fw          Sw          Status
-----+-----+-----+-----+-----+-----
2  0001.6461.39c0 to 0001.6461.39c1  1.1  6.1(3)      6.2(0.97)  Ok
Mod Sub-Module                    Model                               Serial                               Hw  Status
-----+-----+-----+-----+-----+-----
2 Policy Feature Card 2           WS-F6K-PFC2                         SAD04440HVU                          1.0  Ok
2 Cat4k MSFC 2 daughterboard      WS-F6K-MSFC2                         SAD04430J9K                          1.1  Ok
Switch#

```

The following example shows how to display information for all the modules on the switch:

```

Switch# show module
Chassis Type : WS-C4506

Power consumed by backplane : 0 Watts

Mod Ports Card Type                               Model                               Serial No.
-----+-----+-----+-----+-----+-----
1    6 XG (X2), 1000BaseX (SFP) Supervisor(ac  WS-X4517                      ""
3    6 1000BaseX (GBIC)                               WS-X4306                      00000110

M MAC addresses                Hw  Fw          Sw          Status
-----+-----+-----+-----+-----+-----
1 0004.dd46.7700 to 0004.dd46.7705 0.0 12.2(20r)EW( 12.2(20040513:16 Ok
3 0010.7bab.9920 to 0010.7bab.9925 0.2                               Ok
Switch#

```

show monitor

To display information about the SPAN session, use the **show monitor** command.

show monitor [**session**] [**range** *session-range* | **local** | **remote** | **all** | *session-number*] [**detail**]

Syntax Description		
session	(Optional)	Displays the SPAN information for a session.
range	(Optional)	Displays information for a range of sessions.
<i>session-range</i>	(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.
<i>session-number</i>	(Optional)	Session number; valid values are from 1 to 6.
detail	(Optional)	Displays the detailed SPAN information for a session.

Command Default The **detail** keyword only displays lines with a nondefault configuration.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch.
	12.1(13)EW	Added support for differing directions within a single user session.
	12.1(19)EW	Output enhanced to display configuration status of SPAN enhancements.
	12.1(20)EW	Added support to display configuration state for remote SPAN and learning.
	12.2(20)EW	Added support to display ACLs that are applied to SPAN sessions.

Examples The following example shows how to display whether ACLs are applied to a given SPAN session on a Catalyst 4500 series switch:

```
Switch# show monitor

Session 1
-----
Type           : Local Session
Source Ports   :
  Both         : Fa6/1
Destination Ports : Fa6/2
  Encapsulation : Native
  Ingress      : Disabled
  Learning     : Disabled
Filter VLANs   : 1
IP Access-group : 10
```

The following 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:      Fa1/1-3
Dest RSPAN VLAN: 901
Ingress : Enabled, default VLAN=2
Learning : Disabled
Switch#
```

The following example shows how to display the detailed SPAN information for session 1:

```
Switch# show monitor session 1 detail
Session 1
-----
Type           : Local Session
Source Ports   :
    RX Only    : None
    TX Only    : None
    Both       : Gi1/1, CPU
Source VLANs   :
    RX Only    : None
    TX Only    : None
    Both       : None
Source RSPAN VLAN : Fa6/1
Destination Ports : Fa6/1
    Encapsulation : DOT1Q
    Ingress      : Enabled, default VLAN = 2
Filter VLANs   : None
    Filter Types RX : Good
    Filter Types TX : None
Dest Rspan Vlan : 901
Ingress : Enabled, default VLAN=2
Learning : Disabled
IP Access-group : None
Switch#
```

The following 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 monitor capture

To display the capture point details, so that you can see what capture points are defined, what their attributes are, and whether they are active, use the **show monitor capture** command.

show monitor capture [*name* [**parameter**] | **buffer** [**brief** | **detailed** | **dump**]]

Syntax Description	
<i>name</i>	Specifies the capture point name.
parameter	Reconstructs and displays the exec commands for specifying the capture point.
buffer [brief detailed dump]	Source the packets from the capture buffer, decode and display them in brief, detailed or dump mode.

Command Default If the capture point name is not provided, the command displays all the capture point details.
If the display mode is not specified, the command defaults to brief mode.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	IOS XE 3.3.0SG/ 15.1(1)SG	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines When the command is issued with no parameters, it displays the details of all the capture points. When specified with a capture point name and no other parameters, it displays the details of the specific capture point name. With the **parameter** keyword, the command reconstructs the commands that describe the capture point and displays them.

The **buffer** option displays the packets from the capture buffer. This option is applicable only if the capture point directs the captured packets to the buffer. The packets can be decoded and displayed in either the brief, detailed, or dump mode. The default mode is **brief**.

Examples Following are example of how to use the **show monitor capture** command:

```
Switch# show monitor capture mycap buffer brief
0.000000 10.1.1.215 -> 20.1.1.2    UDP Source port: 20001  Destination port: 20002
1.000000 10.1.1.216 -> 20.1.1.2    UDP Source port: 20001  Destination port: 20002
2.000000 10.1.1.217 -> 20.1.1.2    UDP Source port: 20001  Destination port: 20002
3.000000 10.1.1.218 -> 20.1.1.2    UDP Source port: 20001  Destination port: 20002
4.000000 10.1.1.219 -> 20.1.1.2    UDP Source port: 20001  Destination port: 20002
5.000000 10.1.1.220 -> 20.1.1.2    UDP Source port: 20001  Destination port: 20002
6.000000 10.1.1.221 -> 20.1.1.2    UDP Source port: 20001  Destination port: 20002
7.000000 10.1.1.222 -> 20.1.1.2    UDP Source port: 20001  Destination port: 20002
8.000000 10.1.1.223 -> 20.1.1.2    UDP Source port: 20001  Destination port: 20002
9.000000 10.1.1.224 -> 20.1.1.2    UDP Source port: 20001  Destination port: 20002
10.000000 10.1.1.225 -> 20.1.1.2    UDP Source port: 20001  Destination port: 20002
11.000000 10.1.1.226 -> 20.1.1.2    UDP Source port: 20001  Destination port: 20002
```

```

12.000000 10.1.1.227 -> 20.1.1.2      UDP Source port: 20001 Destination port: 20002
13.000000 10.1.1.228 -> 20.1.1.2      UDP Source port: 20001 Destination port: 20002
14.000000 10.1.1.229 -> 20.1.1.2      UDP Source port: 20001 Destination port: 20002
15.000000 10.1.1.230 -> 20.1.1.2      UDP Source port: 20001 Destination port: 20002
16.000000 10.1.1.231 -> 20.1.1.2      UDP Source port: 20001 Destination port: 20002
17.000000 10.1.1.232 -> 20.1.1.2      UDP Source port: 20001 Destination port: 20002
18.000000 10.1.1.233 -> 20.1.1.2      UDP Source port: 20001 Destination port: 20002
19.000000 10.1.1.234 -> 20.1.1.2      UDP Source port: 20001 Destination port: 20002
20.000000 10.1.1.235 -> 20.1.1.2      UDP Source port: 20001 Destination port: 20002
21.000000 10.1.1.236 -> 20.1.1.2      UDP Source port: 20001 Destination port: 20002

```

...

Switch# **show monitor capture mycap buffer detailed**

Frame 1: 256 bytes on wire (2048 bits), 256 bytes captured (2048 bits)

Arrival Time: Apr 15, 2012 15:50:02.398966000 PDT

Epoch Time: 1334530202.398966000 seconds

[Time delta from previous captured frame: 0.000000000 seconds]

[Time delta from previous displayed frame: 0.000000000 seconds]

[Time since reference or first frame: 0.000000000 seconds]

Frame Number: 1

Frame Length: 256 bytes (2048 bits)

Capture Length: 256 bytes (2048 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ip:udp:data]

Ethernet II, Src: 00:00:00:00:03:01 (00:00:00:00:03:01), Dst: 54:75:d0:3a:85:3f

(54:75:d0:3a:85:3f)

Destination: 54:75:d0:3a:85:3f (54:75:d0:3a:85:3f)

Address: 54:75:d0:3a:85:3f (54:75:d0:3a:85:3f)

.... 0 = IG bit: Individual address (unicast)

.... 0. = LG bit: Globally unique address (factory default)

Source: 00:00:00:00:03:01 (00:00:00:00:03:01)

Address: 00:00:00:00:03:01 (00:00:00:00:03:01)

.... 0 = IG bit: Individual address (unicast)

.... 0. = LG bit: Globally unique address (factory default)

...

Switch# **show monitor capture mycap buffer dump**

```

0.000000 10.1.1.215 -> 20.1.1.2      UDP Source port: 20001 Destination port: 20002

```

```

0000 54 75 d0 3a 85 3f 00 00 00 00 03 01 08 00 45 00  Tu...?.....E.
0010 00 ee 00 00 00 00 40 11 59 25 0a 01 01 d7 14 01  .....@.Y%.....
0020 01 02 4e 21 4e 22 00 da 6d e0 00 01 02 03 04 05  ..N!N".m.....
0030 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15  .....
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  ..... !"#$$%
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  &'()*+,-./012345
0060 36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45  6789;,<=>?@ABCDE
0070 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55  FGHIJKLMNOPQRSTU
0080 56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65  VWXYZ[\]^_`abcde
0090 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75  fghijklmnopqrstu
00a0 76 77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85  vwxyz{|}~.....
00b0 86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95  .....
00c0 96 97 98 99 9a 9b 9c 9d 9e 9f a0 a1 a2 a3 a4 a5  .....
00d0 a6 a7 a8 a9 aa ab ac ad ae af b0 b1 b2 b3 b4 b5  .....
00e0 b6 b7 b8 b9 ba bb bc bd be bf c0 c1 c2 c3 c4 c5  .....
00f0 c6 c7 c8 c9 ca cb cc cd ce cf d0 d1 03 3e d0 33  .....>.3

```

show monitor capture file

To decode and display packets from a previously captured .pcap file, use the **show monitor capture file** command.

show monitor capture file *name* [**display-filter** *filter-string*] [**brief** | **detailed** | **dump**]

Syntax Description	
<i>name</i>	Specifies the filename.
display-filter <i>filter-string</i>	Specifies the display filter string according to Wireshark's display-filter syntax.
brief detailed dump	Determines the display mode. <ul style="list-style-type: none"> brief—Displays a one line summary of the packet with key fields detailed—Displays all the fields in the packet for the protocols supported and displays the payload in hexadecimal form. dump—Displays a one line summary of the packet with key fields and also displays the packet in hexadecimal form.

Command Default **brief**

Command Modes Privileged EXEC mode

Command History	Release	Modification
	IOS XE 3.3.0SG/ 15.1(1)SG	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines If no display filter is specified, then all the packets in the file are displayed. Because the display filter must observe the Wireshark display filter syntax, ensure that the display filter is accurate. Also, use a double quotes when specifying the filter.

Examples The following example shows how to display packets from a .pcap file with a display filter:

```
Switch# show monitor capture file bootflash:test.pcap display-filter
```

This example displays a brief output from a .pcap file:

```
Switch# show monitor capture file bootflash:mycap.pcap
 1  0.000000  10.1.1.140 -> 20.1.1.2      UDP Source port: 20001  Destination port:
20002
 2  1.000000  10.1.1.141 -> 20.1.1.2      UDP Source port: 20001  Destination port:
20002
 3  2.000000  10.1.1.142 -> 20.1.1.2      UDP Source port: 20001  Destination port:
20002
```

```

 4  3.000000  10.1.1.143 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
 5  4.000000  10.1.1.144 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
 6  5.000000  10.1.1.145 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
 7  6.000000  10.1.1.146 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
 8  7.000000  10.1.1.147 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
 9  8.000000  10.1.1.148 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
10  9.000000  10.1.1.149 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
11 10.000000  10.1.1.150 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
12 11.000000  10.1.1.151 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
13 12.000000  10.1.1.152 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
14 13.000000  10.1.1.153 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
15 14.000000  10.1.1.154 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
16 15.000000  10.1.1.155 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
17 16.000000  10.1.1.156 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
18 17.000000  10.1.1.157 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
19 18.000000  10.1.1.158 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
20 19.000000  10.1.1.159 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
21 20.000000  10.1.1.160 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
22 21.000000  10.1.1.161 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
23 22.000000  10.1.1.162 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
24 23.000000  10.1.1.163 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
25 24.000000  10.1.1.164 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
26 25.000000  10.1.1.165 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
27 26.000000  10.1.1.166 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
28 27.000000  10.1.1.167 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
29 28.000000  10.1.1.168 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
30 29.000000  10.1.1.169 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
31 30.000000  10.1.1.170 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
32 31.000000  10.1.1.171 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
33 32.000000  10.1.1.172 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
34 33.000000  10.1.1.173 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
35 34.000000  10.1.1.174 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002

```



```

36 35.000000 10.1.1.175 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
37 36.000000 10.1.1.176 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
38 37.000000 10.1.1.177 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
39 38.000000 10.1.1.178 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
40 39.000000 10.1.1.179 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
41 40.000000 10.1.1.180 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
42 41.000000 10.1.1.181 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
43 42.000000 10.1.1.182 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
44 43.000000 10.1.1.183 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
45 44.000000 10.1.1.184 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
46 45.000000 10.1.1.185 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
47 46.000000 10.1.1.186 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
48 47.000000 10.1.1.187 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
49 48.000000 10.1.1.188 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
50 49.000000 10.1.1.189 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
51 50.000000 10.1.1.190 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
52 51.000000 10.1.1.191 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
53 52.000000 10.1.1.192 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
54 53.000000 10.1.1.193 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
55 54.000000 10.1.1.194 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
56 55.000000 10.1.1.195 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
57 56.000000 10.1.1.196 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
58 57.000000 10.1.1.197 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002
59 58.000000 10.1.1.198 -> 20.1.1.2    UDP Source port: 20001 Destination port:
20002

```

The following example shows how to display a detailed output from a .pcap file:

```

Switch# show monitor capture file bootflash:mycap.pcap detailed
Frame 1: 256 bytes on wire (2048 bits), 256 bytes captured (2048 bits)
Arrival Time: Mar 21, 2012 14:35:09.111993000 PDT
Epoch Time: 1332365709.111993000 seconds
[Time delta from previous captured frame: 0.000000000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 0.000000000 seconds]
Frame Number: 1
Frame Length: 256 bytes (2048 bits)
Capture Length: 256 bytes (2048 bits)
[Frame is marked: False]
[Frame is ignored: False]

```

```

[Protocols in frame: eth:ip:udp:data]
Ethernet II, Src: 00:00:00:00:03:01 (00:00:00:00:03:01), Dst: 54:75:d0:3a:85:3f
(54:75:d0:3a:85:3f)
  Destination: 54:75:d0:3a:85:3f (54:75:d0:3a:85:3f)
    Address: 54:75:d0:3a:85:3f (54:75:d0:3a:85:3f)
      ....0.... = IG bit: Individual address (unicast)
      ....0.... = LG bit: Globally unique address (factory default)
  Source: 00:00:00:00:03:01 (00:00:00:00:03:01)
    Address: 00:00:00:00:03:01 (00:00:00:00:03:01)
      ....0.... = IG bit: Individual address (unicast)
      ....0.... = LG bit: Globally unique address (factory default)
  Type: IP (0x0800)
  Frame check sequence: 0x03b07f42 [incorrect, should be 0x08fcee78]
Internet Protocol, Src: 10.1.1.140 (10.1.1.140), Dst: 20.1.1.2 (20.1.1.2)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    0000 00.. = Differentiated Services Codepoint: Default (0x00)
      ....0.. = ECN-Capable Transport (ECT): 0
      ....0.. = ECN-CE: 0
  Total Length: 238
  Identification: 0x0000 (0)
  Flags: 0x00
    0... = Reserved bit: Not set
    .0.. = Don't fragment: Not set
    ..0. = More fragments: Not set
  Fragment offset: 0
  Time to live: 64
  Protocol: UDP (17)
  Header checksum: 0x5970 [correct]
    [Good: True]
    [Bad: False]
  Source: 10.1.1.140 (10.1.1.140)
  Destination: 20.1.1.2 (20.1.1.2)
User Datagram Protocol, Src Port: 20001 (20001), Dst Port: 20002 (20002)
  Source port: 20001 (20001)
  Destination port: 20002 (20002)
  Length: 218
  Checksum: 0x6e2b [validation disabled]
    [Good Checksum: False]
    [Bad Checksum: False]
Data (210 bytes)

0000 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f .....
0010 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f .....
0020 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f !"#%&'()*+,-./
0030 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f 0123456789:;<=>?
0040 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f @ABCDEFGHIJKLMNO
0050 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f PQRSTUVWXYZ[\]^_
0060 60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f `abcdefghijklmnop
0070 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f pqrstuvwxyz{|}~.
0080 80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f .....
0090 90 91 92 93 94 95 96 97 98 99 9a 9b 9c 9d 9e 9f .....
00a0 a0 a1 a2 a3 a4 a5 a6 a7 a8 a9 aa ab ac ad ae af .....
00b0 b0 b1 b2 b3 b4 b5 b6 b7 b8 b9 ba bb bc bd be bf .....
00c0 c0 c1 c2 c3 c4 c5 c6 c7 c8 c9 ca cb cc cd ce cf .....
00d0 d0 d1 ..
      Data: 000102030405060708090a0b0c0d0e0f1011121314151617...
      [Length: 210]

Frame 2: 256 bytes on wire (2048 bits), 256 bytes captured (2048 bits)
Arrival Time: Mar 21, 2012 14:35:10.111993000 PDT

```

show mvr

Use the **show mvr** privileged EXEC command without keywords to display the following: the current Multicast VLAN Registration (MVR) global parameter values (including whether or not MVR is enabled), the MVR multicast VLAN, the maximum query response time, the number of multicast groups, and the MVR mode (dynamic or compatible).

```
show mvr
```

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	Release	Modification
	Release IOS XE 3.5.0E and IOS 15.2(1)E	This command was introduced on the Catalyst 4500 series switch.

Examples This is an example of output from the **show mvr** command:

```
Switch# show mvr
MVR Running: TRUE
MVR multicast VLAN: 1
MVR Max Multicast Groups: 1500
MVR Current multicast groups: 0
MVR Global query response time: 5 (tenths of sec)
MVR Mode: compatible
```

In the preceding display, the maximum number of multicast groups is fixed at 500. The MVR mode is either compatible or dynamic.

Related Commands	Command	Description
	mvr (global configuration)	Enables and configures multicast VLAN registration on the switch.
	mvr (interface configuration)	Configures MVR ports.
	show mvr interface	Displays the configured MVR interfaces, status of the specified interface, or all multicast groups to which the interface belongs when the interface and members keywords are appended to the command.
	show mvr members	Displays all ports that are members of an MVR multicast group or, if there are no members, means the group is inactive.

show mvr interface

To display the Multicast VLAN Registration (MVR) receiver and source ports, use the **show mvr interface** privileged EXEC command without keywords. Use the command with keywords to display MVR parameters for a specific receiver port.

```
show mvr interface [interface-id [members [vlan vlan-id]]]
```

Syntax Description		
<i>interface-id</i>	(Optional) Specifies the MVR type, status, and Immediate Leave setting for the interface.	Valid interfaces include physical ports (including type, module, and port number).
members	(Optional) Displays all MVR groups to which the specified interface belongs.	
vlan <i>vlan-id</i>	(Optional) Displays all MVR group members on this VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094.	

Command Default Output shows all MVR-enabled ports on the switch

Command Modes Privileged EXEC

Command History	Release	Modification
	Release IOS XE 3.5.0E and IOS 15.2(1)E	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines If you enter only the **show mvr interface** command, the output shows all MVR-enabled ports on the switch.

If you enter the **show mvr interface interface-id** command and the specified port is non-MVR, the output displays NON MVR in the Type field. For active MVR ports, it displays the port type (RECEIVER or SOURCE), mode (access or trunk), VLAN, status, and Immediate-Leave setting.

If you enter the **members** keyword, all MVR group members on the interface are displayed. If you enter a VLAN ID, all MVR group members in the VLAN are displayed.

Examples This is an example of output from the **show mvr interface** command:

```
Switch# show mvr interface
Port      Type      Mode      VLAN      Status      Immediate Leave
----      -
Fa0/1    Receiver  Trunk     1          ACTIVE/UP   DISABLED
Fa0/1    Receiver  Trunk     2000      ACTIVE/DOWN DISABLED
Fa0/2    Receiver  Trunk     2          ACTIVE/UP   DISABLED
Fa0/2    Receiver  Trunk     3000      ACTIVE/UP   DISABLED
Fa0/3    Receiver  Trunk     2          ACTIVE/UP   DISABLED
```

```

Fa0/3 Receiver      Trunk      3000  ACTIVE/UP  DISABLED
Fa0/10 Source      Access     10    ACTIVE/UP  DISABLED

```

In the preceding display, Status is defined as follows:

- Active means that the port is part of a VLAN.
- Up/Down means that the port is forwarding or nonforwarding.
- Inactive means that the port is not yet part of any VLAN.

This is an example of output from the **show mvr interface interface-id** command:

```

switch# show mvr interface fa0/10
Port      Type      Mode      VLAN      Status      Immediate Leave
----      ----      ----      ----      -
Fa0/10    RECEIVER  Trunk     201      ACTIVE/DOWN  DISABLED

```

This is an example of output from the **show mvr interface interface-id members** command:

```

Switch# show mvr interface fastethernet1/0/6 members
239.255.0.0    DYNAMIC ACTIVE
239.255.0.1    DYNAMIC ACTIVE
239.255.0.2    DYNAMIC ACTIVE
239.255.0.3    DYNAMIC ACTIVE
239.255.0.4    DYNAMIC ACTIVE
239.255.0.5    DYNAMIC ACTIVE
239.255.0.6    DYNAMIC ACTIVE
239.255.0.7    DYNAMIC ACTIVE
239.255.0.8    DYNAMIC ACTIVE
239.255.0.9    DYNAMIC ACTIVE

```

Related Commands

Command	Description
mvr (global configuration)	Enables and configures multicast VLAN registration on the switch.
mvr (interface configuration)	Configures MVR ports.
show mvr	Displays the global MVR configuration on the switch.
show mvr members	Displays all receiver ports that are members of an MVR multicast group.

show mvr members

To display all receiver and source ports that are currently members of an IP multicast group, use the **show mvr members** privileged EXEC command.

```
show mvr members [ip-address]
```

Syntax Description	<i>ip-address</i>	(Optional) Specifies the IP multicast address. If the address is entered, all receiver and source ports that are members of the multicast group are displayed. If no address is entered, all members of all Multicast VLAN Registration (MVR) groups are listed. If a group has no members, the group is listed as Inactive.
---------------------------	-------------------	---

Command Default	Displays all the static and dynamic MVR members on the switch
------------------------	---

Command Modes	Privileged EXEC
----------------------	-----------------

Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Release IOS XE 3.5.0E and IOS 15.2(1)E</td> <td>This command was introduced on the Catalyst 4500 series switch.</td> </tr> </tbody> </table>	Release	Modification	Release IOS XE 3.5.0E and IOS 15.2(1)E	This command was introduced on the Catalyst 4500 series switch.
Release	Modification				
Release IOS XE 3.5.0E and IOS 15.2(1)E	This command was introduced on the Catalyst 4500 series switch.				

Usage Guidelines	The show mvr members command applies to receiver and source ports. For MVR compatible mode, all source ports are members of all multicast groups.
-------------------------	--

Examples	This is an example of output from the show mvr members command:
-----------------	--

```
Switch# show mvr members
MVR Group      Status  Members  VLAN  Membership
-----
239.1.1.1      ACTIVE  Fa0/1    1      Static
239.1.1.1      ACTIVE  Fa0/1    2000   Static
239.1.1.1      ACTIVE  Fa0/2    2      Static
239.1.1.1      ACTIVE  Fa0/2    3000   Static
239.1.1.2      ACTIVE  Fa0/1    1      Static
239.1.1.2      ACTIVE  Fa0/2    2      Static

<output truncated>

239.255.0.255  INACTIVE  None
239.255.1.0    INACTIVE  None
```

This is an example of output from the **show mvr members ip-address** command. It shows how to view the members of the IP multicast group 239.255.0.2.

```
Switch# show mvr members 239.255.0.2
Switch# show mvr members 239.255.0.2
239.255.0.2      ACTIVE                Fa1/0/1(d), Fa1/0/2(d), Fa1/0/3(d)
                                                Fa1/0/4(d), Fa1/0/5(s)
```

Related Commands

Command	Description
mvr (global configuration)	Enables and configures multicast VLAN registration on the switch.
mvr (interface configuration)	Configures MVR ports.
show mvr	Displays the global MVR configuration on the switch.
show mvr interface	Displays the configured MVR interfaces, status of the specified interface, or all multicast groups to which the interface belongs when the members keyword is appended to the command.

show netflow-lite exporter



Note

NetFlow-lite is only supported on the Catalyst 4948E and Catalyst 4948E-F Ethernet switches.

To display information about the collector and global stats, use the **show netflow-lite exporter** command.

show netflow-lite exporter *exporter-name*

Syntax Description

exporter-name Specifies an exporter name.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
15.0(2)SG	Command introduced on the Catalyst 4500 series switch.

Usage Guidelines

This command displays the total number of export packets sent.

Examples

The following example shows how to display information about the collector and global stats:

```
Switch# show netflow-lite exporter e1
Netflow-lite Exporter e1:
  Description:           Exporter
  Network Protocol Configuration:
    Destination IP address: 192.168.1.1
    VRF label:           cisc
    Source IP Address:    10.1.1.5
    DSCP:                0x1
    TTL:                 30
    COS:                 1
  Transport Protocol Configuration:
    Transport Protocol:   UDP
    Destination Port:    1234
    Source Port:         65535
  Export Protocol Configuration:
    Export Protocol:     netflow-v9
  Exporter Statistics:
    Export packets sent: 36
```


Related Commands	Command	Description
	destination (netflow-lite exporter submode)	
	vrf (netflow-lite exporter submode)	
	cos (netflow-lite exporter submode)	Specifies a cos value for the NetFlow-lite collector.
	source (netflow-lite exporter submode)	Specifies a source Layer 3 interface of the NetFlow-lite collector.
	transport udp (netflow-lite exporter submode)	Specifies a UDP transport destination port for a NetFlow-lite collector.
	ttl (netflow-lite exporter submode)	Specifies a ttl value for the NetFlow-lite collector.
	dscp (netflow-lite exporter submode)	Specifies a cos value for the NetFlow-lite collector.
	template data timeout (netflow-lite exporter submode)	Specifies a template data timeout for the NetFlow-lite collector.
	options timeout (netflow-lite exporter submode)	Specifies an options timeout for the NetFlow-lite collector.
	export-protocol (netflow-lite exporter submode)	Specifies the export protocol for the NetFlow-lite collector.

show netflow-lite monitor



Note

NetFlow-lite is only supported on the Catalyst 4948E and Catalyst 4948E-F Ethernet switches.

To display information about a particular packet or per data source stats, use the **show netflow-lite monitor** command.

```
show netflow-lite monitor monitor-number interface interface-name
```

```
show netflow-lite monitor monitor-number vlan vlan-id
```

Syntax Description

<i>monitor-number</i>	Specifies a monitor name.
<i>interface-name</i>	Specifies an interface.
<i>vlan-id</i>	Specifies a VLAN.

Command Default

None

Command Modes

Privileged EXEC mode

Command History

Release	Modification
15.0(2)SG	Command introduced on the Catalyst 4500 series switch.

Usage Guidelines

This command displays information about a particular packet or per data source stats. The interface can be either a physical port or a VLAN.

This command displays the following packet sampling statistics:

- Total # of packet (samples) exported
- Total # of packet (samples) dropped due to lack of local resources
- Total# of packets seen at the data source

The *packetsObserved* statistic accounts for packets that are dropped by input ACL or QoS policer.

The exported packets only represent samples from the non-dropped packet population.

Examples

These examples show how to display information about a particular packet or per data source stats:

```
Switch# show netflow-lite monitor 1 interface gi1/3
Interface GigabitEthernet1/3:
  Netflow-lite Monitor-1:
    Active:                TRUE
    Sampler:                sampler1
    Exporter:              exporter1
    Average Packet Size: 0
```

```

Statistics:
  Packets exported:      0
  Packets observed:     0
  Packets dropped:      0
  Average Packet Size observed: 64
  Average Packet Size used: 64

Switch# show netflow-lite monitor 1 vlan 2
VlanID-2:
Netflow-lite Monitor-1:
  Active:                TRUE
  Sampler:               sampler1
  Exporter:              exporter1
  Average Packet Size:   0
Statistics:
  Packets exported:      0
  Packets observed:     0
  Packets dropped:      0
  Average Packet Size observed: 64
  Average Packet Size used: 64

```

Related Commands

Command	Description
sampler (netflow-lite monitor submode)	Activates sampling on an interface in netflow-lite monitor submode.
exporter (netflow-lite monitor submode)	Assigns an exporter in netflow-lite monitor submode.
average-packet-size (netflow-lite monitor submode)	Specifies the average packet size at the observation point.

show netflow-lite sampler


Note

NetFlow-lite is only supported on the Catalyst 4948E and Catalyst 4948E-F Ethernet switches.

To display information about a sampler, use the **show netflow-lite sampler** command.

show netflow-lite sampler *sampler-name*

Syntax Description

<i>sampler-name</i>	Specifies a sampler name.
---------------------	---------------------------

Command Default

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
15.0(2)SG	Command introduced on the Catalyst 4500 series switch.

Examples

The following example shows how to display information about a sampler,:

```
Switch# show netflow-lite sampler low-rate
Netflow-lite Sampler low-rate:
  Description:      Sampler
  Sampling rate:    1 out of 256
  Packet Section Size: 64 bytes
  Packet offset:    0 bytes
```

Related Commands

Command	Description
packet-section size (netflow-lite sampler submode)	Specifies a sampled header size in netflow-lite submode.
packet-rate (netflow-lite sampler submode)	Specifies a packet sampling rate in netflow-lite sampler submode.
packet-offset (netflow-lite sampler submode)	Specifies a starting packet offset in netflow-lite submode.

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 your 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. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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	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# show nmsp attachment suppress interface
NMSP Attachment Suppression Interfaces
-----
GigabitEthernet1/1
GigabitEthernet1/2
Switch#
```

This is an example of output from the **show nmosp capability** command:

```
Switch# show nmosp capability
NMSP Switch Capability
-----
Service           Subservice
-----
Attachment        Wired Station
Location          Subscription
Switch#
```

This is an example of output from the **show nmosp notification interval** command:

```
Switch# show nmosp notification interval
NMSP Notification Intervals
-----
Attachment notify interval: 30 sec (default)
Location notify interval: 30 sec (default)
Switch#
```

This is an example of output from the **show nmosp statistics connection** and **show nmosp statistics summary** commands:

```
Switch# show nmosp statistics connection
NMSP Connection Counters
-----
Connection 1:
  Connection status: UP
  Freed connection: 0

  Tx message count           Rx message count
  -----
  Subscr Resp: 1             Subscr Req: 1
  Capa Notif: 1              Capa Notif: 1
  Atta Resp: 1               Atta Req: 1
  Atta Notif: 0
  Loc Resp: 1                 Loc Req: 1
  Loc Notif: 0
                                Unsupported msg: 0
Switch#

Switch# show nmosp statistics summary
NMSP Global Counters
-----
  Send too big msg: 0
  Failed socket write: 0
  Partial socket write: 0
  Socket write would block: 0
  Partial socket write: 0
  Failed socket read: 0
  Socket read would block: 0
  Transmit Q full: 0
  Max Location Nofity Msg: 0
  Max Attachement Notify Msg: 0
  Max TX Q Size: 0
Switch#
```

This is an example of output from the **show nmsp status** command:

```
Switch# show nmsp status
NMSP Status
-----
NMSP: enabled

MSE IP Address      TxEchoResp RxEchoReq TxData RxData
-----
172.19.35.109      5          5          4      4
Switch#
```

This is an example of output from the **show nmsp show subscription detail** and **show nmsp show subscription summary** commands:

```
Switch# show nmsp subscription detail
Mobility Services Subscribed by 172.19.35.109:
Services           Subservices
-----
Attachment:       Wired Station
Location:         Subscription

Switch# show nmsp subscription summary
Mobility Services Subscribed:
MSE IP Address      Services
-----
172.19.35.109      Attachment, Location
Switch#
```

Related Commands

Command	Description
clear nmsp statistics	Clears the NMSP statistic counters.
nmsp	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

<i>group-number</i>	(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.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

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

Usage Guidelines

You can enter any **show pagp** command to display the active PAgP port-channel information. To display the nonactive information, enter the **show pagp** command with a group.

Examples

The following example shows how to display information about the PAgP counter:

```
Switch# show pagp counters
          Information          Flush
Port      Sent  Recv      Sent  Recv
-----
Channel group: 1
  Fa5/4    2660  2452      0     0
  Fa5/5    2676  2453      0     0
Channel group: 2
  Fa5/6    289   261       0     0
  Fa5/7    290   261       0     0
Switch#
```

The following example shows how to display PAgP dual-active information:

```
Switch# show pagp dual-active
PAgP dual-active detection enabled: Yes
PAgP dual-active version: 1.1
```



```

Channel group 30
Dual-Active Partner Partner
Port Detect Capable Name Port Version
Te3/1 Yes VS1-Reg2 Te1/1/7 1.1
Te4/1 Yes VS1-Reg2 Te2/2/8 1.1

```

```

Channel group 32
Dual-Active Partner Partner
Port Detect Capable Name Port Version
Gi1/43 Yes VS3 Gi1/1/43 1.1
Gi1/44 Yes VS3 Gi1/1/44 1.1
Gi1/45 Yes VS3 Gi1/1/45 1.1
Gi1/46 Yes VS3 Gi2/1/46 1.1
Gi1/47 Yes VS3 Gi2/1/47 1.1
Gi1/48 Yes VS3 Gi2/1/48 1.1
Gi2/3 Yes VS3 Gi1/1/1 1.1
Gi2/4 Yes VS3 Gi2/1/1 1.1
Switch#

```

The following 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.
Timers: H - Hello timer is running. Q - Quit timer is running.
        S - Switching timer is running. I - Interface timer is running.

```

```

Channel group 1

```

Port	Flags	State	Timers	Hello Interval	Partner Count	PAgP Priority	Learning Method	IfIndx
Fa5/4	SC	U6/S7		30s	1	128	Any	129
Fa5/5	SC	U6/S7		30s	1	128	Any	129

```

Switch#

```

The following 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

```

Port	Partner Name	Partner Device ID	Partner Port	Age	Partner Flags	Partner Group Cap.
Fa5/4	JAB031301	0050.0f10.230c	2/45	2s	SAC	2D
Fa5/5	JAB031301	0050.0f10.230c	2/46	27s	SAC	2D

```

Channel group 2 neighbors

```

Port	Partner Name	Partner Device ID	Partner Port	Age	Partner Flags	Partner Group Cap.
Fa5/6	JAB031301	0050.0f10.230c	2/47	10s	SAC	2F
Fa5/7	JAB031301	0050.0f10.230c	2/48	11s	SAC	2F

```

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 pagp dual-active (virtual switch)

To display dual-active detection information, use the **show pagp dual-active** command in EXEC mode.

```
show pagp [group-number] dual-active
```

Syntax Description	<i>group-number</i> (Optional) Channel-group number. Range: 1 to 256 with a maximum of 64 values.				
Command Default	This command has no default settings.				
Command Modes	Privileged EXEC mode				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.2(52)SG</td> <td>This command was introduced on the Catalyst 4500 series switch.</td> </tr> </tbody> </table>	Release	Modification	12.2(52)SG	This command was introduced on the Catalyst 4500 series switch.
Release	Modification				
12.2(52)SG	This command was introduced on the Catalyst 4500 series switch.				

Examples

The following example shows how to display dual-active detection information:

```
Router# show pagp dual-active
PAgP dual-active detection enabled: Yes
PAgP dual-active version: 1.1
Channel group 1
Dual-Active trusted group: Yes
Channel group 2
Dual-Active trusted group: Yes
Channel group 3 dual-active detect capability w/nbrs
Dual-Active trusted group: No
      Dual-Active   Partner           Partner   Partner
Port   Detect Capable Name           Port      Version
Fa1/2/33 No             None           None      N/A
Router#
```

The following example shows how to display dual-active detection information for a specific port channel:

```
Router# show pagp dual-active
PAgP dual-active detection enabled: Yes
PAgP dual-active version: 1.1
Channel group 3 dual-active detect capability w/nbrs Dual-Active trusted group: No
      Dual-Active   Partner           Partner   Partner
Port   Detect Capable Name           Port      Version
Fa1/2/33 No             None           None      N/A
Channel group 4
Dual-Active trusted group: Yes
No interfaces configured in the channel group
Channel group 5
Dual-Active trusted group: Yes
Channel group 5 is not participating in PAGP
Channel group 10 dual-active detect capability w/nbrs Dual-Active trusted group: Yes
      Dual-Active   Partner           Partner   Partner
Port   Detect Capable Name           Port      Version
Gi1/6/1 Yes             mr-rogers-nbr   Gi1/5/1   1.1
```

```

Gi2/5/1  Yes          mr-rogers-nbr          Gi1/5/2  1.1
Channel group 11 dual-active detect capability w/nbrs Dual-Active trusted group: No
Dual-Active Partner Partner Partner
Port Detect Capable Name Port Version
Gi1/6/2  Yes          mr-rogers-nbr          Gi1/3/1  1.1
Gi2/5/2  Yes          mr-rogers-nbr          Gi1/3/2  1.1
Channel group 12 dual-active detect capability w/nbrs Dual-Active trusted group: Yes
Dual-Active Partner Partner Partner
Port Detect Capable Name Port Version
Fa1/2/13 Yes          mr-rogers-nbr          Fa1/2/13 1.1
Fa1/2/14 Yes          mr-rogers-nbr          Fa1/2/14 1.1
Gi2/1/15 Yes          mr-rogers-nbr          Fa1/2/15 1.1
Gi2/1/16 Yes          mr-rogers-nbr          Fa1/2/16 1.1
Router#

```

The following example shows how to display dual-active detection information for a specific port channel:

```

Router# show pagp dual-active
PAGP dual-active detection enabled: Yes
PAGP dual-active version: 1.1
Channel group 3 dual-active detect capability w/nbrs
Dual-Active trusted group: No
Dual-Active Partner Partner Partner
Port Detect Capable Name Port Version
Fa1/2/33 No          None          None      N/A
Router#

```

Related Commands

Command	Description
dual-active detection (virtual switch)	Enables and configures dual-active detection.

show policy-map

To display information about the policy map, use the **show policy-map** command.

```
show policy-map [policy_map_name]
```

Syntax Description	<i>policy_map_name</i> (Optional) Name of the policy map.
---------------------------	---

Command Default	This command has no default settings.
------------------------	---------------------------------------

Command Modes	Privileged EXEC mode
----------------------	----------------------

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

Examples The following example shows how to display information for all the policy maps:

```
Switch# show policy-map
Policy Map ipp5-policy
  class ipp5
    set ip precedence 6
Switch#
```

The following example shows how to display information for a specific policy map:

```
Switch# show policy ipp5-policy
Policy Map ipp5-policy
  class ipp5
    set ip precedence 6
Switch#
```

Related Commands	Command	Description
	class-map	Creates a class map to be used for matching packets to the class whose name you specify and to enter class-map configuration mode
	policy-map	Creates a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode
	show class-map	Displays class map information.
	show policy-map interface	Displays the statistics and configurations of the input and output policies that are attached to an interface.

show policy-map control-plane

To display the configuration either of a class or of all classes for the policy map of a control plane, use the **show policy-map control-plane** command.

```
show policy-map control-plane [input [class class-name] | [class class-name]]
```

Syntax Description

input	(Optional) Displays statistics for the attached input policy.
class class-name	(Optional) Displays the name of the class.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

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

Usage Guidelines

This command is not supported on Supervisor Engine 6-E, Supervisor Engine 6L-E, Catalyst 4900M, Catalyst 4948E, and Catalyst 4948E-F.

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

The following 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 2-40](#) describes the fields shown in the display.

```
Switch# show policy-map control-plane

Control Plane

  Service-policy input: system-cpp-policy

    Class-map: system-cpp-eapol (match-all)
      0 packets
      Match: access-group name system-cpp-eapol

    Class-map: system-cpp-bpdu-range (match-all)
      0 packets
      Match: access-group name system-cpp-bpdu-range

    Class-map: system-cpp-cdp (match-all)
      28 packets
      Match: access-group name system-cpp-cdp
      police: Per-interface
      Conform: 530 bytes Exceed: 0 bytes
```

```
Class-map: system-cpp-garp (match-all)
  0 packets
  Match: access-group name system-cpp-garp

Class-map: system-cpp-sstp (match-all)
  0 packets
  Match: access-group name system-cpp-sstp

Class-map: system-cpp-cgmp (match-all)
  0 packets
  Match: access-group name system-cpp-cgmp

Class-map: system-cpp-ospf (match-all)
  0 packets
  Match: access-group name system-cpp-ospf

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-ripv2 (match-all)
  0 packets
  Match: access-group name system-cpp-ripv2

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-sc (match-all)
  0 packets
  Match: access-group name system-cpp-dhcp-sc

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
  Match: any
    0 packets
Switch#
```

Table 2-40 show policy-map control-plane Field Descriptions

Field	Description
Fields Associated with Classes or Service Policies	
Service-policy input	Name of the input service policy that is applied to the control plane. (If configured, this field will also show the output service policy.)
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 <i>Cisco IOS Quality of Service Solutions Configuration Guide</i> .
Fields Associated with Traffic Policing	
police	police command has been configured to enable traffic policing.
conformed	Action to be taken on packets conforming to a specified rate; displays the number of packets and bytes on which the action was taken.
exceeded	Action to be taken on packets exceeding a specified rate; displays the number of packets and bytes on which the action was taken.

Related Commands

Command	Description
control-plane	Enters control-plane configuration mode.
service-policy input (control-plane)	Attaches a policy map to a control plane for aggregate control plane services.

show policy-map interface

To display the statistics and configurations of the input and output policies that are attached to an interface, use the **show policy-map interface** command.

```
show policy-map interface [{fastethernet interface-number} | {gigabitethernet
interface-number} | {port-channel number} | {vlan vlan_id}] [input | output]
```

Syntax Description		
fastethernet <i>interface-number</i>	(Optional)	Specifies the Fast Ethernet 802.3 interface.
gigabitethernet <i>interface-number</i>	(Optional)	Specifies the Gigabit Ethernet 802.3z interface.
port-channel <i>number</i>	(Optional)	Specifies the port channel.
vlan <i>vlan_id</i>	(Optional)	Specifies the VLAN ID; valid values are from 1 to 4094.
input	(Optional)	Specifies input policies only.
output	(Optional)	Specifies output policies only.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW	Added support for extended VLAN addresses.
	12.2(25)SG	Displays results for full flow policing.

Examples The following example shows how to display the statistics and configurations of all input and output policies attached to an interface:

```
Switch# show policy-map interface

FastEthernet6/1

  service-policy input:ipp5-policy

    class-map:ipp5 (match-all)
      0 packets
      match:ip precedence 5
      set:
        ip precedence 6

    class-map:class-default (match-any)
      0 packets
      match:any
      0 packets
```



```

service-policy output:ipp5-policy

class-map:ipp5 (match-all)
  0 packets
  match:ip precedence 5
  set:
    ip precedence 6

class-map:class-default (match-any)
  0 packets
  match:any
  0 packets
Switch#

```

The following 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:ipp5-policy

class-map:ipp5 (match-all)
  0 packets
  match:ip precedence 5
  set:
    ip precedence 6

class-map:class-default (match-any)
  0 packets
  match:any
  0 packets
Switch#

```

With 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# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# class-map c1
Switch(config-cmap)# match flow ip source-address ip destination-address ip protocol 14
source-port 14 destination-port
Switch(config-cmap)# exit
Switch(config)# policy-map p1
Switch(config-pmap)# class c1
Switch(config-pmap-c)# police 1000000 9000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastEthernet 6/1
Switch(config-if)# service-policy input p1
Switch(config-if)# end
Switch# write memory
Switch# show policy-map interface
FastEthernet6/1

class-map c1
  match flow ip source-address ip destination-address ip protocol 14 source-port 14
  destination-port
  !
  policy-map p1

```

```

class c1
  police 1000000 bps 9000 byte conform-action transmit exceed-action drop
!
interface FastEthernet 6/1
  service-policy input p1

Switch# show policy-map p1
  Policy Map p1
    Class c1
      police 1000000 bps 9000 byte conform-action transmit exceed-action drop

Switch# show policy-map interface
  FastEthernet6/1

    Service-policy input: p1

      Class-map: c1 (match-all)
        15432182 packets
        Match: flow ip source-address ip destination-address ip protocol 14 source-port 14
        destination-port
          police: Per-interface
            Conform: 64995654 bytes Exceed: 2376965424 bytes

      Class-map: class-default (match-any)
        0 packets
        Match: any
          0 packets
Switch#

```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to the class whose name you specify and to be used enter class-map configuration mode.
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 <i>interface-id</i>	(Optional) Displays QoS policy-map information for a specific interface.
vlan <i>vlan-id</i>	(Optional) Displays QoS policy-map information for a specific VLAN.

Command Modes

Privileged EXEC mode

Command History

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

Examples

The following example show a configuration on a non-Supervisor Engine 6-E:

```
interface GigabitEthernet3/1
  vlan-range 20,400
  service-policy input p1
  vlan-range 300-301
  service-policy output p2
```

The following example shows how to display policy-map statistics on VLAN 20 on the Gigabit Ethernet 6/1 interface:

```
Switch# show policy-map interface gigabitEthernet 3/1 vlan 20
GigabitEthernet3/1 vlan 20

  Service-policy input: p1

    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets
      police: Per-interface
        Conform: 0 bytes Exceed: 0 bytes
Switch#
```

The following example shows a configuration on a non-Supervisor Engine 6-E:

```
interface fastEthernet6/1
  vlan-range 100
  service-policy in p1
```

The following 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

FastEthernet6/1 vlan 100

  Service-policy input: p1
```

```

Class-map: c1 (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
  vlan-range 100
  service-policy in p1

```

The following 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: c1 (match-all)
  0 packets
  Match: ip dscp af11 (10)
  police:
    rate 128000 bps, burst 4000 bytes
    conformed 0 packets, 0 bytes; action:
      transmit
    exceeded 0 packets, 0 bytes; action:
      drop
    conformed 0 bps, exceeded 0 bps

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 interface.
vlan vlan-id	(Optional)	Displays port security settings for a specific VLAN.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.1(13)EW	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 per-VLAN basis.
	12.2(31)SGA	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

The following 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
      Fa3/10          1             0             0             Shutdown
      Fa3/11          1             0             0             Shutdown
      Fa3/12          1             0             0             Restrict
      Fa3/13          1             0             0             Shutdown
      Fa3/14          1             0             0             Shutdown
      Fa3/15          1             0             0             Shutdown
      Fa3/16          1             0             0             Shutdown
      Po2             3             1             0             Shutdown
-----
Total Addresses in System (excluding one mac per port)  :8
Max Addresses limit in System (excluding one mac per port) :3072
Global SNMP trap control for port-security             :20 (traps per second)
Switch#
```

The following example shows how to display port security settings for interface Fast Ethernet port 1:

```
Switch# show port-security interface fastethernet 5/1
Port Security           : Enabled
Port Status             : Secure-up
Violation Mode          : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses     : 1
Configured MAC Addresses : 0
Sticky MAC Addresses    : 1
Last Source Address     : 0000.0001.001a
Security Violation Count : 0
Switch#
```

The following 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    Fa3/1    15 (I)
      1    0000.0001.0001    SecureConfigured    Fa3/1    14 (I)
      1    0000.0001.0100    SecureConfigured    Fa3/2    -
      1    0000.0001.0101    SecureConfigured    Fa3/2    -
      1    0000.0001.0200    SecureConfigured    Fa3/3    -
      1    0000.0001.0201    SecureConfigured    Fa3/3    -
      1    0000.0001.0300    SecureConfigured    Fa3/4    -
      1    0000.0001.0301    SecureConfigured    Fa3/4    -
      1    0000.0001.1000    SecureDynamic        Fa3/5    -
      1    0000.0001.1001    SecureDynamic        Fa3/5    -
```

```

1 0000.0001.1100 SecureDynamic Fa3/6 -
1 0000.0001.1101 SecureDynamic Fa3/6 -
1 0000.0001.1200 SecureSticky Fa3/7 -
1 0000.0001.1201 SecureSticky Fa3/7 -
1 0000.0001.1300 SecureSticky Fa3/8 -
1 0000.0001.1301 SecureSticky Fa3/8 -
1 0000.0001.2000 SecureSticky Po2 -

```

```

-----
Total Addresses in System (excluding one mac per port) :8
Max Addresses limit in System (excluding one mac per port) :3072

```

The following 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: 22
VLAN Maximum Current
  2         22      3
  3         22      3
  4         22      3
  5         22      1
  6         22      2

```

The following example shows how to display the port security settings on interface GigabitEthernet1/1 for VLANs 2 and 3:

```

Switch# show port-security interface gigabitEthernet1/1 vlan 2-3
Default maximum: 22
VLAN Maximum Current
  2         22      3
  3         22      3

```

The following example shows how to display all secure MAC addresses configured on interface GigabitEthernet1/1 with aging information for each address.

```

Switch# show port-security interface gigabitEthernet1/1 address

```

```

Secure Mac Address Table
-----
Vlan Mac Address Type Ports Remaining Age(mins)
----
  2 0001.0001.0001 SecureConfigured Gi1/1 -
  2 0001.0001.0002 SecureSticky Gi1/1 -
  3 0001.0001.0001 SecureConfigured Gi1/1 -
  3 0001.0001.0002 SecureSticky Gi1/1 -
  3 0001.0001.0003 SecureSticky Gi1/1 -
  4 0001.0001.0001 SecureConfigured Gi1/1 -
  4 0001.0001.0003 SecureSticky Gi1/1 -
  6 0001.0001.0001 SecureConfigured Gi1/1 -
  6 0001.0001.0002 SecureConfigured Gi1/1 -

```

```

Total Addresses: 12

```

The following 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 -
  2 0001.0001.0002 SecureSticky Gi1/1 -

```

```

2    0001.0001.0003    SecureSticky          Gi1/1    -
3    0001.0001.0001    SecureConfigured     Gi1/1    -
3    0001.0001.0002    SecureSticky          Gi1/1    -
3    0001.0001.0003    SecureSticky          Gi1/1    -

```

```

-----
Total Addresses: 12
Switch#

```

The following example shows how to display the maximum allowed number of secure MAC addresses and the current number of secure MAC addresses on Fast Ethernet port 1:

```

Switch# show port-security interface fastethernet5/1 vlan
Default maximum: 22
VLAN Maximum Current
2          22      3
3          22      3
5          22      1
6          22      2
Switch#

```

The following example shows how to display the port security settings on Fast Ethernet port 1 for VLANs 2 and 3:

```

Switch# show port-security interface fastethernet5/1 vlan 2-3
Default maximum: 22
VLAN Maximum Current
2          22      3
3          22      3
Switch#

```

The following 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 -
2    0001.0001.0002 SecureSticky      Gi1/1 -
2    0001.0001.0003 SecureSticky      Gi1/1 -
3    0001.0001.0001 SecureConfigured Gi1/1 -
3    0001.0001.0002 SecureSticky      Gi1/1 -
3    0001.0001.0003 SecureSticky      Gi1/1 -
4    0001.0001.0001 SecureConfigured Gi1/1 -
4    0001.0001.0002 SecureSticky      Gi1/1 -
4    0001.0001.0003 SecureSticky      Gi1/1 -
5    0001.0001.0001 SecureConfigured Gi1/1 -
6    0001.0001.0001 SecureConfigured Gi1/1 -
6    0001.0001.0002 SecureConfigured Gi1/1 -
-----
Total Addresses: 12
Switch#

```

The following 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      SecureSticky          Gi1/1      -
      2      0001.0001.0003      SecureSticky          Gi1/1      -
      3      0001.0001.0001      SecureConfigured      Gi1/1      -
      3      0001.0001.0002      SecureSticky          Gi1/1      -
      3      0001.0001.0003      SecureSticky          Gi1/1      -
-----

```

```

Total Addresses: 12
Switch#

```

The following 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    Fa3/1      15 (I)
      1    0000.0001.0001    SecureConfigured    Fa3/1      14 (I)
      1    0000.0001.0100    SecureConfigured    Fa3/2      -
      1    0000.0001.0101    SecureConfigured    Fa3/2      -
      1    0000.0001.0200    SecureConfigured    Fa3/3      -
      1    0000.0001.0201    SecureConfigured    Fa3/3      -
      1    0000.0001.0300    SecureConfigured    Fa3/4      -
      1    0000.0001.0301    SecureConfigured    Fa3/4      -
      1    0000.0001.1000    SecureDynamic       Fa3/5      -
      1    0000.0001.1001    SecureDynamic       Fa3/5      -
      1    0000.0001.1100    SecureDynamic       Fa3/6      -
      1    0000.0001.1101    SecureDynamic       Fa3/6      -
      1    0000.0001.1200    SecureSticky        Fa3/7      -
      1    0000.0001.1201    SecureSticky        Fa3/7      -
      1    0000.0001.1300    SecureSticky        Fa3/8      -
      1    0000.0001.1301    SecureSticky        Fa3/8      -
-----

```

```

Total Addresses in System (excluding one mac per port) :8
Max Addresses limit in System (excluding one mac per port) :3072
Switch#

```

The following 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: 22
VLAN Maximum Current
      2          22      3
      3          22      3
      4          22      3
      5          22      1
      6          22      2
Switch#

```

The following example shows how to display the port security settings on interface GigabitEthernet1/1 for VLANs 2 and 3:

```

Switch# show port-security interface gigabitethernet1/1 vlan 2-3
Default maximum: 22
VLAN Maximum Current
      2          22      3
      3          22      3
Switch#

```

The following example shows how to display all secure MAC addresses configured on interface GigabitEthernet1/1 with aging information for each address.

```
Switch# show port-security interface gigabitEthernet1/1 address
```

```

Secure Mac Address Table
-----
Vlan    Mac Address      Type                Ports    Remaining Age (mins)
----    -
2       0001.0001.0001  SecureConfigured   Gi1/1    -
2       0001.0001.0002  SecureSticky       Gi1/1    -
3       0001.0001.0001  SecureConfigured   Gi1/1    -
3       0001.0001.0002  SecureSticky       Gi1/1    -
3       0001.0001.0003  SecureSticky       Gi1/1    -
4       0001.0001.0001  SecureConfigured   Gi1/1    -
4       0001.0001.0003  SecureSticky       Gi1/1    -
6       0001.0001.0001  SecureConfigured   Gi1/1    -
6       0001.0001.0002  SecureConfigured   Gi1/1    -
-----
Total Addresses: 12
Switch#
```

The following 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    -
2       0001.0001.0002  SecureSticky       Gi1/1    -
2       0001.0001.0003  SecureSticky       Gi1/1    -
3       0001.0001.0001  SecureConfigured   Gi1/1    -
3       0001.0001.0002  SecureSticky       Gi1/1    -
3       0001.0001.0003  SecureSticky       Gi1/1    -
-----
Total Addresses: 12
Switch#
```

Related Commands

Command	Description
switchport port-security	Enables port security on an interface.

show power

To display information about the power status, use the **show power** command.

show power [**available** | **capabilities** | **detail** | **inline** {[*interface*] **detail** | **consumption default** | **module** *mod* **detail**}] | **module** | **status** | **supplies**]

Syntax Description		
available	(Optional)	Displays the available system power.
capabilities	(Optional)	Displays the individual power supply capabilities.
detail	(Optional)	Displays detailed information on power resources.
inline	(Optional)	Displays the PoE status.
<i>interface</i> detail	(Optional)	Detailed information on the PoE status for the interface
consumption default	(Optional)	Displays the PoE consumption.
module <i>mod</i> default	(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.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch.
	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 Admin
```

The **show power inline** *interface* | *module* command displays the amount of power that is used to operate a Cisco IP Phone. To view the amount of power requested, use the **show cdp neighbors** command.

Because FPGAs 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 nonzero 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 The following 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-C45-1000AC        AC 1000W      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
(in Watts)          Used          Maximum
-----
System Power (12V)   328           1360
Inline Power (-50V)  0             1400
Backplane Power (3.3V) 10            40
-----
Total Used          338 (not to exceed Total Maximum Available = 750)
Switch#
```

The following example shows how to display the amount of available system power:

```
Switch# show power available
Power Summary
(in Watts)  Available  Used  Remaining
-----
System Power  1360      280   1080
Inline Power  1400      0     1400
Maximum Power 2800      280   2520
Switch#
```


Note

The “Inline Power Oper” column displays the PoE consumed by the powered devices attached to the module in addition to the PoE consumed by the FPGAs and other hardware components on the module. The “Inline Power Admin” column displays only the PoE allocated by the powered devices attached to the module.

The following 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 System System Maximum
-----
PS1           1400   1400   1360   1360   2800
PS2           1400   1400   1360   1360   2800
Switch#
```

The following example shows how to verify the PoE consumption for the switch:

```
Switch# show power inline consumption default
Default PD consumption : 5000 mW
Switch#
```

The following 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		
Fa3/1	auto	on	17.3	15.4	Ieee PD	0
Fa3/2	auto	on	4.5	4.0	Ieee PD	1
Fa3/3	auto	on	7.1	6.3	Cisco IP Phone 7960	0
Fa3/4	auto	on	7.1	6.3	Cisco IP Phone 7960	n/a
Fa3/5	auto	on	17.3	15.4	Ieee PD	0
Fa3/6	auto	on	17.3	15.4	Ieee PD	0
Fa3/7	auto	on	4.5	4.0	Ieee PD	1
Fa3/8	auto	on	7.9	7.0	Ieee PD	2
Fa3/9	auto	on	17.3	15.4	Ieee PD	3
Fa3/10	auto	on	17.3	15.4	Ieee PD	4
Fa3/11	auto	off	0	0	n/a	n/a
Fa3/12	auto	off	0	0	n/a	n/a
Fa3/13	auto	off	0	0	n/a	n/a
Fa3/14	auto	off	0	0	n/a	n/a
Fa3/15	auto	off	0	0	n/a	n/a
Fa3/16	auto	off	0	0	n/a	n/a
Fa3/17	auto	off	0	0	n/a	n/a
Fa3/18	auto	off	0	0	n/a	n/a

```
Totals:          10  on  117.5  104.6
```

```
Switch#
```

The following 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#
```

The following example shows how to display the PoE status for Fast Ethernet interface 3/1:

```
Switch# show power inline fastethernet3/1
```

```
Available:677(w) Used:11(w) Remaining:666(w)
```

Interface	Admin	Oper	Power(Watts)		Device	Class
			From PS	To Device		
Fa3/1	auto	on	11.2	10.0	Ieee PD	0

Interface	AdminPowerMax (Watts)	AdminConsumption (Watts)
Fa3/1	15.4	10.0

```
Switch#
```

The output of the commands **show power detail** and **show power module** display the supervisor engine's variable power consumption and its inline power summary:

```
Switch# show power detail
```

```
sh power detail
```

Power Supply	Model No	Type	Status	Fan Sensor	Inline Status
PS1	PWR-C45-1400DC	DCSP1400W	good	good	n.a.

show power

```

PS1-1          12.5A    good
PS1-2          15.0A    off
PS1-3          15.0A    off
PS2    none          --      --      --      --

```

```

Power supplies needed by system : 1
Power supplies currently available : 1

```

```

Power Summary
(in Watts)          Used      Maximum
                    -----
System Power (12V)  360      360
Inline Power (-50V)  0         0
Backplane Power (3.3V)  0         40
                    -----

```

```

Total              360      400

```

```

Module Inline Power Summary (Watts)
(12V -> -48V on board conversion)
-----

```

```

Mod      Used      Maximum
-----
1         5         25
-----

```

```

Mod      Model          Watts Used of System Power (12V)
                    currently  out of reset  in reset
-----
1      WS-X4013+TS          180          180          180
2      WS-X4506-GB-T          60           60           20
3      WS-X4424-GB-RJ45       90           90           50
--     Fan Tray             30           --           --
-----
Total              360          330          250

```

```

Watts used of Chassis Inline Power (-50V)
Inline Power Admin  Inline Power Oper
Mod      Model          PS      Device      PS      Device      Efficiency
-----
2      WS-X4506-GB-T          0         0           0         0           89
3      WS-X4424-GB-RJ45       -         -           -         -           -
-----
Total              0         0           0         0

```

```

Watts used of Module Inline Power (12V -> -50V)
Inline Power Admin  Inline Power Oper
Mod      Model          PS      Device      PS      Device      Efficiency
-----
1      WS-X4013+TS          6         5           3         3           90
-----

```

```

Switch# show power module
sh power module

```

```

Mod      Model          Watts Used of System Power (12V)
                    currently  out of reset  in reset
-----
1      WS-X4013+TS          180          180          180
2      WS-X4506-GB-T          60           60           20
3      WS-X4424-GB-RJ45       90           90           50
--     Fan Tray             30           --           --
-----
Total              360          330          250

```

```

Watts used of Chassis Inline Power (-50V)

```

Mod	Model	Inline Power Admin		Inline Power Oper		Efficiency
		PS	Device	PS	Device	
2	WS-X4506-GB-T	0	0	0	0	89
3	WS-X4424-GB-RJ45	-	-	-	-	-
Total		0	0	0	0	

Watts used of Module Inline Power (12V -> -50V)

Mod	Model	Inline Power Admin		Inline Power Oper		Efficiency
		PS	Device	PS	Device	
1	WS-X4013+TS	6	5	3	3	90

Switch#

The following example shows how to display detailed information on the PoE status for Gigabit interface 2/1:

```
Switch# show power inline g2/1 detail
Available:800(w) Used:71(w) Remaining:729(w)

Interface: Gi2/1
Inline Power Mode: auto
Operational status: on
Device Detected: yes
Device Type: Cisco IP Phone 7970
IEEE Class: 3
Discovery mechanism used/configured: Ieee and Cisco
Police: off

Power Allocated
Admin Value: 20.0
Power drawn from the source: 11.0
Power available to the device: 10.3

Actual consumption
Measured at the port: 5.0
Maximum Power drawn by the device since powered on: 5.2

Absent Counter: 0
Over Current Counter: 0
Short Current Counter: 0
Invalid Signature Counter: 0
Power Denied Counter: 0
```

Switch#

The following example shows how to display the PoE status for all all ports of the module:

```
Switch# show module
Chassis Type : WS-C4503-E

Power consumed by backplane : 0 Watts

Mod Ports Card Type Model Serial No.
-----+-----+-----+-----+-----+
1 6 Sup 6-E 10GE (X2), 1000BaseX (SFP) WS-X45-SUP6-E JAE1132SXR
3 48 10/100/1000BaseT POE E Series WS-X4648-RJ45V-E JAE114740YF

M MAC addresses Hw Fw Sw Status
-----+-----+-----+-----+-----+
1 0017.94c8.f580 to 0017.94c8.f585 0.4 12.2(44r)SG( 12.2(52) Ok
```

```
3 001e.7af1.f5d0 to 001e.7af1.f5ff 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
Device Detected: no
Device Type: n/a
IEEE Class: n/a
Discovery mechanism used/configured: Ieee and Cisco
Police: 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: Gi3/2
Inline Power Mode: auto
Operational status: off
Device Detected: no
Device Type: n/a
IEEE Class: n/a
Discovery mechanism used/configured: Ieee and Cisco
Police: 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: Gi3/3
Inline Power Mode: auto
Operational status: off
Device Detected: no
Device Type: n/a
IEEE Class: n/a
Discovery mechanism used/configured: Ieee and Cisco
Police: 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: Gi3/4
Inline Power Mode: auto
Operational status: off
Device Detected: no
Device Type: n/a
IEEE Class: n/a
Discovery mechanism used/configured: Ieee and Cisco
Police: 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 Power Mode: auto
Operational status: off
Device Detected: no
Device Type: n/a
IEEE Class: n/a
Discovery mechanism used/configured: Ieee and Cisco
Police: 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: Gi3/6
Inline Power Mode: auto
```

```

Operational status: off
Device Detected: no
Device Type: n/a
IEEE Class: n/a
Discovery mechanism used/configured: Ieee and Cisco
Police: off

Power Allocated
Admin Value: 20.0
Power drawn from the source: 0.0
Power available to the device: 0.0
.....

```

Related Commands

Command	Description
power dc input	Configures the power DC input parameters on the switch.
power inline	Sets the inline-power state for the inline-power-capable interfaces.
power inline consumption	Sets the default power that is allocated to an interface for all the inline-power-capable interfaces on the switch.
power redundancy-mode	Configures the power settings for the chassis.

show power inline police

To display PoE policing and monitoring status, use the **show power inline police** command.

show power inline police [*interfacename*] [**module** *n*]

Syntax Description	
<i>interfacename</i>	(optional) Displays PoE policing and monitoring status for a particular interface.
module <i>n</i>	(optional) Display PoE policing and monitoring status for all interfaces on this module.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.2(50)SG	This command was introduced on the Catalyst 4500 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 The following example shows how to display PoE policing status for a interface GigabitEthernet 2/1:

```
Switch# show power inline police gigabitEthernet 2/1
Available:421(w) Used:44(w) Remaining:377(w)

Interface Admin Oper      Admin      Oper      Cutoff Oper
           State State      Police     Police     Power  Power
-----
Gi2/1     auto  on        errdisable ok        22.6   9.6
```

Related Commands	Command	Description
	power inline police	Configures PoE policing on a particular interface.

show pppoe intermediate-agent interface

To display PPPoE Intermediate Agent configuration and statistics (packet counters), use the **show pppoe intermediate-agent interface** command.

show pppoe intermediate-agent information interface *interface*

show pppoe intermediate-agent statistics interface *interface*

Syntax Description	interface <i>interface</i> Interface for which information or statistics are displayed.				
Command Default	This command has no default settings.				
Command Modes	Privileged EXEC mode				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.2(50)SG</td> <td>This command was introduced on the Catalyst 4500 series switch.</td> </tr> </tbody> </table>	Release	Modification	12.2(50)SG	This command was introduced on the Catalyst 4500 series switch.
Release	Modification				
12.2(50)SG	This command was introduced on the Catalyst 4500 series switch.				

Examples

The following 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           IA           Trusted    Vsa Strip   Rate limit (pps)
-----
GigabitEthernet3/4   no          yes        yes         unlimited
PPPoE Intermediate-Agent is configured on following VLANs:
2-3
GigabitEthernet3/7   no          no         no          unlimited
PPPoE Intermediate-Agent is configured on following VLANs:
2-3
```

The following example shows how to display PPPoE Intermediate Agent statistics on an interface:

```
Switch# show pppoe intermediate-agent statistics interface g3/7
Interface : GigabitEthernet3/7
Packets received
All = 3
PADI = 0 PADO = 0
PADR = 0 PADS = 0
PADT = 3
Packets dropped:
Rate-limit exceeded = 0
Server responses from untrusted ports = 0
Client requests towards untrusted ports = 0
Malformed PPPoE Discovery packets = 0
Vlan 2: Packets received PADI = 6 PADO = 0 PADR = 6 PADS = 0 PADT = 6
Vlan 3: Packets received PADI = 4 PADO = 0 PADR = 4 PADS = 0 PADT = 4
```

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.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

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

Usage Guidelines This command is not supported on Supervisor Engine 6-E, Supervisor Engine 6L-E, Catalyst 4900M, Catalyst 4948E, and Catalyst 4948E-F.

Examples The following 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 account layer-all encapsulation	Globally enables QoS functionality on the switch.

show qos aggregate policer

To display QoS aggregate policer information, use the **show qos aggregate policer** command.

```
show qos aggregate policer [aggregate_name]
```

Syntax Description	<i>aggregate_name</i> (Optional) Named aggregate policer.
---------------------------	---

Command Default	This command has no default settings.
------------------------	---------------------------------------

Command Modes	Privileged EXEC mode
----------------------	----------------------

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

Usage Guidelines	This command is not supported on Supervisor Engine 6-E, Supervisor Engine 6L-E, Catalyst 4900M, Catalyst 4948E, and Catalyst 4948E-F.
-------------------------	---

The aggregate policer name is case sensitive.

Examples	The following example shows the output if you do not enter any keywords:
-----------------	--

```
Switch# show qos aggregate policer
Policer aggr-1
Rate(bps):10000000 Normal-Burst(bytes):1000000
conform-action:transmit exceed-action:policed-dscp-transmit
Policymaps using this policer:
    ipp5-policy
Switch#
```

Related Commands	Command	Description
	qos trust	Defines a named aggregate policer.

show qos db1

To display global Dynamic Buffer Limiting (DBL) information, use the **show qos db1** command.

show qos db1

Syntax Description This command has no arguments or keywords.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

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

Usage Guidelines This command is not supported on Supervisor Engine 6-E, Supervisor Engine 6L-E, Catalyst 4900M, Catalyst 4948E, and Catalyst 4948E-F.

Examples The following example shows how to display global DBL information:

```
Switch# show qos db1
DBL is enabled globally
DBL flow includes vlan
DBL flow includes 14-ports
DBL does not use ecn to indicate congestion
DBL exceed-action mark probability:15%
DBL max credits:15
DBL aggressive credit limit:10
DBL aggressive buffer limit:2 packets
DBL DSCPs with default drop probability:
    1-10
Switch#
```

Related Commands	Command	Description
	qos account layer-all encapsulation	Globally enables QoS functionality on the switch.

show qos interface

To display queuing information, use the **show qos interface** command.

```
show qos interface { fastethernet interface-number | gigabitethernet interface-number } |
[vlan vlan_id | port-channel number]
```

Syntax Description	Parameter	Description
	fastethernet <i>interface-number</i>	Specifies the Fast Ethernet 802.3 interface.
	gigabitethernet <i>interface-number</i>	Specifies the Gigabit Ethernet 802.3z interface.
	vlan <i>vlan_id</i>	(Optional) Specifies the VLAN ID; valid values are from 1 to 4094.
	port-channel <i>number</i>	(Optional) Specifies the port channel; valid ranges are from 1 to 64.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch.
	12.1(13)EW	Added support for extended VLAN addresses.
	12.1(19)EW	Display changed to include the Port Trust Device.

Usage Guidelines This command is not supported on Supervisor Engine 6-E, Supervisor Engine 6L-E, Catalyst 4900M, Catalyst 4948E, and Catalyst 4948E-F.

Examples The following example shows how to display queuing information:

```
Switch# show qos interface fastethernet 6/1
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   ShapeRate   Priority   QueueSize
           (bps)      (bps)
1           31250000   disabled    N/A       240
2           31250000   disabled    N/A       240
3           31250000   disabled    normal    240
4           31250000   disabled    N/A       240
Switch#
```

Related Commands	Command	Description
	show qos	Displays QoS information.
	tx-queue	Configures the transmit queue parameters for an interface.

show qos maps

To display QoS map information, use the **show qos maps** command.

```
show qos maps [cos | dscp [policed | tx-queue]]
```

Syntax Description	
cos	(Optional) Displays CoS map information.
dscp	(Optional) Displays DSCP map information.
policed	(Optional) Displays policed map information.
tx-queue	(Optional) Displays tx-queue map information.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

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

Usage Guidelines This command is not supported on Supervisor Engine 6-E, Supervisor Engine 6L-E, Catalyst 4900M, Catalyst 4948E, and Catalyst 4948E-F.

Examples The following example shows how to display QoS map settings:

```
Switch# show qos maps
DSCP-TxQueue 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 02 02 02 02
3 :   02 02 03 03 03 03 03 03 03 03
4 :   03 03 03 03 03 03 03 03 04 04
5 :   04 04 04 04 04 04 04 04 04 04
6 :   04 04 04 04

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
```

■ show qos maps

```
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 account layer-all encapsulation	Globally enables QoS functionality on the switch.

show redundancy

To display redundancy facility information, use the **show redundancy** command.

show redundancy { clients | counters | history | states }

Syntax Description	
clients	(Optional) Displays information about the redundancy facility client.
counters	(Optional) Displays information about the redundancy facility counter.
history	(Optional) Displays a log of past status and related information for the redundancy facility.
states	(Optional) Displays information about the redundancy facility state, such as disabled, initialization, standby, active.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.1.(13)EW	This command was introduced on the Catalyst 4500 series switch
	12.2(31)SGA	Support for ISSU was introduced.

Examples The following example shows how to display information about the redundancy facility:

```
Switch# show redundancy
Switch# show redundancy
4507r-demo#show redundancy
Redundant System Information :
-----
      Available system uptime = 2 days, 2 hours, 39 minutes
Switchovers system experienced = 0
      Standby failures = 0
      Last switchover reason = none

      Hardware Mode = Duplex
Configured Redundancy Mode = Stateful Switchover
Operating Redundancy Mode = Stateful Switchover
Maintenance Mode = Disabled
Communications = Up

Current Processor Information :
-----
      Active Location = slot 1
      Current Software state = ACTIVE
      Uptime in current state = 2 days, 2 hours, 39 minutes
      Image Version = Cisco Internetwork Operating System Software
IOS (tm) Catalyst 4000 L3 Switch Software (cat4000-I5S-M), Version 12.2(20)EWA(3
.92), CISCO INTERNAL USE ONLY ENHANCED PRODUCTION VERSION
Copyright (c) 1986-2004 by cisco Systems, Inc.
```

```

Compiled Wed 14-Jul-04 04:42 by esi
          BOOT = bootflash:cat4000-i5s-mz.122_20_EWA_392,1
          Configuration register = 0x2002

Peer Processor Information :
-----
          Standby Location = slot 2
          Current Software state = STANDBY HOT
          Uptime in current state = 2 days, 2 hours, 39 minutes
          Image Version = Cisco Internetwork Operating System Software
IOS (tm) Catalyst 4000 L3 Switch Software (cat4000-I5S-M), Version 12.2(20)EWA(3
.92), CISCO INTERNAL USE ONLY ENHANCED PRODUCTION VERSION
Copyright (c) 1986-2004 by cisco Systems, Inc.
Compiled Wed 14-Jul-04 0
          BOOT = bootflash:cat4000-i5s-mz.122_20_EWA_392,1
          Configuration register = 0x2002

```

```
Switch#
```

The following example shows how to display redundancy facility client information:

```

Switch# show redundancy clients
clientID = 0          clientSeq = 0          RF_INTERNAL_MSG
clientID = 30         clientSeq = 135         Redundancy Mode RF
clientID = 28         clientSeq = 330         GALIOS_CONFIG_SYNC
clientID = 65000     clientSeq = 65000     RF_LAST_CLIENT Switch

```

The output displays the following information:

- clientID displays the client's ID number.
- clientSeq displays the client's notification sequence number.
- Current redundancy facility state.

The following 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 tx = 0
          null tx by client = 0
          tx failures = 0
          tx msg length invalid = 0

          client not rxing msgs = 0
          rx peer msg routing errors = 0
          null peer msg rx = 0
          errored peer msg rx = 0

          buffers tx = 1535
          tx buffers unavailable = 0
          buffers rx = 1530
          buffer release errors = 0

          duplicate client registers = 0
          failed to register client = 0
          Invalid client syncs = 0
Switch#

```

The following example shows how to display redundancy facility history information:

```
Switch# show redundancy history
00:00:01 client added: RF_INTERNAL_MSG(0) seq=0
00:00:01 client added: RF_LAST_CLIENT(65000) seq=65000
00:00:01 client added: GALIOS_CONFIG_SYNC(28) seq=330
00:00:03 client added: Redundancy Mode RF(30) seq=135
00:00:03 *my state = INITIALIZATION(2) *peer state = DISABLED(1)
00:00:03 RF_PROG_INITIALIZATION(100) RF_INTERNAL_MSG(0) op=0 rc=11
00:00:03 RF_PROG_INITIALIZATION(100) Redundancy Mode RF(30) op=0 rc=11
00:00:03 RF_PROG_INITIALIZATION(100) GALIOS_CONFIG_SYNC(28) op=0 rc=11
00:00:03 RF_PROG_INITIALIZATION(100) RF_LAST_CLIENT(65000) op=0 rc=11
00:00:03 *my state = NEGOTIATION(3) peer state = DISABLED(1)
00:00:25 RF_EVENT_GO_ACTIVE(511) op=0
00:00:25 *my state = ACTIVE-FAST(9) peer state = DISABLED(1)
00:00:25 RF_STATUS_MAINTENANCE_ENABLE(403) Redundancy Mode RF(30) op=0
00:00:25 RF_STATUS_MAINTENANCE_ENABLE(403) GALIOS_CONFIG_SYNC(28) op=0
00:00:25 RF_PROG_ACTIVE_FAST(200) RF_INTERNAL_MSG(0) op=0 rc=11
00:00:25 RF_PROG_ACTIVE_FAST(200) Redundancy Mode RF(30) op=0 rc=11
00:00:25 RF_PROG_ACTIVE_FAST(200) GALIOS_CONFIG_SYNC(28) op=0 rc=11
00:00:25 RF_PROG_ACTIVE_FAST(200) RF_LAST_CLIENT(65000) op=0 rc=11
00:00:25 *my state = ACTIVE-DRAIN(10) peer state = DISABLED(1)
00:00:25 RF_PROG_ACTIVE_DRAIN(201) RF_INTERNAL_MSG(0) op=0 rc=11
00:00:25 RF_PROG_ACTIVE_DRAIN(201) Redundancy Mode RF(30) op=0 rc=11
00:00:25 RF_PROG_ACTIVE_DRAIN(201) GALIOS_CONFIG_SYNC(28) op=0 rc=11
00:00:25 RF_PROG_ACTIVE_DRAIN(201) RF_LAST_CLIENT(65000) op=0 rc=11
00:01:34 RF_PROG_PLATFORM_SYNC(300) RF_INTERNAL_MSG(0) op=0 rc=11
00:01:34 RF_PROG_PLATFORM_SYNC(300) Redundancy Mode RF(30) op=0 rc=11
00:01:34 RF_PROG_PLATFORM_SYNC(300) GALIOS_CONFIG_SYNC(28) op=0 rc=0
00:01:34 RF_EVENT_CLIENT_PROGRESSION(503) GALIOS_CONFIG_SYNC(28) op=1 rc=0
00:01:36 RF_EVENT_PEER_PROG_DONE(506) GALIOS_CONFIG_SYNC(28) op=300
00:01:36 RF_PROG_PLATFORM_SYNC(300) RF_LAST_CLIENT(65000) op=0 rc=0
00:01:36 RF_EVENT_CLIENT_PROGRESSION(503) RF_LAST_CLIENT(65000) op=1 rc=0
00:01:36 RF_EVENT_PEER_PROG_DONE(506) RF_LAST_CLIENT(65000) op=300
00:01:38 *my state = ACTIVE(13) *peer state = STANDBY COLD(4)
Switch#
```

The following example shows how to display information about the redundancy facility state:

```
Switch# show redundancy states
my state = 13 -ACTIVE
    peer state = 8 -STANDBY HOT
        Mode = Duplex
        Unit = Primary
        Unit ID = 2

Redundancy Mode (Operational) = Stateful Switchover
Redundancy Mode (Configured) = Stateful Switchover
    Split Mode = Disabled
    Manual Swact = Enabled
    Communications = Up

    client count = 21
    client_notification_TMR = 240000 milliseconds
        keep_alive TMR = 9000 milliseconds
        keep_alive count = 0
        keep_alive threshold = 18
        RF debug mask = 0x0
Switch#
```

Related Commands

Command	Description
redundancy	Enters the redundancy configuration mode.
redundancy force-switchover	Forces a switchover from the active to the standby supervisor engine.

show redundancy config-sync

To display an 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 prc}
```

```
show redundancy config-sync ignored failures mcl
```

Syntax Description

failures	Displays MCL entries 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.
prc	Displays a Parser 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.

Command Default

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.
12.2(44)SG	Updated command syntax from issu config-sync to redundancy config-sync.

Usage Guidelines

When two versions of Cisco IOS images are involved, the command sets supported by two images might differ. If any of those mismatched commands are executed on the active supervisor engine, the standby supervisor engine might not recognize those commands. This causes a config mismatch condition. If the syntax 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 engines' running configuration.
 - Step 2** Revalidate the MCL with a modified running configuration using the **redundancy config-sync validate mismatched-commands** command.
 - Step 3** Reload the standby supervisor engine.
-

Alternatively, you could ignore the MCL by following these steps:

-
- Step 1** Enter the **redundancy config-sync ignore mismatched-commands** command.
 - Step 2** Reload the standby supervisor engine; the system transitions to SSO mode.



Note If you ignore the mismatched commands, the *out-of-sync* configuration at the active supervisor engine and the standby supervisor engine still exists.

- Step 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 back to the active supervisor engine. PRC failure occurs if these two PRCs do not match. If a PRC error occurs at the standby supervisor engine either during bulk sync or LBL sync, the standby supervisor engine is reset. To display all PRC failures, use the **show redundancy config-sync failures prc** command.

To display 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:

```
Switch# show redundancy config-sync failures bem
BEM Failed Command List
-----
```

```
The list is Empty
Switch#
```

The following example shows how to display the ISSU MCL failures:

```
Switch# show redundancy config-sync failures mcl
Mismatched Command List
-----
```

```
The list is Empty
Switch#
```

The following example shows how to display the ISSU PRC failures:

```
Switch# show redundancy config-sync failures prc
PRC Failed Command List
-----
interface FastEthernet3/2
! <submode> "interface"
- channel-protocol pagp
! </submode> "interface"
```

Related Commands

Command	Description
redundancy config-sync mismatched-commands	Moves the active supervisor engine into the Mismatched Command List (MCL) and resets the standby supervisor engine.

show running-config

To display the module status and configuration, use the **show running-config** command.

```
show running-config [module slot]
```

Syntax Description	module slot (Optional) Specifies the module slot number; valid values are from 1 to 6.				
Command Default	This command has no default settings.				
Command Modes	Privileged EXEC mode				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.1(8a)EW</td> <td>This command was introduced on the Catalyst 4500 series switch.</td> </tr> </tbody> </table>	Release	Modification	12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch.
Release	Modification				
12.1(8a)EW	This command was introduced on the Catalyst 4500 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 speed is configured to be auto and that the duplex mode shown becomes the operational setting once the speed is configured to something other than auto. With this configuration, it is possible that the operating duplex mode for that interface does not match the duplex mode shown with the **show running-config** command.

Examples

The following example shows how to display the module and status configuration for all modules:

```
Switch# show running-config
03:23:36:%SYS-5-CONFIG_I:Configured from console by consolesh runn
Building configuration...

Current configuration:3268 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Switch
!
!
power supplies required 1
ip subnet-zero
```

```
!  
!  
!  
interface FastEthernet1  
  no ip address  
  shutdown  
  duplex auto  
  speed auto  
Switch#
```

The following example shows the output for the **show running-config** command when you have enabled the **switchport voice vlan** command:

```
Switch# show running-config int fastethernet 6/1  
Building configuration...  
  
Current configuration:133 bytes  
!  
interface FastEthernet6/1  
  switchport voice vlan 2  
  no snmp trap link-status  
  spanning-tree portfast  
  channel-group 1 mode on  
end  
  
Switch#
```

show shell functions

Use the **show shell functions** command to display configurations for all builtin shell functions.

show shell functions

Syntax Description	No keywords
---------------------------	-------------

Command Default	None
------------------------	------

Command Modes	Privileged EXEC
----------------------	-----------------

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

Usage Guidelines	This command only displays the contents of builtin shell functions. To display the contents of user created functions, use the show shell triggers command.
-------------------------	--

Examples	This example illustrates how to display configurations included for all the shell functions:
-----------------	--

```
Switch# show shell functions
```

Related Commands	Command	Description
	shell trigger	Creates a user defined trigger.
show shell triggers	Configures a user defined trigger.	

show shell triggers

Use the **show shell triggers** command to display detail for all supported builtin and user created triggers.

show shell triggers

Syntax Description	No keywords
---------------------------	-------------

Command Default	None
------------------------	------

Command Modes	Privileged EXEC
----------------------	-----------------

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

Usage Guidelines	This command displays builtin triggers and user defined triggers (with their mapped functions).
-------------------------	---

Examples	This example illustrates how to display detail for all supported triggers:
-----------------	--

```
Switch# show shell triggers
Trigger Id: testGroup
Trigger description: testGroup
Trigger environment:
Trigger mapping function:
```

Related Commands	Command	Description
	shell trigger	Creates a user defined trigger.
show shell functions	Displays configurations included for all the builtin functions including user created and built-in functions.	

show slavebootflash:

To display information about the standby bootflash file system, use the **show slavebootflash:** command.

show slavebootflash: [all | chips | filesystems]

Syntax Description	all	(Optional) Displays all possible Flash information.
	chips	(Optional) Displays Flash chip information.
	filesystems	(Optional) Displays file system information.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

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

Examples The following example shows how to display file system status information:

```
Switch# show slavebootflash: filesystems

----- 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
  File System Offset = 40000    Length = F40000
  MONLIB Offset     = 100      Length = C628
  Bad Sector Map Offset = 3FFF8  Length = 8
  Squeeze Log Offset = F80000   Length = 40000
  Squeeze Buffer Offset = FC0000  Length = 40000
  Num Spare Sectors = 0
  Spares:
STATUS INFO:
  Writable
  NO File Open for Write
  Complete Stats
  No Unrecovered Errors
  No Squeeze in progress
USAGE INFO:
  Bytes Used      = 917CE8   Bytes Available = 628318
  Bad Sectors    = 0        Spared Sectors  = 0
  OK Files       = 2        Bytes = 917BE8
  Deleted Files  = 0        Bytes = 0
  Files w/Errors = 0        Bytes = 0
Switch>
```


The following example shows how to display system image information:

```
Switch# show slavebootflash:
-# - ED --type-- --crc--- -seek-- nlen -length- -----date/time----- name
1  .. image      8C5A393A  237E3C   14  2063804 Aug 23 1999 16:18:45 c4-boot-mz
2  .. image      D86EE0AD  957CE8    9  7470636 Sep 20 1999 13:48:49 rp.halley
Switch>
```

The following example shows how to display all bootflash information:

```
Switch# show slavebootflash: all
-# - ED --type-- --crc--- -seek-- nlen -length- -----date/time----- name
1  .. image      8C5A393A  237E3C   14  2063804 Aug 23 1999 16:18:45 c4-boot-
mz
2  .. image      D86EE0AD  957CE8    9  7470636 Sep 20 1999 13:48:49 rp.halley

6456088 bytes available (9534696 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
File System Offset = 40000     Length           = F40000
MONLIB Offset     = 100       Length           = C628
Bad Sector Map Offset = 3FFF8   Length           = 8
Squeeze Log Offset = F80000   Length           = 40000
Squeeze Buffer Offset = FC0000  Length           = 40000
Num Spare Sectors = 0

Spares:
STATUS INFO:
Writable
NO File Open for Write
Complete Stats
No Unrecovered Errors
No Squeeze in progress
USAGE INFO:
Bytes Used      = 917CE8   Bytes Available = 628318
Bad Sectors     = 0       Spared Sectors  = 0
OK Files        = 2       Bytes           = 917BE8
Deleted Files   = 0       Bytes           = 0
Files w/Errors  = 0       Bytes           = 0
Switch>
```

show slaveslot0:

To display information about the file system on the standby supervisor engine, use the **show slaveslot0:** command.

show slot0: [all | chips | filesys]

Syntax Description	all	(Optional) Displays all flash information including the output from the show slot0: chips and show slot0: filesys commands.
	chips	(Optional) Displays flash chip register information.
	filesys	(Optional) Displays file system status information.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

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

Examples

The following example shows how to display a summary of the file system:

```
Switch# show slaveslot0:
-# - ED --type-- --crc--- -seek-- nlen -length- -----date/time----- name
1 .. image      6375DBB7  A4F144      6 10678468 Nov 09 1999 10:50:42 halley

5705404 bytes available (10678596 bytes used)
Switch>
```

The following example shows how to display flash chip information:

```
Switch# show slaveslot0: chips
***** Intel Series 2+ Status/Register Dump *****
ATTRIBUTE MEMORY REGISTERS:
  Config Option Reg (4000): 2
  Config Status Reg (4002): 0
  Card Status Reg (4100): 1
  Write Protect Reg (4104): 4
  Voltage Cntrl Reg (410C): 0
  Rdy/Busy Mode Reg (4140): 2

COMMON MEMORY REGISTERS: Bank 0
  Intelligent ID Code : 8989A0A0
  Compatible Status Reg: 8080
  Global Status Reg: B0B0
  Block Status Regs:
    0 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
    8 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
   16 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
   24 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
```

```

COMMON MEMORY REGISTERS: Bank 1
  Intelligent ID Code : 8989A0A0
  Compatible Status Reg: 8080
  Global      Status Reg: B0B0
  Block Status Regs:
    0 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
    8 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
   16 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
   24 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0

COMMON MEMORY REGISTERS: Bank 2
  Intelligent ID Code : 8989A0A0
  Compatible Status Reg: 8080
  Global      Status Reg: B0B0
  Block Status Regs:
    0 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
    8 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
   16 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
   24 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0

COMMON MEMORY REGISTERS: Bank 3
  Intelligent ID Code : 8989A0A0
  Compatible Status Reg: 8080
  Global      Status Reg: B0B0
  Block Status Regs:
    0 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
    8 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
   16 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
   24 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0

COMMON MEMORY REGISTERS: Bank 4
  Intelligent ID Code : FFFFFFFF
  IID Not Intel -- assuming bank not populated

```

The following example shows how to display file system information:

```

Switch# show slaveslot0: filesystems
----- F I L E   S Y S T E M   S T A T U S -----
  Device Number = 0
DEVICE INFO BLOCK: slot0
  Magic Number      = 6887635   File System Vers = 10000   (1.0)
  Length            = 1000000   Sector Size      = 20000
  Programming Algorithm = 4     Erased State     = FFFFFFFF
  File System Offset = 20000    Length = FA0000
  MONLIB Offset     = 100      Length = F568
  Bad Sector Map Offset = 1FFF0  Length = 10
  Squeeze Log Offset = FC0000  Length = 20000
  Squeeze Buffer Offset = FE0000 Length = 20000
  Num Spare Sectors = 0
  Spares:
STATUS INFO:
  Writable
  NO File Open for Write
  Complete Stats
  No Unrecovered Errors
  No Squeeze in progress
USAGE INFO:
  Bytes Used      = 9F365C   Bytes Available = 5AC9A4
  Bad Sectors     = 0       Spared Sectors  = 0
  OK Files        = 1       Bytes = 9F35DC
  Deleted Files   = 0       Bytes = 0
  Files w/Errors = 0       Bytes =
Switch>

```

show slot0:

To display information about the slot0: file system, use the **show slot0:** command.

show slot0: [**all** | **chips** | **fileSYS**]

Syntax Description	all	(Optional) Displays all flash information including the output from the show slot0: chips and show slot0: fileSYS commands.
	chips	(Optional) Displays flash chip register information.
	fileSYS	(Optional) Displays file system status information.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

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

Examples

The following example shows how to display a summary of the file system:

```
Switch# show slot0:
-# - ED --type-- --crc--- -seek-- nlen -length- -----date/time----- name
1  .. image      6375DBB7  A4F144      6 10678468 Nov 09 1999 10:50:42 halley

5705404 bytes available (10678596 bytes used)
Switch>
```

The following example shows how to display flash chip information:

```
Switch# show slot0: chips
***** Intel Series 2+ Status/Register Dump *****
ATTRIBUTE MEMORY REGISTERS:
  Config Option Reg (4000): 2
  Config Status Reg (4002): 0
  Card Status Reg (4100): 1
  Write Protect Reg (4104): 4
  Voltage Cntrl Reg (410C): 0
  Rdy/Busy Mode Reg (4140): 2

COMMON MEMORY REGISTERS: Bank 0
  Intelligent ID Code : 8989A0A0
  Compatible Status Reg: 8080
  Global Status Reg: B0B0
  Block Status Regs:
    0 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
    8 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
   16 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
   24 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
```

```

COMMON MEMORY REGISTERS: Bank 1
  Intelligent ID Code : 8989A0A0
  Compatible Status Reg: 8080
  Global      Status Reg: B0B0
  Block Status Regs:
    0 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
    8 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
   16 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
   24 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0

COMMON MEMORY REGISTERS: Bank 2
  Intelligent ID Code : 8989A0A0
  Compatible Status Reg: 8080
  Global      Status Reg: B0B0
  Block Status Regs:
    0 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
    8 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
   16 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
   24 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0

COMMON MEMORY REGISTERS: Bank 3
  Intelligent ID Code : 8989A0A0
  Compatible Status Reg: 8080
  Global      Status Reg: B0B0
  Block Status Regs:
    0 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
    8 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
   16 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0
   24 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0

COMMON MEMORY REGISTERS: Bank 4
  Intelligent ID Code : FFFFFFFF
  IID Not Intel -- assuming bank not populated
Switch>

```

The following example shows how to display file system information:

```

Switch# show slot0: filesystems
----- F I L E   S Y S T E M   S T A T U S -----
  Device Number = 0
DEVICE INFO BLOCK: slot0
  Magic Number      = 6887635   File System Vers = 10000   (1.0)
  Length            = 1000000   Sector Size      = 20000
  Programming Algorithm = 4     Erased State     = FFFFFFFF
  File System Offset = 20000    Length = FA0000
  MONLIB Offset     = 100      Length = F568
  Bad Sector Map Offset = 1FFF0  Length = 10
  Squeeze Log Offset = FC0000   Length = 20000
  Squeeze Buffer Offset = FE0000  Length = 20000
  Num Spare Sectors = 0
  Spares:
STATUS INFO:
  Writable
  NO File Open for Write
  Complete Stats
  No Unrecovered Errors
  No Squeeze in progress
USAGE INFO:
  Bytes Used      = 9F365C   Bytes Available = 5AC9A4
  Bad Sectors     = 0        Spared Sectors  = 0
  OK Files        = 1        Bytes = 9F35DC
  Deleted Files   = 0        Bytes = 0
  Files w/Errors  = 0        Bytes = 0
Switch>

```

show spanning-tree

To display spanning-tree state information, use the **show spanning-tree** command.

```
show spanning-tree [bridge_group | active | backbonefast | bridge [id] | inconsistentports |
interface type | root | summary [total] | uplinkfast | vlan vlan_id | pathcost method | detail]
```

Syntax Description	
<i>bridge_group</i>	(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.
<i>id</i>	(Optional) Name of the bridge.
inconsistentports	(Optional) Displays the root inconsistency state.
interface <i>type</i>	(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 <i>vlan_id</i>	(Optional) Specifies the VLAN ID; valid values are from 1 to 4094.
pathcost method	(Optional) Displays the default path cost calculation method used.
detail	(Optional) Displays a summary of interface information.

Command Default Interface information summary is displayed.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.1(8a)EW	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

The following example shows how to display spanning-tree information on the active interfaces only:

```
Switch# show spanning-tree active
UplinkFast is disabled
BackboneFast is disabled

VLAN1 is executing the ieee compatible Spanning Tree protocol
Bridge Identifier has priority 32768, address 0050.3e8d.6401
Configured hello time 2, max age 20, forward delay 15
Current root has priority 16384, address 0060.704c.7000
Root port is 265 (FastEthernet5/9), cost of root path is 38
Topology change flag not set, detected flag not set
Number of topology changes 0 last change occurred 18:13:54 ago
Times: hold 1, topology change 24, notification 2
      hello 2, max age 14, forward delay 10
Timers: hello 0, topology change 0, notification 0

Port 265 (FastEthernet5/9) of VLAN1 is forwarding
Port path cost 19, Port priority 128, Port Identifier 129.9.
Designated root has priority 16384, address 0060.704c.7000
Designated bridge has priority 32768, address 00e0.4fac.b000
Designated port id is 128.2, designated path cost 19
Timers: message age 3, forward delay 0, hold 0
Number of transitions to forwarding state: 1
BPDU: sent 3, received 32852
Switch#
```

The following example shows how to display the spanning-tree BackboneFast status:

```
Switch# show spanning-tree backbonefast
BackboneFast is enabled

BackboneFast statistics
-----
Number of transition via backboneFast (all VLANs) : 0
Number of inferior BPDUs received (all VLANs)   : 0
Number of RLQ request PDUs received (all VLANs) : 0
Number of RLQ response PDUs received (all VLANs) : 0
Number of RLQ request PDUs sent (all VLANs)     : 0
Number of RLQ response PDUs sent (all VLANs)    : 0
Switch#
```

The following example shows how to display spanning-tree information for the bridge:

```
Switch# show spanning-tree bridge
VLAN1
  Bridge ID  Priority      32768
            Address      0050.3e8d.6401
            Hello Time    2 sec  Max Age 20 sec  Forward Delay 15 sec
VLAN2
  Bridge ID  Priority      32768
            Address      0050.3e8d.6402
            Hello Time    2 sec  Max Age 20 sec  Forward Delay 15 sec
VLAN3
  Bridge ID  Priority      32768
            Address      0050.3e8d.6403
            Hello Time    2 sec  Max Age 20 sec  Forward Delay 15 sec
Switch#
```

The following 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    0030.94fc.0a00
           This bridge is the root
           Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

Bridge ID  Priority    32768
           Address    0030.94fc.0a00
           Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
           Aging Time  300

Interface
Name          Port ID Prio  Cost Sts  Designated
-----
FastEthernet6/15  129.79 128   19 FWD   0 32768 0030.94fc.0a00 129.79

VLAN2
Spanning tree enabled protocol ieee
Root ID    Priority    32768
           Address    0030.94fc.0a01
           This bridge is the root
           Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

Bridge ID  Priority    32768
           Address    0030.94fc.0a01
           Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
           Aging Time  300

Interface
Name          Port ID Prio  Cost Sts  Designated
-----
FastEthernet6/16  129.80 128   19 FWD   0 32768 0030.94fc.0a01 129.80
Switch#

```

The following example shows how to display spanning-tree information for Fast Ethernet interface 5/9:

```

Switch# show spanning-tree interface fastethernet5/9
Interface Fa0/10 (port 23) in Spanning tree 1 is ROOT-INCONSISTENT
Port path cost 100, Port priority 128
Designated root has priority 8192, address 0090.0c71.a400
Designated bridge has priority 32768, address 00e0.1e9f.8940
Designated port is 23, path cost 115
Timers: message age 0, forward delay 0, hold 0
BPDU: sent 0, received 0
The port is in the portfast mode
Switch#

```

The following example shows how to display spanning-tree information for GigabitEthernet 3/13:

```

Switch# show spanning-tree interface gigabitethernet3/13 detail
Port 269 (GigabitEthernet3/13) of VLAN0002 is forwarding
  Port path cost 4, Port priority 128, Port Identifier 128.269.
  Designated root has priority 32770, address 0002.172c.f400
  Designated bridge has priority 32770, address 0002.172c.f400
  Designated port id is 128.269, designated path cost 0
  Timers: message age 0, forward delay 0, hold 0
  Number of transitions to forwarding state: 1
  Link type is point-to-point by default
  Loop guard is enabled by default on the port
  The port is in the portfast network mode by default
  BPDU: sent 2183, received 0

```

The following 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 0030.94fc.0a00
  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 5 last change occurred 01:50:47 ago
    from FastEthernet6/16
  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 335 (FastEthernet6/15) of VLAN1 is forwarding
  Port path cost 19, Port priority 128, Port Identifier 129.79.
  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#

```

The following example shows how to display spanning-tree information for a specific bridge group:

```

Switch# show spanning-tree vlan 1
  UplinkFast is disabled
  BackboneFast is disabled
Switch#

```

The following example shows how to display a summary of port states:

```

Switch# show spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for: VLAN0199-VLAN0200, VLAN0128
EtherChannel misconfig guard is enabled
Extended system ID is enabled
Portfast Default is network
Portfast Edge BPDU Guard Default is disabled
Portfast Edge BPDU Filter Default is disabled
Loopguard Default is enabled
PVST Simulation Default is enabled but inactive in rapid-pvst mode
Bridge Assurance is enabled
UplinkFast is disabled
BackboneFast is disabled
Configured Pathcost method used is short

Name Blocking Listening Learning Forwarding STP Active
-----
VLAN0199 0 0 0 5 5
VLAN0200 0 0 0 4 4
VLAN0128 0 0 0 4 4
-----
3 vlans 0 0 0 13 13

```

The following example shows how to display the total lines of the spanning-tree state section:

```

Switch# show spanning-tree summary totals
Root bridge for:VLAN1, VLAN2.
PortFast BPDU Guard is disabled
EtherChannel misconfiguration guard is enabled
UplinkFast is disabled
BackboneFast is disabled
Default pathcost method used is short

Name Blocking Listening Learning Forwarding STP Active

```

```

-----
Switch#          2 VLANs 0      0      0      2      2

```

The following example shows how to determine whether any ports are in root inconsistent state:

```
Switch# show spanning-tree inconsistentports
```

```

Name              Interface          Inconsistency
-----
VLAN1             FastEthernet3/1    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 bridge assurance	Enables Bridge Assurance
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	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.
<i>instance-id</i>	(Optional) Instance identification number; valid values are from 0 to 15.
detail	(Optional) Displays detailed MST protocol information.
interface <i>interface</i>	(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.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.1(12c)EW	This command was introduced on the Catalyst 4500 series switch.
12.2(25)EW	Added support for the 10-Gigabit Ethernet interface.

Usage Guidelines

In the output display of the **show spanning-tree mst configuration** command, a warning message might display. This message appears if you do not map secondary VLANs to the same instance as the associated primary VLAN. The display includes a list of the secondary VLANs that are not mapped to the same instance as the associated primary VLAN. The warning message is as follows:

```
These secondary vlans are not mapped to the same instance as their primary:
-> 3
```

See the [show spanning-tree](#) command for output definitions.

Examples

The following example shows how to display region configuration information:

```
Switch# show spanning-tree mst configuration
```

```
Name      [leo]
Revision  2702
Instance  Vlans mapped
-----
0         1-9,11-19,21-29,31-39,41-4094
1         10,20,30,40
-----
```

```
Switch#
```

The following example shows how to display additional MST protocol values:

```
Switch# show spanning-tree mst 3 detail
```

```
# # # # # MST03 vlans mapped: 3,3000-3999
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
id 128.1
Timers: message expires in 0 sec, forward delay 0, forward transitions 1
Bpdus (MRecords) sent 4, received 0
```

```
FastEthernet4/2 of MST03 is backup blocking
Port info port id 128.194 priority 128 cost
200000
Designated root address 0002.172c.f400 priority 32771
cost 0
Designated bridge address 0002.172c.f400 priority 32771 port id
128.193
Timers: message expires in 2 sec, forward delay 0, forward transitions 1
Bpdus (MRecords) sent 3, received 252
Switch#
```

The following example shows how to display MST information for a specific interface:

```
Switch# show spanning-tree mst 0 interface fastethernet4/1 detail
```

```
Edge port: no (trunk) port guard : none
(default)
Link type: point-to-point (point-to-point) bpdu filter: disable
(default)
Boundary : internal bpdu guard : disable
(default)
FastEthernet4/1 of MST00 is designated forwarding
Vlans mapped to MST00 1-2,4-2999,4000-4094
Port info port id 128.193 priority 128 cost
200000
Designated root address 0050.3e66.d000 priority 8193
cost 20004
Designated ist master address 0002.172c.f400 priority 49152
cost 0
Designated bridge address 0002.172c.f400 priority 49152 port id
128.193
Timers: message expires in 0 sec, forward delay 0, forward transitions 1
Bpdus sent 492, received 3
Switch#
```

Related Commands	Command	Description
	<code>spanning-tree mst</code>	Sets the path cost and port-priority parameters for any MST instance.
	<code>spanning-tree mst forward-time</code>	Sets the forward delay timer for all the instances.
	<code>spanning-tree mst hello-time</code>	Sets the hello-time delay timer for all the instances.
	<code>spanning-tree mst max-hops</code>	Specifies the number of possible hops in the region before a BPDU is discarded.
	<code>spanning-tree mst root</code>	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 4900M chassis

```
show storm-control [interface-id | broadcast | multicast]
```

Syntax Description

<i>interface-id</i>	(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.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.1(19)EW	This command was introduced on the Catalyst 4500 series switch.
12.2(25)EW	Added support for the 10-Gigabit Ethernet interface.
12.2(40)SG	Added support for the Supervisor Engine 6-E and Catalyst 4900M 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# show storm-control
Interface  Filter State  Upper   Lower   Current
-----  -
Gi2/1     Forwarding    30.00%  30.00%  N/A
Gi4/1     Forwarding    30.00%  30.00%  N/A
Gi4/3     Forwarding    30.00%  30.00%  N/A
Switch#
```

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
-----
Fa6/2 Blocking Enabled Enabled 61%
Switch#
```

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
-----
Fa6/1 Blocking Enabled Disabled 81%
Fa6/2 Blocking Enabled Enabled 61%
Switch#
```

This is an example of output from the **show storm-control** command for a specified interface:

```
Switch# show storm-control fastethernet2/17
Interface Filter State Level Current
-----
Fa2/17 Forwarding 50.00% 0.00%
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 fastethernet6/1
Interface Filter State Broadcast Multicast Level
-----
Fa6/1 Blocking Enabled Disabled 81%
Switch#
```

Table 2-41 describes the fields in the **show storm-control** display.

Table 2-41 show storm-control Field Descriptions

Field	Description
Interface	Displays the ID of the interface.
Filter State	Displays the status of the filter: <ul style="list-style-type: none"> 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. <p>Note N/A is displayed for interfaces that do storm control in the hardware.</p>

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 switch virtual (virtual switch)

To display configuration and status information for a virtual switching system (VSS), use the **show switch virtual** command in EXEC mode.

```
show switch virtual [dual-active { pagp | fast-hello | summary } | link [counters | detail |
port-channel | ports] | redundancy | role | slot-map]
```

Syntax Description

detail	(Optional) Displays detailed virtual switch information.
detail-active	(Optional) Displays virtual switch dual-active information.
pagp	Specifies a summary of dual-active PAgP information
fast-hello	Specifies a summary of dual-active fast-hello information,
summary	Specifies a summary of dual-active configuration information,
link	(Optional) Displays the virtual switch link information.
counters	(Optional) Displays VSL counter information
port-channel	(Optional) Displays VSL port channel information.
ports	(Optional) Displays VSL port information.
redundancy	(Optional) Displays the VSS redundancy status.
role	(Optional) Displays the VSS role information.
slot-map	(Optional) Displays the VSS slot map table.

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.
Release IOS XE 3.5.0E and IOS 15.2(1)SG	This command was introduced.

Usage Guidelines

Use this command to display configuration and status information for a VSS.

The **show switch virtual link detail** command displays the output of the **show switch virtual link** commands and the **show vslp lmp internal** commands. In the output, the entry "show int" is displayed for all the VSL members.

The **show switch virtual dual-active pagp** command displays dual-active trust mode status.

Examples

The following example shows how to display configuration and status information for the VSS:

- In virtual switch mode without skipping config-register:

```
Router# show switch virtual

Switch mode : Virtual Switch
Virtual switch domain number : 1
Local switch number : 2
Local switch operational role: Virtual Switch Active
Peer switch number : 1
Peer switch operational role : Virtual Switch Standby
Router#
```

- In virtual switch mode with skipping config-register but not yet rebooted:

```
Router# show switch virtual

Switch mode : Virtual Switch
Virtual switch domain number : 1
Local switch number : 2
Local switch operational role: Virtual Switch Active
Peer switch number : 1
Peer switch operational role : Virtual Switch Standby
Warning: Config-register set or will be set to skip configuration 0x2142 in the next
reload.
Change config-register; otherwise, switch will be boot in Standalone mode with some
default config.
Router#
```

- In standalone mode without skipping config-register:

```
Router# show switch virtual
Switch Mode : Standalone
Not in Virtual Switch mode due to:
  Domain ID is not configured
Router#
```

- In standalone mode with skipping config-register:

```
Router# show switch virtual
Switch Mode : Standalone
Not in Virtual Switch mode due to:
  Domain ID is not configured
Warning: config-register is set to skip parse 0x2142 in RP or SP
Use [show boot] on RP/SP to verify.
Router#
```

The following example shows how to display the virtual switch priority for local and peer switches:

```
Router# show switch virtual
Switch mode          : Virtual Switch
Virtual switch domain number : 100
Local switch number  : 1
Local switch operational role: Virtual Switch Active
Peer switch number   : 2
Peer switch operational role : Virtual Switch Standby
Router#
```

The following example shows how to display the virtual switch link information:

```
Router# show switch virtual link
VSL Status          : UP
VSL Uptime          : 4 hours, 26 minutes
VSL SCP Ping        : Pass (or Fail)   OK (or Not OK)
```

```
VSL ICC (Ping)          : Pass (or Fail)
VSL Control Link       : Tel/3/1
Router#
```

The following example shows how to display the virtual switch link counter information:

```
Router# show switch virtual link counters
Port                InOctets    InUcastPkts  InMcastPkts  InBcastPkts
Po10                66340451    190415       15637         112069
Tel/3/1            66981250    194528       15770         112072
Po20                42116619    92926        16406         128593
Te2/2/1            42117401    92932        16406         128593

Port                OutOctets    OutUcastPkts  OutMcastPkts  OutBcastPkts
Po10                39030669    112680       105482         0
Tel/3/1            42133252    129182       108824         0
Po20                66948309    112069       210227         0
Te2/2/1            66957613    112070       210233         0

Port                Align-Err    FCS-Err      Xmit-Err      Rcv-Err  UnderSize  OutDiscards
Tel/3/1            0            0            0            0         0          0
Po10                0            0            0            0         0          0
Tel/3/1            0            0            0            0         0          0
Po20                0            0            0            0         0          0
Te2/3/1            0            0            0            0         0          0
Router#
```

The following example shows how to display the virtual switch link port-channel information:

```
Router# show switch virtual link port-channel

VSL Port Channel Information

Flags: D - down          P - bundled in port-channel
       I - stand-alone  s - suspended
       H - Hot-standby (LACP only)
       R - Layer3       S - Layer2
       U - in use       N - not in use, no aggregation
       f - failed to allocate aggregator

       M - not in use, no aggregation due to minimum links not met
       m - not in use, port not aggregated due to minimum links not met
       u - unsuitable for bundling
       w - waiting to be aggregated
```

The following example shows how to display the virtual switch link port information:

```
Router# show switch virtual link port

VSL Link Info          : Configured: 3   Operational: 1

Interface  State          Peer          Peer          Peer
           State          MAC           Switch        Interface
-----
Gi1/3/1   link_down     -             -             -
Gi1/5/4   operational   0013.5fcb.1480  2             Gi1/6/4
Gi1/5/5   link_down     -             -             -

Interface          Last operational          Current packet          Last Diag          Time since
Interface          Failure state              State                   Result              Last Diag
-----
Gi1/1/1           No failure                 Hello bidir              Never ran           7M:51S
Gi1/1/2           No failure                 No failure                Never ran           7M:51S
```

show switch virtual (virtual switch)

```

                                Hello Tx (T4) ms          Hello Rx (T5*) ms
Interface  State           Cfg    Cur    Rem    Cfg    Cur    Rem
-----
Tel1/1/1   operational  500    500    404    5000   5000   4916
Tel1/1/2   link_down   500    -      -      500000 -      -
Tel1/3/3   link_down   500    -      -      500000 -      -
Tel1/3/4   operational  500    500    404    500000 500000 499916
*T5 = min_rx * multiplier
Router#

```

The following example shows how to display redundancy status information for each switch in the virtual switch:

```

Router# show switch virtual redundancy
My Switch Id = 1
Peer Switch Id = 2
Last switchover reason = user forced
Configured Redundancy Mode = sso
Operating Redundancy Mode = sso
Switch 1 Slot 5 Processor Information :
-----
Current Software state = ACTIVE
Uptime in current state = 9 hours, 32 minutes
Image Version = Cisco IOS Software, s72033_rp Software
(s72033_rp-ADVENTERPRISEK9_WAN_DBG-VM), Version 12.2(SIERRA_INTEG_090405) INTERIM SOFTWARE
Synced to V122_32_8_11, 12.2(32.8.11)SR on rainier, Weekly 12.2(32.8.11)SX261
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Mon 06-Apr-09 02:54 by kchristi
BOOT = disk0:mz_good_image,12;
CONFIG_FILE =
BOOTLDR =
Configuration register = 0x2
Fabric State = ACTIVE
Control Plane State = ACTIVE
Switch 1 Slot 6 Processor Information :
-----
Current Software state = RPR-Warm
Uptime in current state = 4 days, 17 hours, 36 minutes
Image Version =
BOOT = disk0:mz-rbh,12;
CONFIG_FILE =
BOOTLDR =
Configuration register = 0x2
Fabric State = RPR-Warm
Control Plane State = RPR-Warm
Switch 2 Slot 5 Processor Information :
-----
Current Software state = STANDBY HOT (switchover target)
Uptime in current state = 9 hours, 24 minutes
Image Version = Cisco IOS Software, s72033_rp Software
(s72033_rp-ADVENTERPRISEK9_WAN_DBG-VM), Version 12.2(SIERRA_INTEG_090405) INTERIM SOFTWARE
Synced to V122_32_8_11, 12.2(32.8.11)SR on rainier, Weekly 12.2(32.8.11)SX261
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Mon 06-Apr-09 02:54 by kchristi
BOOT = disk0:mz_good_image,12;
CONFIG_FILE =
BOOTLDR =
Configuration register = 0x2
Fabric State = ACTIVE
Control Plane State = STANDBY

```

```
Switch 2 Slot 6 Processor Information :
-----
Current Software state = RPR-Warm
Uptime in current state = 4 days, 17 hours, 36 minutes
Image Version =
BOOT = disk0:mz-rbh,12;
CONFIG_FILE =
BOOTLDR =
Configuration register = 0x2
Fabric State = RPR-Warm
Control Plane State = RPR-Warm
Router#
```

The following example shows how to display role and configuration and status information for each switch in the virtual switch:

```
Router# show switch virtual role
```

Switch	Switch Number	Status	Preempt	Priority	Role	Session ID	
						Local	Remote
Local	1	UP	TRUE	200	ACTIVE	0	0
Remote	2	UP	FALSE	100	STANDBY	9272	271

```
In dual-active recovery mode: No
```

```
Valid flag can be moved to detail
SID
```

The following example shows how to display the virtual switch slot map table:

```
Router# show switch virtual slot-map
```

```
Virtual Slot to Remote Switch/Physical Slot Mapping Table:
```

Virtual Slot No	Remote / Switch No	Physical Slot No	Module Uptime
17	1	1	03:04:51
18	1	2	03:04:50
19	1	3	03:00:25
20	1	4	03:04:53
21	1	5	03:04:59
22	1	0	-
23	1	0	-
24	1	0	-
25	1	0	-
26	1	0	-
27	1	0	-
28	1	0	-
29	1	0	-
30	1	0	-
31	1	0	-
32	1	0	-
33	2	1	02:59:25
34	2	2	02:59:23
35	2	3	02:59:23
36	2	4	02:59:27
37	2	5	03:03:17
38	1	0	-
39	1	0	-
40	1	0	-
41	1	0	-
42	1	0	-
43	1	0	-

show switch virtual (virtual switch)

```

44      1      0      -
45      1      0      -
46      1      0      -
47      1      0      -
48      1      0      -
49      1      0      -
Router#

```

The following example shows how to display virtual switch priority for local and peer switches:

```

Router# show switch virtual
Switch mode           : Virtual Switch
Virtual switch domain number : 100
Local switch number   : 1
Local switch operational role: Virtual Switch Active
Peer switch number    : 2
Peer switch operational role : Virtual Switch Standby
Router#

```

Related Commands

Command	Description
dual-active detection (virtual switch)	Enables and configures dual-active detection.
switch (virtual switch)	Configures the VSS domain number and enter the virtual switch domain configuration submenu.

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.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

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

Examples The following example shows how to display the global MTU setting:

```
Switch# show system mtu  
Global Ethernet MTU is 1550 bytes.  
Switch#
```

Related Commands	Command	Description
	system mtu	Sets the maximum Layer 2 or Layer 3 payload size.

show tech-support

To display troubleshooting information for TAC, use the **show tech-support** command.

```
show tech-support [bridging | cef | ipmulticast | isis | password [page] | page]
```

Syntax Description	
bridging	(Optional) Specifies bridging-related information.
cef	(Optional) Specifies CEF-related information.
ipmulticast	(Optional) Specifies IP multicast-related information.
isis	(Optional) Specifies CLNS and ISIS-related information.
password	(Optional) Includes passwords and other security information in the output.
page	(Optional) Displays one page of information at a time in the output.

Command Default

The defaults are as follows:

- Outputs are displayed without page breaks.
- Passwords and other security information are removed from the output.

Command Modes

Privileged EXEC mode

Command History

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

Usage Guidelines

Output from the **show tech-support** command may be terminated in midstream with the key combination Ctrl+Alt+6. The command output is buffered so that the command terminates when 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 encrypted form appears in the output.

If you do not enter the **password** keyword, the passwords and other security-sensitive information in the output are replaced in the output with the word “removed.”

The **show tech-support** 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 these **show** commands:

- **show version**
- **show running-config**
- **show stacks**

- **show interfaces**
- **show controllers**
- **show process memory**
- **show process cpu**
- **show buffers**
- **show logging**
- **show module**
- **show power**
- **show environment**
- **show interfaces switchport**
- **show interfaces trunk**
- **show vlan**

If you enter the **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 mroute count**
- **show ip mroute**
- **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** privileged EXEC command.

```
show udld interface-id | neighbors | fast-hello {interface id}
```

Syntax Description	
<i>interface id</i>	Specifies the administrative and operational UDLD status for a specific interface.
neighbors	Specifies the UDLD neighbor summary.
fast-hello	Specifies Fast UDLD neighbor summary and interface specific status.
<i>interface-id</i>	Specifies the name of the interface.

Command Default None

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch.
	12.2(25)EW	Added support for the 10-Gigabit Ethernet interface.
	12.2(54)SG	Added support for show udld fast-hello and show udld fast-hello interface id .

Usage Guidelines If you do not enter an *interface_id* value, the administrative and operational UDLD status for all interfaces is displayed.

Examples To verify status for a particular link as reported by UDLD, enter the following command:

```
Switch# show udld g1/34
Interface Gi1/34
---
Port enable administrative configuration setting: Enabled / in aggressive mode
Port enable operational state: Enabled / in aggressive mode
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single neighbor detected
Message interval: 15000 ms
Time out interval: 5000 ms

Port fast-hello configuration setting: Disabled
Port fast-hello interval: 0 ms
Port fast-hello operational state: Disabled
Neighbor fast-hello configuration setting: Disabled
Neighbor fast-hello interval: Unknown
```

```
Entry 1
---
```

```

Expiration time: 43300 ms
Cache Device index: 1
Current neighbor state: Bidirectional
Device ID: FOX10430380
Port ID: Gi1/34
Neighbor echo 1 device: FOX104303NL
Neighbor echo 1 port: Gi1/34

```

```

TLV Message interval: 15 sec
No TLV fast-hello interval
TLV Time out interval: 5
TLV CDP Device name: Switch

```

To verify link status as reported by UDLD, enter the following command:

```
Switch# show udld neighbors
```

Port	Device Name	Device ID	Port ID	Neighbor State
Gi1/33	FOX10430380	1	Gi1/33	Bidirectional
Gi1/34	FOX10430380	1	Gi1/34	Bidirectional

To verify Fast UDLD configuration, enter the following command:

```
Switch# show udld fast-hello
```

```

Total ports on which fast hello can be configured: 16
Total ports with fast hello configured: 3
Total ports with fast hello operational: 3
Total ports with fast hello non-operational: 0

```

Port-ID	Hello	Neighbor-Hello	Neighbor-Device	Neighbor-Port	Status
Gi1/45	200	200	FOX104303NL	Gi1/45	Operational
Gi1/46	200	200	FOX104303NL	Gi1/46	Operational
Gi1/47	200	200	FOX104303NL	Gi1/47	Operational

To verify status for a particular link as reported by Fast UDLD, enter the following command:

```
Switch# show udld fast-hello g1/33
```

```
Interface Gi1/33
```

```

---
Port enable administrative configuration setting: Enabled / in aggressive mode
Port enable operational state: Enabled / in aggressive mode
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single neighbor detected
Message interval: 200 ms
Time out interval: 5000 ms

```

```

Port fast-hello configuration setting: Enabled
Port fast-hello interval: 200 ms
Port fast-hello operational state: Enabled
Neighbor fast-hello configuration setting: Enabled
Neighbor fast-hello interval: 200 ms

```

```
Entry 1
```

```

---
Expiration time: 500 ms
Cache Device index: 1
Current neighbor state: Bidirectional
Device ID: FOX10430380
Port ID: Gi1/33
Neighbor echo 1 device: FOX104303NL
Neighbor echo 1 port: Gi1/33

```

```
TLV Message interval: 15
TLV fast-hello interval: 200 ms
TLV Time out interval: 5
TLV CDP Device name: Switch
```

Related Commands	Command	Description
	udld (global configuration mode)	Enables aggressive or normal mode in the UDLD protocol and sets the configurable message timer time.
	udld (interface configuration mode)	Enables UDLD on an individual interface or prevents a fiber interface from being enabled by the udld (global configuration mode) command.

show vlan

To display VLAN information, use the **show vlan** command.

```
show vlan [brief | id vlan_id | name name]
```

```
show vlan private-vlan [type]
```

Syntax Description	
brief	(Optional) Displays only a single line for each VLAN, naming the VLAN, status, and ports.
id <i>vlan_id</i>	(Optional) Displays information about a single VLAN identified by VLAN ID number; valid values are from 1 to 4094.
name <i>name</i>	(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.
<i>type</i>	(Optional) Private VLAN type.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch.
	12.1(12c)EW	Added support for extended VLAN addresses.

Examples The following 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...>
```

```

850 VLAN0850          active Fa5/9
917 VLAN0917          active Fa5/9
999 VLAN0999          active Fa5/9
1002 fddi-default     active Fa5/9
1003 trcrf-default    active Fa5/9
1004 fddinet-default  active Fa5/9
1005 trbrf-default    active Fa5/9

```

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
2	enet	100002	1500	-	-	-	-	-	0	0
3	enet	100003	1500	-	-	-	-	-	303	0
4	enet	100004	1500	-	-	-	-	-	304	0
5	enet	100005	1500	-	-	-	-	-	305	0
6	enet	100006	1500	-	-	-	-	-	0	0
10	enet	100010	1500	-	-	-	-	-	0	0
20	enet	100020	1500	-	-	-	-	-	0	0
50	enet	100050	1500	-	-	-	-	-	0	0

<...Output truncated...>

```

850 enet 100850      1500 - - - - - 0 0
917 enet 100917      1500 - - - - - 0 0
999 enet 100999      1500 - - - - - 0 0
1002 fddi 101002      1500 - 0 - - - 0 0
1003 trcrf 101003     4472 1005 3276 - - srb 0 0
1004 fdnet 101004     1500 - - - - - ieee - 0 0
1005 trbrf 101005     4472 - - - 15 - - - 0 0

```

```
VLAN AREHops STEHops Backup CRF
```

```

-----
802 0      0      off
1003 7     7      off

```

Switch#

The following example shows how to display the VLAN name, status, and associated ports only:

```
Switch# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa5/9
2	VLAN0002	active	Fa5/9
3	VLAN0003	active	Fa5/9
4	VLAN0004	active	Fa5/9
5	VLAN0005	active	Fa5/9
10	VLAN0010	active	Fa5/9
.			
.			
.			
999	VLAN0999	active	Fa5/9
1002	fddi-default	active	Fa5/9
1003	trcrf-default	active	Fa5/9
1004	fddinet-default	active	Fa5/9
1005	trbrf-default	active	Fa5/9

Switch#

The following 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  -     -     -     -     -     303    0
Switch#
```

Table 2-42 describes the fields in the **show vlan** command output.

Table 2-42 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.
BrdgNo	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    Fa3/1, Fa3/2
```

The following example shows how to remove the VLAN association:

```
Switch(config)# vlan 10
Switch(config-vlan)# private-vlan association remove 100
Switch(config-vlan)# end
Switch# show vlan private

Primary Secondary Type          Ports
-----
10      100      primary
          community
```

This example show how to verify PVLAN configuration on the interface:

```
Switch# show interface f3/2 status
Port      Name              Status      Vlan      Duplex  Speed Type
Fa3/2                    connected  pvlan seco a-full  a-100  10/100BaseTX

Switch# show interface f3/1 status
Port      Name              Status      Vlan      Duplex  Speed Type
Fa3/1                    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	<i>map-name</i> (Optional) Name of the VLAN access map.				
Command Default	This command has no default settings.				
Command Modes	Privileged EXEC mode				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.1(12c)EW</td> <td>This command was introduced on the Catalyst 4500 series switch.</td> </tr> </tbody> </table>	Release	Modification	12.1(12c)EW	This command was introduced on the Catalyst 4500 series switch.
Release	Modification				
12.1(12c)EW	This command was introduced on the Catalyst 4500 series switch.				
Examples	<p>This command shows how to display the contents of a VLAN access map:</p> <pre>Switch# show vlan access-map mordred Vlan access-map "mordred" 1 match: ip address 13 action: forward capture Switch#</pre>				
Related Commands	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>vlan access-map</td> <td>Enters VLAN access-map command mode to create a VLAN access map.</td> </tr> </tbody> </table>	Command	Description	vlan access-map	Enters VLAN access-map command mode to create a VLAN access map.
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 *vlanid*] counters

Syntax Description	id <i>vlanid</i> (Optional) Displays the software-cached counter values for a specific VLAN.
---------------------------	---

Command Default	This command has no default settings.
------------------------	---------------------------------------

Command Modes	Privileged EXEC mode
----------------------	----------------------

Command History	Release	Modification
	12.1(13)EW	This command was introduced on the Catalyst 4500 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	The following example shows how to display the software-cached counter values for a specific VLAN:
-----------------	--

```
Switch# show vlan counters
* Multicast counters include broadcast packets

Vlan Id                : 1
L2 Unicast Packets     : 0
L2 Unicast Octets      : 0
L3 Input Unicast Packets : 0
L3 Input Unicast Octets : 0
L3 Output Unicast Packets : 0
L3 Output Unicast Octets : 0
L3 Output Multicast Packets : 0
L3 Output Multicast Octets : 0
L3 Input Multicast Packets : 0
L3 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.

Command Default This command has no default settings.

Command Modes User EXEC mode

Command History	Release	Modification
	12.1(18)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 Mode	Native VLAN Tagging State
f3/2	trunk	enabled
f3/16	PVLAN trunk	disabled
f3/16	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 group

To display the VLANs mapped to VLAN groups, use the **show vlan group** privileged EXEC command.

```
show vlan group [group-name group-name]
```

Syntax Description	group-name (Optional) Displays the VLANs mapped to the specified VLAN group. <i>group-name</i>
---------------------------	--

Command Default	None
------------------------	------

Command Modes	Privileged EXEC
----------------------	-----------------

Command History	Release	Modification
	12.2(54)SG	This command was modified to support user distribution on the Catalyst 4500 series switch.

Usage Guidelines The **show vlan group** command displays the existing VLAN groups and lists the VLANs and VLAN ranges that are members of each VLAN group. If you use the **group-name** keyword, you display only the members of the VLAN group specified by the *group-name* argument.

Examples The following example shows how to display the members of a specified VLAN group:

```
Switch# show vlan group group-name ganymede
```

```
Group Name Vlans Mapped
-----
ganymede      7-9
```

Related Commands	Command	Description
	vlan group	Creates or modifies a VLAN group.

show vlan internal usage

To display information about the internal VLAN allocation, use the **show vlan internal usage** command.

show vlan [id *vlan-id*] internal usage

Syntax Description	id <i>vlan-id</i> (Optional) Displays internal VLAN allocation information for the specified VLAN; valid values are from 1 to 4094.
---------------------------	--

Command Default	This command has no default settings.
------------------------	---------------------------------------

Command Modes	Privileged EXEC mode
----------------------	----------------------

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

Examples The following 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-channel6
1030 GigabitEthernet1/2
1032 FastEthernet3/20
1033 FastEthernet3/21
1129 -
```

The following example shows how to display information about the internal VLAN allocation for a specific VLAN:

```
Switch# show vlan id 1030 internal usage
```

```
VLAN Usage
-----
1030 GigabitEthernet1/2
```

Related Commands	Command	Description
	vlan internal allocation policy	Configures the internal VLAN allocation scheme.

show vlan mapping

Use the **show vlan mapping** privileged EXEC command to display information about VLAN mapping on trunk ports.

show vlan mapping [**interface** *interface-id*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description	interface <i>interface-id</i>	(Optional) Displays VLAN mapping information for the specified interface.
	begin	(Optional) Displays begins with the line that matches the <i>expression</i> .
	exclude	(Optional) Displays excludes lines that match the <i>expression</i> .
	include	(Optional) Displays includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Specifies an expression in the output to use as a reference point.

Command Default None

Command Modes Privileged EXEC

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

Usage Guidelines Expressions are case sensitive. For example, if you enter | **exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples This is a sample output from the **show vlan mapping** command:

```
Switch# show vlan mapping
Interface Fa0/5:
VLANs on wire      Translated VLAN      Operation
-----
default QinQ      1                    selective QinQ
Interface Fa0/2:
VLANs on wire      Translated VLAN      Operation
-----
2                  104                  1-to-1 mapping
```

This is a sample output from the **show vlan mapping** command for an interface:

```
Switch# show vlan mapping interface fa0/6
Interface fa0/6:
VLAN on wire      Translated VLAN      Operation
1                  11                   1-to-1 mapping
12,16-18          100                  selective QinQ
*                  101                  default QinQ
```

Related Commands	Command	Description
	switchport vlan mapping	Configures VLAN mapping on an interface.

show vlan mtu

To display the minimum and maximum transmission unit (MTU) sizes of each VLAN, use the **show vlan mtu** command.

show vlan mtu

Syntax Description This command has no arguments or keywords

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.1(13)EW	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 a port 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 names of the port with the MinMTU and the port with the MaxMTU are displayed. For a VLAN, if the SVI_MTU is bigger than the MinMTU, “TooBig” is displayed after the SVI_MTU.

Examples This is an example of output from the **show vlan mtu** command:

```
Switch# show vlan mtu
```

```
VLAN      SVI_MTU      MinMTU(port)  MaxMTU(port)  MTU_Mismatch
-----
1         1500         1500          1500          No
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 vlan private-vlan

To display private VLAN information, use the **show vlan private-vlan** command.

```
show vlan private-vlan [type]
```

Syntax Description	<i>type</i>	(Optional) Displays the private VLAN type; valid types are isolated, primary, community, twoway-community nonoperational, and normal.
---------------------------	-------------	---

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch.
	12.2(20)EW	Support for community VLAN was added.
	15.1.0 SG	Support for PVLAN modes over EtherChannel. Modes include: private-vlan host, private-vlan promiscuous, private-vlan trunk secondary, and private-vlan trunk promiscuous.

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 The following 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 Fa5/3, Po63
10 10 community
100 101 isolated
150 151 non-operational
202 community
303 twoway-community
401 402 non-operational
Switch#
```



Note

A blank Primary value indicates that no association exists.

The following example shows how to display information about all currently configured private VLAN types:

```
Switch# show vlan private-vlan type
```

```
Vlan Type
-----
202 primary
303 community
304 community
305 community
306 community
307 community
308 normal
309 community
440 isolated
Switch#
```

Table 2-43 describes the fields in the `show vlan private-vlan` command output.

Table 2-43 *show vlan private-vlan Command Output Fields*

Field	Description
Primary	Number of the primary VLAN.
Secondary	Number of the secondary VLAN.
Secondary-Type	Secondary VLAN type is isolated or community .
Ports	Indicates the ports within a VLAN.
Type	Type of VLAN; possible values are primary, isolated , community, 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.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

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

Examples The following example shows how to display a list of RSPAN VLANs:

```
Router# show vlan remote-span
Remote SPAN VLANs
-----
2,20
```

Related Commands	Command	Description
	remote-span	Converts a VLAN into an RSPAN VLAN.
	vlan (VLAN Database mode)	Configures a specific VLAN.

show vmps

To display the VLAN Query Protocol (VQP) version, reconfirmation interval, retry count, VLAN Membership Policy Server (VMPS) IP addresses, current servers, and primary servers, use the **show vmps** command.

show vmps [statistics]

Syntax Description	statistics (Optional) Displays the client-side statistics.				
Command Default	This command has no default settings.				
Command Modes	Privileged EXEC mode				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.1(13)EW</td> <td>This command was introduced on the Catalyst 4500 series switch.</td> </tr> </tbody> </table>	Release	Modification	12.1(13)EW	This command was introduced on the Catalyst 4500 series switch.
Release	Modification				
12.1(13)EW	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 Denied:           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 vslp (virtual switch)

To display Virtual Switch Link Protocol (VSLP) instance information, use the **show vslp** command in EXEC mode.

```
show vslp {lmp | rrp [type]} | {instances | lmp [type] | packet [counters] | rrp [type]}
```

Syntax Description	Parameter	Description
	lmp	Specifies the Link Maintenance Protocol (LMP) information.
	rrp	Specifies the Role Resolution Protocol (RRP) information.
	<i>type</i>	Specifies the type of information; see the "Usage Guidelines" section for valid values.
	instances	Displays the VSLP instance mappings.
	packet	Displays the VSLP packet information.
	counters	(Optional) Displays the VSLP packet counter information.

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.

Usage Guidelines The valid values for the *type* argument are as follows:

- **counters**—Displays counter information.
- **detail**—Displays detailed information.
- **fsm**—Displays Finite State Machine (FSM) information.
- **neighbors**—Displays neighbor information (supported with the *lmp* keyword only).
- **status**—Displays status information.
- **summary**—Displays a summary of information.
- **timer**—Displays Tx and Rx hello timer values.

The timers already displayed in the show vslp lmp timers output are shown in the output of the show vslp lmp summary command.

The output of the **show vslp rrp detail** command includes the information from the following commands:

- **show vslp rrp summary**
- **show vslp rrp counters**
- **show vslp rrp fsm**

Examples

The following example shows how to display a summary of LMP information for a specific VSLP instance.

```
Router# show vslp 2 lmp summary
LMP summary
  Link info:          Configured: 2          Operational: 0
                    Peer Peer          Peer Peer
                    Flag MAC          Swtch Port
Port   Flag State          Flag MAC          Swtch Port
-----
4/1   v   link_down          -   -             -   -
4/2   v   link_down          -   -             -   -
Router#
```

The following example shows how to displays the VSLP instance mappings.

```
Router# show vslp instances
VSLP instance mappings:
Instance Num  Name                               Switch Num  Flag
-----
2             VSL                                2           0x00000001
Router#
```

The following example shows how to display LMP neighbor information:

```
Router# show vslp 2 lmp neighbors
LMP neighbors
  Peer Group info:      # Groups: 0
Router#
```

The following example shows how to display a summary of LMP information:

```
Router# show vslp lmp summary
Instance #1:
LMP summary
Link info:          Configured: 3          Operational: 1
                    Peer Peer          Peer Peer          Timer(s) running
                    Flag MAC          Switch Interface (Time remaining)
-----
Gi1/3/1   v   link_down          -   -             -   -
Gi1/5/4   vf  operational        vf  0013.5fcb.1480  2   Gi1/6/4   T4(240ms) T5(2.22s)
Gi1/5/5   v   link_down          -   -             -   -
Flags:  V - valid          f -> B - bidirectional
```

The following examples shows how to display the LMP Tx and Rx hello timer values:

```
Router# show vslp lmp timer
Instance #1:
LMP hello timer
Interface  State          Hello Tx (T4) ms    Hello Rx (T5*) ms
          Cfg      Cur      Rem          Cfg      Cur      Rem
-----
Gi1/9/1   link_down     1000   -      -           500000  -      -
Gi1/9/3   link_down     1000   -      -           500000  -      -
Gi1/9/5   link_down     1000   -      -           500000  -      -
Router#
```

The following example shows how to display VSLP packet information:

```
Router# show vslp packet
VSLP packet counters
Transmitted:
total      = 1543
error      = 0
err_cksum  = 0
eobc       = 0
```

```

    ibc          = 0
    eobc[LMP]    = 0
    eobc[RRP]    = 0
    eobc[PING]   = 0
  Received:
    total       = 1564
    error       = 0
    err_cksum   = 0
    eobc        = 1564
    ibc         = 0
    total[LMP]  = 0
    total[RRP]  = 0
    total[PING] = 0
    eobc[LMP]   = 1559
    eobc[RRP]   = 5
    eobc[PING]  = 0
Router#

```

The following example shows how to display VSLP packet counter information:

```
Router# show vslp packet counters
```

```

VSLP packet counters
  Transmitted:
    total       = 28738
    error       = 0
    err_cksum   = 0
    eobc        = 28738
    eobc[LMP]   = 28701
    eobc[RRP]   = 17
    eobc[PING]  = 20
    ibc         = 0
    ibc[LMP]    = 0
    ibc[RRP]    = 0
    ibc[PING]   = 0
  Received:
    total       = 28590
    error       = 0
    err_cksum   = 0
    eobc        = 28590
    eobc[LMP]   = 28552
    eobc[RRP]   = 18
    eobc[PING]  = 20
    ibc         = 0
    ibc[LMP]    = 0
    ibc[RRP]    = 0
    ibc[PING]   = 0
Router#

```

The following example shows how to display a summary of RRP information:

```
Router# show vslp rrp summary
```

```
RRP information for Instance 1
```

```

-----
Valid  Flags   Peer      Preferred  Reserved
Count          Peer
-----
TRUE   V        1         1          1
Switch Peer  Switch  Status  Preempt  Priority  Role   Local  Remote
      Group Number
-----
Local   0    1    UP    TRUE    200    ACTIVE  0      0
Remote  1    2    UP    FALSE   100    STANDBY 9272   271
Flags:  V - valid

```


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.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

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

Examples The following example shows how to display the VTP statistics:

```
Switch# show vtp counters
VTP statistics:
Summary advertisements received      : 1
Subset advertisements received      : 1
Request advertisements received     : 0
Summary advertisements transmitted  : 31
Subset advertisements transmitted   : 1
Request advertisements transmitted  : 0
Number of config revision errors    : 0
Number of config digest errors     : 0
Number of V1 summary errors        : 0

VTP pruning statistics:

Trunk          Join Transmitted Join Received   Summary advts received from
-----          -----
Fa5/9          1555          1564          0
Switch#
```

The following 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 : 33
VTP Operating Mode   : Server
VTP Domain Name      : Lab_Network
VTP Pruning Mode     : Enabled
VTP V2 Mode          : Enabled
VTP Traps Generation : Disabled
```

```

MD5 digest                : 0xE6 0xF8 0x3E 0xDD 0xA4 0xF5 0xC2 0x0E
Configuration last modified by 172.20.52.18 at 9-22-99 11:18:20
Local updater ID is 172.20.52.18 on interface V11 (lowest numbered VLAN interface found)
Switch#

```

The following 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      : 1
Summary advertisements transmitted : 32
Trunk                               Join Transmitted Join Received   Summary advts received from
Switch#

```

Table 2-44 describes the fields in the **show vtp** command output.

Table 2-44 show vtp Command Output Fields

Field	Description
Summary advertisements received	Total number of summary advertisements received.
Subset advertisements received	Total number of subset advertisements received.
Request advertisements received	Total number of request advertisements received.
Summary advertisements transmitted	Total number of summary advertisements transmitted.
Subset advertisements transmitted	Total number of subset advertisements transmitted.
Request advertisements transmitted	Total number of request advertisements transmitted.
Number of config revision errors	Number of config revision errors.
Number of config digest errors	Number of config revision digest errors.
Number of V1 summary errors	Number of V1 summary errors.
Trunk	Trunk port participating in VTP pruning.
Join Transmitted	Number of VTP-Pruning Joins transmitted.
Join Received	Number of VTP-Pruning Joins received.
Summary advts received from non-pruning-capable device	Number of Summary advertisements received from nonpruning-capable devices.
Number of existing VLANs	Total number of VLANs in the domain.
Configuration Revision	VTP revision number used to exchange VLAN information.
Maximum VLANs supported locally	Maximum number of VLANs allowed on the device.
Number of existing VLANs	Number of existing VLANs.
VTP Operating Mode	Indicates whether VTP is enabled or disabled.
VTP Domain Name	Name of the VTP domain.
VTP Pruning Mode	Indicates whether VTP pruning is enabled or disabled.
VTP V2 Mode	Indicates the VTP V2 mode as server, client, or transparent.
VTP Traps Generation	Indicates whether VTP trap generation mode is enabled or disabled.
MD5 digest	Checksum values.

Related Commands	Command	Description
	vtp (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.

Command Default This command has no default settings.

Command Modes Interface configuration mode

Command History	Release	Modification
	12.1(19)EW	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 The following example shows how to enable ifIndex persistence for all interfaces:

```
Router(config)# snmp-server ifindex persist
```

The following 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
```

The following 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 Interfaces MIB (IF-MIB) that persist across reboots (ifIndex persistence) on a specific interface, use the **snmp ifindex persist** command. To disable ifIndex persistence only on a specific interface, use the **no** form of this command.

snmp ifindex persist

no snmp ifindex persist

Syntax Description This command has no arguments or keywords.

Command Default Disabled.

Command Modes Interface configuration mode

Command History	Release	Modification
	12.1(19)EW	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 ifDescr and ifIndex entries in the ifIndex table of the IF-MIB.

Examples The following 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
```

The following 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** | **stpx** | **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** | **stpx** | **vlancreate** | **vlandelete** | **vtp**] [**mac-notification**]

Syntax Description		
flash	(Optional)	Controls the SNMP FLASH trap notifications.
insertion	(Optional)	Controls the SNMP flash insertion trap notifications.
removal	(Optional)	Controls the SNMP flash removal trap notifications.
fru-ctrl	(Optional)	Controls the SNMP entity FRU control trap notifications.
port-security	(Optional)	Controls the SNMP trap generation.
trap-rate <i>trap-rate</i>	(Optional)	Sets the number of traps per second.
stpx	(Optional)	Controls all the traps defined in CISCO-STP-EXTENSIONS-MIB notifications.
vlancreate	(Optional)	Controls the SNMP VLAN created trap notifications.
vlandelete	(Optional)	Controls the SNMP VLAN deleted trap notifications.
vtp	(Optional)	Controls the SNMP VTP trap notifications.
mac-notification	(Optional)	Controls the SNMP MAC trap notifications.
change	(Optional)	Controls the SNMP MAC change trap notifications.
move	(Optional)	Controls the SNMP MAC move trap notifications.
threshold	(Optional)	Controls the SNMP MAC threshold trap notifications.

Command Default SNMP notifications are disabled.

Command Modes Global configuration mode

Command History	Release	Modification
	12.1(13)EW	This command was introduced on the Catalyst 4500 series switch.
	12.2(31)SG	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 Flash insertion trap notifications.
 - **removal**—Controls the SNMP Flash removal trap notifications.
- **fru-ctrl**—Controls the FRU 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.
- **vlancreate**—Controls SNMP VLAN created trap notifications.
- **vlandelete**—Controls SNMP VLAN deleted trap notifications.
- **vtp**—Controls the VTP traps from the CISCO-VTP-MIB.

Examples

The following 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)#
```

The following 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 rate-limit to detect port-security violations due to restrict mode. The following example shows how to enable traps for port-security with a rate of 5 traps per second:

```
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.

Command Default Disabled.

Command Modes Global configuration mode

Command History	Release	Modification
	12.1(19)EW	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 command does not override the interface-specific configuration. To override the interface-specific configuration of ifIndex persistence, enter the **no snmp ifindex persist** and **snmp ifindex clear** interface configuration commands.

Entering the **no snmp-server ifindex persist** global configuration command enables and disables ifIndex persistence for all interfaces on the routing device using ifDescr and ifIndex entries in the ifIndex table of the IF-MIB.

Examples The following 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 Interfaces 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.

Command Default Disabled

Command Modes Global configuration mode.

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

Usage Guidelines This command is hidden because the ifIndex table is always in a compressed format on those supervisor engines.

Examples The following example shows how to enable compression of the ifIndex table:

```
Router(config)# snmp-server ifindex persist compress
```

The following example shows how to disable compression of the ifIndex table:

```
Router(config)# no snmp-server ifindex persist compress
```

Related Commands	Command	Description
	snmp ifindex clear	Clears any previously configured snmp ifindex commands that were entered for a specific interface.
	snmp ifindex persist	Enables ifIndex values in the Interfaces MIB (IF-MIB) that 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	removed
	Specifies enabling the MAC address notification trap whenever a MAC address is added to an interface.	Specifies enabling the MAC address notification trap whenever a MAC address is removed from an interface.

Command Default MAC address addition and removal are disabled.

Command Modes Interface configuration mode

Command History	Release	Modification
	12.2(31)SG	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 The following 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.

Command	Description
show mac-address-table notification	Displays the MAC address table notification status and history.
snmp-server enable traps	Enables SNMP notifications.

source (netflow-lite exporter submode)



Note

NetFlow-lite is only supported on the Catalyst 4948E and Catalyst 4948E-F Ethernet switches.

To specify a source Layer 3 interface of the NetFlow-lite collector, use the **source** command. To delete a source address, use the **no source** form of this command.

```
source source-address
```

```
no source source-address
```

Syntax Description	<i>source-address</i>	Specifies a source Layer 3 interface for a NetFlow-lite exporter.
Command Default	None	
Command Modes	netflow-lite exporter submode	
Command History	Release	Modification
	15.0(2)SG	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines One of the mandatory parameters for a minimally configured exporter along with the destination address and the UDP destination port of the collector.

Examples The following example shows how to specify a source Layer 3 interface of the NetFlow-lite collector:

```
Switch# config terminal
Switch(config)# netflow-lite exporter exporter1
Switch(config-netflow-lite-exporter)# destination 5.5.5.6
Switch(config-netflow-lite-exporter)# source 5.5.5.5
Switch(config-netflow-lite-exporter)# transport udp 8188
Switch(config-netflow-lite-exporter)# ttl 128
Switch(config-netflow-lite-exporter)# cos 7
Switch(config-netflow-lite-exporter)# dscp 32
Switch(config-netflow-lite-exporter)# template data timeout 1
Switch(config-netflow-lite-exporter)# options sampler-table timeout 1
Switch(config-netflow-lite-exporter)# options interface-table timeout 1
Switch(config-netflow-lite-exporter)# export-protocol netflow-v9
Switch(config-netflow-lite-exporter)# exit
Switch(config)#

Display the exporter
Switch# show netflow-lite exporter exporter1
Netflow-lite Exporter exporter1:
  Network Protocol Configuration:
    Destination IP address: 5.5.5.6
```

■ source (netflow-lite exporter submode)

```

Source IP Address:      5.5.5.5
VRF label:
DSCP:                  0x20
TTL:                   128
COS:                   7
Transport Protocol Configuration:
Transport Protocol:    UDP
Destination Port:      8188
Source Port:           61670
Export Protocol Configuration:
Export Protocol:       netflow-v9
Template data timeout: 60
Options sampler-table timeout: 1800
Options interface-table timeout: 1800
Exporter Statistics:
Packets Exported:     0

```

You can verify your settings with the **show netflow-lite exporter** privileged EXEC command.

Related Commands	Command	Description
	options timeout (netflow-lite exporter submode)	Specifies an options timeout for the NetFlow-lite collector.
	cos (netflow-lite exporter submode)	Specifies a cos value for the NetFlow-lite collector.
	source (netflow-lite exporter submode)	Specifies a source Layer 3 interface of the NetFlow-lite collector.
	transport udp (netflow-lite exporter submode)	Specifies a UDP transport destination port for a NetFlow-lite collector.
	ttl (netflow-lite exporter submode)	Specifies a ttl value for the NetFlow-lite collector.
	destination (netflow-lite exporter submode)	Specifies a destination address in netflow-lite submode.
	template data timeout (netflow-lite exporter submode)	Specifies a template data timeout for the NetFlow-lite collector.
	export-protocol (netflow-lite exporter submode)	Specifies the export protocol for the NetFlow-lite collector.
	dscp (netflow-lite exporter submode)	Specifies a cos value for the NetFlow-lite collector.

source-interface

To send out call home email messages with specific source interface, use the **source-interface** command.

source-interface *interface name*

Syntax Description	<i>interface name</i>	Source interface name for call home email messages
Command Default	None	
Command Modes	cfg-call-home	
Command History	Release	Modification
	15.0(2)SG	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

You should configure **no shut** on an interface and provide a valid IP address before specifying it as a source interface for Call Home. Doing this avoids a connection failure when sending Call Home email messages. You should only specify a source interface name under Call Home if source-ip-address is not specified. You can only specify either a source interface or source-ip-address in call-home mode, not simultaneously.

Examples

The following example shows how to configure source interface for Call Home. Generally, the interface should already be configured with a valid IP address as usually configured for an interface.

```
Switch# config terminal
Switch(config)# call-home
Switch(cfg-call-home)# source-interface fastEthernet 1/1
Switch(cfg-call-home)# source-ip
Switch(cfg-call-home)# source-ip-address 10.2.4.1
Error:a source-interface has already been configured,please remove source-interface config
first if you want to configure source-ip-address
Switch(cfg-call-home)# no source-interface
Switch(cfg-call-home)# source-ip-address 10.2.4.1
```



Note

If Call Home is configured to use http or https as the transport method, you must use **ip http client source-interface** to configure the source interface for all http clients. You cannot specify a source interface for Call Home http messages only.

Related Commands

Command	Description
source-ip-address	Sends out Call Home email messages with specific source IP address.

source-ip-address

To send out Call Home email messages with specific source IP address, use the **source-ip-address** command.

source-ip-address *ip address*

Syntax Description	<i>ip address</i>	Source IP address for Call Home messages.
Command Default	None	
Command Modes	cfg-call-home	
Command History	Release	Modification
	15.0(2)SG	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

It is best to configure **no shut** an interface with this valid IP address before specifying it as source-ip-address for Call Home. Doing this avoids a connection failure when sending Call Home email messages. You should only specify source-ip-address under Call Home if source-interface is not specified. You can only specify either source interface or source-ip-address in Call Home mode, not both simultaneously.

Examples

The following example shows how to configure source-ip-address for Call Home:

```
Switch# config terminal
Switch(config)# call-home
Switch(cfg-call-home)# source-interface fastEthernet 1/1
Switch(cfg-call-home)# source-ip
Switch(cfg-call-home)# source-ip-address 10.2.4.1
Error:a source-interface has already been configured,please remove source-interface config
first if you want to configure source-ip-address
Switch(cfg-call-home)# no source-interface
Switch(cfg-call-home)# source-ip-address 10.2.4.1
```

Related Commands

Command	Description
source-interface	Sends out call home email messages with specific source interface.

spanning-tree backbonefast

To enable BackboneFast on a spanning-tree VLAN, use the **spanning-tree backbonefast** command. To disable BackboneFast, use the **no** form of this command.

spanning-tree backbonefast

no spanning-tree backbonefast

Syntax Description This command has no arguments or keywords.

Command Default BackboneFast is disabled.

Command Modes Global configuration mode

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

Usage Guidelines BackboneFast should be enabled on all Catalyst 4506 series switches to allow the detection of indirect link failures. Enabling BackboneFast starts the spanning-tree reconfiguration more quickly.

Examples The following 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	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 bpdudfilter

To enable BPDU filtering on an interface, use the **spanning-tree bpdudfilter** command. To return to the default settings, use the **no** form of this command.

spanning-tree bpdudfilter { **enable** | **disable** }

no spanning-tree bpdudfilter

Syntax Description	enable	Disable
	Enables BPDU filtering on this interface.	Disables BPDU filtering on this interface.

Command Default Disabled

Command Modes Interface configuration mode

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

Usage Guidelines



Caution

Use care when entering the **spanning-tree bpdudfilter 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 Layer 2 protocol tunneling on all the service provider edge switches, you must enable spanning-tree BPDU filtering on the 802.1Q tunnel ports by entering the **spanning-tree bpdudfilter 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 bpdudfilter enable**—This state unconditionally enables the BPDU filter feature on the interface.
- **spanning-tree bpdudfilter disable**—This state unconditionally disables the BPDU filter feature on the interface.
- **no spanning-tree bpdudfilter**—This state enables the BPDU filter feature on the interface if the interface is in operational PortFast state and if the **spanning-tree portfast edge bpdudfilter default** command is configured.

Examples

The following example shows how to enable the BPDU filter feature on this interface:

```
Switch(config-if)# spanning-tree bpdudfilter enable  
Switch(config-if)#
```

Related Commands

Command	Description
show spanning-tree	Displays spanning-tree information.
spanning-tree portfast edge bpdudfilter 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 settings, 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 guard on this interface.

Command Default

BPDU guard is disabled.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(12c)EW	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 protective 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 edge bpduguard default** command is configured.

Examples

The following 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 edge bpduguard default	Enables the BPDU filtering by default on all PortFast ports.

spanning-tree bridge assurance

To enable Bridge Assurance on your network, use the **spanning-tree bridge assurance** command. To disable the feature, use the **no** form of the command.

spanning-tree bridge assurance

no spanning-tree bridge assurance

Syntax Description This command has no arguments or keywords.

Command Default Bridge Assurance is enabled

Command Modes Global configuration mode

Command History	Release	Modification
	3.8.0E and 15.2.(4)E	Support for the command was introduced.

Usage Guidelines This feature protects your network from bridging loops. It monitors the receipt of BPDUs on point-to-point links on all network ports. When a port does not receive BPDUs within the allotted hello time period, the port is put into a blocked state (the same as a port inconsistent state, which stops forwarding of frames). When the port resumes receipt of BPDUs, the port resumes normal spanning tree operations.

By default, Bridge Assurance is enabled on all operational network ports, including alternate and backup ports. If you have configured the **spanning-tree portfast network** command on all the required ports that are connected Layer 2 switches or bridges, Bridge Assurance is automatically effective on all those network ports.

Only Rapid PVST+ and MST spanning tree protocols support Bridge Assurance. PVST+ does not support Bridge Assurance.

For Bridge Assurance to work properly, it must be supported and configured on both ends of a point-to-point link. If the device on one side of the link has Bridge Assurance enabled and the device on the other side does not, then the connecting port is blocked (a Bridge Assurance inconsistent state). We recommend that you enable Bridge Assurance throughout your network.

To enable Bridge Assurance on a port, BPDU filtering and BPDU Guard must be disabled.

You can enable Bridge Assurance in conjunction with Loop Guard.

You can enable Bridge Assurance in conjunction with Root Guard. The latter is designed to provide a way to enforce the root bridge placement in the network.

Disabling Bridge Assurance causes all configured network ports to behave as normal spanning tree ports.

Use the **show spanning-tree summary** command to see if the feature is enabled on a port.

Examples

The following example shows how to enable Bridge Assurance on all network ports on the switch, and how to configure a network port:

```
Switch(config)# spanning-tree bridge assurance
Switch(config)# interface gigabitethernet 5/8
Switch(config-if)# spanning-tree portfast network
Switch(config-if)# exit
```

This example show how to display spanning tree information and verify if Bridge Assurance is enabled. Look for these details in the output:

- Portfast Default—Network
- Bridge Assurance—Enabled

```
Switch# show spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for: VLAN0199-VLAN0200, VLAN0128
EtherChannel misconfig guard is enabled
Extended system ID is enabled
Portfast Default is network
Portfast Edge BPDU Guard Default is disabled
Portfast Edge BPDU Filter Default is disabled
Loopguard Default is enabled
PVST Simulation Default is enabled but inactive in rapid-pvst mode
Bridge Assurance is enabled
UplinkFast is disabled
BackboneFast is disabled
Configured Pathcost method used is short
```

```
Name Blocking Listening Learning Forwarding STP Active
```

```
-----
VLAN0199 0 0 0 5 5
VLAN0200 0 0 0 4 4
VLAN0128 0 0 0 4 4
-----
```

```
3 vlans 0 0 0 13 13
```

Related Commands

Command	Description
spanning-tree portfast	Globally enables a default state for all ports (whether edge, network, or, normal)
spanning-tree portfast (interface configuration mode)	Configures a port type on an individual interface ((whether edge, network, or, normal).
show spanning-tree	Displays spanning-tree information.

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.

Command Default

The default settings are as follows:

- FastEthernet—19
- GigabitEthernet—1

Command Modes

Interface configuration mode

Command History

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

Usage Guidelines

When you configure the cost, the higher values indicate higher costs. The range applies regardless of the protocol type that is specified. The path cost is calculated, based on the interface bandwidth.

Examples

The following 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 2/1
Switch(config-if)# spanning-tree cost 250
Switch(config-if)#
```

Related Commands

Command	Description
spanning-tree portfast	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.

Command Default Spanning-tree EtherChannel guard is enabled.

Command Modes Global configuration mode

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

Usage Guidelines When an EtherChannel guard misconfiguration is detected, this message is displayed:

```
%SPANTREE-2-CHNL_MISCFG:Detected loop due to etherchannel misconfig of interface
Port-Channel11
```

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 The following 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.

Command Default Enabled on systems that do not provide 1024 MAC addresses.

Command Modes Global configuration mode

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

Usage Guidelines Releases 12.1(13)E and later support chassis with 64 or 1024 MAC addresses. For chassis with 64 MAC addresses, STP uses the extended system ID plus a MAC address to make the bridge ID unique for each VLAN.

You cannot disable the extended system ID on chassis that support 64 MAC addresses.

Enabling or disabling the extended system ID updates the bridge IDs of all active STP instances, which might change the spanning-tree topology.

Examples The following 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.

Command Default

Root guard is disabled.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch.
12.1(12c)EW	Loop guard support was added.

Examples

The following 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.

Command Default Link type is derived from the duplex mode.

Command Modes Interface configuration mode

Command History	Release	Modification
	12.1(12c)EW	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 The following example shows how to configure the port as a shared link:

```
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.

Command Default Loop guard is disabled.

Command Modes Global configuration mode

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

Usage Guidelines

Loop guard provides an additional security in the bridge network. Loop guard prevents alternate or root ports from becoming the designated port because of a failure leading to a unidirectional link.

Loop guard operates only on ports that are considered point-to-point by the spanning tree.

Individual loop-guard port configuration overrides this global default.

Examples The following 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.

Command Default

PVST+ mode

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(8a)EW	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

The following example shows how to switch to MST mode:

```
Switch(config)# spanning-tree mode mst
Switch(config)#
```

The following 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

<i>instance-id</i>	Instance ID number; valid values are from 0 to 15.
cost <i>cost</i>	(Optional) Specifies the path cost for an instance; valid values are from 1 to 200000000.
port-priority <i>prio</i>	(Optional) Specifies the port priority for an instance; valid values are from 0 to 240 in increments of 16.

Command Default

Port priority is **128**.

Command Modes

Interface configuration mode

Command History

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

Usage Guidelines

The higher **cost** *cost* values indicate higher costs. When entering the *cost* value, do not include a comma in the entry; for example, enter **1000**, not **1,000**.

The higher **port-priority** *prio* values indicate smaller priorities.

By default, the cost depends on the port speed; faster interface speeds indicate smaller costs. MST always uses long path costs.

Examples

The following example shows how to set the interface path cost:

```
Switch(config-if)# spanning-tree mst 0 cost 17031970
Switch(config-if)#
```

The following 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.

Command Default 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(12c)EW	This command was introduced on the Catalyst 4500 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 VLANs that are not mapped to the same instance as the associated primary VLAN. The message is as follows:

```
These secondary vlans are not mapped to the same instance as their primary:
->3
```

The **abort** command leaves the MST configuration submode without committing any changes.

Whenever you change an MST configuration submode 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 all the changes at once by using the **exit** keyword, or you can exit the submode without committing any change to the configuration by using the **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

The following example shows how to enter the MST configuration submode:

```
Switch(config)# spanning-tree mst configuration
Switch(config-mst)#
```

The following 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 timer 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	<i>seconds</i>	Number of seconds to set the forward delay timer for all the instances on the Catalyst 4500 series switch; valid values are from 4 to 30 seconds.
---------------------------	----------------	---

Command Default	The forward delay timer is set for 15 seconds.
------------------------	--

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

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

Examples	The following example shows how to set the forward-delay timer:
-----------------	---

```
Switch(config)# spanning-tree mst forward-time 20
Switch(config)#
```

Related Commands	Command	Description
	show spanning-tree mst	Displays MST protocol information.

spanning-tree mst hello-time

To set the hello-time delay timer for all the instances, use the **spanning-tree mst hello-time** command. To return to the default settings, use the **no** form of this command.

spanning-tree mst hello-time *seconds*

no spanning-tree mst hello-time

Syntax Description	<i>seconds</i>	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.
Command Default	The hello-time delay timer is set for 2 seconds.	
Command Modes	Global configuration mode	
Command History	Release	Modification
	12.1(12c)EW	This command was introduced on the Catalyst 4500 series switch.
Usage Guidelines	If you do not specify the <i>hello-time</i> value, the value is calculated from the network diameter.	
Examples	The following example shows how to set the hello-time delay timer: <pre>Switch(config)# spanning-tree mst hello-time 3 Switch(config)#</pre>	
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	<i>seconds</i>	Number of seconds to set the max-age timer for all the instances on the Catalyst 4500 series switch; valid values are from 6 to 40 seconds.
---------------------------	----------------	---

Command Default	The max-age timer is set for 20 seconds.
------------------------	--

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

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

Examples The following example shows how to set the max-age timer:

```
Switch(config)# spanning-tree mst max-age 40
Switch(config)#
```

Related Commands	Command	Description
	show spanning-tree mst	Displays MST protocol information.

spanning-tree mst max-hops

To specify the number of possible hops in the region before a BPDU is discarded, use the **spanning-tree mst max-hops** command. To return to the default settings, use the **no** form of this command.

spanning-tree mst max-hops *hopnumber*

no spanning-tree mst max-hops

Syntax Description	<i>hopnumber</i> Number of possible hops in the region before a BPDU is discarded; valid values are from 1 to 40 hops.
---------------------------	--

Command Default	Number of hops is 20.
------------------------	-----------------------

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

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

Examples The following 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 simulate pvst global

To enable PVST+ simulation globally, use the **spanning-tree mst simulate pvst global** command. This is enabled by default. To disable PVST+ simulation, use the **no** form of this command.

spanning-tree mst simulate pvst global

no spanning-tree mst simulate pvst global

Syntax Description This command has no arguments or keywords.

Command Default PVST+ simulation is enabled by default.

Command Modes Global configuration mode

Command History	Release	Modification
	3.8.0E and 15.2.(4)E	Support for the command was introduced.

Usage Guidelines This feature configures MST switches (in the same region) to seamlessly interact with PVST+ switches. Use the **show spanning-tree summary** command to see if the feature is enabled. To enable PVST+ simulation on a port, see [spanning-tree mst simulate pvst \(interface configuration mode\)](#).

Examples The following example shows the spanning tree summary when PVST+ simulation is enabled in the MSTP mode:

```
Switch# show spanning-tree summary
Switch is in mst mode (IEEE Standard)
Root bridge for: MST0
EtherChannel misconfig guard is enabled
Extended system ID is enabled
Portfast Default is disabled
PortFast BPDU Guard Default is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default is disabled
UplinkFast is disabled
BackboneFast is disabled
Pathcost method used is long
PVST Simulation Default is enabled

Name Blocking Listening Learning Forwarding STP Active
-----
MST0 2 0 0 0 2
-----
1 mst 2 0 0 0 2
```


The following example shows the spanning tree summary when the switch is not in MSTP mode, that is, the switch is in PVST or Rapid-PVST mode. The output string displays the current STP mode:

```
Switch# show spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for: VLAN0001, VLAN2001-VLAN2002
EtherChannel misconfig guard is enabled
Extended system ID is enabled
Portfast Default is disabled
PortFast BPDU Guard Default is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default is disabled
UplinkFast is disabled
BackboneFast is disabled
Pathcost method used is short
PVST Simulation Default is enabled but inactive in rapid-pvst mode

Name Blocking Listening Learning Forwarding STP Active
-----
VLAN0001 2 0 0 0 2
VLAN2001 2 0 0 0 2
VLAN2002 2 0 0 0 2
-----
3 vlans 6 0 0 0 6
```

Related Commands

Command	Description
spanning-tree mst simulate pvst (interface configuration mode)	Enables PVST+ simulation on a port.
show spanning-tree	Displays spanning-tree state information.

spanning-tree mst simulate pvst (interface configuration mode)

To enable PVST+ simulation on a port, use the **spanning-tree mst simulate pvst** command in the interface configuration mode. This is enabled by default. To disable PVST+ simulation, use the **no** form of this command, or enter the **spanning-tree mst simulate pvst disable** command.

spanning-tree mst simulate pvst [disable]

no spanning-tree mst simulate pvst

Syntax Description

disable	Disables the PVST+ simulation feature. This prevents a port from automatically interoperating with a connecting device that is running Rapid PVST+.
----------------	---

Command Default

PVST+ simulation is enabled by default.

Command Modes

Interface configuration mode

Command History

Release	Modification
3.8.0E and 15.2.(4)E	Support for the command was introduced.

Usage Guidelines

This feature configures MST switches (in the same region) to seamlessly interact with PVST+ switches. Use the **show spanning-tree interface *interface-id* detail** command to see if the feature is enabled. To enable PVST+ simulation globally, see [spanning-tree mst simulate pvst global](#).

Examples

The following example shows the interface details when PVST+ simulation is explicitly enabled on the port:

```
Switch# show spanning-tree interface gi3/13 detail
Port 269 (GigabitEthernet3/13) of VLAN0002 is forwarding
Port path cost 4, Port priority 128, Port Identifier 128.297.
Designated root has priority 32769, address 0013.5f20.01c0
Designated bridge has priority 32769, address 0013.5f20.01c0
Designated port id is 128.297, designated path cost 0
Timers: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state: 1
Link type is point-to-point by default
PVST Simulation is enabled
BPDU: sent 132, received 1
```

The following example shows the interface details when the PVST+ simulation feature is disabled and a PVST Peer inconsistency has been detected on the port:

```
Switch# show spanning-tree interface gi3/13 detail
Port 269 (GigabitEthernet3/13) of VLAN0002 is broken (PVST Peer Inconsistent)
Port path cost 4, Port priority 128, Port Identifier 128.297.
Designated root has priority 32769, address 0013.5f20.01c0
Designated bridge has priority 32769, address 0013.5f20.01c0
Designated port id is 128.297, designated path cost 0
Timers: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state: 1
Link type is point-to-point by default
PVST Simulation is disabled
BPDU: sent 132, received 1
```

Related Commands

Command	Description
spanning-tree mst simulate pvst global	Globally enables PVST+ simulation
show spanning-tree	Displays spanning-tree state 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 prio} [diameter dia
  [hello-time hello]]
```

```
no spanning-tree mst root
```

Syntax Description

<i>instance-id</i>	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 <i>prio</i>	Sets the bridge priority; see the “Usage Guidelines” section for valid values and additional information.
diameter <i>dia</i>	(Optional) Sets the timer values for the bridge based on the network diameter; valid values are from 2 to 7.
hello-time <i>hello</i>	(Optional) Specifies the duration between the generation of configuration messages by the root switch.

Command Default

Bridge priority is 32768.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(12c)EW	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 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

The following example shows how to set the priority and timer values for the bridge:

```
Switch(config)# spanning-tree mst 0 root primary diameter 7 hello-time 2
Switch(config)# spanning-tree mst 5 root primary
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.

Command Default Port path cost has 16-bit-based values.

Command Modes Global configuration mode

Command History	Release	Modification
	12.1(8a)EW	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 The following example shows how to set the path cost calculation method to long:

```
Switch(config) spanning-tree pathcost method long
Switch(config)
```

The following 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 configure a port type on an individual interface **spanning-tree portfast** command. To return to the default setting, use the **no** form of this command.

spanning-tree portfast { **disable** | **edge** [**trunk**] | **network** }

no spanning-tree portfast

Syntax Description	
disable	(Optional) Configures the port as a normal spanning tree port.
edge	Configures the specified interfaces as an edge port.
[trunk]	(Optional) trunk —Configures the trunk port as an edge port.
network	Configures all interfaces as network ports.

Command Default Port type is **normal**.

Command Modes Interface configuration mode

Command History	Release	Modification
	12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch..
	12.1(12c)EW	The disable and trunk options were added.
	3.8.0E and 15.2.(4)E	Support for the edge , and network , keywords was introduced. Beginning with this release, if you enter the spanning-tree portfast [trunk] command in the interface configuration mode, the system automatically saves it as spanning-tree portfast edge [trunk] .

Usage Guidelines On any given interface, the type of port you can configure depends on the type of device to which the interface is connected:

- A PortFast edge port—is connected to a Layer 2 host, which can be an access port or an edge trunk port. An edge port is moved directly to the spanning-tree forwarding state when linkup occurs, without waiting for the standard forward-time delay.

Set this port type only on interfaces that connect to end stations (hosts or servers); otherwise, an accidental topology loop could cause a data packet loop and disrupt the Catalyst 4500 series switch and network operation.

- A PortFast network port—is connected only to a Layer 2 switch or bridge.

Set this port type on interfaces where you want to enable Bridge Assurance (Bridge Assurance is enabled on all network ports by default). If you configure a port that is connected to a Layer 2 host as a spanning tree network port, the port will automatically move into the blocking state.

- A PortFast normal port—is the default type of spanning tree port.

Using the **no spanning-tree portfast** interface configuration command resets the interface to the port type you have specified in the **spanning-tree portfast** global configuration command.

Using the **spanning-tree portfast disable** command resets the interface to the port type you have specified in the **spanning-tree portfast** global configuration command.

If you have not configured spanning-tree portfast globally, using the **no spanning-tree portfast** interface configuration command is equivalent to the **spanning-tree portfast disable** interface configuration command.

Use the **show spanning-tree interface type detail** command to know what is configured on a given port.

Examples

The following example shows how to enable edge behavior on GigabitEthernet interface 5/7 and verify configuration:

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/7
Switch(config-if)# spanning-tree portfast edge
Switch(config-if)# end
Switch#
```

The following example shows how to configure GigabitEthernet interface 5/8 as a network port and verify configuration:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet 5/8
Switch(config-if)# spanning-tree portfast network
Switch(config-if)# end
Switch#
```

Related Commands

Command	Description
spanning-tree cost	Calculates the path cost of STP on an interface.
spanning-tree bridge assurance	Enables Bridge Assurance.
spanning-tree portfast	Globally enables a default state for all ports.
show spanning-tree	Displays spanning-tree state information.

spanning-tree portfast edge bpdudfilter default

To enable the BPDU filtering by default on all PortFast edge ports, use the **spanning-tree portfast edge bpdudfilter default** command. To return to the default settings, use the **no** form of this command.

spanning-tree portfast edge bpdudfilter default

no spanning-tree portfast edge bpdudfilter default

Syntax Description This command has no keywords or arguments.

Command Default BPDU filtering is disabled.

Command Modes Global configuration mode

Command History	Release	Modification
	12.1(12c)EW	This command was introduced on the Catalyst 4500 series switch.
	3.8.0E and 15.2.(4)E	Support for the edge keyword was introduced.

Usage Guidelines The **spanning-tree portfast edge bpdudfilter 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 edge bpdudfilter default** command by configuring BPDU filtering at the interface level.



Note

Be careful when enabling BPDU filtering. Functionality is different when enabling on a per-port basis or globally. When enabled globally, BPDU filtering is applied only on ports that are in an operational PortFast state. Ports still send a few BPDUs at linkup before they effectively filter outbound BPDUs. If a BPDU is received on an edge port, it immediately loses its operational PortFast status and BPDU filtering is disabled.

When enabled locally on a port, BPDU filtering prevents the Catalyst 4500 series switch from receiving or sending BPDUs on this port.



Caution

Be careful when using this command. This command can cause bridging loops if not used correctly.

Examples The following example shows how to enable BPDU filtering by default:

```
Switch(config)# spanning-tree portfast edge bpdudfilter 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 edge bpduguard default

To enable BPDU guard by default on all the PortFast ports, use the **spanning-tree portfast edge bpduguard default** command. To return to the default settings, use the **no** form of this command.

spanning-tree portfast edge bpduguard default

no spanning-tree portfast edge bpduguard default

Syntax Description This command has no keywords or arguments.

Command Default BPDU guard is disabled.

Command Modes Global configuration mode

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

Usage Guidelines



Caution

Use this command only with the interfaces that connect to the end stations; otherwise, an accidental topology loop could cause a data packet loop and disrupt the Catalyst 4500 series switch and network operation.

BPDU guard disables a port if it receives a BPDU. BPDU guard is applied only on ports that are PortFast enabled and are in an operational PortFast state.

Examples The following example shows how to enable BPDU guard by default:

```
Switch(config)# spanning-tree portfast edge 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

To globally enable a default state for all ports, use the **spanning-tree portfast** command. To return to the default settings, use the **no** form of this command, or enter the **spanning-tree portfast default** command.

spanning-tree portfast { edge | network | normal } default

no spanning-tree portfast

Syntax Description

edge	Configures all interfaces as edge ports.
network	Configures all interfaces as network ports.
normal	Configures all interfaces as normal spanning tree ports.
default	Sets the port type that you entered (whether edge , network , or normal) as the default port type on all interfaces.

Command Default

The default port type is **normal**.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(12c)EW	This command was introduced on the Catalyst 4500 series switch.
3.8.0E and 15.2.(4)E	Support for the edge , network , and normal keywords was introduced. Beginning with this release, if you enter the spanning-tree portfast [trunk] command in the global configuration mode, the system automatically saves it as spanning-tree portfast edge [trunk] .

Usage Guidelines

On any given interface, the type of port you can configure depends on the type of device to which the interface is connected:

- A PortFast edge port—is connected to a Layer 2 host, which can be an access port or an edge trunk port. An edge port is moved directly to the spanning-tree forwarding state when linkup occurs, without waiting for the standard forward-time delay.

Set this port type only on interfaces that connect to end stations (hosts or servers); otherwise, an accidental topology loop could cause a data packet loop and disrupt the Catalyst 4500 series switch and network operation.

- A PortFast network port—is connected only to a Layer 2 switch or bridge.

Set this port type on interfaces where you want to enable Bridge Assurance (Bridge Assurance is enabled on all network ports by default). For more information, see the [spanning-tree bridge assurance](#) global configuration command.

If you configure a port that is connected to a Layer 2 host as a spanning tree network port, the port will automatically move into the blocking state.

- A PortFast normal port—is the default type of spanning tree port.

You can configure a port type on individual interfaces using the **spanning-tree portfast (interface configuration mode)** command.

Examples

The following example shows how to globally configure all access and trunk ports connected to hosts as edge ports:

```
Switch# configure terminal  
Switch(config)# spanning-tree portfast edge default
```

Related Commands

Command	Description
show spanning-tree	Displays spanning-tree state information.
spanning-tree portfast (interface configuration mode)	Configures a port type on an individual interface.
spanning-tree bridge assurance	Enables Bridge Assurance.

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.

Command Default

Port priority value is set to 128.

Command Modes

Interface configuration mode

Command History

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

Examples

The following example shows how to increase the possibility that the spanning-tree instance 20 will be chosen as the root-bridge on interface FastEthernet 2/1:

```
Switch(config-if)# spanning-tree port-priority 0
Switch(config-if)#
```

Related Commands

Command	Description
spanning-tree cost	Calculates the path cost of STP on an interface.
spanning-tree portfast	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 <i>packets_per_second</i>	(Optional) Specifies the maximum rate (in packets per second) at which update packets are sent; valid values are from 0 to 65535.
---	---

Command Default

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	This command was introduced on the Catalyst 4500 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 instances are also increased by 3000.

When spanning tree detects that the root interface has failed, the UplinkFast feature causes an immediate switchover 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 multicast packet is sent to 01-00-0C-CD-CD-CD for each station address in the forwarding bridge except for those associated with the old root interface.

Use the **spanning-tree uplinkfast max-update-rate** command to enable UplinkFast (if not already enabled) and change the rate at which the update packets are sent. Use the **no** form of this command to return the default rate of 150 packets per second.

Examples

The following 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	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	
<i>vlan_id</i>	VLAN identification number; valid values are from 1 to 4094.
forward-time <i>seconds</i>	(Optional) Sets the STP forward delay time; valid values are from 4 to 30 seconds.
hello-time <i>seconds</i>	(Optional) Specifies, in seconds, the time between configuration messages generated by the root switch; valid values are from 1 to 10 seconds.
max-age <i>seconds</i>	(Optional) Sets the maximum time, in seconds, that the information in a BPDU is valid; valid values are from 6 to 40 seconds.
priority <i>priority</i>	(Optional) Sets the STP bridge priority; valid values are from 0 to 65535.
protocol <i>protocol</i>	(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 <i>net-diameter</i>	(Optional) Specifies the maximum number of bridges between two end stations; valid values are from 2 to 7.

Command Default

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(8a)EW	This command was introduced on the Catalyst 4500 series switch.
12.1(12c)EW	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, then the bridge priority is changed to 100 less than the bridge priority of the current bridge. If the switch does not become root, an error 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

The following example shows how to enable spanning tree on VLAN 200:

```
Switch(config)# spanning-tree vlan 200
Switch(config)#
```

The following 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)#
```

The following 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	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 exact values to advertise when autonegotiating.
nonegotiate	Enables the interface to not negotiate the speed.

Command Default

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	This command was introduced on the Catalyst 4500 series switch.
12.2(20)EWA	Support for auto negotiating specific speeds added.

Usage Guidelines

Table 2-44 lists the supported command options by interface.

Table 2-44 Supported speed Command Options

Interface Type	Supported Syntax	Default Setting	Guidelines
10/100-Mbps module	speed [10 100 auto]	auto	If the speed is set to 10 or 100 and you do not configure the duplex setting, the duplex is set to half.
100-Mbps fiber modules	Not applicable.	Not applicable.	Not applicable.
Gigabit Ethernet Interface	speed nonegotiate	nonegotiate is enabled.	This is only applicable to Gigabit Ethernet ports.
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 or auto with any subset containing 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, 10 or 100 Mbps), make sure that you configure the connecting interface speed command to a matching speed but do not use the auto parameter.

When manually configuring the interface speed to either 10 or 100 Mbps, the switch prompts you to also configure duplex mode on the interface.

**Note**

Catalyst 4506 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 reenables the interface during the reconfiguration.

Table 2-45 describes the system's performance for different combinations of the duplex and speed modes. The specified **duplex** command that is configured with the specified **speed** command produces the resulting system action.

Table 2-45 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

The following example shows how to set the interface speed to 100 Mbps on the Fast Ethernet interface 5/4:

```
Switch(config)# interface fastethernet 5/4
Switch(config-if)# speed 100
```

The following example shows how to allow Fast Ethernet interface 5/4 to autonegotiate the speed and duplex mode:

```
Switch(config)# interface fastethernet 5/4
Switch(config-if)# speed auto
```

**Note**

The **speed auto 10 100** command is similar to the **speed auto** command on a Fast Ethernet interface.

The following example shows how to limit the interface speed to 10 and 100 Mbps on the Gigabit Ethernet interface 1/1 in auto-negotiation mode:

```
Switch(config)# interface gigabitethernet 1/1
Switch(config-if)# speed auto 10 100
```

The following example shows how to limit the speed negotiation to 100 Mbps on the Gigabit Ethernet interface 1/1:

```
Switch(config)# interface gigabitethernet 1/1
Switch(config-if)# speed auto 100
```

Related Commands

Command	Description
duplex	Configures the duplex operation on an interface.
interface (refer to Cisco IOS documentation)	Configures an interface type and enter interface configuration mode.
show 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 is to be done 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 {high-level | bps bps [k | m | g] | pps pps [k | m | g]} | action {shutdown | trap}}
```

```
no storm-control {broadcast level | action {shutdown | trap}}
```

Syntax Description	
broadcast	Enables the broadcast storm control on the port.
level { <i>high-level</i> bps <i>bps</i> [k m g] pps <i>pps</i> [k m g]}	<p>Defines traffic suppression levels. You can configure the following:</p> <ul style="list-style-type: none"> • <i>high-level</i>—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 <i>level</i> is reached. • bps <i>bps</i>—Specifies the threshold level for broadcast traffic, in bits per second (bps) (up to one decimal place). The port blocks only the traffic that exceeds this level. The range is 0.0 to 10000000000.0. • pps <i>pps</i>—Specifies the threshold level for broadcast traffic, in packets per second (pps) (up to one decimal place). The port blocks all traffic when traffic utilization exceeds this level. The range is 0.0 to 10000000000.0. • (Optional) [k m g]—Specifies the metric suffixes for large number thresholds, in bps and pps settings.
action	Directs the switch to take action when a storm occurs in a port.
shutdown	Disables the port during a storm.
trap	<p>Sends an Simple Network Management Protocol (SNMP) trap when a storm occurs.</p> <p>In Cisco IOS Release 12.1(19)EW, this keyword is available but not supported..</p>

Command Default Broadcast storm control is disabled.

Command Modes Interface configuration (config-if)

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

12.2(40)SG	This command was introduced on Supervisor Engine 6-E and Catalyst 4900M.
3.8.0E and 15.2.(4)E	This command was modified. The the bps <i>bps</i> and pps <i>pps</i> keywords were added.

Usage Guidelines

Enter the **storm-control broadcast level** command to enable traffic storm control on the interface, configure the traffic storm control level, and apply the traffic storm control level to the broadcast traffic on the interface.

The 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 ignored for the interfaces that perform storm control in the hardware.

Examples

The following example shows how to enable broadcast storm control in a port with a 75.67 percent rising suppression level:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet 2/1
Switch(config-if)# storm-control broadcast level 75.67
Switch(config-if)# end
```

The following example shows how to disable a port during a storm:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet 2/1
Switch(config-if)# storm-control action shutdown
Switch(config-if)# end
```

The following 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 gigabitethernet 2/1
Switch(config-if)# no storm-control broadcast level
Switch(config-if)# end
```

The following 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 gigabitethernet 2/1
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.

Command Default

Multicast storm control is disabled.

Command Modes

Global configuration mode (config)

Interface configuration mode on Catalyst 4900M, Catalyst 4948E, Catalyst 4948E-F, Supervisor Engines 6-E, 6L-E, 7-E, 7L-E, and 8-E.

Command History

Release	Modification
12.2(18)EW	This command was introduced on the Catalyst 4500 series switch.
12.2(40)SG	This command was introduced on the Catalyst 4900M and Supervisor Engine 6-E.
3.8.0E and 15.2.(4)E	This command was modified. The the bps <i>bps</i> and pps <i>pps</i> keywords were added.

Usage Guidelines

This command prompts the hardware to filter multicast packets if it is already filtering broadcast packets.

When you specify threshold levels for traffic as a percentage of the bandwidth or in bps, the traffic that is suppressed is a combined rate of multicast and broadcast traffic that exceeds the threshold (if the action is filtering).

When you specify threshold levels for traffic in pps, the rate at which traffic is suppressed is considered separately for broadcast and multicast traffic, and the storm action (if the action is filtering) is taken separately.

The switch 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

The following example shows how to enable multicast storm control globally:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# storm-control broadcast include multicast
Switch(config)# end
```

The following 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 fastethernet2/4  
Switch(config-if)# storm-control broadcast include multicast  
Switch(config)# end
```

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.

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.

Command Default This command has no default settings.

Command Modes cfg-call-home-profile

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

Usage Guidelines To enter profile call-home configuration submode, use the **profile** command in call-home configuration mode.

Examples The following example shows how to subscribe to all available alert groups:

```
Switch(config)# call-home
Switch(cfg-call-home)# profile cisco
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 <i>hh:mm</i>	Sets a daily alert in hours and minutes.	
monthly <i>date hh:mm</i>	Sets a monthly alert in day, hour, and minute.	
weekly <i>day hh:mm</i>	Sets a weekly alert in day, hour, and minutes.	

Command Default This command has no default settings.

Command Modes cfg-call-home-profile

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

Usage Guidelines To enter 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 The following 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).

Command Default normal

Command Modes cfg-call-home-profile

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

Usage Guidelines To enter profile call-home configuration submode, use the **profile** command in call-home configuration mode.

Examples The following example shows how to configure the "diagnostic" alert-group with "normal" severity:

```
Switch(config)# call-home
Switch(cfg-call-home)# profile cisco
Switch(cfg-call-home-profile)# subscribe-to-alert-group diagnostic severity normal
```

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

subscribe-to-alert-group environment

To subscribe a destination profile to the Environment alert group, use the **subscribe-to-alert-group environment** command.

subscribe-to-alert-group environment [**severity catastrophic** | **disaster** | **fatal** | **critical** | **major** | **minor** | **warning** | **notification** | **normal** | **debugging**]

Syntax Description	
severity catastrophic	(Optional) Specifies network wide catastrophic failure (highest severity).
disaster	(Optional) Specifies significant network impact.
fatal	(Optional) Specifies that the system is unusable (system log level 0).
critical	(Optional) Specifies that immediate attention is needed (system log level 1).
major	(Optional) Specifies a major condition (System log level 2).
minor	(Optional) Specifies a minor condition (System log level 3).
warning	(Optional) Specifies a warning condition (System log level 4).
notification	(Optional) Specifies an informational message (System log level 5).
normal	(Optional) Specifies returning to a normal state (System log level 6).
debugging	(Optional) Specifies a debugging message (Lowest severity).

Command Default normal

Command Modes cfg-call-home-profile

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

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 The following 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	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 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 <i>hh:mm</i>	Sets a daily alert in hours and minutes.
monthly <i>date hh:mm</i>	Sets a monthly alert in day, hour, and minute.
weekly <i>day hh:mm</i>	Sets a weekly alert in day, hour, and minutes.

Command Default This command has no default settings.

Command Modes cfg-call-home-profile

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

Usage Guidelines To enter profile call-home configuration submode, use the **profile** command in call-home configuration mode.

The Inventory alert group can be configured for periodic notification.

Examples The following 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

Command	Description
subscribe-to-alert-group all	Subscribes to all available alert groups.
subscribe-to-alert-group configuration	Subscribes this destination profile to the Configuration alert group.
subscribe-to-alert-group 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 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).

Command Default normal

Command Modes cfg-call-home-profile

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

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 The following example shows how to configure the syslog alert group with severity notification:

```
Switch(config)# call-home
Switch(cfg-call-home)# profile cisco
Switch(cfg-call-home-profile)# subscribe-to-alert-group syslog severity notification
pattern "UPDOWN"
```

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

switch (virtual switch)

To assign a switch number, use the **switch** command in virtual switch domain configuration submode.

```
switch num [preempt delay | priority priority-value]
```

Syntax Description	
<i>num</i>	Specifies the switch number; valid values are 1 or 2.
preempt <i>delay</i>	(Optional) Enables preemption and specifies a delay in minutes before the standby chassis takes over as the active chassis. Range: 5 (default) to 20
priority <i>priority-value</i>	(Optional) Specifies a priority number to determine the standby chassis that will become the new active chassis if the active chassis fails. Range: 1 (lowest priority) to 255 (highest priority)

Command Default *priority-value* settings for Switch 1 and Switch 2 are 100.

Command Modes Virtual switch domain configuration submode (config-vs-domain)

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

Usage Guidelines

You must set the virtual domain name and the switch number prior to converting the chassis into a virtual switch. You cannot configure the switch number after the chassis is in virtual switch mode.

When you boot the virtual switch, the role resolution logic validates that the chassis numbers in the two chassis differ.

When you configure **preempt**, the switch with the highest priority assumes the active role during role negotiation.

Examples The following example shows how to assign a switch number and to configure the virtual switch domain:

```
Router1(config)# switch virtual domain 100
Router1(config-vs-domain)# switch 1 priority 20
Router1(config-vs-domain)# switch 1 preempt 12
Router1(config-vs-domain)#
```

Related Commands	Command	Description
	switch virtual domain (virtual switch)	Configures the virtual switch domain number and enter the virtual switch domain configuration submode.

switch convert mode (virtual switch)

To select the switch mode, use the **switch convert mode** command in privileged EXEC mode.

```
switch convert mode {easy-virtual-switch | stand-alone | virtual}
```

Syntax Description	easy-virtual-switch	stand-alone	virtual
	Specifies execution on the standalone switch, which will be made the master, and switches to easy-vss mode.	Specifies standalone mode.	Specifies virtual switch mode.

Command Default stand-alone

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.2(52)SG	This command was introduced on the Catalyst 4500 series switch.
	Cisco IOS XE 3.6.0E and 15.2(2)E	easy-virtual-switch keyword introduced.

Usage Guidelines

You must reboot both switches when you convert a switch to virtual switch mode.

You execute the **switch convert mode easy-virtual-switch** command on the Catalyst 4500 switch intended as the “master” after the switch boots and comes up as VSS. In the easy-vss sub-exec mode, you specify the local interfaces [of the switch where the command is executed] that you want to select as a VSL interface.

In a VSS, the interface naming convention includes the switch number. For example, you must use switch/module/port to specify a port on a switching module. The **switch convert mode virtual** command converts the configuration file to use the VSS naming convention, and saves a backup copy of the file in the RP bootflash.



Note

After you confirm the command (with **yes** at the prompt), the switch converts the configuration file and restarts both chassis. Subsequently, the chassis is in virtual switch mode and you must specify interfaces with three identifiers (switch/module/port).

A **no** form of this command does not exist. You must specify either stand-alone or virtual mode.

You can enter the **switch convert mode virtual** command only after the standby switch is fully operational (in hot standby mode). If you enter the command before the standby switch is fully operational, a message is displayed telling you to try again later.

**Note**

If you have configured your config-register with a value that would skip file parsing during the bootup process, your change to either a standalone or virtual switch will not take place until you reconfigure your config-register. The config-register must be allowed to parse files to ensure a conversion from either a standalone or virtual switch.

Examples

The following example shows how to convert a switch to the “master” after the switch boots and comes up as VSS. In the easy-vss sub-exec mode, you specify the local interfaces GigabitEthernet3/5 [of the switch where the command is executed] that you want to select as a VSL interface:

```
Switch# switch convert mode easy-virtual-switch
Switch(easy-vss)#VSL ?
Local Interface          Remote Interface        Hostname  Standby-IP
GigabitEthernet3/5      TenGigabitEthernet1/1  4K-DEMO  2.2.2.4
GigabitEthernet3/6      TenGigabitEthernet1/2  4K-DEMO  2.2.2.4
Switch(easy-vss)#VSL GigabitEthernet3/5
```

The following example shows how to configure a device in the distribution layer as a standalone switch that has a switch number of 1:

```
Router1# switch convert mode virtual
This command will convert all interface names to naming convention "interface-type
chassis-number/slot/port", save the running config to startup-config and reload the
switch.
Do you want proceed? [yes/no]: yes
Converting interface names
Building Configuration...
[OK]
Saving converted configuration to bootflash: ...
Destination filename [startup-config.converted_vs-20070723-235834]?
```

switch virtual domain (virtual switch)

To configure the virtual switch domain number and enter the virtual switch domain configuration submode, use the **switch virtual domain** command in global configuration mode.

switch virtual domain *number*

Syntax Description	<i>number</i>	Specifies the virtual switch domain number. Range: 1 to 255.
---------------------------	---------------	--

Command Default	No virtual switch domain number is configured.	
------------------------	--	--

Command Modes	Global configuration (config)	
----------------------	-------------------------------	--

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

Usage Guidelines When you enter the **switch virtual domain** command, you enter the virtual switch domain configuration submode, and the prompt changes to Router1(config-vs-domain)#. Within the virtual switch domain configuration submode, the following commands are available:

- **default**—Sets a command to its defaults.
- **exit**—Exits the virtual-switch-domain-mode and returns to the global configuration mode.
- **no**—Negates a command or set its defaults.
- **switch num**—Assigns the switch number. See the switch (virtual switch) command for additional information.

You must configure the same virtual switch domain number on both chassis of the virtual switch. The virtual switch domain is a number between 1 and 255, and must be unique for each virtual switch in your network.



Note The domain identification takes effect only after you enter the **switch convert mode virtual** command.



Note The switch number is not stored in the startup or running configuration, because both chassis use the same configuration file (but must not have the same switch number).

Examples The following example shows how to configure the virtual switch number and virtual switch domain on two switches:

```
Router1(config)# switch virtual domain 100
Router1(config-vs-domain)# switch 1
Router1(config-vs-domain)# exit
```

```
Router2(config)# switch virtual domain 100  
Router2(config-vs-domain)# switch 2  
Router2(config-vs-domain)# exit
```

Related Commands

Command	Description
switch (virtual switch)	Assigns a switch number and enters virtual switch domain configuration submode.

switch virtual link (virtual switch)

To associate a switch to an interface, use the **switch virtual link** command in interface configuration mode.

switch virtual link *switch-number*

Syntax Description

<i>switch-number</i>	Switch number; valid values are 1 and 2.
----------------------	--

Command Default

The interfaces are not associated by default.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

The virtual switch link (VSL) is configured with a unique port channel on each chassis. You must add the VSL physical ports to the port channel. The VSL channel group must contain a minimum of two ports.

Examples

The following example shows how to associate switch 2 to a port channel:

```
Router-2(config)# interface port-channel 20
Router-2(config-if)# switch virtual link 2
Router-2(config-if)#
```

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 | name vlan_name}] | [nonegotiate] | [voice vlan {vlan-id | dot1p | name vlan_name | none | untagged}]
```

```
no switchport [access vlan | nonegotiate | voice vlan]
```

Syntax Description

access vlan <i>vlan_num</i>	(Optional) Sets the VLAN when the interface is in access mode; valid values are from 1 to 1005 or a VLAN name.
nonegotiate	(Optional) Specifies that the DISL/DTP negotiation packets will not be sent on the interface.
voice vlan <i>vlan-id</i>	(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.
name <i>vlan_name</i>	(Optional) Specifies the VLAN name. You can enter up to 128 characters.

Command Default

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(8a)EW	This command was introduced on the Catalyst 4500 series switch.
12.1(11)EW	Support for voice VLAN was added.
IOS XE 3.8.0E and IOS 15.2(4)E	Option to specify a VLAN name for access and voice VLAN.

Usage Guidelines

The **no switchport** command shuts the port down and then reenables it, which may generate messages on the device to which the port is connected.

The **no** form of the **switchport access** command resets the access mode VLAN to the appropriate default VLAN for the device. The **no** form of the **switchport nonegotiate** command removes the **nonegotiate** status.

When you are using the **nonegotiate** keyword, DISL/DTP negotiation packets will not be sent on the interface. The device will trunk or not trunk according to the **mode** parameter given: **access** or **trunk**. This command will return an error if you attempt to execute it in **dynamic (auto or desirable)** mode.

The voice VLAN is automatically set to VLAN 1 unless you use one of the optional keywords.

If you use the **switchport 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.

Before you configure the **switchport voice vlan name** command, note the following:

- The VLAN ID and VLAN name association should be configured and present in the VLAN database (See example below).
- Different switches can have a different ID for the same name. The VLAN name is internally converted to the VLAN ID.

Examples

The following 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)#
```

The following 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)#
```

The following 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)#
```

The following example shows how to set the voice VLAN for the interface to VLAN 2:

```
Switch(config-if)# switchport voice vlan 2
Switch(config-if)#
```

The following example shows how to set the voice VLAN for the interface to VLAN test.

```
Switch# configure terminal
Switch(config-vlan)# vlan 55
Switch(config-vlan)# name test
Switch(config-vlan)# end

Switch# configure terminal
Switch(config)# interface GigabitEthernet5/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport voice vlan name test
Switch(config-if)# end
```

```
Switch# show running-config interface GigabitEthernet5/1
Building configuration...
Current configuration : 113 bytes
!
interface GigabitEthernet5/1
switchport voice vlan 55
Switch#
```

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 **no** form of this command.

switchport access [**vlan** {*vlan-id* | **dynamic** | **name** *vlan_name*}]

no switchport access vlan

Syntax Description

<i>vlan-id</i>	(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.
name <i>vlan_name</i>	(Optional) Name of the VLAN on the interface, in access mode. You can enter up to 128 characters.

Command Default

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(12c)EW	This command was introduced on the Catalyst 4500 series switch.
12.1(13)EW	Support for VPMS was added.
IOS XE 3.8.0E and IOS 15.2(4)E	Option to specify an access VLAN name. The name keyword 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 already entered the **switchport** command for the interface.

Entering the **no switchport** command shuts the port down and then reenables it, which could generate messages on the device to which the port is connected.

The **no** form of the **switchport access vlan** command resets the access mode VLAN to the appropriate default VLAN for the device.

Before you configure the **switchport access vlan name** command, note the following:

- The VLAN ID and VLAN name association should be configured and present in the VLAN database (See example below).
- Different switches can have a different ID for the same name. The VLAN name is internally converted to the VLAN ID.

Examples

The following 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.

The following 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)#
```

The following example shows how to first populate the VLAN database by associating a VLAN ID with a VLAN name, and then setting the VLAN (using the name) on an interface, in the access mode:

Part 1—Making the entry in the VLAN database:

```
Switch# configure terminal
Switch(config)# vlan 33
Switch(config-vlan)# name test
Switch(config-vlan)# end
```

Part 2—Checking the VLAN database

```
Switch# show vlan id 33
```

VLAN Name	Status	Ports
33 test	active	Po21

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
33	enet	100033	1500	-	-	-	-	-	0	0


```
Remote SPAN VLAN
-----
Disabled
```

Primary	Secondary	Type	Ports
-----	-----	-----	-----

Part 3—Setting the VLAN on the interface, by using the name test.

```
Switch# configure terminal
Switch(config)# interface GigabitEthernet5/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan name test
Switch(config-if)# end
```



```
Switch# show running-config interface GigabitEthernet5/1
Building configuration...
Current configuration : 113 bytes
!
interface GigabitEthernet5/1
 switchport access vlan 33
 switchport mode access
Switch#
```



```
Switch# show interface GigabitEthernet5/1 switchport
Name: Gi5/1
Switchport: Enabled
```

```

Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 33 (test)
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: none
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: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
Switch#

```

Related Commands

Command	Description
show 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.

Command Default All ports are included in the VLAN interface link-up calculation.

Command Modes Interface configuration mode

Command History	Release	Modification
	12.2(37)SG	This command was introduced on the Catalyst 4500 series switch.

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 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 The following example shows how to exclude a port from the VLAN interface link-up calculation:

```
Switch(config-if)# switchport autostate exclude
Switch(config-if)#
```

The following example shows how to include a port in the VLAN interface link-up calculation:

```
Switch(config-if)# no switchport autostate exclude
Switch(config-if)#
```

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

Related Commands	Command	Description
	show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.

switchport block

To prevent the unknown multicast or unicast packets from being forwarded, use the **switchport block** interface configuration command. To allow the unknown multicast or unicast packets to be forwarded, use the **no** form of this command.

```
switchport block {multicast | unicast}
```

```
no switchport block {multicast | unicast}
```

Syntax Description

multicast	Specifies that the unknown multicast traffic should be blocked.
unicast	Specifies that the unknown unicast traffic should be blocked.

Command Default

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(19)EW	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

The following 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 ports with a valid PVLAN trunk association become active host private VLAN trunk ports.
private-vlan promiscuous	Specifies that the ports with a valid PVLAN mapping become active promiscuous ports.
private-vlan trunk promiscuous	Specifies that the ports with valid PVLAN trunk mapping become active promiscuous trunk ports.
private-vlan trunk secondary	Specifies that the ports with a valid PVLAN trunk association become active host private VLAN trunk ports.

Command Default

Link converts to a trunk link.
dot1q tunnel ports are disabled.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(8a)EW	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** or **desirable** mode.

If you enter **dynamic desirable** mode, the interface becomes a trunk interface if the neighboring interface is set to **trunk**, **desirable**, or **auto** mode.

If you specify the **dot1q-tunnel** keyword, the port is set unconditionally as an 802.1Q tunnel port. The port becomes inactive if you configure it as a private VLAN trunk port and one of the following applies:

- The port does not have a valid PVLAN association.
- The port does not have valid allowed normal VLANs.

If a private port PVLAN association or mapping is deleted, or if a private port is configured as a SPAN destination, it becomes inactive.

Examples

The following example shows how to set the interface to dynamic desirable mode:

```
Switch(config-if) # switchport mode dynamic desirable
Switch(config-if) #
```

The following example shows how to set a port to PVLAN host mode:

```
Switch(config-if) # switchport mode private-vlan host
Switch(config-if) #
```

The following example shows how to set a port to private VLAN trunk:

```
Switch(config-if) # switchport mode private-vlan trunk
Switch(config-if) #
```

The following example shows how to configure a port for an 802.1Q tunnel port:

```
Switch(config-if) # switchport mode dot1q-tunnel
Switch(config-if) #
```

The following example shows how to configure a promiscuous trunk port:

```
Switch(config-if) # switchport mode private-vlan trunk promiscuous
Switch(config-if) #
```

The following example shows how to configure an isolated trunk port:

```
Switch(config-if) # switchport mode private-vlan trunk
OR
Switch(config-if) # switchport mode private-vlan trunk secondary
Switch(config-if) #
```

You can verify your settings by entering the **show interfaces switchport** command and examining information in the Administrative Mode and Operational Mode rows.

The following 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 Promiscuous 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

```

The following example shows how to configure interface FastEthernet 5/1 as a PVLAN host port and verify the configuration:

```

Switch# configure terminal
Switch(config)# interface fastethernet 5/1
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 202 440
Switch(config-if)# end

Switch# show interfaces fastethernet 5/1 switchport
Name: Fa5/1
Switchport: Enabled
Administrative Mode: private-vlan host
Operational Mode: private-vlan host
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Appliance trust: none
Administrative Private Vlan
    Host 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

```

The following example shows how to configure interface FastEthernet 5/2 as a secondary trunk port, and verify the configuration:

```

Switch# configure terminal
Switch(config)# interface fastethernet 5/2
Switch(config-if)# switchport mode private-vlan trunk secondary
Switch(config-if)# switchport private-vlan trunk native vlan 10

```



```

Switch(config-if)# switchport private-vlan trunk allowed vlan 10, 3-4
Switch(config-if)# switchport private-vlan association trunk 3 301
Switch(config-if)# end
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 A
  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 (VLAN0003) 301 (VLAN0301)
  Administrative private-vlan trunk mappings: none
  Operational private-vlan: none
  Operational Normal VLANs: none
  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-if)#

```

The following example shows how to configure interface FastEthernet 5/2 as a promiscuous trunk port and to verify the configuration:

```

Switch# configure terminal
Switch(config)# interface fastethernet 5/2
Switch(config-if)# switchport mode private-vlan trunk promiscuous
Switch(config-if)# switchport private-vlan trunk native vlan 10
Switch(config-if)# switchport private-vlan trunk allowed vlan 10, 3-4
Switch(config-if)# switchport private-vlan mapping trunk 3 301, 302
Switch(config-if)# end
Switch# show interfaces fastethernet 5/2 switchport
Name: Fa5/2
  Switchport: Enabled
  Administrative Mode: private-vlan trunk promiscuous
  Operational Mode: private-vlan trunk promiscuous
  Administrative Trunking Encapsulation: negotiate
  Operational Trunking Encapsulation: dot1q
  Negotiation of Trunking: On
  Access Mode VLAN: 1 (default)
  Trunking Native Mode VLAN: 1 (default)
  Administrative Native VLAN tagging: enabled
  Voice VLAN: none
  Administrative private-vlan host-association: none
  Administrative private-vlan mapping: none
  Administrative private-vlan trunk native VLAN: 10
  Administrative private-vlan trunk Native VLAN tagging: enabled
  Administrative private-vlan trunk encapsulation: dot1q

```

```

Administrative private-vlan trunk normal VLANs: 3-4,10
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings:
    3 (VLAN0003) 301 (VLAN0301) 302 (VLAN0302)
Operational private-vlan:
    3 (VLAN0003) 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-if)#

```

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.
switchport	Enables port security on an interface.
switchport private-vlan host-association	Defines a PVLAN association for an isolated or community port.
switchport private-vlan mapping	Defines private VLAN mapping for a promiscuous port.

switchport port-security

To enable port security on an interface, use the **switchport port-security** command. To disable port security and set parameters to their default states, use the **no** form of this command.

```
switchport port-security [aging {static | time time | type {absolute | inactivity}} |
  limit rate invalid-source-mac [N | none] | mac-address mac-address [vlan {access | voice} |
  mac-address sticky [mac-address] [vlan access | voice] | maximum value [vlan {access |
  voice} | violation {restrict | shutdown | shutdown vlan}]
```

```
no switchport port-security [aging {static | time time | type {absolute | inactivity}} |
  limit rate invalid-source-mac [N | none] | mac-address mac-address [vlan {access | voice} |
  mac-address sticky [mac-address] [vlan access | voice] | maximum value [vlan {access |
  voice} | violation {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 <i>time</i>	(Optional) Specifies the aging time for this port. The valid values are from 0 to 1440 minutes. If the time is 0, aging is disabled for this port.
type absolute	(Optional) Sets the aging type as absolute aging. All the secure addresses on this port age out exactly after the time (minutes) specified and are removed from the secure address list.
type inactivity	(Optional) Sets the aging type as inactivity aging. The secure addresses on this port age out only if there is no data traffic from the secure source address for the specified time period.
limit rate invalid-source-mac	(Optional) Sets the rate limit for bad packets. This rate limit also applies to the port where DHCP snooping security mode is enabled as filtering the IP and MAC address.
N none	(Optional) Supplies a rate limit (N) or indicates none (none).
mac-address <i>mac-address</i>	(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 that is configured.
sticky	(Optional) Configures the dynamic addresses as sticky on the interface.
vlan access	(Optional) Deletes the secure MAC addresses from access VLANs.
vlan voice	(Optional) Deletes the secure MAC addresses from voice VLANs.
maximum <i>value</i>	(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 action to be taken if port security is violated.
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.

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.

Command Default

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	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 Fast EtherChannel or Gigabit EtherChannel port group.

When a secure port is in the error-disabled state, you can remove it from this state by entering the **errdisable recovery cause psecure-violation** global configuration command, or you can manually re-enable it by entering the **shutdown** and **no shut down** interface configuration commands. If a port is 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 than 0 for that port.

To allow limited time access to particular secure addresses, set the aging type as **absolute**. When the aging time lapses, the secure addresses are deleted.

To allow continuous access to a limited number of secure addresses, set the aging type as **inactivity**. This action removes the secure address when it becomes inactive, and other addresses can become secure.

To allow unlimited access to a secure address, configure it as a secure address, and disable aging for the statically configured secure address by using the **no switchport port-security aging static** interface configuration command.

If the sticky command is executed without a MAC address specified, all MAC addresses that are learned on that port will be made sticky. You can also specify a specific MAC address to be a sticky address by entering the **sticky** keyword 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

The following 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 0/12
Switch(config-if)# switchport port-security aging time 120
Switch(config-if)#
```

The following 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 0/12
Switch(config-if)# switch port-security aging type inactivity
Switch(config-if)#
```

The following example shows how to configure rate limit for invalid source packets on Fast Ethernet port 12:

```
Switch(config)# interface fastethernet 0/12
Switch(config-if)# switchport port-security limit rate invalid-source-mac 100
Switch(config-if)#
```

The following example shows how to configure rate limit for invalid source packets on Fast Ethernet port 12:

```
Switch(config)# interface fastethernet 0/12
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.

The following 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)
```

The following example shows how to configure a secure MAC address on Fast Ethernet port 12:

```
Switch(config)# interface fastethernet 0/12
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)
```

The following 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)
```

The following 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)
```

The following 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.

The following example shows how to configure sticky MAC addresses 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 port-security
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.obob vlan voice
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.0005 vlan access
Switch(config-if)# end
```

The following 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# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 5/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# switchport port-security maximum 1 vlan voice
Switch(config-if)# switchport port-security maximum 1 vlan access
Switch(config-if)# end
```

The following 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 ports causes the system to configure the port with sticky secure addresses.

You can verify your settings by using the **show port-security address** privileged EXEC command.

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.
show port-security	Displays the port security settings for an interface or for the switch.
switchport block	Prevents the unknown multicast or unicast packets from being forwarded.

switchport private-vlan association trunk

To configure the association between a secondary VLAN and a VLAN on a private VLAN trunk port, use the **switchport private-vlan association trunk** command. To remove the private VLAN mapping from the port, use the **no** form of this command.

```
switchport private-vlan association trunk {primary-vlan-id} {secondary-vlan-id}
```

```
no switchport private-vlan association trunk {primary-vlan-id}
```

Syntax Description

primary-vlan-id Number of the primary VLAN of the private VLAN relationship.

secondary-vlan-id Number of the secondary VLAN of the private VLAN relationship.

Command Default

Private VLAN mapping is disabled.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(12c)EW	This command was introduced on the Catalyst 4500 series switch.
12.2(20)EW	Support for community VLAN 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

The following 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)#
```

The following 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)#
```


The following example shows how to configure interface FastEthernet 5/2 as a secondary trunk port, and verify the configuration:

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/2
Switch(config-if)# switchport mode private-vlan trunk secondary
Switch(config-if)# switchport private-vlan trunk native vlan 10
Switch(config-if)# switchport private-vlan trunk allowed vlan 10. 3-4
Switch(config-if)# switchport private-vlan association trunk 3 301
Switch(config-if)# end
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 A
  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 (VLAN0003) 301 (VLAN0301)
  Administrative private-vlan trunk mappings: none
  Operational private-vlan: none
  Operational Normal VLANs: none
  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-if)#
```

Related Commands	Command	Description
	show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.
	switchport mode	Enables the interface type.

switchport private-vlan host-association

To define a PVLAN association for an isolated or community port, use the **switchport private-vlan host-association** command. To remove the PVLAN mapping from the port, use the **no** form of this command.

```
switchport private-vlan host-association {primary-vlan-id} {secondary-vlan-id}
```

```
no switchport private-vlan host-association
```

Syntax Description		
	<i>primary-vlan-id</i>	Number of the primary VLAN of the PVLAN relationship; valid values are from 1 to 4094.
	<i>secondary-vlan-list</i>	Number of the secondary VLAN of the private VLAN relationship; valid values are from 1 to 4094.

Command Default Private VLAN mapping is disabled.

Command Modes Interface configuration mode

Command History	Release	Modification
	12.1(8a)EW	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 The following 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)#
```

The following example shows how to remove the PVLAN association from the port:

```
Switch(config-if)# no switchport private-vlan host-association
Switch(config-if)#
```

The following example shows how to configure interface FastEthernet 5/1 as a PVLAN host port and verify the configuration:

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/1
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 202 440
```

```

Switch(config-if)# end
Switch# show interfaces fastethernet 5/1 switchport
Name: Fa5/1
Switchport: Enabled
Administrative Mode: private-vlan host
Operational Mode: private-vlan host
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Appliance trust: none
Administrative Private Vlan
  Host 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 **no** form of this command.

```
switchport private-vlan mapping {primary-vlan-id} {secondary-vlan-list} |
  {add secondary-vlan-list} | {remove secondary-vlan-list}
```

```
switchport private-vlan mapping trunk {primary-vlan-id} [add | remove] secondary-vlan-list
```

```
no switchport private-vlan mapping [trunk]
```

Syntax Description

<i>primary-vlan-id</i>	Number of the primary VLAN of the private VLAN relationship; valid values are from 2 to 4094 (excluding 1002 to 1005).
<i>secondary-vlan-list</i>	Number of the secondary VLANs to map to the primary VLAN; valid values are from 2 to 4094.
add	Maps the secondary VLANs to the primary VLAN.
remove	Clears mapping between the secondary VLANs and the primary VLAN.
trunk	Maps the trunks secondary VLANs to the primary VLAN.

Command Default

Private VLAN mapping is disabled.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch.
12.1(12c)EW	Support for extended addressing was added.
12.2(20)EW	Support for community VLAN was added.
12.2(31)SG	Support for trunk VLAN was added.

Usage Guidelines

There is no run-time effect on the port unless it is in private VLAN promiscuous mode. If the port is in private VLAN promiscuous mode but the VLANs do not exist, the command is allowed, but the port is made inactive.

The secondary VLAN may be an isolated or community VLAN.



Note

The maximum number of unique private VLAN pairs supported by the **switchport private-vlan mapping trunk** command above is 500. For example, one thousand secondary VLANs could map to one primary VLAN, or one thousand secondary VLANs could map one to one to one thousand primary VLANs.

Examples

The following example shows how to configure the mapping of primary VLAN 18 to the secondary isolated VLAN 20 on a port:

```
Switch(config-if) # switchport private-vlan mapping 18 20
Switch(config-if) #
```

The following example shows how to add a VLAN to the mapping:

```
Switch(config-if) # switchport private-vlan mapping 18 add 21
Switch(config-if) #
```

The following example shows how to add a range of secondary VLANs to the mapping:

```
Switch(config-if) # switchport private-vlan mapping 18 add 22-24
Switch(config-if) #
```

The following example shows how to add a range of secondary VLANs to the trunk mapping:

```
Switch(config-if) # switchport private-vlan mapping trunk 18 add 22-24
Switch(config-if) #
```

The following 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 Promiscuous 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
```

The following example shows how to configure interface FastEthernet 5/2 as a promiscuous trunk port and to verify the configuration:

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/2
Switch(config-if)# switchport mode private-vlan trunk promiscuous
Switch(config-if)# switchport private-vlan trunk native vlan 10
Switch(config-if)# switchport private-vlan trunk allowed vlan 10, 3-4
Switch(config-if)# switchport private-vlan mapping trunk 3 301, 302
Switch(config-if)# end
Switch# show interfaces fastethernet 5/2 switchport
```

```

Name: Fa5/2
Switchport: Enabled
Administrative Mode: private-vlan trunk promiscuous
Operational Mode: private-vlan trunk promiscuous
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: 10
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: 3-4,10
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings:
    3 (VLAN0003) 301 (VLAN0301) 302 (VLAN0302)
Operational private-vlan:
    3 (VLAN0003) 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-if)#

```

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		
<i>vlan_list</i>		Sets the list of allowed VLANs; see the “Usage Guidelines” section for formatting guidelines for <i>vlan_list</i> .
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.
<i>vlan_atom</i>		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.

Command Default All allowed normal VLANs are removed from a private VLAN trunk port.

Command Modes Interface configuration mode

Command History	Release	Modification
	12.1(12c)EW	This command was introduced on the Catalyst 4500 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 association trunk** command to configure a port that can carry private VLANs on a private VLAN trunk port.

Examples

The following 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)#
```

The following 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)#
```

The following example shows how to configure interface FastEthernet 5/2 as a secondary trunk port, and verify the configuration:

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/2
Switch(config-if)# switchport mode private-vlan trunk secondary
Switch(config-if)# switchport private-vlan trunk native vlan 10
Switch(config-if)# switchport private-vlan trunk allowed vlan 10, 3-4
Switch(config-if)# switchport private-vlan association trunk 3 301
Switch(config-if)# end
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 A
  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 (VLAN0003) 301 (VLAN0301)
  Administrative private-vlan trunk mappings: none
  Operational private-vlan: none
  Operational Normal VLANs: none
  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-if)#
```

The following example shows how to configure interface FastEthernet 5/2 as a promiscuous trunk port and to verify the configuration:

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/2
Switch(config-if)# switchport mode private-vlan trunk promiscuous
Switch(config-if)# switchport private-vlan trunk native vlan 10
Switch(config-if)# switchport private-vlan trunk allowed vlan 10, 3-4
```



```

Switch(config-if)# switchport private-vlan mapping trunk 3 301, 302
Switch(config-if)# end
Switch# show interfaces fastethernet 5/2 switchport
Name: Fa5/2
Switchport: Enabled
Administrative Mode: private-vlan trunk promiscuous
Operational Mode: private-vlan trunk promiscuous
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: 10
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: 3-4,10
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings:
    3 (VLAN0003) 301 (VLAN0301) 302 (VLAN0302)
Operational private-vlan:
    3 (VLAN0003) 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-if)#

```

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.
switchport mode	Enables the interface type.

switchport 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.

Command Default 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	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 The following example shows how to enable 802.1Q native VLAN tagging on a PVLAN trunk:

```
Switch(config-if)# switchport private-vlan trunk native vlan tag
Switch(config-if)#
```

Related Commands	Command	Description
	show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.
	switchport mode	Enables the interface type.

switchport trunk

To set the trunk characteristics when an interface is in trunking mode, use the **switchport trunk** command. To reset all of the trunking characteristics back to the original defaults, use the **no** form of this command.

switchport trunk native vlan {tag | *vlan_id*}

no switchport trunk native vlan {tag | *vlan_id*}

switchport trunk allowed vlan *vlan_list*

no switchport trunk allowed vlan *vlan_list*

switchport trunk pruning vlan *vlan_list*

no switchport trunk pruning vlan *vlan_list*

Syntax Description		
native vlan <i>tag</i>		Specifies the tagging of native VLAN traffic on 802.1Q trunks.
native vlan <i>vlan_id</i>		Sets the native VLAN for the trunk in 802.1Q trunking mode.
allowed vlan <i>vlan_list</i>		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 <i>vlan_list</i> .
pruning vlan <i>vlan_list</i>		Sets the list of VLANs that are enabled for VTP pruning when the switch is in trunking mode. See the “Usage Guidelines” section for formatting guidelines for <i>vlan_list</i> .

Command Default

The default settings are as follows:

- IOS-XE only supports dot1Q.
- The access VLANs and trunk interface native VLANs are a default VLAN that corresponds to the platform or the interface hardware.
- All 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(8a)EW	This command was introduced on the Catalyst 4500 series switch..
12.1(12c)EW	Support for extended addressing was added.
12.2(18)EW	Support for native VLAN tagging was added.

Usage Guidelines

The *vlan_list* format is **all** | **none** | [**add** | **remove** | **except**] *vlan_atom* [, *vlan_atom*...], where:

- **all** specifies all VLANs from 1 to 4094. This keyword is not supported on commands that do not permit all VLANs in the list to be set at the same time.
- **none** indicates an empty list. This keyword is 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 **no** form of the **native vlan** command resets the native mode VLAN to the appropriate default VLAN for the device.

The **no** form of the **allowed vlan** command resets the list to the default list, which allows all VLANs.

The **no** 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 BPDUs on each VLAN that is allowed on the trunks. The BPDUs on the native VLAN of the trunk are sent untagged to the reserved 802.1d spanning-tree multicast MAC address (01-80-C2-00-00-00). The BPDUs on all other VLANs on the trunk are sent tagged to the reserved SSTP 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 the CST.
- Because Cisco switches transmit BPDUs to the SSTP multicast MAC address on the VLANs other than the native VLAN of the trunk, non-Cisco switches do not recognize these frames as 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 a per-VLAN spanning-tree topology across a network of non-Cisco 802.1Q switches. The non-Cisco 802.1Q network separating the Cisco switches is treated as a single broadcast segment between all switches that are connected to the non-Cisco 802.1Q network through the 802.1Q trunks.
- Ensure that the native VLAN is the same on *all* of the 802.1Q trunks connecting the Cisco switches to the non-Cisco 802.1Q network.

- If you are connecting multiple Cisco switches to a non-Cisco 802.1Q network, all of the connections must be through the 802.1Q trunks. You cannot connect Cisco switches to a non-Cisco 802.1Q network through the 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.

Follow these guidelines for native VLAN tagging:

- The **no switchport trunk native vlan tag** command disables the native VLAN tagging operation on a port. This overrides the global tagging configuration.
- The **switchport trunk native vlan tag** command can be used to reenables tagging on a disabled port.
- The **no** option is saved to NVRAM so that the user does not have to manually select the ports to disable the tagging operation each time that the switch reboots.
- When the **switchport trunk native vlan tag** command is enabled and active, all packets on the native VLAN are tagged, and incoming untagged data packets are dropped. Untagged control packets are accepted.

Examples

The following example shows how to cause a port interface that is configured as a switched interface to encapsulate in 802.1Q trunking format regardless of its default trunking format in trunking mode:

```
Switch(config-if) # switchport trunk encapsulation dot1q
Switch(config-if) #
```

The following example shows how to enable 802.1Q tagging on a port:

```
Switch(config-if) # switchport trunk native vlan tag
Switch(config-if) #
```

The following example shows how to configure a secure MAC-address and a maximum limit of secure MAC addresses on Gigabit Ethernet port 1 for all VLANs:

```
Switch(config) # interface gigabitethernet1/1
Switch(config-if) # switchport trunk encapsulation dot1q
Switch(config-if) # switchport mode trunk
Switch(config-if) # switchport port-security
Switch(config-if) # switchport port-security maximum 3
```

The following 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 trunk encapsulation dot1q
Switch(config-if) # switchport mode trunk
Switch(config-if) # switchport port-security
Switch(config-if) # vlan-range 2-6
Switch(config-if-vlan-range) # port-security maximum 3
```

The following example shows how to configure a secure MAC-address in a VLAN on Gigabit Ethernet port 1:

```
Switch(config) # interface gigabitethernet1/1
Switch(config-if) # switchport trunk encapsulation dot1q
Switch(config-if) # switchport mode trunk
Switch(config-if) # switchport port-security
Switch(config-if) # switchport port-security mac-address sticky
Switch(config-if) # vlan-range 2-6
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.

switchport vlan mapping

To configure VLAN mapping on a trunk port, including one-to-one VLAN mapping, traditional IEEE 802.1Q tunneling (Q-in-Q) mapping, and selective Q-in-Q mapping, use the **switchport vlan mapping** interface configuration command. To disable configuration, use the **no** form of the command.

```
switchport vlan mapping original-vlan-id {translated-id | dot1q tunnel outer vlan-id} | default
{dot1q tunnel outer vlan-id | drop}
```

```
no switchport vlan mapping original-vlan-id {translated-id | dot1q tunnel outer vlan-id} |
default {dot1q tunnel outer vlan-id | drop}
```

```
no switchport vlan mapping all
```

Syntax Description

<i>original-vlan-id</i>	Specifies the original (customer) VLAN or C-VLANs IDs, also known as the VLAN on the wire, for one-to-one or selective Q-in-Q mapping. You can enter multiple VLAN IDs separated by a comma or a series of VLAN IDs separated by a hyphen (For example, 1,2,3-5). The VLAN ID range is from 1 to 4094.
<i>translated-id</i>	The translated VLAN-ID (S-VLAN ID) that is used in the service provider network. The range is from 1 to 4094.
dot1q-tunnel <i>outer vlan-id</i>	Adds a translated VLAN ID to specify a VLAN tunnel (add an outer S-VLAN tag). The range of the S-VLAN tag is 1 to 4094. Use this keyword for traditional Q-in-Q mapping.
default	Specifies default behavior for all the packets in the port.
drop	Specifies that all the packets in the port be dropped if they do not match the mapped VLAN IDs.
all	In the no switchport vlan mapping command, this keyword specifies that all VLAN mapping configurations on the interface are deleted.

Command Default

No VLAN mapping is configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
IOS 12.2(54)SG	This command was introduced on the Catalyst 4500 Series switch.
3.8.0E and 15.2.(4)E	The no switchport vlan mapping default drop command was added.

Usage Guidelines

Before configuring VLAN mapping on an interface, enter the **switchport mode trunk** interface configuration command to configure the interface as a trunk port.

You can configure VLAN mapping on a physical interface or on a port channel of multiple interfaces with the same configuration.

To configure one-to-one VLAN mapping, use the **switchport vlan mapping** *original-vlan-id translated-id* command.

**Note**

To avoid mixing customer traffic, when you configure traditional Q-in-Q on a trunk port, use the **switchport trunk allowed vlan** *vlan-id* interface configuration command to configure the outer VLAN ID (S-VLAN) as an allowed VLAN on the trunk port.

**Note**

You cannot configure one-to-one mapping and selective Q-in-Q on the same interface.

The **no** form of the **switchport vlan mapping** command clears the specified mapping configuration.

The **no switchport vlan mapping all** command clears all mapping configurations on the interface.

You cannot configure encapsulation replicate on a SPAN destination port if the source port is configured as a tunnel port or has a 1-to-2 mapping configured. Encapsulation replicate is supported with 1-to-1 VLAN mapping.

The **no switchport vlan mapping default drop** command ensures that packets that do not match, are not dropped. If this is not configured, by default, the packets that do not match are dropped.

Examples

The following example shows how to use one-to-one mapping to map VLAN IDs 1 and 2 in a customer network to VLANs 1001 and 1002 in the service provider network and drop traffic from other VLAN IDs:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport vlan mapping 1 1001
Switch(config-if)# switchport vlan mapping 2 1002
Switch(config-if)# exit
```

The following example shows how to configure selective Q-in-Q mapping on a port so that traffic with a C-VLAN ID of 5, 7, or 8 enters the switch with an S-VLAN ID of 100. The traffic of other VLAN IDs is dropped.

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport vlan mapping 5, 7-8 dot1q-tunnel 100
Switch(config-if)# exit
```

The following example shows how to configure selective Q-in-Q mapping on a port so that traffic with a C-VLAN ID of 1 to 5 enters the switch with an S-VLAN ID of 100. The traffic of other VLAN IDs is allowed.

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport vlan mapping 1-5 dot1q-tunnel 100
Switch(config-if)# no switchport vlan mapping default drop
Switch(config-if)# exit
```

Related Commands

Command	Description
show vlan mapping	Displays VLAN mapping information.

system mtu

To set the maximum Layer 2 or Layer 3 payload size, use the **system mtu** command. To revert to the default MTU setting, use the **no** form of this command.

system mtu *datagram-size*

no system mtu

Syntax Description	<i>datagram-size</i> Layer 2 payload size; valid values from 1500 to 1552 bytes.
---------------------------	--

Command Default	The default MTU setting is 1500 bytes.
------------------------	--

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

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

Usage Guidelines	<p>The <i>datagram-size</i> 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.</p> <p>For ports from 3 to 18 on model WS-X4418-GB and ports from 1 to 12 on model WS-X4412-2GB-TX, only the standard IEEE Ethernet payload size of 1500 bytes is supported.</p> <p>For other modules, an Ethernet payload size of up to 1552 bytes is supported with a total Ethernet frame size of up to 1600 bytes.</p>
-------------------------	--

Examples	The following 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#
```

The following 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.

template data timeout (netflow-lite exporter submode)



Note

NetFlow-lite is only supported on the Catalyst 4948E and Catalyst 4948E-F Ethernet switches.

To specify a template data timeout for the NetFlow-lite collector, use the **template data timeout** command. To delete the value, use the **no** form of this command.

template data timeout *seconds*

no dscp *dscp-value*

Syntax Description	<i>seconds</i>	Specifies a template data timeout value for the NetFlow-lite collector.
Command Default	1800 seconds	
Command Modes	netflow-lite exporter submode	
Command History	Release	Modification
	15.0(2)SG	This command was introduced on the Catalyst 4948E and Catalyst 4948E-F Ethernet switches.

Usage Guidelines

Default timeout value is 1800 seconds or 30 minutes. The timeout value configured really depends on the collector and how often it needs the templates to be refreshed.

Examples

The following example shows how to specify a template data timeout for the NetFlow-lite collector:

```
Switch# config terminal
Switch(config)# netflow-lite exporter exporter1
Switch(config-netflow-lite-exporter)# destination 5.5.5.6
Switch(config-netflow-lite-exporter)# source 5.5.5.5
Switch(config-netflow-lite-exporter)# transport udp 8188
Switch(config-netflow-lite-exporter)# ttl 128
Switch(config-netflow-lite-exporter)# cos 7
Switch(config-netflow-lite-exporter)# dscp 32
Switch(config-netflow-lite-exporter)# template data timeout 1
Switch(config-netflow-lite-exporter)# options sampler-table timeout 1
Switch(config-netflow-lite-exporter)# options interface-table timeout 1
Switch(config-netflow-lite-exporter)# export-protocol netflow-v9
Switch(config-netflow-lite-exporter)# exit
Switch(config)#
```

```

Display the exporter
Switch# show netflow-lite exporter exporter1
Netflow-lite Exporter exporter1:
  Network Protocol Configuration:
    Destination IP address: 5.5.5.6
    Source IP Address:    5.5.5.5
    VRF label:
    DSCP:                 0x20
    TTL:                  128
    COS:                  7
  Transport Protocol Configuration:
    Transport Protocol:   UDP
    Destination Port:     8188
    Source Port:          61670
  Export Protocol Configuration:
    Export Protocol:      netflow-v9
    Template data timeout: 60
    Options sampler-table timeout: 1800
    Options interface-table timeout: 1800
  Exporter Statistics:
    Packets Exported:    0

```

You can verify your settings with the **show netflow-lite exporter** privileged EXEC command.

Related Commands

Command	Description
options timeout (netflow-lite exporter submode)	Specifies an options timeout for the NetFlow-lite collector.
cos (netflow-lite exporter submode)	Specifies a cos value for the NetFlow-lite collector.
source (netflow-lite exporter submode)	Specifies a source Layer 3 interface of the NetFlow-lite collector.
transport udp (netflow-lite exporter submode)	Specifies a UDP transport destination port for a NetFlow-lite collector.
ttl (netflow-lite exporter submode)	Specifies a ttl value for the NetFlow-lite collector.
destination (netflow-lite exporter submode)	Specifies a destination address in netflow-lite submode.
template data timeout (netflow-lite exporter submode)	Specifies a template data timeout for the NetFlow-lite collector.
export-protocol (netflow-lite exporter submode)	Specifies the export protocol for the NetFlow-lite collector.
dscp (netflow-lite exporter submode)	Specifies a cos value for the NetFlow-lite collector.

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 <i>interface</i>	Interface type; valid values are fastethernet and gigabitethernet .
<i>interface-number</i>	Module and port number.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.2(25)SG	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

The following example shows how to start the TDR test on port 1 on module 2:

```
Switch# test cable-diagnostics tdr int gi2/1
Switch#
```

The following example shows the message that displays when the TDR test is not supported on a module:

```
Switch# test cable-diagnostics tdr int gi2/1
00:03:15:%C4K_IOSDIAGMAN-4-TESTNOTSUPPORTEDONMODULE: Online cable
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 a “TDR test is in progress on interface...” message.

Related Commands

Command	Description
show cable-diagnostics tdr	Displays the test results for the TDR cable diagnostics.

traceroute mac

To display the Layer 2 path taken by the packets from the specified source MAC address to the specified destination MAC address, use the **traceroute mac** command.

```
traceroute mac [interface interface-id] {source-mac-address} [interface interface-id]
  {destination-mac-address} [vlan vlan-id] [detail]
```

Syntax Description		
interface <i>interface-id</i>	(Optional)	Specifies the source or destination switch interface.
<i>source-mac-address</i>		MAC address of the source switch in hexadecimal format.
<i>destination-mac-address</i>		MAC address of the destination switch in hexadecimal format.
vlan <i>vlan-id</i>	(Optional)	Specifies the VLAN on which to trace the Layer 2 path that the packets take from the source switch to the destination switch; valid VLAN IDs are from 1 to 4094. Do not enter leading zeros.
detail	(Optional)	Displays detail information.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.1(15)EW	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines Do not use leading 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(15)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 function properly, Cisco Discovery Protocol (CDP) must be enabled on all of the switches in the network. Do not disable CDP.

When the switch detects a device in the Layer 2 path that does not support Layer 2 traceroute, the switch continues to send Layer 2 trace queries and lets them time out.

The maximum number of hops identified in the path is ten.

Layer 2 traceroute supports only unicast traffic. If you specify a multicast source or destination MAC address, the physical path is not identified, and a message appears.

The **tracertoe mac** command output shows the Layer 2 path when the specified source and destination addresses belong to the same VLAN. If you specify source and destination addresses that belong to different VLANs, the Layer 2 path is not identified, and a message appears.

If the source or destination MAC address belongs to multiple VLANs, you must specify the VLAN to which both the source and destination MAC addresses belong. If the VLAN is not specified, the path is not identified, and a message appears.

Layer 2 traceroute is not supported when multiple devices are attached to one port through hubs (for example, multiple CDP neighbors are detected on a port). When 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

The following example shows how to display the Layer 2 path by specifying the source and destination MAC addresses:

```
Switch# tracertoe mac 0000.0201.0601 0000.0201.0201

Source 0000.0201.0601 found on con6[WS-C2950G-24-EI] (2.2.6.6)
con6 (2.2.6.6) :Fa0/1 =>Fa0/3
con5          (2.2.5.5       ) : Fa0/3 =>Gi0/1
con1          (2.2.1.1       ) : Gi0/1 =>Gi0/2
con2          (2.2.2.2       ) : Gi0/2 =>Fa0/1
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed
Switch#
```

The following example shows how to display the detailed Layer 2 path:

```
Switch# tracertoe mac 0000.0201.0601 0000.0201.0201 detail
Source 0000.0201.0601 found on con6[WS-C2950G-24-EI] (2.2.6.6)
con6 / WS-C2950G-24-EI / 2.2.6.6 :
      Fa0/1 [auto, auto] =>Fa0/3 [auto, auto]
con5 / WS-C2950G-24-EI / 2.2.5.5 :
      Fa0/3 [auto, auto] =>Gi0/1 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
      Gi0/1 [auto, auto] =>Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
      Gi0/2 [auto, auto] =>Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
Switch#
```

The following example shows the Layer 2 path when the switch is not connected to the source switch:

```
Switch# tracertoe mac 0000.0201.0501 0000.0201.0201 detail
Source not directly connected, tracing source ....
Source 0000.0201.0501 found on con5[WS-C2950G-24-EI] (2.2.5.5)
con5 / WS-C2950G-24-EI / 2.2.5.5 :
      Fa0/1 [auto, auto] =>Gi0/1 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
      Gi0/1 [auto, auto] =>Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
      Gi0/2 [auto, auto] =>Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
Switch#
```


The following example shows the Layer 2 path when the switch cannot find the destination port for the source MAC address:

```
Switch# traceroute mac 0000.0011.1111 0000.0201.0201
Error:Source Mac address not found.
Layer2 trace aborted.
Switch#
```

The following example shows the Layer 2 path when the source and destination devices are in different VLANs:

```
Switch# traceroute mac 0000.0201.0601 0000.0301.0201
Error:Source and destination macs are on different vlans.
Layer2 trace aborted.
Switch#
```

The following example shows the Layer 2 path when the destination MAC address is a multicast address:

```
Switch# traceroute mac 0000.0201.0601 0100.0201.0201
Invalid destination mac address
Switch#
```

The following example shows the Layer 2 path when the source and destination switches belong to multiple VLANs:

```
Switch# traceroute mac 0000.0201.0601 0000.0201.0201
Error:Mac found on multiple vlans.
Layer2 trace aborted.
Switch#
```

The following example shows how to display the Layer 2 path by specifying the interfaces on the source and destination switches:

```
Switch# traceroute mac interface fastethernet0/1 0000.0201.0601 interface fastethernet0/3 0000.0201.0201
Source 0000.0201.0601 found on con6[WS-C2950G-24-EI] (2.2.6.6)
con6 (2.2.6.6) :Fa0/1 =>Fa0/3
con5 (2.2.5.5 ) : Fa0/3 =>Gi0/1
con1 (2.2.1.1 ) : Gi0/1 =>Gi0/2
con2 (2.2.2.2 ) : Gi0/2 =>Fa0/1
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed
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.

tracert 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 **tracert mac** command.

```
tracert mac ip {source-ip-address | source-hostname} {destination-ip-address | destination-hostname} [detail]
```

Syntax Description		
<i>source-ip-address</i>	IP address of the source switch as a 32-bit quantity in dotted-decimal format.	
<i>destination-ip-address</i>	IP address of the destination switch as a 32-bit quantity in dotted-decimal format.	
<i>source-hostname</i>	IP hostname of the source switch.	
<i>destination-hostname</i>	IP hostname of the destination switch.	
detail	(Optional) Displays detailed tracert MAC IP information.	

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

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

Usage Guidelines The Layer 2 tracert 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(15)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 tracert to function properly, Cisco Discovery Protocol (CDP) must be enabled on all the switches in the network. Do not disable CDP.

When the switch detects a device in the Layer 2 path that does not support Layer 2 tracert, the switch continues to send Layer 2 trace queries and lets them time out.

The maximum number of hops identified in the path is ten.

The **traceroute mac ip** command output shows the Layer 2 path when the specified source and destination IP addresses are in the same subnet. When you specify the IP addresses, the switch uses Address Resolution Protocol (ARP) to associate the IP addresses with the corresponding MAC addresses and the VLAN IDs.

- If an ARP entry exists for the specified IP address, the switch uses the associated MAC address and identifies the physical path.
- If an ARP entry does not exist, the switch sends an ARP query and tries to resolve the IP address. The IP addresses must be in the same subnet. If the IP address is not resolved, the path is not identified, and 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

The following example shows how to display the Layer 2 path by specifying the source and destination IP addresses and by using the **detail** keyword:

```
Switch# traceroute mac ip 2.2.66.66 2.2.22.22 detail
Translating IP to mac....
2.2.66.66 =>0000.0201.0601
2.2.22.22 =>0000.0201.0201

Source 0000.0201.0601 found on con6[WS-C2950G-24-EI] (2.2.6.6)
con6 / WS-C2950G-24-EI / 2.2.6.6 :
      Fa0/1 [auto, auto] =>Fa0/3 [auto, auto]
con5 / WS-C2950G-24-EI / 2.2.5.5 :
      Fa0/3 [auto, auto] =>Gi0/1 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
      Gi0/1 [auto, auto] =>Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
      Gi0/2 [auto, auto] =>Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
Switch#
```

The following example shows how to display the Layer 2 path by specifying the source and destination hostnames:

```
Switch# traceroute mac ip con6 con2
Translating IP to mac ....
2.2.66.66 =>0000.0201.0601
2.2.22.22 =>0000.0201.0201

Source 0000.0201.0601 found on con6
con6 (2.2.6.6) :Fa0/1 =>Fa0/3
con5          (2.2.5.5)      ) : Fa0/3 =>Gi0/1
con1          (2.2.1.1)      ) : Gi0/1 =>Gi0/2
con2          (2.2.2.2)      ) : Gi0/2 =>Fa0/1
Destination 0000.0201.0201 found on con2
Layer 2 trace completed
Switch#
```

The following 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 2.2.66.66 2.2.77.77
Arp failed for destination 2.2.77.77.
```

```
Layer2 trace aborted.  
Switch#
```

Related Commands

Command	Description
traceroute mac	Displays the Layer 2 path taken by the packets from the specified source MAC address to the specified destination MAC address.

transport udp (netflow-lite exporter submode)



Note

NetFlow-lite is only supported on the Catalyst 4948E and Catalyst 4948E-F Ethernet switches.

To specify a UDP transport destination port for a NetFlow-lite collector, use the **transport udp** command. To delete a transport UDP, use the **no** form of this command.

```
transport udp destination-port
```

```
no transport udp destination-port
```

Syntax Description	<i>destination-port</i>	Specifies a UDP transport destination port for a NetFlow-lite collector.
Command Default	None	
Command Modes	netflow-lite exporter submode	
Command History	Release	Modification
	15.0(2)SG	This command was introduced on the Catalyst 4948E and Catalyst 4948E-F Ethernet switches.

Usage Guidelines

One of the mandatory parameters for a minimally configured exporter along with the destination address and UDP destination port of the NetFlow-lite collector.

Examples

The following example shows how to specify a UDP transport destination port for a NetFlow-lite collector:

```
Switch# config terminal
Switch(config)# netflow-lite exporter exporter1
Switch(config-netflow-lite-exporter)# destination 5.5.5.6
Switch(config-netflow-lite-exporter)# source 5.5.5.5
Switch(config-netflow-lite-exporter)# transport udp 8188
Switch(config-netflow-lite-exporter)# ttl 128
Switch(config-netflow-lite-exporter)# cos 7
Switch(config-netflow-lite-exporter)# dscp 32
Switch(config-netflow-lite-exporter)# template data timeout 1
Switch(config-netflow-lite-exporter)# options sampler-table timeout 1
Switch(config-netflow-lite-exporter)# options interface-table timeout 1
Switch(config-netflow-lite-exporter)# export-protocol netflow-v9
Switch(config-netflow-lite-exporter)# exit
Switch(config)#
```

```

Display the exporter
Switch# show netflow-lite exporter exporter1
Netflow-lite Exporter exporter1:
  Network Protocol Configuration:
    Destination IP address: 5.5.5.6
    Source IP Address:     5.5.5.5
    VRF label:
    DSCP:                  0x20
    TTL:                   128
    COS:                   7
  Transport Protocol Configuration:
    Transport Protocol:    UDP
    Destination Port:      8188
    Source Port:           61670
  Export Protocol Configuration:
    Export Protocol:       netflow-v9
    Template data timeout: 60
    Options sampler-table timeout: 1800
    Options interface-table timeout: 1800
  Exporter Statistics:
    Packets Exported:     0

```

You can verify your settings with the **show netflow-lite exporter** privileged EXEC command.

Related Commands

Command	Description
options timeout (netflow-lite exporter submode)	Specifies an options timeout for the NetFlow-lite collector.
cos (netflow-lite exporter submode)	Specifies a cos value for the NetFlow-lite collector.
source (netflow-lite exporter submode)	Specifies a source Layer 3 interface of the NetFlow-lite collector.
transport udp (netflow-lite exporter submode)	Specifies a UDP transport destination port for a NetFlow-lite collector.
ttl (netflow-lite exporter submode)	Specifies a ttl value for the NetFlow-lite collector.
destination (netflow-lite exporter submode)	Specifies a destination address in netflow-lite submode.
template data timeout (netflow-lite exporter submode)	Specifies a template data timeout for the NetFlow-lite collector.
export-protocol (netflow-lite exporter submode)	Specifies the export protocol for the NetFlow-lite collector.
dscp (netflow-lite exporter submode)	Specifies a cos value for the NetFlow-lite collector.

transport udp load-share (netflow-lite exporter submode)



Note

NetFlow-lite is only supported on the Catalyst 4948E and Catalyst 4948E-F Ethernet switches.

To specify the number of destination ports to load balance on for a NetFlow-lite collector, use the **transport udp load-share** command. To delete a transport UDP, use the **no** form of this command.

```
transport udp load-share destination-port
```

```
no transport udp load-share destination-port
```

Syntax Description	<i>destination-port</i>	Specifies number of destination ports to load balance on.
Command Default	1	
Command Modes	netflow-lite exporter submode	
Command History	Release	Modification
	15.0(2)SG	This command was introduced on the Catalyst 4948E and Catalyst 4948E-F Ethernet switches.

Usage Guidelines

The CLI for UDP destination port load sharing allows you leverage multiple receive packet queues in current server NICs, where the collector is running. This is an optional parameter. When **number** ≥ 2 is configured, a switch exports datagrams with a UDP destination port number that “round robins” between a set of consecutive destination UDP port numbers starting with the base *udp port number* and ending with base *udp port number + num ports - 1*. Typically, netflow templates are sent on the base UDP port number and the packet sample netflow records are sent on the remaining UDP ports. So, the collector provides optimized processing for templates or metadata and packet sample records on a socket.

Examples

The following example shows how to specify a UDP transport destination port for a NetFlow-lite collector:

```
Switch# config terminal
Switch(config)# netflow-lite exporter exporter1
Switch(config-netflow-lite-exporter)# destination 5.5.5.6
Switch(config-netflow-lite-exporter)# source 5.5.5.5
Switch(config-netflow-lite-exporter)# transport udp 8188
Switch(config-netflow-lite-exporter)# transport udp load-share
Switch(config-netflow-lite-exporter)# ttl 128
Switch(config-netflow-lite-exporter)# cos 7
Switch(config-netflow-lite-exporter)# dscp 32
Switch(config-netflow-lite-exporter)# template data timeout 1
Switch(config-netflow-lite-exporter)# options sampler-table timeout 1
```

```
Switch(config-netflow-lite-exporter)# options interface-table timeout 1
Switch(config-netflow-lite-exporter)# export-protocol netflow-v9
Switch(config-netflow-lite-exporter)# exit
Switch(config)#
```

```
Display the exporter
Switch# show netflow-lite exporter exporter1
Netflow-lite Exporter exporter1:
Network Protocol Configuration:
  Destination IP address: 5.5.5.6
  Source IP Address:    5.5.5.5
  VRF label:           none
  DSCP:                0x20
  TTL:                 128
  COS:                 7
Transport Protocol Configuration:
  Transport Protocol:  UDP
  Source Port:        50441
  Destination Port:   8188
  Destination Ports to Load-share: 1
Export Protocol Configuration:
  Export Protocol:    netflow-v9
  Template data timeout: 1800
  Options sampler-table timeout: 1800
  Options interface-table timeout: 1800
Exporter Statistics:
  Packets Exported: 56
```

You can verify your settings with the **show netflow-lite exporter** privileged EXEC command.

Related Commands

Command	Description
dscp (netflow-lite exporter submode)	Specifies a cos value for the NetFlow-lite collector.
options timeout (netflow-lite exporter submode)	Specifies an options timeout for the NetFlow-lite collector.
cos (netflow-lite exporter submode)	Specifies a cos value for the NetFlow-lite collector.
source (netflow-lite exporter submode)	Specifies a source Layer 3 interface of the NetFlow-lite collector.
transport udp (netflow-lite exporter submode)	Specifies a UDP transport destination port for a NetFlow-lite collector.
ttl (netflow-lite exporter submode)	Specifies a ttl value for the NetFlow-lite collector.
destination (netflow-lite exporter submode)	Specifies a destination address in netflow-lite submode.
template data timeout (netflow-lite exporter submode)	Specifies a template data timeout for the NetFlow-lite collector.
export-protocol (netflow-lite exporter submode)	Specifies the export protocol for the NetFlow-lite collector.

trust

To define a trust state for traffic classified through the **class** policy-map configuration command, use the **trust** policy-map class configuration command. To return to the default setting, use the **no** form of this command.

trust [**cos** | **dscp**]

no trust [**cos** | **dscp**]

Syntax Description	
cos	(Optional) Classifies an ingress packet by using the packet class of service (CoS) value. For an untagged packet, the port default CoS value is used.
dscp	(Optional) Classifies an ingress packet by using the packet Differentiated Services Code Point (DSCP) values (most significant 6 bits of 8-bit service-type field). For a non-IP packet, the packet CoS value is used if the packet is tagged. If the packet is untagged, the default port CoS value is used to map CoS to DSCP.

Command Default The action is not trusted.

Command Modes Policy-map class configuration

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

Usage Guidelines This command is not supported on the Supervisor Engine 6-E, Supervisor Engine 6L-E, Catalyst 4900M Catalyst 4948E, and Catalyst 4948E-F.

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

The following 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.

ttl (netflow-lite exporter submode)



Note

NetFlow-lite is only supported on the Catalyst 4948E and Catalyst 4948E-F Ethernet switches.

To specify a ttl value for the NetFlow-lite collector, use the **ttl** command. To delete the value, use the **no** form of this command.

```
ttl ttl-value
```

```
no ttl ttl-value
```

Syntax Description	<i>ttl-value</i>	Specifies a ttl value for the NetFlow-lite collector. Valid values are from 1 to 254.
Command Default	254	
Command Modes	netflow-lite exporter submode	
Command History	Release	Modification
	15.0(2)SG	This command was introduced on the Catalyst 4948E and Catalyst 4948E-F Ethernet switches.

Usage Guidelines The ttl limit takes effect only when the export packets are based on IPv4. It has no effect on IPv6.

Examples The following example shows how to specify a ttl value for the NetFlow-lite collector:

```
Switch# config terminal
Switch(config)# netflow-lite exporter exporter1
Switch(config-netflow-lite-exporter)# destination 5.5.5.6
Switch(config-netflow-lite-exporter)# source 5.5.5.5
Switch(config-netflow-lite-exporter)# transport udp 8188
Switch(config-netflow-lite-exporter)# ttl 128
Switch(config-netflow-lite-exporter)# cos 7
Switch(config-netflow-lite-exporter)# dscp 32
Switch(config-netflow-lite-exporter)# template data timeout 1
Switch(config-netflow-lite-exporter)# options sampler-table timeout 1
Switch(config-netflow-lite-exporter)# options interface-table timeout 1
Switch(config-netflow-lite-exporter)# export-protocol netflow-v9
Switch(config-netflow-lite-exporter)# exit
Switch(config)#
```

```
Display the exporter
Switch# show netflow-lite exporter exporter1
Netflow-lite Exporter exporter1:
  Network Protocol Configuration:
```

```

Destination IP address: 5.5.5.6
Source IP Address:     5.5.5.5
VRF label:
DSCP:                  0x20
TTL:                   128
COS:                   7
Transport Protocol Configuration:
Transport Protocol:    UDP
Destination Port:      8188
Source Port:           61670
Export Protocol Configuration:
Export Protocol:       netflow-v9
Template data timeout: 60
Options sampler-table timeout: 1800
Options interface-table timeout: 1800
Exporter Statistics:
Packets Exported:     0

```

You can verify your settings with the **show netflow-lite exporter** privileged EXEC command.

Related Commands	Command	Description
	dscp (netflow-lite exporter submode)	Specifies a cos value for the NetFlow-lite collector.
	options timeout (netflow-lite exporter submode)	Specifies an options timeout for the NetFlow-lite collector.
	cos (netflow-lite exporter submode)	Specifies a cos value for the NetFlow-lite collector.
	source (netflow-lite exporter submode)	Specifies a source Layer 3 interface of the NetFlow-lite collector.
	transport udp (netflow-lite exporter submode)	Specifies a UDP transport destination port for a NetFlow-lite collector.
	destination (netflow-lite exporter submode)	Specifies a destination address in netflow-lite submode.
	template data timeout (netflow-lite exporter submode)	Specifies a template data timeout for the NetFlow-lite collector.

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-rate | priority high | shape shape-rate }
```

```
no tx-queue
```

Syntax Description	
<i>queue-id</i>	(Optional) Number of the queue; valid values are from 1 to 4.
bandwidth <i>bandwidth-rate</i>	Specifies traffic bandwidth; valid values are from 16000 to 1000000000 bits per second.
priority high	Specifies high priority.
shape <i>shape-rate</i>	Specifies the maximum rate that packets are passed through a transmit queue; valid values are from 16000 to 1000000000 bits per second.

Command Default

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(8a)EW	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

This command is not supported on Supervisor Engine 6-E, Supervisor Engine 6L-E, Catalyst 4900M, Catalyst 4948E, and Catalyst 4948E-F.

The bandwidth and shape rates cannot exceed the maximum speed of the interface.

The bandwidth can be configured only on the following:

- Ports on the WS-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

The following example shows how to allocate bandwidth on queue 1 to 100 Mbps:

```
Switch(config-if)# tx-queue 1  
Switch(config-if-tx-queue)# bandwidth 1000000000  
Switch(config-if-tx-queue)#
```

The following example shows how to configure transmit queue 3 to the high priority:

```
Switch(config-if)# tx-queue 3  
Switch(config-if-tx-queue)# priority high  
Switch(config-if-tx-queue)#
```

The following example shows how to configure the traffic shaping rate of 64 kbps to transmit queue 1:

```
Switch(config-if)# tx-queue 1  
Switch(config-if-tx-queue)# shape 64000  
Switch(config-if-tx-queue)#
```

Related Commands

Command	Description
show qos interface	Displays queueing information.

udld (global configuration mode)

To enable aggressive or normal mode in the UDLD protocol and to set the configurable message timer time, use the **udld** global configuration command. You can also use this command to set the error reporting mode for Fast UDLD.

Use the **no** form of this command to do the following:

- Disable normal mode UDLD on all the fiber ports by default
- Disable aggressive mode UDLD on all the fiber ports by default
- Disable the message timer
- Disable Fast UDLD error reporting mode

udld enable | aggressive

no udld enable | aggressive

udld message time *message-timer-time*

no udld message time

udld fast-hello error-reporting

no udld fast-hello error-reporting

Syntax Description		
enable		Enables UDLD in normal mode by default on all the fiber-optic interfaces.
aggressive		Enables UDLD in aggressive mode by default on all the fiber-optic interfaces.
message time <i>message-timer-time</i>		Sets the period of time between the UDLD probe messages on the ports that are in advertisement mode and are currently determined to be bidirectional; valid values are from 1 to 90 seconds.
fast-hello error-reporting		If Fast UDLD is enabled and a link failure is detected, reports the link failure through a log message instead of errdisabling the port.

Command Default All fiber-optic interfaces are disabled and the message timer for UDLD is set to 15 seconds. Fast UDLD is disabled on all interfaces.

Command Modes Global configuration

Command History	Release	Modification
	12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch.
	12.2(54)SG	Support for Fast UDLD was added.

Usage Guidelines

If you enable aggressive mode, once all the switch port's neighbors have aged out either in the advertisement or in the detection phase, UDLD and Fast UDLD restart the linkup sequence. They can resynchronize with any potentially out-of-sync neighbor and shut down the port if the UDLD messages from the neighbor indicate that the link state is still undetermined.

This command affects fiber interfaces only. Use the [udld \(interface configuration mode\)](#) command to enable UDLD on other interface types.

Examples

The following example shows how to enable UDLD on all the fiber interfaces:

```
Switch (config)# udld enable
Switch (config)#
```

Related Commands

Command	Description
show udd	Displays the administrative and operational UDLD status.
udld (interface configuration mode)	Enables UDLD and Fast UDLD on an individual interface or prevents a fiber interface from being enabled by the udld (global configuration mode) command.

udld (interface configuration mode)

To enable UDLD and Fast UDLD on an individual interface or to prevent a fiber-optic interface from being enabled by the `udld (global configuration mode)` command, use the `udld` interface level command. Use the `no` form of this command to disable UDLD, or to return a nonfiber port to the setting specified with the `udld (global configuration mode)` command.

`udld port {aggressive | disable}`

`no udld port {aggressive | disable}`

`udld fast-hello interval`

`no udld fast-hello`

Syntax Description

aggressive	Enables UDLD in aggressive mode.
disable	Disables UDLD.
fast-hello	Enables Fast UDLD with the configured timer.
<i>interval</i>	Sets the timer interval.

Command Default

The fiber-optic interfaces are enabled with the state of the global `udld (enable or aggressive)` command. The nonfiber interfaces are enabled with UDLD disabled.

Fast UDLD is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch.
12.2(54)SG	Support was added for Fast UDLD.

Usage Guidelines

If you enable aggressive mode, once all the switch port's neighbors have aged out either in the advertisement or in the detection phase, UDLD and Fast UDLD restart the linkup sequence. They can resynchronize with any potentially out-of-sync neighbor and shut down the port if the UDLD messages from the neighbor indicate that the link state is still undetermined.

Use the `udld port aggressive` command on fiber-optic ports to override the setting of the global `udld (enable or aggressive)` command. Use the `no` form of the command on fiber-optic ports to restore the UDLD state as configured by the global `udld` command.

If `udld enable` is configured globally, UDLD is enabled on all fiber-optic interfaces in nonaggressive mode. You can configure `udld port aggressive` on a fiber-optic interface to override the `udld enable` command setting and to enter aggressive mode. If you enter the `no udld port aggressive` command, the settings of the previous global state are reestablished and the aggressive mode is removed.

The **disable** keyword is supported on fiber-optic ports only. Use the **no** form of the **udld** command to reset UDLD to the value specified by the **udld (global configuration mode)** command.

If the port changes from fiber-optic to nonfiber-optic or vice versa, all configurations are maintained.

Examples

The following example shows how to enable UDLD on any port interface for any global **udld (global configuration mode)** setting:

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

The following example shows how to enable UDLD in aggressive mode on any port interface for any global **udld (enable or aggressive)** setting:

```
Switch (config-if)# udld port aggressive
Switch (config-if)#
```

The following example shows how to disable UDLD on a fiber port interface for any global **udld (global configuration mode)** setting:

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

The following example shows how to enable Fast UDLD on a port interface with a timer value of 200 ms. To enable Fast UDLD on a port, you must first enable UDLD in normal or aggressive mode:

```
Switch (config-if)# udld port
Switch (config-if)# udld fast-hello 200
Switch (config-if)#
```

Related Commands

Command	Description
show udld	Displays the administrative and operational UDLD and Fast UDLD status.
udld (global configuration mode)	Enables aggressive or normal mode in the UDLD protocol and sets the configurable message timer time.

udld reset

To reset all the UDLD ports in the shutdown state (that is, errdisabled by UDLD), use the **udld reset** privileged EXEC command.

udld reset

Syntax Description This command has no arguments or keywords.

Command Default This command has no default settings.

Command Modes Privileged EXEC

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

Usage Guidelines If the interface configuration is still enabled for UDLD, those ports will begin to run UDLD again and may shut down if the reason for the shutdown has not been resolved.

The **udld reset** command permits the traffic to flow on the ports again. Other features, operate normally if enabled, such as STP, PAgP, and DTP.

Examples The following example shows how to reset all the ports that are shut down by UDLD:

```
Switch# udld reset
Switch#
```

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.

Command Default

Disabled

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(13)EW	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

The following example shows how to set Gigabit Ethernet interface 1/1 to receive traffic unidirectionally:

```
Switch# config terminal
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
```

Syntax Description	
<i>name</i>	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).
<i>password</i>	Password of the user.

Command Default No username-based authentication system is established.

Command Modes Global configuration mode

Command History	Release	Modification
	12.1(8a)EW	This command was introduced on the Catalyst 4500 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 retrievable. 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 The following 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)#
```

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-filesystem:] [filename] [expected-md5-signature]
```

Syntax Description		
/md5	(Optional)	Verifies the MD5 signatures.
<i>flash-filesystem:</i>	(Optional)	Device where the fash resides; valid values are bootflash: , slot0: , flash: , or sup-bootflash: .
<i>filename</i>	(Optional)	Name of the Cisco IOS image.
<i>expected-md5-signature</i>	(Optional)	MD5 signature.

Command Default The current working device is specified.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.1(8a)EW	This command was introduced on the Catalyst 4500 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 Readme file, which is included with the image on the disk, lists the name, file size, and checksum of the image. Review the contents of the Readme file before loading or duplicating the new image so that you can verify the checksum when you copy it into the flash memory or on to a server.

Use the **verify /md5** command to verify the MD5 signature of a file before using it. This command validates the integrity of a copied file by comparing a precomputed MD5 signature with the signature that is computed by this command. If the two MD5 signatures match, the copied file is identical to the original file.

You can find the MD5 signature posted on the Cisco.com page with the image.

You can use the **verify /md5** command in one of the following ways:

- Verify the MD5 signatures 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 signatures by entering the **verify /md5 {flash-filesystem:filename} {expected-md5-signature}** command.

After completing the comparison, the system returns with a verified message. If an error is detected, the output is similar to the following:

```
Switch# verify /md5 slot0:c4-jsv-mz 0f
.....
.....
.....
.....
.....
.....
.....Done!
%Error verifying slot0:c4-jsv-mz
Computed signature = 0f369ed9e98756f179d4f29d6e7755d3
Submitted signature = 0f
```

To display the contents of the flash memory, enter the **show flash** command. The flash contents listing does not include the checksum of the individual files. To recompute and verify the image checksum after the image has been copied into the flash memory, enter the **verify** command.

A colon (:) is required after the specified device.

Examples

The following example shows how to use the **verify** command:

```
Switch# verify cat6k_r47_1.cbi
.....
File cat6k_r47_1.cbi verified OK.
Switch#
```

The following example shows how to manually verify the MD5 signature:

```
Switch# verify /md5 c4-jsv-mz
.....
.....
.....
.....
.....
.....Done!
verify /md5 (slot0:c4-jsv-mz) = 0f369ed9e98756f179d4f29d6e7755d3
Switch#
```

The following example shows how to allow the system to compare the MD5 signatures:

```
Switch# verify /md5 slot0:c4-jsv-mz 0f369ed9e98756f179d4f29d6e7755d3
.....
.....
.....
.....
.....
.....Done!
verified /md5 (slot0:c6sup12-jsv-mz) = 0f369ed9e98756f179d4f29d6e7755d3
Switch#
```

Related Commands

Command	Description
show file system (Flash file system) (refer to Cisco IOS documentation)	Displays available file systems.
show flash (refer to Cisco IOS documentation)	Displays the contents of flash memory.

vlan (VLAN Database mode)

To configure a specific VLAN, use the **vlan** command. To delete a VLAN, use the **no** form of this command.

```
vlan vlan_id [are hops] [backupcrf mode] [bridge type | bridge-num] [media type] [mtu mtu-size]
[name vlan-name] [parent parent-vlan-id] [ring ring-number] [said said-value] [state
{suspend | active}] [stp type type] [tb-vlan1 tb-vlan1-id] [tb-vlan2 tb-vlan2-id]
```

```
no vlan vlan
```

Syntax Description	
<i>vlan_id</i>	Number of the VLAN; valid values are from 1 to 4094.
are <i>hops</i>	(Optional) Specifies the maximum number of All Route Explorer hops for this VLAN; valid values are from 0 to 13. Zero is assumed if no value is specified.
backupcrf <i>mode</i>	(Optional) Enables or disables the backup CRF mode of the VLAN; valid values are enable and disable .
bridge <i>type</i>	(Optional) Specifies the bridging characteristics of the VLAN or identification number of the bridge; valid <i>type</i> values are srb and srt .
<i>bridge_num</i>	(Optional) Valid <i>bridge_num</i> values are from 0 to 15.
media <i>type</i>	(Optional) Specifies the media type of the VLAN; valid values are fast ethernet , fd-net , fddi , trcrf , and trbrf .
mtu <i>mtu-size</i>	(Optional) Specifies the maximum transmission unit (packet size, in bytes) that the VLAN can use; valid values are from 576 to 18190.
name <i>vlan-name</i>	(Optional) Defines a text string used as the name of the VLAN (1 to 32 characters).
parent <i>parent-vlan-id</i>	(Optional) Specifies the ID number of the parent VLAN of FDDI or Token Ring-type VLANs; valid values are from 2 to 1001.
ring <i>ring-number</i>	(Optional) Specifies the ring number of FDDI or Token Ring-type VLANs; valid values are from 2 to 1001.
said <i>said-value</i>	(Optional) Specifies the security association identifier; valid values are from 1 to 4294967294.
state	(Optional) Specifies the state of the VLAN.
suspend	Specifies that the state of the VLAN is suspended. VLANs in the suspended state do not pass packets.
active	Specifies that the state of the VLAN is active.
stp <i>type</i> <i>type</i>	(Optional) Specifies the STP type; valid values are ieee , ibm , and auto .
tb-vlan1 <i>tb-vlan1-id</i>	(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 <i>tb-vlan2-id</i>	(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.

Command Default

The defaults are as follows:

- The `vlan-name` is “VLANxxxx” where “xxxx” represents four numeric digits (including leading zeroes) equal to the VLAN ID number.
- The media type is Fast Ethernet.
- The state is active.
- The `said-value` is 100,000 plus the VLAN ID number.
- The `mtu-size` default is dependent upon the VLAN type:
 - `fddi`—1500
 - `trcrf`—1500 if V2 is not enabled; 4472 if it is enabled
 - `fd-net`—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	This command was introduced on the Catalyst 4500 series switch.

Usage Guidelines

VLAN 1 parameters are factory configured and cannot be changed.

When you define *vlan-name*, the name must be unique within the administrative domain.

The SAID is documented in 802.10. When the **no** form is used, the 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 in other types of VLANs. When the **no** form is used, the VLANs source-route bridging number returns to the default.

The parent VLAN resets to the default if the parent VLAN is deleted or the **media** keyword changes the VLAN type or the VLAN type of the parent VLAN.

The *tb-vlan1* and *tb-vlan2* are used to configure translational bridge VLANs of a specified type of VLAN and are not allowed in other types of VLANs. The translational bridge VLANs must be a different VLAN type than the affected VLAN; if two VLANs are specified, the two must be different VLAN types.

A translational bridge VLAN will reset to the default if the translational bridge VLAN is deleted or the **media** keyword changes the VLAN type or the VLAN type of the corresponding translational bridge VLAN.

Examples

The following 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.

The following 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 modified:
  Media type FASTETHERNET
  Parent VLAN 3
```

The following example shows how to delete VLAN 2:

```
Switch(vlan)# no vlan 2
Switch(vlan)#
```

The following example shows how to return the MTU to the default for its type and the translational bridging VLANs to the default:

```
Switch(vlan)# no vlan 2 mtu tb-vlan1 tb-vlan2
Switch(vlan)#
```

Related Commands

Command	Description
show vlan	Displays VLAN information.

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#*]

no vlan access-map *name* [*seq#*]

Syntax Description

<i>name</i>	VLAN access-map tag.
<i>seq#</i>	(Optional) Map sequence number; valid values are from 0 to 65535.

Command Default

This command has no default settings.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(12c)EW	This command was introduced on the Catalyst 4500 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 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 reset its defaults.

Examples

The following example shows how to enter VLAN access-map mode:

```
Switch(config)# vlan access-map cisco
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	<i>vlan</i> Specifies a list of VLANs. “,” “-” operators can be used; such as, 1-10,20.				
Command Default	This command has no default settings.				
Command Modes	Global configuration mode				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.2(40)SG</td> <td>This command was introduced on Catalyst 4900M and Supervisor Engine 6E.</td> </tr> </tbody> </table>	Release	Modification	12.2(40)SG	This command was introduced on Catalyst 4900M and Supervisor Engine 6E.
Release	Modification				
12.2(40)SG	This command was introduced on Catalyst 4900M and Supervisor Engine 6E.				

Usage Guidelines Even though an SVI is not needed in all cases, such as when you use your Catalyst 4500 series switch as a pure Layer 2 switch, you are required to create an SVI.

VLAN configuration mode has been introduced to remove the requirement of creating an SVI. With this command you can specify lists of VLANs and the input and output policies that are applied. To configure your system in this mode there is no requirement for you to create SVIs, or create VLAN or VTP mode interactions. Once the VLAN becomes active the configuration becomes active on that VLAN. You can use “-” or “,” extensions to specifying VLAN list.

Examples The following example shows how to configure a service policy while in VLAN configuration mode and display the new service policy:

```
Switch# configure terminal
Switch(config)# vlan configuration 30-40
Switch(config-vlan-config)# service-policy input p1
Switch(config-vlan-config)# end
Switch# show running configuration | begin vlan configuration
!
vlan configuration 30-40
    service-policy input p1
!
vlan internal allocation policy ascending !
vlan 2-1000
!
Switch#
```

The following 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:
    rate 128000 bps, burst 4000 bytes
    conformed 0 packets, 0 bytes; action:
      transmit
    exceeded 0 packets, 0 bytes; action:
      drop
    conformed 0 bps, exceeded 0 bps
Switch#
```

Related Commands

Command	Description
vlan (VLAN Database mode)	Configures a specific VLAN.
policy-map	Creates a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.

vlan database

To enter VLAN configuration mode, use the **vlan database** command.

vlan database

Syntax Description This command has no arguments or keywords.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.1(8a)EW	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 The following example shows how to enter VLAN configuration mode:

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

The following example shows how to exit VLAN configuration mode without applying changes after you are in VLAN configuration mode:

```
Switch(vlan)# abort
Aborting...
Switch#
```


The following example shows how to delete a VLAN after you are in VLAN configuration mode:

```
Switch(vlan)# no vlan 100  
Deleting VLAN 100...  
Switch(vlan)#
```

The following example shows how to turn off pruning after you are in VLAN configuration mode:

```
Switch(vlan)# no vtp pruning  
Pruning switched OFF  
Switch(vlan)#
```

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.

Command Default 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 expands VLAN space by using a VLAN-in-VLAN hierarchy and by tagging the tagged packets. You must use the 802.1Q trunk ports for sending out the packets to the service-provider network. However, the packets going through the core of the service-provider network might also be carried on the 802.1Q trunks. If the native VLANs of an 802.1Q trunk match the native VLAN of a tunneling port on the same switch, the traffic on the native VLAN is not tagged on the sending trunk port. This command ensures that the native VLAN packets on all 802.1Q trunk ports are tagged.

Examples The following example shows how to enable 802.1Q tagging on the native VLAN frames and verify the configuration:

```
Switch# config terminal
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]}
```

Syntax Description

<i>map-name</i>	VLAN access-map tag.
vlan-list <i>vlan-list</i>	Specifies the VLAN list; see the “Usage Guidelines” section for valid values.

Command Default

This command has no default settings.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(12c)EW	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

The following example shows how to apply a VLAN access map on VLANs 7 through 9:

```
Switch(config)# vlan filter ganymede vlan-list 7-9
Switch(config)#
```

vlan group

To create or modify a VLAN group, use the **vlan group** command in global configuration mode. Use the **no** form of this command to remove a VLAN list from the VLAN group.

vlan group *group-name* **vlan-list** *vlan-list*

no vlan group *group-name* **vlan-list** *vlan-list*

Syntax Description

<i>group-name</i>	Specifies the VLAN group name.
<i>vlan-list</i>	Specifies a VLAN list name. See the Usage Guidelines section below for additional information about this argument.

Command Default

This command has no arguments or keywords.

Command Modes

Global configuration

Command History

Release	Modification
12.2(54)SG	This command was modified to support user distribution on the Catalyst 4500 series switch.

Usage Guidelines

The VLAN group name can contain up to 31 characters and must begin with a letter.

The *vlan-list* argument can be a single VLAN ID, a list of VLAN IDs, or VLAN ID ranges (*vlan-id-vlan-id*). Multiple entries are separated by a hyphen (-) or a comma (,).

If the named VLAN group does not exist, the **vlan group** command creates the group and maps the specified VLAN list to the group. If the named VLAN group exists, the specified VLAN list is mapped to the group.

The **no** form of the **vlan group** command removes the specified VLAN list from the VLAN group. When you remove the last VLAN from the VLAN group, you delete the VLAN group.

You can configure a maximum of 100 VLAN groups, and map a maximum of 4094 VLANs to a VLAN group.

Examples

The following example shows how to map VLANs 7 through 9 and 11 to a VLAN group:

```
Switch(config)# vlan group ganymede vlan-list 7-9,11
```

The following example shows how to remove VLAN 7 from the VLAN group:

```
Switch(config)# no vlan group ganymede vlan-list 7
```

Related Commands

Command	Description
show vlan group	Displays the VLANs mapped to VLAN groups.

vlan internal allocation policy

To configure the internal VLAN allocation scheme, use the **vlan internal allocation policy** command. To return to the default setting, use the **no** form of this command.

vlan internal allocation policy {ascending | descending}

no vlan internal allocation policy

Syntax Description

ascending	Specifies to allocate internal VLANs from 1006 to 4094.
descending	Specifies to allocate internal VLANs from 4094 to 1006.

Command Default

The default is the ascending allocation scheme.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(19)EW	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

The following 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	<i>interval</i>	Queries to the VLAN Membership Policy Server (VMPS) to reconfirm dynamic VLAN assignments; valid values are from 1 to 120 minutes.
---------------------------	-----------------	--

Command Default	The reconfirmation interval is 60 minutes.
------------------------	--

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

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

Examples The following 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).

vmmps 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 **vmmps reconfirm** command.

vmmps reconfirm

Syntax Description This command has no arguments or keywords.

Command Default This command has no default settings.

Command Modes Privileged EXEC mode

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

Usage Guidelines You can verify your setting by entering the **show vmmps** command and examining the VMPS Action row of the Reconfirmation Status section. The **show vmmps** command shows the result of the last time that the assignments were reconfirmed either because the reconfirmation timer expired or because the **vmmps reconfirm** command was entered.

Examples The following example shows how to immediately send VQP queries to the VMPS:

```
Switch# vmmps reconfirm
Switch#
```

Related Commands	Command	Description
	show vmmps	Displays the VLAN Query Protocol (VQP) version, reconfirmation interval, retry count, VLAN Membership Policy Server (VMPS) IP addresses, current servers, and primary servers.
	vmmps 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	<i>count</i> Number of attempts to contact the VLAN Membership Policy Server (VMPS) by the client before querying the next server in the list; valid values are from 1 to 10.				
Command Default	The retry count is 3.				
Command Modes	Global configuration mode				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.1(13)EW</td> <td>This command was introduced on the Catalyst 4500 series switch.</td> </tr> </tbody> </table>	Release	Modification	12.1(13)EW	This command was introduced on the Catalyst 4500 series switch.
Release	Modification				
12.1(13)EW	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	<p>The following example shows how to set the retry count to 7:</p> <pre>Switch(config)# vmps retry 7</pre>				
Related Commands	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>show vmps</td> <td>Displays the VLAN Query Protocol (VQP) version, reconfirmation interval, retry count, VLAN Membership Policy Server (VMPS) IP addresses, current servers, and primary servers.</td> </tr> </tbody> </table>	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.
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.				

vmmps server

To configure the primary VLAN Membership Policy Server (VMPS) and up to three secondary servers, use the **vmmps server** command. To remove a VMPS server, use the **no** form of this command.

```
vmmps server ipaddress [primary]
```

```
no vmmps server ipaddress
```

Syntax Description	
<i>ipaddress</i>	IP address or host name of the primary or secondary VMPS servers. 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.

Command Default No primary or secondary VMPS servers are defined.

Command Modes Global configuration mode

Command History	Release	Modification
	12.1(4)EA1	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 vmmps** command and examining information in the VMPS Domain Server row.

Examples The following 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)# vmmps server 191.10.49.20 primary
Switch(config)# vmmps server 191.10.49.21
Switch(config)# vmmps server 191.10.49.22
Switch(config)#
```

The following 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.

vrf (netflow-lite exporter submode)



Note

NetFlow-lite is only supported on the Catalyst 4948E and Catalyst 4948E-F Ethernet switches.

To specify a VRF label for the NetFlow-lite collector, use the **vrf** command. To delete a VRF label, use the **no** form of this command.

```
vrf source-address
```

```
no vrf source-address
```

Syntax Description	<i>vrf-label</i>	Specifies a VRF label for the NetFlow-lite collector.
---------------------------	------------------	---

Command Default	global vrf
------------------------	------------

Command Modes	netflow-lite exporter submode
----------------------	-------------------------------

Command History	Release	Modification
	15.0(2)SG	This command was introduced on the Catalyst 4948E and Catalyst 4948E-F Ethernet switches.

Usage Guidelines	By default when no vrf label is specified the global vrf is used for routing. The vrf label is ignored if the collector's address is IPv6. Default global routing table is used to route the IPv6 export packets to the collector.
-------------------------	--



Note

Support for VRF with IPv6 will be provided in a later release.

Examples	The following example shows how to specify a VRF label for the NetFlow-lite collector:
-----------------	--

```
Switch# config terminal
Switch(config)# netflow-lite exporter exporter1
Switch(config-netflow-lite-exporter)# destination 5.5.5.6
Switch(config-netflow-lite-exporter)# source 5.5.5.5
Switch(config-netflow-lite-exporter)# transport udp 8188
Switch(config-netflow-lite-exporter)# ttl 128
Switch(config-netflow-lite-exporter)# cos 7
Switch(config-netflow-lite-exporter)# dscp 32
Switch(config-netflow-lite-exporter)# template data timeout 1
Switch(config-netflow-lite-exporter)# options sampler-table timeout 1
Switch(config-netflow-lite-exporter)# options interface-table timeout 1
Switch(config-netflow-lite-exporter)# export-protocol netflow-v9
Switch(config-netflow-lite-exporter)# exit
Switch(config)#
```

```

Display the exporter
Switch# show netflow-lite exporter exporter1
Netflow-lite Exporter exporter1:
  Network Protocol Configuration:
    Destination IP address: 5.5.5.6
    Source IP Address:     5.5.5.5
    VRF label:
    DSCP:                  0x20
    TTL:                   128
    COS:                   7
  Transport Protocol Configuration:
    Transport Protocol:    UDP
    Destination Port:      8188
    Source Port:           61670
  Export Protocol Configuration:
    Export Protocol:       netflow-v9
    Template data timeout: 60
    Options sampler-table timeout: 1800
    Options interface-table timeout: 1800
  Exporter Statistics:
    Packets Exported:      0

```

You can verify your settings with the **show netflow-lite exporter** privileged EXEC command.

Related Commands	Command	Description
	dscp (netflow-lite exporter submode)	Specifies a cos value for the NetFlow-lite collector.
	cos (netflow-lite exporter submode)	Specifies a cos value for the NetFlow-lite collector.
	source (netflow-lite exporter submode)	Specifies a source Layer 3 interface of the NetFlow-lite collector.
	transport udp (netflow-lite exporter submode)	Specifies a UDP transport destination port for a NetFlow-lite collector.
	ttl (netflow-lite exporter submode)	Specifies a ttl value for the NetFlow-lite collector.
	destination (netflow-lite exporter submode)	Specifies a destination address in netflow-lite submode.
	template data timeout (netflow-lite exporter submode)	Specifies a template data timeout for the NetFlow-lite collector.
	options timeout (netflow-lite exporter submode)	Specifies an options timeout for the NetFlow-lite collector.
	export-protocol (netflow-lite exporter submode)	Specifies the export protocol for the NetFlow-lite collector.

vslp interval (virtual switch)

To configure the virtual switch link protocol (VSLP) hello packet interval, use the **vslp interval** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

vslp interval *interval* **min_rx** *min-interval* **multiplier** *factor*

no vslp interval

Syntax Description		
<i>interval</i>	Specifies the hello packet interval in milliseconds between the transmission of hello packets. Range: 300 to 5000.	
min_rx <i>min-interval</i>	Specifies the minimum interval in milliseconds for received hello packets. Range: 300 to 10000.	
multiplier <i>factor</i>	Specifies a factor in which, if no hello packets are received, the link is flagged as non operational. Range: 3 to 50.	

Command Default The interfaces are not associated.

Command Modes Interface configuration (config-if)

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

Usage Guidelines When you specify a factor, the formula is if no hello packets are received in (min_rx * multiplier) milliseconds, the link is flagged as non-operational.

Examples The following example shows how to configure the virtual switch link protocol (VSLP) hello packet interval:

```
Router-2(config-if)# vslp interval 400 min_rx 500
Router-2(config-if)#
```

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.

Command Default	Disabled
-----------------	----------

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

Command History	Release	Modification
	12.1(8a)EW	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 to a network, and triggers a VTP updater to inform the rest of the system of the changes.

Examples

The following 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)#
```

The following 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.

Command Default Disabled

Command Modes VLAN configuration mode

Command History	Release	Modification
	12.1(8a)EW	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 The following 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	<i>domain-name</i> Name of the domain.
---------------------------	--

Command Default	This command has no default settings.
------------------------	---------------------------------------

Command Modes	VLAN configuration mode
----------------------	-------------------------

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

Usage Guidelines	<p>When you define the <i>domain-name</i>, 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.</p> <p>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.</p> <p>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 reenter the number except by cleaning NVRAM and reloading.</p>
-------------------------	--

Examples	The following example shows how to set the devices administrative domain:
-----------------	---

```
Switch(vlan-config)# vtp domain DomainChandon
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 password

To create a VTP domain password, use the **vtp password** command. To delete the password, use the **no** form of this command.

vtp password *password-value*

no vtp password

Syntax Description	<i>password-value</i> An ASCII string, from 1 to 32 characters, identifying the administrative domain for the device.						
Command Default	Disabled						
Command Modes	VLAN configuration mode						
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.1(8a)EW</td> <td>This command was introduced on the Catalyst 4500 series switch.</td> </tr> </tbody> </table>	Release	Modification	12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch.		
Release	Modification						
12.1(8a)EW	This command was introduced on the Catalyst 4500 series switch.						
Examples	<p>The following example shows how to create a VTP domain password:</p> <pre>Switch(vlan-config)# vtp password DomainChandon Switch(vlan-config)#</pre> <p>The following example shows how to delete the VTP domain password:</p> <pre>Switch(vlan-config)# no vtp password Clearing device VLAN database password. Switch(vlan-config)#</pre>						
Related Commands	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>show vtp</td> <td>Displays VTP statistics and domain information.</td> </tr> <tr> <td>vtp (global configuration mode)</td> <td>Configures the name of a VTP configuration storage file.</td> </tr> </tbody> </table>	Command	Description	show vtp	Displays VTP statistics and domain information.	vtp (global configuration mode)	Configures the name of a VTP configuration storage file.
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.

Command Default Disabled

Command Modes VLAN configuration mode

Command History	Release	Modification
	12.1(8a)EW	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 The following example shows how to enable pruning in the VLAN database:

```
Switch(vlan-config)# vtp pruning
Pruning switched ON
Switch(vlan-config)#
```

The following example shows how to disable pruning in the VLAN database:

```
Switch(vlan-config)# no vtp pruning
Pruning switched OFF
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 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.

Command Default Enabled

Command Modes VLAN configuration mode

Command History	Release	Modification
	12.1(8a)EW	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 **no vtp client**, except that it does not return an error if the device is not in client mode.

Examples The following 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.

Command Default Disabled

Command Modes VLAN configuration mode

Command History	Release	Modification
	12.1(8a)EW	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 The following example shows how to place the device in VTP transparent mode:

```
Switch(vlan-config)# vtp transparent
Switch(vlan-config)#
```

The following example shows how to return the device to VTP server mode:

```
Switch(vlan-config)# no vtp transparent
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 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.

Command Default Disabled

Command Modes VLAN configuration mode

Command History	Release	Modification
	12.1(8a)EW	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 The following example shows how to enable version 2 mode in the VLAN database:

```
Switch(vlan-config)# vtp v2-mode
Switch(vlan-config)#
```

The following 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.



Abbreviations

A

ACE	access control entry
ACL	access control list
AFI	authority and format identifier
Agport	aggregation port
AMP	Active Monitor Present
APaRT	Automated Packet Recognition and Translation
ARP	Address Resolution Protocol

B

BEM	best effort method
BGP	Border Gateway Protocol
BPDU	bridge protocol data unit
BRF	bridge relay function
BSC	Bisync
BSTUN	Block Serial Tunnel
BUS	broadcast and unknown server
BVI	bridge-group virtual interface

C

CAM	content-addressable memory
CAR	committed access rate
CCA	circuit card assembly
CDP	Cisco Discovery Protocol
CEF	Cisco Express Forwarding
CHAP	Challenge Handshake Authentication Protocol
CIR	committed information rate
CLI	command-line interface
CLNS	Connection-Less Network Service
CMNS	Connection-Mode Network Service
COPS	Common Open Policy Server
COPS-DS	Common Open Policy Server Differentiated Services
CoS	class of service
CPLD	Complex Programmable Logic Device
CRC	cyclic redundancy check
CRF	concentrator relay function
CST	Common Spanning Tree

D

DAI	Dynamic ARP Inspection
DBL	Dynamic Buffer Limiting
DCC	Data Country Code
dCEF	distributed Cisco Express Forwarding
DDR	dial-on-demand routing
DE	discard eligibility

DEC	Digital Equipment Corporation
DFI	Domain-Specific Part Format Identifier
DFP	Dynamic Feedback Protocol
DISL	Dynamic Inter-Switch Link
DLC	Data Link Control
DLSw	Data Link Switching
DMP	data movement processor
DNS	Domain Name System
DoD	Department of Defense
DOS	denial of service
DRAM	dynamic RAM
DRiP	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
MD5	Message Digest 5
MET	Multicast Expansion Table
MFIB	Multicast Forwarding Information Base
MIB	Management Information Base
MII	media-independent interface
MLS	Multilayer Switching
MLSE	maintenance loop signaling entity
MOP	Maintenance Operation Protocol
MOTD	message-of-the-day
MRM	multicast routing monitor
MRQ	Multicast Replication Queue
MSDP	Multicast Source Discovery Protocol
MST	Multiple Spanning Tree
MTU	maximum transmission unit
MVAP	multiple VLAN access port

N

NBP	Name Binding Protocol
NCIA	Native Client Interface Architecture
NDE	NetFlow Data Export
NET	network entity title
NetBIOS	Network Basic Input/Output System
NFFC	NetFlow Feature Card

NMP	Network Management Processor
NSAP	network service access point
NTP	Network Time Protocol
NVRAM	nonvolatile RAM

O

OAM	Operation, Administration, and Maintenance
OSI	Open System Interconnection
OSPF	open shortest path first

P

PAE	port access entity
PAgP	Port Aggregation Protocol
PBD	packet buffer daughterboard
PC	Personal Computer (formerly PCMCIA)
PCM	pulse code modulation
PCR	peak cell rate
PDP	policy decision point
PDU	protocol data unit
PEM	Power Entry Module
PEP	policy enforcement point
PGM	Pragmatic General Multicast
PHY	physical sublayer
PIB	policy information base
PIM	Protocol Independent Multicast
PM	Port manager

PPP	Point-to-Point Protocol
PRC	Parser Return Code
PRID	Policy Rule Identifiers
PVLAN	Private VLAN
PVST+	Per VLAN Spanning Tree+

Q

QM	QoS manager
QoS	Quality of Service

R

RACL	Router Interface Access Control List
RADIUS	Remote Access Dial-In User Service
RAM	random-access memory
RCP	Remote Copy Protocol
RGMP	Router Group Management Protocol
RIF	Routing Information Field
RMON	Rmote Network Monitor
ROM	read-only memory
RP	route processor or rendezvous point
RPC	remote procedure call
RPF	reverse path forwarding
RPR	Router Processor Redundancy
RSPAN	remote SPAN
RST	reset

RSVP	ReSerVation Protocol
Rx	Receive

S

SAID	Security Association Identifier
SAP	service access point
SCM	service connection manager
SCP	Switch-Module Configuration Protocol
SDLC	Synchronous Data Link Control
SGBP	Stack Group Bidding Protocol
SIMM	single in-line memory module
SLB	server load balancing
SLCP	Supervisor Line-Card Processor
SLIP	Serial Line Internet Protocol
SMDS	Software Management and Delivery Systems
SMF	software MAC filter
SMP	Standby Monitor Present
SMRP	Simple Multicast Routing Protocol
SMT	Station Management
SNAP	Subnetwork Access Protocol
SNMP	Simple Network Management Protocol
SPAN	Switched Port Analyzer
SRB	source-route bridging
SRT	source-route transparent bridging
SSTP	Cisco Shared Spanning Tree
STP	Spanning Tree Protocol

SVC	switched virtual circuit
SVI	switched virtual interface

T

TACACS+	Terminal Access Controller Access Control System Plus
TARP	Target Identifier Address Resolution Protocol
TCAM	Ternary Content Addressable Memory
TCL	table contention level
TCP/IP	Transmission Control Protocol/Internet Protocol
TFTP	Trivial File Transfer Protocol
TIA	Telecommunications Industry Association
TLV	type-length-value
TopN	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
TVX	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
-----	----------------------

