A Commands

aaa accounting dot1x default start-stop group radius
aaa accounting system default start-stop group radius clear mac-address-table
access-group mode
access-list hardware capture mode
access-list hardware entries
access-list hardware region
action
apply
apply client server
apply 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-sync

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
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 wccp
clear lacp counters
clear nmsp statistics
clear mac-address-table dynamic
clear pagp
D Commands

clear port-security

clear pppoe intermediate-agent statistics

clear qos

clear vlan counters

clear vmps statistics

control-plane

counter

debug adjacency

debug backup

debug condition interface

debug condition standby

debug condition vlan

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
Chapter

disable sw-vlan ifs

disable sw-vlan notification

disable sw-vlan vtp

disable udld

disable vqpc

define interface-range

deny

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

duplex

E Commands

erase

errend detect

erendisable recovery
Chapter F

Commands

flowcontrol

H Commands

hardware statistics

hw-module beacon

hw-module power

hw-module system max-queue-limit

I Commands

instance

interface

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
Chapter 2873 8-01

ip igmp snooping
ip igmp snooping report-suppression
ip igmp snooping vlan
ip igmp snooping vlan explicit-tracking
ip igmp snooping vlan immediate-leave
ip igmp snooping vlan mrouter
ip igmp snooping vlan static
ip local-proxy-arp
ip mfib fastdrop
ip source binding
ip sticky-arp
ip verify header vlan all
ip verify source
ip verify unicast source reachable-via
ip wccp check services all
ip wccp group-listen
ip wccp redirect
ip wccp redirect exclude-in
ipv6 mld snooping
ipv6 mld snooping last-listener-query-count
ipv6 mld snooping last-listener-query-interval
ipv6 mld snooping listener-message-suppression
ipv6 mld snooping robustness-variable
ipv6 mld snooping tcn
ipv6 mld snooping vlan
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
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
name
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 redundancy-mode
Chapter

power inline police

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

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

service-policy (interface configuration)

service-policy (policy-map class)

service-policy input (control-plane)

session module

set

set cos
Chapter

show environment
show errdisable detect
show errdisable recovery
show etherchannel
show flowcontrol
show idprom
show interfaces
show interfaces capabilities
show interfaces counters
show interfaces description
show interfaces link
show interfaces mtu
show interfaces private-vlan mapping
show interfaces status
show interfaces switchport
show interfaces transceiver
show interfaces trunk
show ip arp inspection
show ip arp inspection log
show ip 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
clear errdisable
2-90
clear hw-module slot password
2-91
clear interface gigabitethernet
2-92
clear interface vlan
2-93
clear ip access-template
2-94
clear ip arp inspection log
2-95
clear ip arp inspection statistics
2-96
clear ip dhcp snooping binding
2-97
clear ip dhcp snooping database
2-99
clear ip dhcp snooping database statistics
2-100
clear ip igmp group
2-101
clear ip igmp snooping membership
2-103
clear ip mfib counters
2-104
clear ip mfib fastdrop
2-105
clear ip wccp
2-106
clear lacp counters
2-107
clear mac-address-table
2-108
clear mac-address-table dynamic
2-110
clear nmsp statistics
2-111
clear pagp
2-112
clear port-security
2-113
clear pppoe intermediate-agent statistics
2-115
clear qos
2-116
clear vlan counters
2-117
clear vmps statistics
2-118
control-plane
2-119
counter
2-121
dbl
2-123
debug adjacency
2-124
debug backup
2-125
debug condition interface
2-126
debug condition standby
2-127
debug condition vlan
2-129
debug dot1x
2-131
- diagnostic monitor action
- diagnostic start
- dot1x auth-fail max-attempts
- dot1x auth-fail vlan
- dot1x control-direction
- dot1x credentials (global configuration)
- dot1x critical
- dot1x critical eapol
- dot1x critical recovery delay
- dot1x critical vlan
- 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
- duplex
- epm access control
- erase
- errdisable detect
- errdisable recovery
- flowcontrol
- hardware statistics
- hw-module beacon
- hw-module power
- hw-module system max-queue-limit
- instance
- interface
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 device tracking maximum
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 dhcp snooping vlan information option format-type circuit-id string
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 multicast multipath
2-272
ip source binding
2-274
ip sticky-arp
2-275
ip verify header vlan all
2-277
ip verify source
2-278
ip verify unicast source reachable-via
2-280
ip wccp
2-281
ip wccp check services all
2-284
ip wccp group-list en
2-286
ip wccp redirect
2-288
ip wccp redirect exclude in
2-290
ipv6 mld snooping
2-291
ipv6 mld snooping last-listener-query-count
2-293
ipv6 mld snooping last-listener-query-interval
2-295
ipv6 mld snooping listener-message-suppression
2-297
ipv6 mld snooping robustness-variable
2-298
ipv6 mld snooping tcn
2-300
ipv6 mld snooping vlan
2-301
issu abortversion
2-303
issu acceptversion
2-304
issu commitversion
2-306
issu loadversion
2-308
issu runversion
2-310
issu set rollback-timer
2-311
l2protocol-tunnel
2-312
l2protocol-tunnel cos
2-313
l2protocol-tunnel drop-threshold
2-314
l2protocol-tunnel shutdown-threshold
2-315
lacp port-priority
2-317
lacp system-priority
2-318
lldp tlv-select power-management
2-319
logging event link-status global (global configuration)
2-320
logging event link-status (interface configuration)
2-321
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
name
nmsp
nmsp attachment suppress
pagp learn-method
pagp port-priority
passive-interface
permit
police
police (percent)
police rate
police (two rates)
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-mode
pppoe intermediate-agent (global)
<table>
<thead>
<tr>
<th>Service Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>service-policy (interface configuration)</strong></td>
</tr>
<tr>
<td><strong>service-policy (policy-map class)</strong></td>
</tr>
<tr>
<td><strong>service-policy input (control-plane)</strong></td>
</tr>
<tr>
<td><strong>session module</strong></td>
</tr>
<tr>
<td><strong>set</strong></td>
</tr>
<tr>
<td><strong>set cos</strong></td>
</tr>
<tr>
<td><strong>set dscp</strong></td>
</tr>
<tr>
<td><strong>set precedence</strong></td>
</tr>
<tr>
<td><strong>set qos-group</strong></td>
</tr>
<tr>
<td><strong>shape (class-based queueing)</strong></td>
</tr>
<tr>
<td><strong>shape (interface configuration)</strong></td>
</tr>
<tr>
<td><strong>shell trigger</strong></td>
</tr>
<tr>
<td><strong>show access-group mode interface</strong></td>
</tr>
<tr>
<td><strong>show adjacency</strong></td>
</tr>
<tr>
<td><strong>show acp multicast</strong></td>
</tr>
<tr>
<td><strong>show arp access-list</strong></td>
</tr>
<tr>
<td><strong>show authentication</strong></td>
</tr>
<tr>
<td><strong>show auto install status</strong></td>
</tr>
<tr>
<td><strong>show auto qos</strong></td>
</tr>
<tr>
<td><strong>show bootflash:</strong></td>
</tr>
<tr>
<td><strong>show bootvar</strong></td>
</tr>
<tr>
<td><strong>show cable-diagnostics tdr</strong></td>
</tr>
<tr>
<td><strong>show call-home</strong></td>
</tr>
<tr>
<td><strong>show cdp neighbors</strong></td>
</tr>
<tr>
<td><strong>show class-map</strong></td>
</tr>
<tr>
<td><strong>show diagnostic content</strong></td>
</tr>
<tr>
<td><strong>show diagnostic result module</strong></td>
</tr>
<tr>
<td><strong>show diagnostic result module test</strong></td>
</tr>
<tr>
<td><strong>show diagnostic result module test 2</strong></td>
</tr>
<tr>
<td><strong>show diagnostic result module test 3</strong></td>
</tr>
<tr>
<td><strong>show dot1x</strong></td>
</tr>
<tr>
<td><strong>show environment</strong></td>
</tr>
<tr>
<td><strong>show errdisable detect</strong></td>
</tr>
<tr>
<td><strong>show err disable recovery</strong></td>
</tr>
</tbody>
</table>
show ipv6 snooping counters
show ipv6 mld snooping
show ipv6 mld snooping mrouter
show ipv6 mld snooping querier
show issu capability
show issu clients
show issu comp-matrix
show issu endpoints
show issu 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 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
2-695
show macro auto monitor type
2-697
show module
2-700
show monitor
2-702
show monitor capture
2-704
show monitor capture file
2-706
show nmsp
2-710
show pagp
2-713
show policy-map
2-715
show policy-map control-plane
2-716
show policy-map interface
2-719
show policy-map interface vlan
2-722
show port-security
2-724
show power
2-730
show power inline police
2-738
show pppoe intermediate-agent interface
2-739
show qos
2-741
show qos aggregate policer
2-742
show qos d bl
2-743
show qos interface
2-744
show qos maps
2-745
show redundancy
2-747
show redundancy config-sync
2-750
show running-config
2-752
show shell functions
2-754
show shell triggers
2-755
show slavebootflash:
2-756
show slaveslot0:
2-758
show slot0:
2-760
show spanning-tree
2-762
show spanning-tree mst
2-766
show storm-control
2-768
show system mtu
2-770
show tech-support
2-771
show udld
2-773
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 vtp
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-interface
source-ip-address
spanning-tree backbonefast
spanning-tree bpdufilter
spanning-tree bpduguard
spanning-tree cost
spanning-tree etherchannel guard misconfig
spanning-tree extend system-id
spanning-tree guard
spanning-tree link-type
spanning-tree loopguard default
spanning-tree mode
spanning-tree mst
spanning-tree mst configuration
spanning-tree mst forward-time
Contents

Catalyst 4500 Series Switch Cisco IOS Command Reference—Release IOS XE 3.3.0XO(15.1(1)XO)

OL-28738 -01

test cable-diagnostics tdr

2-882

traceroute mac

2-884

traceroute mac ip

2-887

trust

2-889

tax-queue

2-891

udld (global configuration mode)

2-893

udld (interface configuration mode)

2-895

udld reset

2-897

unidirectional

2-898

username

2-899

verify

2-900

vlan (VLAN Database mode)

2-902

vlan access-map

2-905

vlan configuration

2-906

vlan database

2-908

vlan dot1q tag native

2-910

vlan filter

2-911

vlan group

2-912

vlan internal allocation policy

2-913

vmps reconfirm (global configuration)

2-914

vmps reconfirm (privileged EXEC)

2-915

vmps retry

2-916

vmps server

2-917

vtp (global configuration mode)

2-919

vtp client

2-920

vtp domain

2-921

vtp password

2-922

vtp pruning

2-923

vtp server

2-924

vtp transparent

2-925

vtp v2-mode

2-926

APPENDIX A

Abbreviations     A-1

INDEX
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 software 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 publication is organized as follows:
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 12.4 Configuration Guides
- Cisco IOS Release 12.4 Command References

For information about MIBs, refer to this URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Conventions

This document uses these conventions:

<table>
<thead>
<tr>
<th>Table 1 Command Syntax Guide</th>
</tr>
</thead>
<tbody>
<tr>
<td>Convention</td>
</tr>
<tr>
<td><strong>boldface</strong></td>
</tr>
<tr>
<td><strong>italic</strong></td>
</tr>
<tr>
<td>[     ]</td>
</tr>
<tr>
<td>{ x</td>
</tr>
</tbody>
</table>
CHAPTER 1-1

Catalyst 4500 Series Switch Cisco IOS Command Reference—Release IOS XE 3.5(0)XO

1-1

Command-Line Interface

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

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

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

Getting Help

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

<table>
<thead>
<tr>
<th>Command Purpose</th>
<th>Command Syntax</th>
</tr>
</thead>
</table>
| Displays a list of commands that begin with a particular character string. (Do not leave a space between the command and question mark.) | abbreviated-command-entry |?
| Completes a partial command name. | abbreviated-command-entry |<Tab>
| Lists all commands for the command mode. | command |?
| Lists all keywords for the command. Leave a space between the command and the question mark. | command |?
| Lists all arguments for the keyword. Leave a space between the keyword and the question mark. | command |keyword |?
Chapter 1      Command-Line Interface

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

<table>
<thead>
<tr>
<th>Command Purpose</th>
<th>Switch &gt; enable &lt;password&gt;</th>
<th>Switch #</th>
</tr>
</thead>
</table>
| 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

Enter interface configuration mode by specifying the Gigabit Ethernet interface that you want to configure using the interface gigabitethernet global configuration command. Enter a ? to display what you must enter next on the command line. In this example, you must enter an interface number from 1 to 9 in the format module-number/port-number.

You are in interface configuration mode when the prompt changes to Switch(config-if)#.
How to Find Command Options

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
disable            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
How to Find Command Options

Switch(config-if)#
channel-group ?
<1-256>  Channel group number

Switch(config-if)#channel-group
After you enter the group keyword, enter a ? to display what you must enter next on the command line. In this example, you must enter a channel group number from 1 to 256.

Switch(config-if)#channel-group 1 ?
mode  Etherchannel Mode of the interface

Switch(config-if)#
After you enter the channel group number, enter a ? to display what you must enter next on the command line. In this example, you must enter the mode keyword.

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)#
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.

Switch(config-if)#channel-group 1 mode auto ?
<cr>
Switch(config-if)#
In this example, the auto keyword is entered. After you enter the auto keyword, enter a ? to display what you must enter next on the command line.

Switch(config-if)#channel-group 1 mode auto
Switch(config-if)#
In this example, press Return to complete the command. If additional keywords are listed, you can enter more keywords or press Return to complete the command.

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

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>
<thead>
<tr>
<th>Command Mode Access Method</th>
<th>Prompt</th>
<th>Exit Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>User EXEC mode</td>
<td>Log in.</td>
<td>Switch&gt;</td>
</tr>
<tr>
<td>Privileged EXEC mode</td>
<td>From user EXEC mode, enter the enable EXEC command.</td>
<td>Switch#</td>
</tr>
<tr>
<td></td>
<td>To exit to user EXEC mode, enter the disable command.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>To enter global configuration mode, enter the configure terminal privileged EXEC command.</td>
<td></td>
</tr>
<tr>
<td>Global configuration mode</td>
<td>From privileged EXEC mode, enter the configure terminal privileged EXEC command.</td>
<td>Switch(config)#</td>
</tr>
<tr>
<td></td>
<td>To exit to privileged EXEC mode, enter the exit command or press Ctrl-Z.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>To enter interface configuration mode, enter an interface configuration command.</td>
<td></td>
</tr>
<tr>
<td>Interface configuration mode</td>
<td>From global configuration mode, enter by specifying an interface with an interface command.</td>
<td>Switch(config-if)#</td>
</tr>
<tr>
<td></td>
<td>To exit to global configuration mode, enter the exit command.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>To exit to privileged EXEC mode, enter the exit command or press Ctrl-Z.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>To enter subinterface configuration mode, specify a subinterface with the interface command.</td>
<td></td>
</tr>
</tbody>
</table>
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 though 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.

Table 1-3 Summary of Main Command Modes (continued)
Chapter 1      Command-Line Interface

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.

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.

```
\$
_ 
+
```

<table>
<thead>
<tr>
<th>Character</th>
<th>Special Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>.</td>
<td>Matches any single character, including white space.</td>
</tr>
<tr>
<td>*</td>
<td>Matches 0 or more sequences of the pattern.</td>
</tr>
<tr>
<td>+</td>
<td>Matches 1 or more sequences of the pattern.</td>
</tr>
<tr>
<td>?</td>
<td>Matches 0 or 1 occurrences of the pattern.</td>
</tr>
<tr>
<td>^</td>
<td>Matches the beginning of the string.</td>
</tr>
<tr>
<td>$</td>
<td>Matches the end of the string.</td>
</tr>
<tr>
<td>_ (underscore)</td>
<td>Matches a comma (,), left brace ({), right brace (}), left parenthesis ( ( ), right parenthesis ( ) ), the beginning of the string, the end of the string, or a space.</td>
</tr>
</tbody>
</table>
Using the CLI String Search

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:

\[a-d A-D\]

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

\[a-d A-D\-\]

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

\[a-d A-D\-\]\]

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.

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.

### Table 1-5 Special Characters Used as Multipliers

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Matches 0 or more single- or multiple-character patterns.</td>
</tr>
<tr>
<td>+</td>
<td>Matches 1 or more single- or multiple-character patterns.</td>
</tr>
<tr>
<td>?</td>
<td>Matches 0 or 1 occurrences of the single- or multiple-character patterns.</td>
</tr>
</tbody>
</table>
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.

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_
```

Table 1-6 Special Characters Used for Anchoring

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>^</td>
<td>Matches the beginning of the string.</td>
</tr>
<tr>
<td>$</td>
<td>Matches the end of the string.</td>
</tr>
</tbody>
</table>
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.

**Note**

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

```
[keyword1] [keyword2] [keyword3]
```

**Syntax Description**

**Defaults**

This command has no default settings.

**Command Modes**

Global configuration mode

**Usage Guidelines**

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

**Examples**

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

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

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

```
Switch(config-if)#
macro apply test
```

**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.
### macro keywords

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>macro apply cisco-desktop</td>
<td>Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a standard desktop.</td>
</tr>
<tr>
<td>macro apply cisco-phone</td>
<td>Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a standard desktop and a Cisco IP phone.</td>
</tr>
<tr>
<td>macro apply cisco-router</td>
<td>Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a router.</td>
</tr>
<tr>
<td>macro apply cisco-switch</td>
<td>Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to another switch.</td>
</tr>
</tbody>
</table>
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.

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

**Defaults**
Accounting is disabled.

**Command Modes**
Global configuration mode

**Usage Guidelines**
802.1X accounting requires a RADIUS server.

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

**Examples**
This example shows how to configure 802.1X accounting:

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

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

**Related Commands**
<table>
<thead>
<tr>
<th>Command Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>aaa accounting system default start-stop group radius</code></td>
</tr>
</tbody>
</table>

Receives the session termination messages after the switch reboots.
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.

Syntax Description
This command has no arguments or keywords.

Defaults
Accounting is disabled.

Command Modes
Global configuration mode

Usage Guidelines
802.1X accounting requires the RADIUS server.

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

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

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

**Syntax Description**

- **prefer port**
  - Specifies that the PACL mode take precedence if PACLs are configured. If no PACL features are configured on the port, other features applicable to the interface are merged and applied on the interface.

- **prefer vlan**
  - Specifies that the VLAN-based ACL mode take precedence. If no VLAN-based ACL features are configured on the port's VLAN, the PACL features on the port are applied.

- **merge**
  - Merges applicable ACL features before they are programmed into the hardware.

**Defaults**

- PACL override mode

**Command Modes**

- Interface configuration mode

**Usage Guidelines**

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

**Examples**

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

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

This example shows how to merge applicable ACL features:

```
(config-if) access-group mode merge
```
## Chapter 2

### Cisco IOS Commands for the Catalyst 4500 Series Switches

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-group mode</td>
<td>Displays the ACL configuration on a Layer 2 interface.</td>
</tr>
<tr>
<td>show access-group mode</td>
<td>Displays the IP interface configuration.</td>
</tr>
<tr>
<td>show ip interface</td>
<td>Displays the ACL configuration on a Layer 2 interface.</td>
</tr>
</tbody>
</table>

**Note:** `show ip interface` is a command from Cisco IOS documentation.
To select the mode of capturing control packets, use the `access-list hardware capture mode` command.

```
access-list hardware capture mode
  {
    global | vlan
  }
```

**Syntax Description**

- **global**: Specifies the capture of control packets globally on all VLANs.
- **vlan**: Specifies the capture of control packets on a specific VLAN.

**Defaults**

The control packets are globally captured.

**Command Modes**

Global configuration mode

**Usage Guidelines**

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

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

You must ensure that any access control configuration on a member port or VLAN does not deny or drop the control packets from being forwarded to the CPU for the features which are enabled on the VLAN. If control packets are not permitted then the specific feature does not function.

**Examples**

This example shows how to configure the switch to capture control packets on VLANs that are configured to enable capturing control packets:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# access-list hardware capture mode vlan
Switch(config)# end
Switch#
```

This example shows how to configure the switch to capture control packets globally across all VLANs (using a static ACL):

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# access-list hardware capture mode global
Switch(config)# end
Switch#
```

This example shows another way to configure the switch to capture control packets globally across all VLANs:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# no access-list hardware capture mode vlan
Switch(config)# end
Switch#
```
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

- **Defaults**
  - The ACLs are programmed as packed.

### Command Modes

- **Global configuration mode**

### Usage Guidelines

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

- **The goal is to use TCAM resources more efficiently:** that is, to minimize the number of masks per ACL entries. To compare TCAM utilization when using the `scattered` or `packed` 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

This 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#
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
```

- **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.
This 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
```

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

```
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#
```
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**

**Defaults**
The default region balance for each TCAM is 50.

**Command Modes**
Global configuration mode

**Usage Guidelines**
P and V is a TCAM region containing entries which mask in both the port and VLAN tag portions of the flow label.

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

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

Balances for the four TCAMs can be modified independently.

**Examples**

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

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

- **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** specifies relative sizes of the PandV and PorV regions in the TCAM; valid values are between 1 and 99.
To specify an action to be taken when a match occurs in a V ACL, use the `action` command. To remove an action clause, use the `no` form of this command.

```
action {
  drop | forward
}
```

**Syntax Description**

- **drop**: Sets the action to drop packets.
- **forward**: Sets the action to forward packets to their destination.

**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.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

To enable the destination profile, use the `active` command.

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

**Defaults**
This command has no default settings.

**Command Modes**
cfg-call-home-profile

**Usage Guidelines**
By default the profile is enabled upon creation.

**Examples**
This example shows how to enable the destination profile:

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

**Related Commands**

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

### Syntax Description

**Defaults**
This command has no default settings.

**Command Modes**
Global configuration mode

### Usage Guidelines

The ANCP server can use either the DHCP option 82 circuit ID or an identifier created with this command to identify the port. Use only one of the two methods; do not interchange them. If you use the DHCP option 82, the port identifier used by the ANCP server should be (in hex) 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

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

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

### Related Commands

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

### Command Description

- `ancp mode client`
  - Sets the router to become an ANCP client.
To set the IP address of the remote ANCP server, use the `ancp client server` command.

```
ancp client server
```

**Syntax Description**

This command has no default settings.

**Command Modes**

Global configuration mode

**Usage Guidelines**

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

Once you enter this command, the ANCP client tries to connect to the remote server.

**Examples**

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

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

**Related Commands**

- **ipaddr of server**: IP address of the ANCP server the client must connect with TCP.
- **interface**: Interface to use for the connection.

**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.

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Global configuration mode

**Usage Guidelines**

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

**Examples**

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

```
Switch# ancp mode client
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ancp client server</td>
<td>Displays multicast streams activated by ANCP.</td>
</tr>
</tbody>
</table>
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.

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

VLAN configuration mode

**Usage Guidelines**

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

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

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

**Examples**

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

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>exit</td>
<td>Closes an active terminal session by logging off the switch.</td>
</tr>
<tr>
<td>reset</td>
<td>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.</td>
</tr>
<tr>
<td>show vlan</td>
<td>Displays VLAN information.</td>
</tr>
<tr>
<td>shutdown vlan</td>
<td>(refer to Cisco IOS documentation)</td>
</tr>
<tr>
<td>vtp</td>
<td>(global configuration mode)</td>
</tr>
<tr>
<td>vtp</td>
<td>Modifies the name of a VTP configuration storage file.</td>
</tr>
</tbody>
</table>
To define an ARP access list or add clauses at the end of a predefined list, use the `arp access-list` command.

**Syntax Description**

This command has no default settings.

**Command Modes**

Global configuration mode

**Examples**

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

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

**Related Commands**

- `name`
  - Specifies the access control list name.
- `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.

**Syntax Description**

This command has no default settings.

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Usage Guidelines**

This command applies only to the Access Gateway Module on Catalyst 4500 series switches. The valid values for `mod` 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.

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

This command is identical in the resulting action to the `session module mod` and the `remote login module mod` commands.

**Examples**

This example shows how to remotely log in to an Access Gateway Module:

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>remo te login module</code></td>
</tr>
<tr>
<td><code>session module</code></td>
</tr>
</tbody>
</table>

**Command Target**

module for the command.
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**

- **Command Default**: both
- **Command Modes**: Interface configuration mode

**Usage Guidelines**

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

```

dot1x control-direction

both
in

no dot1x control-direction
```

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
```

The following example shows how to enable bidirectional control:
```
Switch(config-if)# authentication control-direction both
```

The following example shows how to return to the default settings:
```
Switch(config-if)# no authentication control-direction
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show authentication</td>
<td>Displays Authentication Manager information.</td>
</tr>
</tbody>
</table>
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 authentication critical recovery delay` command.

**Syntax**

```plaintext
authentication critical recovery delay milliseconds
```

**Command Default**

10000 milliseconds

**Command Modes**

Global configuration mode

**Usage Guidelines**

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

```
dot1x critical recovery delay milliseconds
```

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

**Examples**

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

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

**Related Commands**

- `milliseconds`: Specifies the recovery delay period in milliseconds to wait to reinitialize a critical port when an unavailable RADIUS server becomes available. The range is 1 to 10000 milliseconds.
- `show authentication`: Displays Authentication Manager information.
To configure the actions for authentication events, use the `authentication event` 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}

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

**Syntax Description**

- **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

- **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`

- **fail** Specifies the behavior when an authentication fails due to bad user credentials.
- **retry** (Optional) Specifies the number of times to retry failed authentications. Range is 0 to 5. Default is 2.
- **fail action** authorize vlan: 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 vlan]: Configures the AAA server dead actions to authorize data or voice clients for the authentication events.
- **server dead action** reinitialize vlan: 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.
The authentication event 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:

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

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

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

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

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

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

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show authentication</td>
<td>Displays Authentication Manager information.</td>
</tr>
</tbody>
</table>
To enable WebAuth fallback and to specify the fallback profile to use when failing over to WebAuth, use the `authentication fallback` command. To return to the default setting, use the `no` form of this command.

**Syntax Description**

`authentication fallback profile ...`

**Command Default**

Disabled

**Command Modes**

Interface configuration mode

**Usage Guidelines**

By default, if 802.1X times out and if MAB fails, WebAuth is enabled. The `authentication fallback` command replaces the following dot1x command, which is deprecated in Cisco IOS Release 12.2(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**

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

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

This example shows how to disable WebAuth fallback:

```bash
Switch(config-if)# no authentication fallback fallbacktest1
```

**Related Commands**

- `show authentication`
  
  Displays Authentication Manager information.
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 }
``` 

(Optional) Configures the host-mode with open policy on the port.

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

### Command Modes
Interface configuration mode

### Usage Guidelines

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

- **Multi-host** mode classifies the session as an interface session, but 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 single-host mode.
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**

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

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show authentication</code></td>
<td>Displays Authentication Manager information.</td>
</tr>
</tbody>
</table>
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 authentication open` command.

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Disabled.

**Command Modes**

Interface configuration mode

**Usage Guidelines**

Open Access allows clients or devices to gain network access before authentication is performed. You can verify your settings with the `show authentication` privileged EXEC command. This command overrides the `authentication host-mode session-type open` global configuration mode command for the port only. This command operates per-port rather than globally.

**Examples**

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

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

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

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

**Related Commands**

- `show authentication` Displays Authentication Manager information.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

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]]
```

### Syntax Description

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

**Command Modes**
Interface configuration mode

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

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

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

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

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

**Related Commands**
- `show authentication`:
  Displays Authentication Manager information.

**Notes**

- `method1`:
  Authentication method to be attempted. The valid values are as follows:
  - `dot1x`—Adds the dot1x authentication method.
  - `mab`—Adds the MAB authentication method.
  - `webauth`—Adds the WebAuth authentication method.
- `method2` and `method3`:
  (Optional) Authentication method to be attempted. The valid values are as follows:
  - `dot1x`—Adds the dot1x authentication method.
  - `mab`—Adds the MAB authentication method.
  - `webauth`—Adds the WebAuth authentication method.
To enable reauthentication for this port, use the `authentication periodic` command in interface configuration mode. To disable reauthentication for this port, use the `no authentication periodic` command.

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Disabled.

**Command Modes**

Interface configuration mode.

**Usage Guidelines**

The reauthentication period can be set using the `authentication timer` command. You can verify your settings by entering the `show authentication` privileged EXEC command.

**Examples**

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

Switch(config-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**

- `authentication timer`: Configures the authentication timer.
- `show authentication`: Displays Authentication Manager information.
To configure the port-control value, use the `authent ica tion 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>`: Enables 802.1X port-based authentication and causes the port to begin in the unauthorized state.
- `<force-authorized>`: 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>`: Denies all access through this interface by forcing the port to change to the unauthorized state, ignoring all attempts by the client to authenticate.

**Command Default**

- `force-authorized`

**Command Modes**

- Interface configuration mode

**Usage Guidelines**

The following guidelines apply to Ethernet switch network modules:

- The 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 (Optional) Enables 802.1X port-based authentication and causes the port to begin in the unauthorized state.

The `no` form of this command.

The `force-authorized` keyword is the default.

The `force-unauthorized` 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 (Optional) Enables 802.1X port-based authentication and causes the port to begin in the unauthorized state.

The `force-unauthorized` 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 (Optional) Enables 802.1X port-based authentication and causes the port to begin in the unauthorized state.

The `force-unauthorized` 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 (Optional) Enables 802.1X port-based authentication and causes the port to begin in the unauthorized state.
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show authentication</td>
<td>Displays Authentication Manager information.</td>
</tr>
</tbody>
</table>
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.

```
method1 [method2 [method3]]
```

**Syntax Description**

- **Command Default**: The default order is dot1x, MAB, then webauth.
- **Command Modes**: Interface configuration mode
- **Usage Guidelines**: Configuring priorities for authentication methods allows a higher priority method (not currently running) to interrupt an authentication in progress with a lower priority method. Alternatively, if the client is already authenticated, an interrupt from a higher priority method can cause a client, which was previously authenticated using a lower priority method, to reauthenticate.
- You can verify your settings with the `show authentication` privileged EXEC command.

**method1**

- **Authentication method to be attempted**. The valid values are as follows:
  - `dot1x` — Adds the dot1x authentication method.
  - `mab` — Adds the MAB authentication method.
  - `webauth` — Adds the Webauth authentication method.

**method2**, **method3**

(Optional) Authentication method to be attempted. The valid values are as follows:

- `dot1x` — Adds the dot1x authentication method.
- `mab` — Adds the MAB authentication method.
- `webauth` — Adds the Webauth authentication method.
Chapter 2 Cisco IOS Commands for the Catalyst 4500 Series Switches

authentication priority

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.
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

- **Command Default:**
  - `inactivity value`: Off.
  - `reauthenticate value`: 3600
  - `restart value`: Off

- **Command Modes:** Interface configuration mode

### Usage Guidelines

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

- **inactivity value**: Specifies the amount of time in seconds that a host is allowed to be inactive before being authorized. Range is 1 to 65535. Default is Off.
  - Note: The inactivity value should be less than the reauthenticate 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 value**: Specifies the amount of time in seconds after which an automatic reauthentication is initiated. Range is 1 to 65535. Default is 3600.

- **restart value**: Specifies the amount of time in seconds after which an attempt is made to authenticate an unauthorized port. Range is 1 to 65535. Default is Off.
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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show authentication</td>
<td>Displays Authentication Manager information.</td>
</tr>
</tbody>
</table>
Use the `authentication violation` 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 multiple-host or multiauthentication mode.

```
{ restrict | shutdown | replace }
```

**Syntax Description**
- **Defaults:** Shut down the port. If the `restrict` keyword is configured, the port does not shutdown.

**Command Modes**
- Interface configuration

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

**Examples**
This 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**
- `restrict`: Generates a syslog error when a violation error occurs.
- `shutdown`: Error disables the [virtual] port on which an unexpected MAC address occurs.
- `replace`: Replaces the existing host with the new host, instead of errordisabling or restricting the port.
Chapter 2  Cisco IOS Commands for the Catalyst 4500 Series Switches

**authentication violation**

Sets the authorization manager mode on a port.

**authentication order**

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 a 802.1x-enabled port.

**show authentication**

 Displays information about authentication manager events on the switch.
To generate a QoS configuration for an untrusted interface, use the `auto qos classify` command.

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Interface configuration mode

**Usage Guidelines**

This command generates a QoS configuration for untrusted interfaces. It places a service-policy to classify the traffic coming from untrusted desktops or devices and marks them accordingly. The service-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.

```plaintext
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
```
auto qos classify
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
auto qos 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 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
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
Chapter 2      Cisco IOS Commands for  the Catalyst 4500 Series Switches

auto qos classify

Examples

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

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

Related Commands

- 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.
To police traffic from an untrusted interface, use the `auto qos classify police` command.

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Interface configuration mode

**Usage Guidelines**

This command generates a QoS configuration for untrusted interfaces. It places a service-policy to classify the traffic arriving from these untrusted desktops or devices and marks them accordingly. The generated service-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
```
auto qos classify police

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.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

auto qos classify police
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
accomodate 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 qosclassify police command, traffic flows that violate the defined rate limit are remarked to cs1 but retain
auto qos class

classify police

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
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
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-Police-Input-Policy

service-policy output AutoQos-4.0-Output-Policy

Examples

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

Switch(config)#

interface gigabitethernet1/1

Switch(config-if)#

auto qos classify police

Switch(config-if)#

do sh run interface
gigabitethernet1

Interface gigabitethernet1

auto qos classify police

service-policy input AutoQos-4.0-Classify-Police-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.

Syntax Description
This command has no arguments or keywords.

Defaults
This command has no default settings.

Command Modes
Global configuration

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

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

Typically, a command generates a series of class-maps that either match on ACLs or on DSCP and CoS values 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
auto qos srnd4

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, 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
auto qos srnd4
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 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
auto qos srnd4

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 configurations for interfaces connected to PCs running the Cisco IP SoftPhone application and marks police traffic coming from such interfaces.
To generate QoS configurations for trusted interfaces, use the `auto qos trust` command.

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Interface configuration mode

**Usage Guidelines**

**Global Level Commands Generated**

After you apply auto-QoS 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.

**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`, 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
```
Catalyst 4500 Series Switch Cisco IOS Command Reference—Release IOS XE 3.3.0XO(15.1(1)XO)

Chapter 2      Cisco IOS Commands for  the Catalyst 4500 Series Switches

auto qos trust
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
auto qos trust
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
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
This 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 trust
Generates a QoS configuration for an untrusted interface.

auto qos classify
Generates QoS configurations based on solution reference network design 4.0.
auto qos video

To generate QoS configuration for Cisco TelePresence or Cisco video surveillance camera interfaces (conditional trust through CDP), use the `auto qos video` interface configuration command.

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

**Syntax Description**

**Defaults**

This command has no default settings.

**Command Modes**

Interface configuration mode

**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 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
```
auto qos video
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
auto qos video
class-map match-all AutoQos-4.0-Multimedia-Conf-Queue
match qos-group 26
match qos-group 34
match qos-group 18
match qos-group 10
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

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

Examples

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

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

- `auto qos trust` Generates QoS configurations for trusted interfaces.
- `auto qos srnd4` Generates QoS configurations based on solution reference network design 4.0.
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}
```

**Syntax Description**

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

**Defaults**

Auto-QoS is disabled on all interfaces.

**Command Modes**

Interface configuration mode

**Usage Guidelines**

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

Apply the `cisco-phone` keyword on those ports (at the edge of the network) that are connected to Cisco IP phones. The switch 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**

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

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

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

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

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

```
Switch#
configure terminal
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**

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

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Interface configuration mode

**Usage Guidelines**

Ports configured with `auto qos voip` command are considered untrusted.

**Global Level Commands Generated**

After auto-QoS 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
```
auto qos voip cisco-softphone

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
  class-map match-all AutoQos-4.0-Signaling-Classify
  class-map match-all AutoQos-4.0-Transaction-Classify
  class-map match-all AutoQos-4.0-Bulk-Data-Classify

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
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

auto qos voip cisco-softphone
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
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 remapped 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
  class AutoQos-4.0-Bulk-Data-Queue
    bandwidth remaining percent 4
  class class-default
    bandwidth remaining percent 25
  interface GigabitEthernet1/1

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

Switch(config)# interface gigabitethernet1/1
Switch(config-if)# auto qos voip cisco-softphone
Switch(config-if)# 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
 Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto qos voip cisco-softphone</td>
<td>Generate QoS configuration for interfaces connected to PCs running the Cisco IP SoftPhone application and marks police traffic coming from such interfaces.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto qos classify</td>
<td>Generate a QoS configuration for an untrusted interface.</td>
</tr>
<tr>
<td>auto qos classify police</td>
<td>Police traffic form an untrusted interface.</td>
</tr>
</tbody>
</table>
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**

- **Defaults**: Standard automatic synchronization of all configuration files.
- **Command Modes**: Redundancy main-cpu mode.

**Usage Guidelines**

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

**Examples**

This example 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
```

**Related Commands**

- `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 BOOTV AR configuration.
- `standard`: Specifies automatic synchronization of the startup configuration, BOOTV AR, and configuration registers.

**Command Description**

- `redundancy`: Enters the redundancy configuration mode.
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 }
```

**Syntax Description**

- **Defaults**: No bandwidth is specified.
- **Command Modes**: Policy-map class configuration mode
- **Usage Guidelines**: Use the `bandwidth` command only in a policy map attached to a physical port. The `bandwidth` command specifies the minimum bandwidth for traffic in that class when there is traffic congestion in the switch. If the switch is not congested, the class receives more bandwidth than you specify with this command. When queuing class is configured without any explicit bandwidth configuration, since the queue is not guaranteed any minimum bandwidth, this queue will get a share 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**

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

```
bandwidth-kbps
Amount of bandwidth in kbps assigned to the class. The range is 32 to 16000000.
percent
Percentage of available bandwidth assigned to the parent class. The range is 1 to 100.
remaining percent
Percentage of remaining bandwidth assigned to parent class. The range is 1 to 100. This command is supported only when priority queuing class is configured, and the priority queuing class is not rate-limited.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

This example shows how to guarantee 30 percent of the bandwidth for class 1 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
```

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

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>class</code></td>
<td>Specifies the name of the class whose traffic policy you want to create or change.</td>
</tr>
<tr>
<td><code>dbl</code></td>
<td>Enables active queue management on a transmit queue used by a class of traffic.</td>
</tr>
<tr>
<td><code>policy-map</code></td>
<td>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.</td>
</tr>
</tbody>
</table>
Chapter 2  Cisco IOS Commands for the Catalyst 4500 Series Switches

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.
call-home (global configuration)

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

call-home

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Global configuration mode

Usage Guidelines

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

- alert-group
  - 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.
call-home (global configuration)

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

Examples

```
This example shows how to configure the contact information:
Switch# 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)#
```

```
This example shows how to configure the call-home message rate-limit threshold:
Switch(config)# call-home
Switch(cfg-call-home)# rate-limit 50
```

```
This example shows how to set the call-home message rate-limit threshold to the default setting:
Switch(config)# call-home
Switch(cfg-call-home)# default rate-limit
```

```
This example shows how to create a new destination profile with the same configuration settings as an existing profile:
Switch(config)# call-home
Switch(cfg-call-home)# copy profile profile1 profile1a
```

```
This example shows how to configure the general e-mail parameters, including a primary and secondary e-mail server:
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# call-home
Switch(cfg-call-home)# mail-server smtp.example.com priority 1
Switch(cfg-call-home)# mail-server 192.168.0.1 priority 2
Switch(cfg-call-home)# sender from username@example.com
Switch(cfg-call-home)# sender reply-to username@example.com
Switch(cfg-call-home)# exit
Switch(config)#
```

```
This example shows how to specify MgmtVrf as the vrf name where the call-home email message is forwarded:
Switch(cfg-call-home)# vrf MgmtVrf
```
Chapter 2      Cisco IOS Commands for  the Catalyst 4500 Series Switches

call-home (global configuration)

Related Commands

- `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.
To submit information about your system to Cisco for report and analysis using the 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 } ]

Syntax Description
Command Default
This command has no default settings.

Command Modes
Privileged EXEC mode

Usage Guidelines
The recipient profile does not need to be enabled for the call-home request. The profile should specify the e-mail address where the transport gateway is configured so that the request message can be forwarded to the Cisco TAC and the user can receive the reply from the Smart Call Home service.

Based on the keyword specifying the type of report requested, the following information is returned in response to the request:

- `config-sanity` — Information on best practices as related to the current running configuration.
- `bugs-list` — Known bugs in the running version and in the currently applied features.
- `command-reference` — Reference links to all commands in the running configuration.
- `product-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
This example shows a request for analysis of a user-specified show command:

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

**Output-Analysis**
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**
**name** (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**
**user-id** (Optional) Specifies the identifier of a registered Smart Call Home user. If a user-id is specified, the resulting analysis report is sent to the e-mail address of the registered user. If no user-id is specified, the report is sent to the contact e-mail address of the device.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

call-home request

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

```
cli-command
```

**Syntax Description**

**Command Default**
No default settings.

**Command Modes**
Privileged EXEC mode

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

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

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

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

**Related Commands**
- `call-home (global configuration)`
- `call-home send alert-group`
- `service call-home`

Enables or disables Call Home.

- `show call-home`

Displays call-home configuration information.
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**

- **Command Default:** This command has no default settings.
- **Command Modes:** Privileged EXEC mode
- **Usage Guidelines:**
  - When you enter the module number, you can enter the number of the module.
  - If you do not specify the `profile profile-name`, the message is sent to all subscribed destination profiles.
  - Only the configuration, diagnostic, and inventory alert groups can be manually sent. The destination profile need not be subscribed to the alert group.

**Examples**

- This example shows how to send the configuration alert-group message to the destination profile:
  ```
  Switch# call-home send alert-group configuration
  ```
- This example shows how to send the diagnostic alert-group message to the destination profile for a specific module number:
  ```
  Switch# call-home send alert-group diagnostic module 3
  ```
- This example shows how to send the diagnostic alert-group message to all destination profiles for a specific module number:
  ```
  Switch# call-home send alert-group diagnostic module 3 profile Ciscotac1
  ```
- This example shows how to send the inventory call-home message:
  ```
  Switch# call-home send alert-group inventory
  ```

**Related Commands**

- `configuration` Sends the configuration alert-group message to the destination profile.
- `diagnostic module number` Sends the diagnostic alert-group message to the destination profile for a specific module number.
- `inventory` Sends the inventory call-home message.
- `profile profile-name` (Optional) Specifies the name of the destination profile.
- `call-home (global configuration)` Enters call home configuration mode.
- `call-home test` Sends a call-home test message that you define.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

call-home send alert-group

Enables or disables Call Home.

show call-home
Displays call-home configuration information.
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**

- `test-message`: (Optional) Test message text.
- `profile`: profile-name

**Command Default**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Usage Guidelines**

This command sends a test message to the specified destination profile. If you enter test message text, you must enclose the text in quotes ("""") if it contains spaces. If you do not enter a message, a default message is sent.

**Examples**

This example shows how to manually send a Call Home test message:

```
Switch# call-home test "test of the day" profile Ciscotac1
```

**Related Commands**

- `call-home`: (global configuration) Enters call home configuration mode.
- `call-home send alert-group`: Sends a specific alert group message.
- `service call-home`: Enables or disables Call Home.
- `show call-home`: Displays call-home configuration information.
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]
}
```

**Syntax Description**

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

**Defaults**

No channel groups are assigned.

**Command Modes**

Interface configuration mode

**Usage Guidelines**

- You do not have to create a port-channel interface before assigning a physical interface to a channel group. If a port-channel interface has not been created, it is automatically created when the first physical interface for the channel group is created.
- If a specific channel number is used for the PAgP-enabled interfaces of a channel group, that same channel number cannot be used for configuring a channel that has LACP-enabled interfaces or vice versa.
- You can also create port channels by entering the `interface port-channel` command. This will create a Layer 3 port channel. To change the Layer 3 port channel into a 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 on mode a usable EtherChannel by connecting two port groups together.
Caution
Do not enable Layer 3 addresses on the physical EtherChannel interfaces. Do not assign bridge groups on the physical EtherChannel interfaces because it creates loops.

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

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

Related Commands
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface port-channel</td>
<td>Accesses or creates a port-channel interface.</td>
</tr>
<tr>
<td>show interfaces port-channel</td>
<td>Displays the information about the Fast EtherChannel.</td>
</tr>
</tbody>
</table>
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}
```

**Syntax Description**

- **lacp**: Enables LACP to manage channeling.
- **pagp**: Enables PAgP to manage channeling.

**Defaults**

```
pagp
```

**Command Modes**

Interface configuration mode

**Usage Guidelines**

- You can also select the protocol using the `channel-group` command.
- If the interface belongs to a channel, the `no` form of this command is rejected.
- All ports in an EtherChannel must use the same protocol; you cannot run two protocols on one module.
- PAgP and LACP are not compatible; both ends of a channel must use the same protocol.
- You can manually configure a switch with PAgP on one side and LACP on the other side in the `on` mode.
- You can change the protocol at any time, but this change causes all existing EtherChannels to reset to the default channel mode for the new protocol. You can use the `channel-protocol` command to restrict anyone from selecting a mode that is not applicable to the selected protocol.
- Configure all ports in an EtherChannel to operate at the same speed and duplex mode (full duplex only for LACP mode).
- For a complete list of guidelines, refer to the “Configuring EtherChannel” section of the Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide.

**Examples**

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

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

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

## Chapter 2  Cisco IOS Commands for the Catalyst 4500 Series Switches

<table>
<thead>
<tr>
<th>channel-protocol</th>
<th>Assigns and configures an EtherChannel interface to an EtherChannel group.</th>
</tr>
</thead>
<tbody>
<tr>
<td>show etherchannel</td>
<td>Displays EtherChannel information for a channel.</td>
</tr>
</tbody>
</table>
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

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**

- **Defaults:** None
- **Command Modes:** Global configuration

**Usage Guidelines**

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

**Examples**

This example shows how to enable CISP:

```
switch(config) #
cisp enable
```

**Related Commands**

- `cisp enable`: Enable CISP.
- `dot1x credentials (global configuration)`: Configures a profile on a supplicant switch.
- `show cisp (IOS command)`: Displays CISP information for a specified interface.
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.

### Syntax Description

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

### Command Modes

Policy-map configuration mode

### Usage Guidelines

Before using the `class` command, you must create a class map for matching packets to the class by using the `class-map` global configuration command. You also must use the `policy-map` global configuration command to 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 `policer` command. For more information about the two-rate policer, see the `policer (two rates)` and the `policer (percent)` command.
- `priority`: Enables the strict priority queue for a class of traffic. For more information, see the `priority` command.
Chapter 2  Cisco IOS Commands for the Catalyst 4500 Series Switches

class

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 (for example, set policies to police or to shape it) just like any other traffic class, but you cannot delete it.

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

Examples

This example shows how to create a policy map called policy1. When attached to an ingress port, the policy matches all the inbound traffic defined in class1, sets the IP DSCP to 10, and polices the traffic at an average rate of 1 Mbps and bursts of 20 KB. 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

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

**Syntax Description**

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

**Defaults**

No class maps are defined.

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

**Command Modes**

- Global configuration mode

**Usage Guidelines**

Use this command to specify the name of the class for which you want to create or modify class-map match criteria and to enter class-map configuration mode. Packets are checked against the match criteria configured for a class map to decide if the packet belongs to that class. If a packet matches the specified criteria, the packet is considered a member of the class and is forwarded according to the quality of service (QoS) specifications set in the traffic policy.

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

- `description` Describes the class map (up to 200 characters). The `show class-map` privileged EXEC command displays the description and the name of the class map.
- `exit` Exits from QoS class-map configuration mode.
- `match` Configures classification criteria. For more information, see the `match (class-map configuration)` command.
- `no` Removes a match statement from a class map.

**Examples**

This example shows how to configure the class map called `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
```

**match-all**

(Optional) Perform a logical-AND of all matching under this class map. All criteria in the class map must be matched.

**match-any**

(Optional) Perform a logical-OR of the matching statements under this class map. One or more criteria in the class map must be matched.

**class-map-name**

Name of the class map.
This 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.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>class</code></td>
<td>Specifies the name of the class whose traffic policy you want to create or change.</td>
</tr>
<tr>
<td><code>match</code></td>
<td>Defines the match criteria for a class map.</td>
</tr>
<tr>
<td><code>policy-map</code></td>
<td>Creates a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.</td>
</tr>
<tr>
<td><code>show class-map</code></td>
<td>Displays class map information.</td>
</tr>
</tbody>
</table>
To clear the interface counters, use the `clear counters` command.

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

Defaults
This command has no default settings.

Command Modes
Privileged EXEC mode

Usage Guidelines
This command clears all the current interface counters from all the interfaces unless you specify an interface.

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

Examples
This example shows how to clear all the interface counters:
```
Switch# clear counters
Clear "show interface" counters on all interfaces [confirm] y
Switch#
```

This example shows how to clear the counters on a specific interface:
```
Switch# clear counters vlan 200
Clear "show interface" counters on this interface [confirm] y
Switch#
```

Related Commands
- `show interface counters` (refer to Cisco IOS documentation)
  Displays interface counter information.
To re-enable error-disabled VLANs on an interface, use the `clear errdisable` command.

```
clear errdisable interface {name} vlan [range]
```

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

**Defaults**
This command has no default settings.

**Command Modes**
Global configuration mode

**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.

**Examples**
This 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**
- `interface name`: Specifies the interface of the VLAN(s) to recover.
- `vlan`: Specifies all VLANs on the interface be recovered.
- `range` (Optional): Specifies the VLAN range to be recovered.
- `errdisable detect`: Enables error-disable detection.
- `show errdisable detect`: Displays the error-disable detection status.
- `show interfaces status`: Displays the interface status or a list of interfaces in error-disabled state.
- `switchport port-security`: Enables port security on an interface.
To clear the password on an intelligent line module, use the `clear hw-module slot password` command.

**Syntax Description**

**Command Modes**

*Privileged EXEC mode*

**Defaults**

The password is not cleared.

**Usage Guidelines**

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

**Examples**

This example shows how to clear the password from slot 5 on a line module:

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

**Related Commands**

- `slot_num`:
  - Slot on a line module.
- `hw-module power`:
  - Turns the power off on a slot or line module.
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.

### Syntax Description

**clear interface gigabitethernet**

**Defaults**
This command has no default settings.

**Command Modes**
Privileged EXEC mode

### Examples

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

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

**Related Commands**

- **show interfaces status**
  Displays the interface status.
To clear the hardware logic from a VLAN, use the `clear interface vlan` command.

```
Switch# clear interface vlan 5
Switch#
```

Syntax Description

This command has no default settings.

Command Modes

Privileged EXEC mode

Related Commands

- **number**: Number of the VLAN interface; valid values are from 1 to 4094.
- **show interfaces status**: Displays the interface status.
To clear the statistical information in access lists, use the `clear ip access-template` command.

Access-list

Number of the access list; valid values are from 100 to 199 for an IP extended access list, and from 2000 to 2699 for an expanded range IP extended access list.
To clear the status of the log buffer, use the `clear ip arp inspection log` command.

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Examples**

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

```
Switch# clear ip arp inspection log
Switch#
```
To clear the dynamic ARP inspection statistics, use the `clear ip arp inspection statistics` command.

Syntax Description
- `vlan` (Optional) Specifies the VLAN range.

Command Modes
- Privileged EXEC mode

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

```
Switch# clear ip arp inspection statistics vlan 1
Switch# show ip arp inspection statistics vlan 1
Vlan      Forwarded        Dropped     DHCP Drops     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
- `vlan`
- `vlan-range`

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.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

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

**Syntax Description**

- `clear ip dhcp snooping binding [ip-address] [vlan vlan_num] [interface interface_num]`

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Usage Guidelines**

These commands are mainly used to clear DHCP snooping binding entries. DHCP snooping is enabled on a VLAN only if both the global snooping and the VLAN snooping are enabled.

**Examples**

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

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

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

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

This 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#
```

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

```
Switch# clear ip dhcp snooping binding vlan 40
Switch#
```
# Chapter 2  
Cisco IOS Commands for the Catalyst 4500 Series Switches

## clear ip dhcp snooping binding

<table>
<thead>
<tr>
<th>Command Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ip dhcp snooping</strong></td>
</tr>
<tr>
<td><strong>ip dhcp snooping binding</strong></td>
</tr>
<tr>
<td><strong>ip dhcp snooping information option</strong></td>
</tr>
<tr>
<td><strong>ip dhcp snooping trust</strong></td>
</tr>
<tr>
<td><strong>ip dhcp snooping vlan</strong></td>
</tr>
<tr>
<td><strong>show ip dhcp snooping</strong></td>
</tr>
<tr>
<td><strong>show ip dhcp snooping binding</strong></td>
</tr>
</tbody>
</table>
To clear the DHCP binding database, use the `clear ip dhcp snooping database` command.

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Examples**

This example shows how to clear the DHCP binding database:

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip dhcp snooping</code></td>
<td>Globally enables DHCP snooping.</td>
</tr>
<tr>
<td><code>ip dhcp snooping binding</code></td>
<td>Sets up and generates a DHCP binding configuration to restore bindings across reboots.</td>
</tr>
<tr>
<td><code>ip dhcp snooping information option</code></td>
<td>Enables DHCP option 82 data insertion.</td>
</tr>
<tr>
<td><code>ip dhcp snooping trust</code></td>
<td>Enables DHCP snooping on a trusted VLAN.</td>
</tr>
<tr>
<td><code>ip dhcp snooping vlan</code></td>
<td>Enables DHCP snooping on a VLAN or a group of VLANs.</td>
</tr>
<tr>
<td><code>show ip dhcp snooping</code></td>
<td>Displays the DHCP snooping configuration.</td>
</tr>
<tr>
<td><code>show ip dhcp snooping binding</code></td>
<td>Displays the DHCP snooping binding entries.</td>
</tr>
</tbody>
</table>
To clear the DHCP binding database statistics, use the `clear ip dhcp snooping database statistics` command.

### Syntax Description

This command has no arguments or keywords.

### Defaults

This command has no default settings.

### Command Modes

Privileged EXEC mode

### Examples

This example shows how to clear the DHCP binding database:

```
Switch# clear ip dhcp snooping database statistics
Switch#
```
To delete the IGMP group cache entries, use the `clear ip igmp group` command.

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

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Usage Guidelines**

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

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

**Examples**

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

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

This 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip host</td>
<td>Defines a static host name-to-address mapping in the host cache.</td>
</tr>
<tr>
<td>show ip igmp groups</td>
<td>Displays the multicast groups with receivers that are directly connected to</td>
</tr>
<tr>
<td></td>
<td>the router and that were learned through Internet Group Management Protocol</td>
</tr>
<tr>
<td></td>
<td>(IGMP), use the show ip igmp groups command in EXEC mode.</td>
</tr>
<tr>
<td>show ip igmp interface</td>
<td>Displays the information about the IGMP-interface status and configuration.</td>
</tr>
</tbody>
</table>
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** (Optional) Specifies a VLAN; valid values are from 1 to 1001 and from 1006 to 4094.

**Defaults**
This command has no default settings.

**Command Modes**
Privileged EXEC mode

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

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

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

**Related Commands**
- `ip igmp snooping vlan explicit-tracking`: Enables per-VLAN explicit host tracking.
- `show ip igmp snooping membership`: Displays host membership information.
To clear the global MFIB counters and the counters for all active MFIB routes, use the `clear ip mfib counters` command.

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Examples**

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

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip mfib</code></td>
<td>Displays all active Multicast Forwarding Information Base (MFIB) routes.</td>
</tr>
</tbody>
</table>
To clear all the MFIB fast-drop entries, use the `clear ip mfib fastdrop` command.

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

### Defaults
This command has no default settings.

### Command Modes
Privileged EXEC mode

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

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

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

### Related Commands
- `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.
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**
- **Defaults**: No default behavior or values.
- **Command Modes**: Privileged EXEC (##)

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

**Examples**

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

**Related Commands**
- `web-cache` (Optional) Directs the router to remove statistics for the web cache service.
- `service-number` (Optional) Number of the cache service to be removed. The number can be from 0 to 99.

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

```
clear lacp [channel-group]
```

**Syntax Description**
- channel-group: (Optional) Channel-group number; valid values are from 1 to 64.

**Defaults**
This command has no default settings.

**Command Modes**
- Privileged EXEC mode

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

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

**Related Commands**
- `channel-group`: Command Description
- `show lacp`: Displays LACP information.
To clear the global counter entries from the Layer 2 MAC address table, use the `clear mac-address-table` command.

**Syntax Description**

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

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Usage Guidelines**

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

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

**Examples**

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

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

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

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

**dynamic**

Specifies dynamic entry types.

**address**

mac_addr

(Optional) Specifies the MAC address.

**interface**

(Optional) Specifies the interface and clears the entries associated with it; valid values are FastEthernet and GigabitEthernet.

**vlan**

vlan_id

(Optional) Specifies the VLANs; valid values are from 1 to 4094.

**notification**

Specifies MAC change notification global counters.
clear mac-address-table

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

Syntax Description
- `address <mac_addr>`: Specifies the MAC address.
- `interface <interface>`: Specifies the interface and clears the entries associated with it; valid values are `FastEthernet` and `GigabitEthernet`.
- `vlan <vlan_id>`: Specifies the VLANs; valid values are from 1 to 4094.

Defaults
This command has no default settings.

Command Modes
- Privileged EXEC mode

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

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

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

Related Commands
- `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 synchronize the configurations on two supervisor engines.
- `show mac-address-table address`: Displays the information about the MAC-address table.
To clear the Network Mobility Services Protocol (NMSP) statistics, use the `clear nmsp statistics` command. This command is available only when your switch is running the cryptographic (encrypted) software image.

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

**Defaults**
No default is defined.

**Command Modes**
Privileged EXEC mode

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

```
Switch# clear nmsp statistics
Switch# You can verify that information was deleted by entering the `show nmsp statistics` command.
```

**Related Commands**
- `show nmsp`
  Displays the NMSP information.
To clear the port-channel information, use the `clear pagp` command.

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

**Syntax Description**

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

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Examples**

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

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

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

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

**Related Commands**

- `show pagp`: Displays information about the port channel.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

clear port-security

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

clear port-security dynamic

[address mac-addr]
[vlan vlan-id]
[interface interface-id]
[vlan access | vlan voice]

Syntax Description

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

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

Note

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

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

Examples

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

Switch# clear port-security dynamic

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

Switch# clear port-security dynamic address 0008.0070.0007

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

Switch# clear port-security dynamic interface gigabitethernet0/1

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

Related Commands

- `show port-security` Displays information about the port-security setting.
- `switchport port-security` Enables port security on an interface.
To clear PPPoE Intermediate Agent statistics (packet counters), use the `clear pppoe intermediate-agent statistics` command.

### Syntax Description

This command has no default settings.

### Command Modes

Privileged EXEC mode

### Examples

This example shows how to clear PPPoE Intermediate Agent statistics:

```
Switch# clear pppoe intermediate-agent statistics
```
To clear the global and per-interface aggregate QoS counters, use the `clear qos` command.

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

**Syntax Description**
- `aggregate-policer name`: Specifies an aggregate policer.
- `interface fastethernet | GigabitEthernet`: Specifies an interface.
- `mod/interface`: Number of the module and interface.
- `vlan vlan_num`: Specifies a VLAN.
- `port-channel number`: Specifies the channel interface; valid values are from 1 to 64.

**Defaults**
This command has no default settings.

**Command Modes**
Privileged EXEC mode

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

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

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

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

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

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

**Related Commands**
- `aggregate-policer name` (Optional) Specifies an aggregate policer.
- `interface fastethernet | GigabitEthernet` (Optional) Specifies an interface.
- `mod/interface` (Optional) Number of the module and interface.
- `vlan vlan_num` (Optional) Specifies a VLAN.
- `port-channel number` (Optional) Specifies the channel interface; valid values are from 1 to 64.

**Command Description**
- `show qos` Displays QoS information.
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**

- **Defaults**: This command has no default settings.
- **Command Modes**: Privileged EXEC mode
- **Usage Guidelines**: If you do not specify a `vlan-id` value, the software-cached counter values for all the existing VLANs are cleared.

**Examples**

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

```
Switch# clear vlan 10 counters
Clear "show vlan" counters on this vlan [confirm] y
Switch#
```

**Related Commands**

- `vlan-id` (Optional) VLAN number; see the "Usage Guidelines" section for valid values.
- `show vlan counters` Displays VLAN counter information.
To clear the VMPS statistics, use the `clear vmps statistics` command.

This command has no arguments or keywords.

This command has no default settings.

Command Modes

- Privileged EXEC mode

Examples

This example shows how to clear the VMPS statistics:

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

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show vmps</code></td>
<td>Displays VMPS information.</td>
</tr>
<tr>
<td><code>vmps reconfirm</code> (privileged EXEC)</td>
<td>Changes the reconfirmation interval for the VLAN Query Protocol (VQP) client.</td>
</tr>
</tbody>
</table>
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.

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

Default service policy `system-cpp-policy` is attached.

**Command Modes**

Global configuration mode

**Usage Guidelines**

After you enter the `control-plane` command, you can define control plane services for your 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
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>class</td>
<td>Specifies the name of the class whose traffic policy you want to create or change.</td>
</tr>
<tr>
<td>class-map</td>
<td>Creates a class map to be used for matching packets to the class whose name you specify and to enter class-map configuration mode.</td>
</tr>
<tr>
<td>match access-group</td>
<td>Configures the match criteria for a class map on the basis of the specified access control list (ACL).</td>
</tr>
<tr>
<td>policy-map</td>
<td>Creates a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.</td>
</tr>
<tr>
<td>service-policy</td>
<td>Attaches a policy map to an interface.</td>
</tr>
<tr>
<td>show policy-map control-plane</td>
<td>Displays the configuration either of a class or of all classes for the policy map of a control plane.</td>
</tr>
</tbody>
</table>
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

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

```
counter {ipv4 | ipv6 | ipv4 ipv6 separate}
```

**Defaults**
Not enabled

**Command Modes**
Interface configuration

**Usage Guidelines**
Entering the `counter` command without keywords displays the statistics as a sum. The total number of switch ports that can 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.

- `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.
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#
```

In this situation, you must release a counter from another interface so the new interface can use it.
To enable active queue management on a transmit queue used by a class of traffic, use the `dbl` command. Use the `no` form of this command to return to the default setting.

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

**Defaults**
Active queue management is disabled.

**Command Modes**
Policy-map class configuration

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

**Examples**
This example shows how to enable dbl action in a class:

```
Switch# configure terminal
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# dbl
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet 1/1
Switch(config-if)# service-policy output policy1
Switch(config-if)# end
```

**Related Commands**
- `bandwidth`: Creates a signaling class structure that can be referred to by its name.
- `class`: Creates a class map to be used for matching packets to the class whose name you specify and to enter class-map configuration mode.
- `policy-map`: Creates a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.
- `service-policy (policy-map class)`: Creates a service policy that is a quality of service (QoS) policy within a policy map.
- `show policy-map`: Displays information about the policy map.
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
```

### Syntax Description

This command has no default settings.

### Command Modes

Privileged EXEC mode

### Examples

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

```
Switch# debug adjacency
4d02h: 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
5c02h: ADJ: remove 172.20.52.36 (GigabitEthernet1/1) via ARP will expire: 04:00:00
5c02h: ADJ: remove 172.20.52.36 (GigabitEthernet1/1) via ARP will expire: 04:00:00
```

Switch#

### Related Commands

- ```ipc``` (Optional) Displays the IPC entries in the adjacency database.
- ```undebug adjacency``` (same as `no debug adjacency`) Disables debugging output.
To debug the backup events, use the `debug backup` command. To disable the debugging output, use the `no debug backup` command.

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

### Defaults
This command has no default settings.

### Command Modes
Privileged EXEC mode

### Examples
This example shows how to debug the backup events:

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

### Related Commands
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>undebug backup</td>
<td>(same as no debug backup)</td>
</tr>
</tbody>
</table>
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}
```

**Syntax Description**

- `fastethernet mod/port` Limits the debugging to Fast Ethernet interfaces.
- `GigabitEthernet mod/port` Limits the debugging to Gigabit Ethernet interfaces.
- `null interface_num` Limits the debugging to null interfaces; the valid value is 0.
- `port-channel interface-num` Limits the debugging to port-channel interfaces; valid values are from 1 to 64.
- `vlan vlan_id` Specifies the VLAN interface number; valid values are from 1 to 4094.

**Command Modes**

Privileged EXEC mode

**Examples**

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

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

**Related Commands**

- `debug interface` Abbreviates the entry of the `debug condition interface` command.
- `undebug condition interface` (same as `no debug condition interface`) Disables interface related activities.
To limit the debugging output for the standby state changes, use the `debug condition standby` command.

To disable the debugging output, use the `no debug condition standby` command.

## Syntax Description

```plaintext
debug condition standby
```

- **fastethernet**
  - **mod/port**
    - Limits the debugging to Fast Ethernet interfaces.

- **GigabitEthernet**
  - **mod/port**
    - Limits the debugging to Gigabit Ethernet interfaces.

- **port-channel**
  - **interface-num**
    - Limits the debugging output to port-channel interfaces; valid values are from 1 to 64.

- **vlan**
  - **vlan_id**
    - Limits the debugging of a condition on a VLAN interface; valid values are from 1 to 4094.

- **group-number**
  - VLAN group number; valid values are from 0 to 255.

## Defaults

This command has no default settings.

## Command Modes

- Privileged EXEC mode

## Usage Guidelines

If you attempt to remove the only condition set, you will be prompted with a message asking if you want to abort the removal operation. You can enter `n` to abort the removal or `y` to proceed with the removal. If you remove the only condition set, an excessive number of debugging messages might occur.

## Examples

This example shows how to limit the debugging output to group 0 in VLAN 1:

```
Switch# debug condition standby vlan 1 0
Condition 3 set
Switch#
```
This example shows the display if you try to turn off the last standby debug condition:

```
Switch# no debug condition standby vlan 1 0
```

This condition is the last standby condition set. 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
```

Related Commands

```
undebug condition standby
``` (same as no debug condition standby)

Disables debugging output.
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
```

**Syntax Description**

This command has no default settings.

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Usage Guidelines**

If you attempt to remove the only VLAN condition set, you will be prompted with a message asking if you want to abort the removal operation. You can enter `n` to abort the removal or `y` to proceed with the removal. If you remove the only condition set, it could result in the display of an excessive number of messages.

**Examples**

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

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

This example shows the message that is displayed when you attempt to disable the last VLAN debug condition:

```
Switch# no debug condition vlan 1
This condition is the last vlan condition set.
Removing 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#
```

**vlan_id**

Number of the VLAN; valid values are from 1 to 4096.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug condition vlan</td>
<td>Enables debugging output.</td>
</tr>
<tr>
<td>undebug condition vlan</td>
<td>(same as no debug condition vlan) Disables debugging output.</td>
</tr>
</tbody>
</table>
To enable the debugging for the 802.1X feature, use the `debug dot1x` command. To disable the debugging output, use the `no debug dot1x` command.

```
dot1x debug dot1x

Syntax Description

Options:

- 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 state-machine flag.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC mode

Examples

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

```
Switch# debug dot1x all
```

Related Commands

- `show dot1x`: Displays dot1x information.
- `undebug dot1x` (same as `no debug dot1x`): Disables debugging output.
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]
```

**Syntax Description**

**Defaults**

The default settings are as follows:

- Debug is disabled.
- All messages are displayed.

**Command Modes**

Privileged EXEC mode

**Usage Guidelines**

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

**Examples**

This example shows how to display all the EtherChannel debug messages:

```
Switch# debug etherchnl
PAgP 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 (Fa4/1)
22:46:33:FEC:comparing GC values of Fa2/25 Fa2/15 flag = 1 1
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#
```

This example shows how to display the EtherChannel IDB debug messages:

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

This example shows how to disable the debugging:

```
Switch# no debug etherchnl
Switch#
```
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug etherchnl</td>
<td>Enables debugging output.</td>
</tr>
<tr>
<td>undebug etherchnl</td>
<td>(same as no debug etherchnl) Disables debugging output.</td>
</tr>
</tbody>
</table>
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.

```
ddebug interface
```

```
no debug interface
```

**Syntax Description**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Examples**

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

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

**Related Commands**

- **FastEthernet**
  - Limits the debugging to Fast Ethernet interfaces.
- **mod/port**
  - Number of the module and port.
- **GigabitEthernet**
  - Limits the debugging to Gigabit Ethernet interfaces.
- **null**
  - Limits the debugging to null interfaces; the only valid value is 0.
- **port-channel**
  - Limits the debugging to port-channel interfaces; valid values are from 1 to 64.
- **vlan**
  - Specifies the VLAN interface number; valid values are from 1 to 4094.

**Command Description**

- `debug condition interface`
  - Limits the debugging output of interface-related activities.
- `undebug etherchnl`
  - Same as `no debug etherchnl`
  - Enables debugging output.
To debug the IPC activity, use the `debug ipc` command. To disable the debugging output, use the `no` form of this command.

```
depipe [all | errors | events | headers | packets | ports | seats]
```

### Syntax Description

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

### Examples

This example shows how to enable the debugging of the IPC events:

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

### Related Commands

- `undebug ipc` (same as `no debug ipc`)
  - Disables debugging output.
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.

```
depth ip dhcp snooping event
no debug ip dhcp snooping event
```

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

### Defaults
Debugging of snooping event is disabled.

### Command Modes
Privileged EXEC mode

### Examples
This example shows how to enable the debugging for the DHCP snooping events:

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

This example shows how to disable the debugging for the DHCP snooping events:

```
Switch# no debug ip dhcp snooping event
Switch#
```

### Related Commands
- `debug ip dhcp snooping`: Debugs the DHCP snooping messages.
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
```

### Syntax Description

This command has no arguments or keywords.

### Defaults

Debugging of snooping packet is disabled.

### Command Modes

Privileged EXEC mode

### Examples

This example shows how to enable the debugging for the DHCP snooping packets:

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

This example shows how to disable the debugging for the DHCP snooping packets:

```
Switch# no debug ip dhcp snooping packet
Switch# 
```

### Related Commands

- `debug ip dhcp snooping event`  
  Debugs the DHCP snooping events.
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.

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

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

Debugging of snooping security packets is disabled.

**Command Modes**

Privileged EXEC mode

**Related Commands**

- `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.
To debug the LACP activity, use the `debug lacp` command. To disable the debugging output, use the `no debug lacp` form of this command.

```
debug lacp [all | event | fsm | misc | packet]
```

**Syntax Description**

- `all` (Optional) Enables all LACP debugging.
- `event` (Optional) Enables the debugging of the LACP events.
- `fsm` (Optional) Enables the debugging of the LACP finite state machine.
- `misc` (Optional) Enables the miscellaneous LACP debugging.
- `packet` (Optional) Enables the LACP packet debugging.

**Defaults**

Debugging of LACP activity is disabled.

**Command Modes**

Privileged EXEC mode

**Usage Guidelines**

This command is supported only by the supervisor engine and can be entered only from the Catalyst 4500 series switch console.

**Examples**

This example shows how to enable the LACP miscellaneous debugging:

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

**Related Commands**

- `undebug pagp` (same as `no debug pagp`) Disables debugging output.
To display the monitoring activity, use the `debug monitor` command. To disable the debugging output, use the `no debug monitor` command.

```
debug monitor

no debug monitor
```

**Syntax Description**

- `all`
- `errors`
- `idb-update`
- `list`
- `notifications`
- `platform`
- `requests`

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Examples**

This example shows how to debug the monitoring errors:

```
Switch# debug monitor errors
SPAN error detail debugging is on
Switch#
```

**Related Commands**

- `undebug monitor` (same as `no debug monitor`)

  Disables debugging output.
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 debug nmsp` command to disable debugging.

```
 debug nmsp {all | connection | error | event | packet | rx | tx}
```

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

Debugging is disabled.

**Command Modes**

Privileged EXEC mode

**Usage Guidelines**

The `undebug nmsp` command is the same as the `no debug nmsp` command.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show debugging</code></td>
<td>Displays information about the types of debugging that are enabled.</td>
</tr>
<tr>
<td><code>show nmsp</code></td>
<td>Displays the NMSP information.</td>
</tr>
</tbody>
</table>
debug nvram

To debug the NVRAM activity, use the `debug nvram` command. To disable the debugging output, use the `no debug nvram` form of this command.

### Syntax Description

This command has no arguments or keywords.

### Defaults

This command has no default settings.

### Command Modes

Privileged EXEC mode

### Examples

This example shows how to debug NVRAM:

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

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>undebug nvram</td>
<td>(same as no debug nvram)</td>
</tr>
</tbody>
</table>
To debug the PAgP activity, use the `debug pagp` command. To disable the debugging output, use the `no debug pagp` form of this command.

### Syntax Description

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

#### `no debug pagp`

### Defaults

This command has no default settings.

### Command Modes

- Privileged EXEC mode

### Usage Guidelines

This command is supported only on the supervisor engine and can be entered only from the Catalyst 4500 series switch console.

### Examples

This example shows how to enable the PAgP miscellaneous debugging:

```
Switch# debug pagp misc
Port Aggregation Protocol Miscellaneous debugging is on
```

```
*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
```

### Related Commands

- `undebug pagp` (same as `no debug pagp`): Disables debugging output.

### Command 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.
To debug the LACP protocol packets, use the `debug platform packet protocol lacp` command. To disable the debugging output, use the `no debug platform packet protocol lacp` command.

**Syntax Description**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Examples**

This example shows how to enable all PM debugging:

```
Switch# debug platform packet protocol lacp
Switch#
```

**Related Commands**

- `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 Description**

`undebug platform packet protocol lacp` (same as `no debug platform packet protocol lacp`) Disables debugging output.
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.

```
d debug platform packet protocol pagp
```

**Syntax Description**

- `receive` (Optional): Enables the platform packet reception debugging functions.
- `transmit` (Optional): Enables the platform packet transmission debugging functions.
- `vlan` (Optional): Enables the platform packet VLAN debugging functions.

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Examples**

This example shows how to enable all PM debugging:

```
Switch# debug platform packet protocol pagp
Switch# no debug platform packet protocol pagp
```

**Related Commands**

- `undebug platform packet protocol pagp` (same as `no debug platform packet protocol pagp`): Disables debugging output.
To debug the port manager (PM) activity, use the `debug pm` command. To disable the debugging output, use the `no` form of this command.

```
d 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**

**Defaults**
This command has no default settings.

**Command Modes**
Privileged EXEC mode

**Examples**
This example shows how to enable all PM debugging:

```
Switch# debug pm all
Switch# debug pm all
```

**Related Commands**

- `show debug`: Displays the current debugging state.
- `undebug pm`: (same as no debug pm) Disables debugging output.

**Command 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.
To debug port security, use the `debug port-security` command. To disable the debugging output, use the `no debug port-security` command.

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Examples**

This example shows how to enable all PM debugging:

Switch# debug port-security
Switch#
To turn on debugging of the PPPoE Intermediate Agent feature, use the `debug pppoe intermediate-agent` command. To turn off debugging, use the `no debug pppoe intermediate-agent` command.

```
debug pppoe intermediate-agent {event | packet | all}
no debug pppoe intermediate-agent {event | packet | all}
```

**Syntax Description**
- `event`: Activates event debugging
- `packet`: Activates packet debugging
- `all`: Activates both event and packet debugging

**Defaults**
All debugging is turned off.

**Command Modes**
Privileged EXEC mode

**Examples**
This example shows how to turn on packet debugging:

```
Switch# debug pppoe intermediate-agent packet
PPPOE IA Packet debugging is on
```

```
*Sep  2 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 input interface (GigabitEthernet3/4)
*Sep  2 06:12:56.137: PPPOE_IA: received new PPPOE packet from input interface (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 input interface (GigabitEthernet3/7)
*Sep  2 06:12:56.145: 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 input interface (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
```

This example shows how to turn off packet debugging:

```
Switch# debug pppoe intermediate-agent packet
PPPOE IA Packet debugging is off
```
# Chapter 2: Cisco IOS Commands for the Catalyst 4500 Series Switches

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug pppoe intermediate-agent</td>
<td>Enables the PPPoE Intermediate Agent feature on an interface.</td>
</tr>
<tr>
<td>pppoe intermediate-agent limit rate</td>
<td>Limits the rate of the PPPoE Discovery packets arriving on an interface.</td>
</tr>
<tr>
<td>pppoe intermediate-agent trust</td>
<td>Sets the trust configuration of an interface.</td>
</tr>
</tbody>
</table>
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}`

**Syntax Description**

- `errors`: Enables the redundancy facility for error debugging.
- `fsm`: Enables the redundancy facility for FSM event debugging.
- `kpa`: Enables the redundancy facility for keepalive debugging.
- `msg`: Enables the redundancy facility for messaging event debugging.
- `progression`: Enables the redundancy facility for progression event debugging.
- `status`: Enables the redundancy facility for status event debugging.
- `timer`: Enables the redundancy facility for timer event debugging.

**Defaults**

This command has no default settings.

**Command Modes**

- Privileged EXEC mode

**Examples**

This example shows how to debug the redundancy facility timer event debugging:

```
Switch# debug redundancy timer
Redundancy timer debugging is on
Switch#
```
To debug the spanning tree activities, use the `debug spanning-tree` command. To disable the debugging output, use the `no` form of this command.

```
debug spanning-tree
{
  all  |  backbonefast  |  bpdu  |  bpdu-opt  |  etherchannel  |  config  |  events  |  exceptions  |  general  |  ha  |  mstp  |  pvst+  |  root  |  snmp  |  switch  |  synchronization  |  uplinkfast
}
no debug spanning-tree
{
  all  |  bpdu  |  bpdu-opt  |  etherchannel  |  config  |  events  |  exceptions  |  general  |  mst  |  pvst+  |  root  |  snmp  |
}
```

**Syntax Description**

- `all` Displays all the spanning tree debugging messages.
- `backbonefast` Debugs the BackboneFast events.
- `bpdu` Debugs the spanning tree BPDU.
- `bpdu-opt` Debugs the optimized BPDU handling.
- `etherchannel` Debugs the spanning tree EtherChannel support.
- `config` Debugs the spanning tree configuration changes.
- `events` Debugs the TCAM events.
- `exceptions` Debugs the spanning tree exceptions.
- `general` Debugs the general spanning tree activity.
- `ha` Debugs the HA events.
- `mstp` Debugs the multiple spanning tree events.
- `pvst+` Debugs the PVST+ events.
- `root` Debugs the spanning tree root events.
- `snmp` Debugs the spanning tree SNMP events.
- `switch` Debugs the switch debug events.
- `synchronization` Debugs the STP state synchronization events.
- `uplinkfast` Debugs the UplinkFast events.

**Defaults**

This command has no default settings.

**Command Modes**

- Privileged EXEC mode

**Examples**

This example shows how to debug the spanning-tree PVST+:

```
Switch# debug spanning-tree pvst+
Spanning Tree PVST+ debugging is on
Switch#
```
**debug spanning-tree**

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>undebug spanning-tree</td>
<td>(same as no debug spanning-tree)</td>
</tr>
</tbody>
</table>
To enable debugging of the spanning tree BackboneFast events, use the `debug spanning-tree backbonefast` command. To disable the debugging output, use the `no debug spanning-tree backbonefast` command.

### Syntax Description

This command has no default settings.

### Command Modes

Privileged EXEC mode

### Usage Guidelines

This command is supported only on the supervisor engine and enterable only from the switch console.

### Examples

This example shows how to enable the 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

- `debug spanning-tree backbonefast [detail | exceptions]` (Optional) Displays the detailed BackboneFast debugging messages.
- `no debug spanning-tree backbonefast` (same as `undebug spanning-tree backbonefast`) Disables debugging output.
To enable the switch shim debugging, use the `debug spanning-tree switch` command. To disable the debugging output, use the `no debug spanning-tree switch` command.

```
debug spanning-tree switch {
  all | errors | general | pm | rx {
    decode | errors | interrupt | process | state | tx [decode]}
}
```

```
no debug spanning-tree switch {
  all | errors | general | pm | rx {
    decode | errors | interrupt | process | state | tx [decode]}
}
```

**Syntax Description**

- **all**: Displays all the spanning-tree switch shim debugging messages.
- **errors**: Enables the debugging of switch shim errors or exceptions.
- **general**: Enables the debugging of general events.
- **pm**: Enables the debugging of port manager events.
- **rx**: Displays the received BPDU-handling debugging messages.
- **decode**: Enables the debugging of the decode-received packets of the spanning-tree switch shim.
- **errors**: Enables the debugging of the receive errors of the spanning-tree switch shim.
- **interrupt**: Enables the shim ISR receive BPDU debugging on the spanning-tree switch.
- **process**: Enables the process receive BPDU debugging on the spanning-tree switch.
- **state**: Enables the debugging of the state changes on the spanning-tree port.
- **tx**: Enables the transmit BPDU debugging on the spanning-tree switch shim.
- **decode**: (Optional) Enables the decode-transmitted packets debugging on the spanning-tree switch shim.

**Defaults**

This command has no default settings.

**Command Modes**

- Privileged EXEC mode

**Usage Guidelines**

This command is supported only on the supervisor engine and is only usable from the switch console.
debug spanning-tree switch

Examples
This example shows how to enable the transmit BPDU debugging on the spanning tree switch shim:

Switch#
d 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 FastEthernet5/9 351
*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
undebug spanning-tree switch
(same as no debug spanning-tree switch)
Disables debugging output.
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
```

**Syntax Description**

This command has no default settings.

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Usage Guidelines**

This command is supported only on the supervisor engine and enterable only from the switch console.

**Examples**

This example shows how to debug the spanning tree UplinkFast exceptions:

```
Switch# debug spanning-tree uplinkfast exceptions
Spanning Tree uplinkfast exceptions debugging is on
Switch#
```

**Related Commands**

- `exceptions`: (Optional) Enables the debugging of the spanning tree UplinkFast exceptions.
- `undebug spanning-tree uplinkfast`: (same as `no debug spanning-tree uplinkfast`) Disables debugging output.
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

- **Defaults:** This command has no default settings.

### Command Modes

Privileged EXEC mode

### Examples

This example shows how to debug the software VLAN events:

```
Switch# debug sw-vlan events
vlan manager events debugging is on
Switch#
```

### Related Commands

- `undebug sw-vlan` (same as `no debug sw-vlan`)
  - Disables debugging output.

### 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.

```
default 1 | 2 | 3 | 4
```

**Syntax Description**

**Defaults**
This command has no default settings.

**Command Modes**
Privileged EXEC mode

**Usage Guidelines**

The following are four types of file read operations:

1. Operation 1 — Reads the file header, which contains the header verification word and the file version number.
2. Operation 2 — Reads the main body of the file, which contains most of the domain and VLAN information.
4. Operation 4 — Reads TLV data.

**Examples**

This example shows how to debug the TLV data errors during a file-read operation:

```
Switch# debug sw-vlan ifs read 4
vlan manager ifs read # 4 errors debugging is on
Switch#
```

**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.

```
open 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.
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug sw-vlan ifs</code></td>
<td>Enables debugging output</td>
</tr>
<tr>
<td><code>undebug sw-vlan ifs</code></td>
<td>(same as no debug sw-vlan ifs)</td>
</tr>
<tr>
<td></td>
<td>Disables debugging output</td>
</tr>
</tbody>
</table>
```
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 debug sw-vlan notification` command.

```
debug sw-vlan notification 
accfwdchange | allowedvlancfgchange | fwdchange | linkchange | modechange | pruningcfgchange | statechange
```

```
no debug sw-vlan notification 
accfwdchange | allowedvlancfgchange | fwdchange | linkchange | modechange | pruningcfgchange | statechange
```

**Syntax Description**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Examples**

This example shows how to debug the software VLAN interface mode change notifications:

```
Switch# debug sw-vlan notification modechange
vlan manager port mode change notification debugging is on
Switch#
```

**Related Commands**

- `accfwdchange` - Enables the VLAN manager notification of aggregated access interface STP forward changes.
- `allowedvlancfgchange` - 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.
- `pruningcfgchange` - Enables the VLAN manager notification of changes to pruning configuration.
- `statechange` - Enables the VLAN manager notification of interface state changes.

**Command Description**

- `undebug sw-vlan notification` (same as `no debug sw-vlan notification`) - Disables debugging output.
debug sw-vlan vtp

to enable the debugging of messages to be generated by the VTP protocol code, use the debug sw-vlan vtp command. to disable the debugging output, use the no form of this command.

depug sw-vlan vtp {events | packets | pruning [packets | xmit] | xmit}

no debug sw-vlan vtp {events | packets | pruning [packets | xmit] | xmit}

Syntax Description

Defaults
This command has no default settings.

Command Modes
Privileged EXEC mode

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

Examples
This 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

- **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** (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; does not include pruning packets.

Command Description

- **undebug sw-vlan vtp** (same as no debug sw-vlan vtp): Disables debugging output.
To enable the debugging of UDLD activity, use the `debug udld` command. To disable the debugging output, use the `no` form of this command.

```
debug udld {events | packets | registries}
```

```
no debug udld {events | packets | registries}
```

**Syntax Description**

- `events`: Enables the debugging of UDLD process events as they occur.
- `packets`: Enables the debugging of the UDLD process as it receives packets from the packet queue and attempts to transmit packets at the request of the UDLD protocol code.
- `registries`: Enables the debugging of the UDLD process as it processes registry upcalls from the UDLD process-dependent module and other feature modules.

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Usage Guidelines**

This command is supported only on the supervisor engine and enterable only from the switch console.

**Examples**

This example shows how to debug the UDLD events:

```
Switch# debug udld events
UDLD events debugging is on
Switch#
```

This example shows how to debug the UDLD packets:

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

This example shows how to debug the UDLD registry events:

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

**Command Description**
Disables debugging output.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>undebug udld</td>
<td>(same as no debug udld)</td>
</tr>
</tbody>
</table>
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]
```

**Syntax Description**

- **all** (Optional) Debugs all the VQP events.
- **cli** (Optional) Debugs the VQP command-line interface.
- **events** (Optional) Debugs the VQP events.
- **learn** (Optional) Debugs the VQP address learning.
- **packet** (Optional) Debugs the VQP packets.

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Examples**

This example shows how to enable all VQP debugging:

```
Switch# debug vqpc all
```

**Related Commands**

- `v mps reconfirm (privileged EXEC)`
  
  Immediately sends VLAN Query Protocol (VQP) queries to reconfirm all the dynamic VLAN assignments with the VLAN Membership Policy Server (VMPS).
To create a macro of interfaces, use the **define interface-range** command.

**Syntax Description**

This command has no default settings.

**Command Modes**

Global configuration mode

**Usage Guidelines**

The macro name is a character string of up to 32 characters.

A macro can contain up to five ranges. An interface range cannot span modules.

When entering the **interface-range**, use these formats:

1. `interface-type {mod} / {first-interface} - {last-interface}`
2. `interface-type {mod} / {first-interface} - {last-interface}`

The valid values for **interface-type** are as follows:

- FastEthernet
- GigabitEthernet
- Vlan vlan_id

**Examples**

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

```
Switch(config)#
define interface-range macro1 gigabitethernet 4/1-6, fastethernet 2/1-5
Switch(config)#
```

**Related Commands**

- **macro-name**
  - Name of the interface range macro; up to 32 characters.
- **interface-range**
  - List of valid ranges when specifying interfaces; see the “Usage Guidelines” section.
- **interface range**
  - Runs a command on multiple ports at the same time.
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]
```

### Syntax Description

- **request** (Optional) Requests a match for the ARP request. When `request` is not specified, matching is performed against all ARP packets.
- **ip** Specifies the sender IP address.
  - **any** Specifies that any IP or MAC address will be accepted.
  - **host** `sender-ip` Specifies that only a specific sender IP address will be accepted.
  - **sender-ip** `sender-ip mask` Specifies that a specific range of sender IP addresses will be accepted.
- **mac** Specifies the sender MAC address.
  - **host** `sender-mac` Specifies that only a specific sender MAC address will be accepted.
  - **sender-mac** `sender-mac mask` Specifies that a specific range of sender MAC addresses will be accepted.
- **response** Specifies a match for the ARP responses.
  - **ip** Specifies the IP address values for the ARP responses.
  - **host** `target-ip` (Optional) Specifies that only a specific target IP address will be accepted.
  - `target-ip mask` (Optional) Specifies that a specific range of target IP addresses will be accepted.
  - **mac** Specifies the MAC address values for the ARP responses.
  - **host** `target-mac` (Optional) Specifies that only a specific target MAC address will be accepted.
  - `target-mac mask` (Optional) Specifies that a specific range of target MAC addresses will be accepted.
- **log** (Optional) Logs a packet when it matches the access control entry (ACE).
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

deny

Usage Guidelines
Deny clauses can be added to forward or drop ARP packets based on some matching criteria.

Examples
This example shows a host with a MAC address of 0000.0000.abcd and an IP address of 1.1.1.1. This example shows how to deny both requests and responses from this host:

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

Related Commands
Command Description
arp access-list
Defines an ARP access list or adds clauses at the end of a predefined list.
ip arp inspection filter vlan
Permits ARPs from hosts that are configured for static IP when DAI is enabled and to define an ARP access list and applies it to a VLAN.
permit
Permits an ARP packet based on matches against the DHCP bindings.
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**: Specifies the destination e-mail address in 1 to 200 characters.
- **http url**: Specifies the destination HTTP URL in 2 to 200 characters.

### Defaults

This command has no default settings.

### Command Modes

- `cfg-call-home-profile`

### Usage Guidelines

To enter profile call-home configuration submode, use the `profile` command in call-home configuration mode.

When entering the `https://` destination URL for the secure server, you must also configure a trustpoint CA.

### Examples

This example shows how to set the destination to the e-mail address `callhome@cisco.com`:

```
Switch(config)#
call-home
Switch(cfg-call-home)#
profile cisco
Switch(cfg-call-home-profile)#
destination address email callhome@cisco.com
```
To configure a maximum destination message size for the destination profile, use the `destination message-size-limit bytes` command.

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

3,145,728 bytes

**Command Modes**

cfg-call-home-profile

**Usage Guidelines**

To enter profile call-home configuration submode, use the `profile` command in call-home configuration mode.

**Examples**

This example shows how to configure the maximum message size for the destination profile as 3,000,000:

```
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**

- **destination address**
  Configures the destination e-mail address or URL to which Call Home messages will be sent.
- **destination preferred-msg-format**
  Configures a preferred message format.
- **destination transport-method**
  Enables the message transport method.
- **profile**
  Enters profile call-home configuration submode
- **subscribe-to-alert-group all**
  Subscribes to all available alert groups.
- **subscribe-to-alert-group configuration**
  Subscribes this destination profile to the Configuration alert group.
- **subscribe-to-alert-group diagnostic**
  Subscribes this destination profile to the Diagnostic alert group.
- **subscribe-to-alert-group environment**
  Subscribes this destination profile to the Environment alert group.
- **subscribe-to-alert-group inventory**
  Subscribes this destination profile to the Inventory alert group.
- **subscribe-to-alert-group syslog**
  Subscribes this destination profile to the Syslog alert group.
To configure a preferred message format, use the `destination preferred-msg-format` command.

```
destination preferred-msg-format {long-text | short-text | xml}
```

**Syntax Description**

- `long-text`: Sends the message in long-text format.
- `short-text`: Sends the message in short-text format.
- `xml`: Sends the message in XML format.

**Defaults**

- `xml`

**Command Modes**

- `cfg-call-home-profile`

**Usage Guidelines**

To enter profile call-home configuration submode, use the `profile` command in call-home configuration mode.

**Examples**

This example shows how to configure the preferred message format as long text:

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

**Related Commands**

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

```
destination transport-method {email | http}
```

**Syntax Description**

- **email**: Enables e-mail as transport method.
- **http**: Enables HTTP as transport method.

**Defaults**

- **email**
- **http**

**Command Modes**

- **cfg-call-home-profile**

**Usage Guidelines**

To enter profile call-home configuration submode, use the `profile` command in call-home configuration mode.

**Examples**

This example shows how to 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**

- **email**: Enables e-mail as transport method.
- **http**: Enables HTTP as transport method.

**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.
- **subscribe-to-alert-group inventory**: Subscribes this destination profile to the Inventory alert group.
- **subscribe-to-alert-group syslog**: Subscribes this destination profile to the Syslog alert group.
diagnostic fpga soft-error recover

To configure the SEU behavior, use the diagnostic fpga soft-error recover command. To return to the default setting, use the no form of this command.

diagnostic fpga soft-error recover {conservative | aggressive}

no diagnostic fpga soft-error recover

Syntax Description

Defaults

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

Usage Guidelines

SEU events on the system FPGAs result in a potentially unstable switch. The only recovery is to reload the affected supervisor engine. However, SEU events may be harmless, so you might want to delay the reload until a maintenance window, to avoid impacting users. Alternatively, you might want to force an immediate reload to avoid an instance where the switch crashes or drops traffic because of the SEU.

Examples

This example shows how to configure the SEU behavior as conservative:

Switch(config)#
diagnostic fpga soft-error recover conservative

This example shows how to revert to the default behavior:

Switch(config)#
no diagnostic fpga soft-error recover

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.
To direct the action of the switch when it detects a packet memory failure, use the `diagnostic monitor action` command.

**Syntax Description**

```
[conservative | normal | aggressive]
```

**Defaults**

- **normal** mode

**Command Modes**

Global configuration mode

**Usage Guidelines**

- Use the `conservative` keyword when you do not want the switch to reboot so that the problem can be fixed.
- Use the `aggressive` keyword when you have redundant supervisor engines, or when network-level redundancy has been provided.

**Examples**

This example shows how to configure the switch to initiate an RPR switch over when an ongoing failure occurs:

```
Switch# configure terminal
Switch (config)# diagnostic monitor action normal
```

**Related Commands**

- `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 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.
To run the specified diagnostic test, use the `diagnostic start` command.

```
diagnostic start
  {module num} {test test-id} [port num]
```

**Syntax Description**

- `module num`: Module number.
- `test`: Specifies a test to run.
- `test-id`: Specifies an identification number for the test to be run; can be the cable diagnostic test-id, or the `cable-tdr` keyword.
- `port num`: (Optional) Specifies the interface port number.

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode.

**Examples**

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

```
This exec command starts the TDR test on specified interface
Switch# diagnostic start module 1 test cable-tdr port 3
Switch# module 1: Running test(s) 5 Run interface level cable diags
Switch# module 1: Running test(s) 5 may disrupt normal system operation
Do you want to continue? [no]: yes
```

```
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
```

**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**

- `module num`: Module number.
- `test`: Specifies a test to run.
- `test-id`: Specifies an identification number for the test to be run; can be the cable diagnostic test-id, or the `cable-tdr` keyword.
- `port`: (Optional) Specifies the interface port number.

**Command Description**

- `show diagnostic content`: Displays diagnostic content information.
To configure the maximum 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.

```
Syntax Description

Defaults

Default is 3.

Command Modes

Interface configuration mode

Examples

This example shows how to configure the maximum number of attempts before the port is moved to the auth-fail VLAN 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

- `max-attempts` specifies a maximum number of attempts before a port is moved to the auth-fail VLAN in the range of 1 to 10.
- `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.
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]
```

**Defaults**
This command has no default settings.

**Command Modes**
Interface configuration mode

**Examples**
This example shows how to configure the auth-fail VLAN on Fast Ethernet interface 4/3:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config) #
interface fastethernet4/3
Switch(config-if) #
dot1x auth-fail vlan 40
Switch(config-if) #
end
Switch#
```

**Related Commands**
- `vlan-id`: Specifies a VLAN in the range of 1 to 4094.
- `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.
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.

```
[ in | both ]
```

**Syntax Description**

- **Defaults**: Both in-bound and out-bound traffic will be controlled.
- **Command Modes**: Interface configuration mode

**Usage Guidelines**

You can manage remote systems using unidirectional control. Unidirectional control enables you to turn on systems remotely using a specific Ethernet packet, known as a magic packet.

Using unidirectional control enables you to remotely manage systems using 802.1X ports. In the past, the port became unauthorized after the system was turned off. In this state, the port only allowed the receipt and transmission of EAPoL packets. Therefore, there was no way for the unidirectional control magic packet to reach the host and without being turned on there was no way for the system to authenticate and open the port.

**Examples**

This example shows how to enable unidirectional control on incoming packets:

```
Switch(config-if)# dot1x control-direction in
Switch(config-if)#
```

**Related Commands**

- `in` *(Optional)* Specifies controlling in-bound traffic on a port.
- `both` *(Optional)* Specifies controlling both in-bound and out-bound traffic on a port.
- `show dot1x` Displays dot1x information.
Use the `dot1x credentials` global configuration command to configure a profile on a supplicant switch.

**Syntax Description**

- **Defaults**
  - No profile is configured for the switch.

- **Command Modes**
  - Global configuration

- **Usage Guidelines**
  - You must have another switch set up as the authenticator for this switch to be the supplicant.

**Examples**

This example shows how to configure a switch as a supplicant:

```
Switch(config) # dot1x credentials
Switch(config)# dot1x profile
```

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

**Related Commands**

- **cisp enable**
  - Enables Client Information Signalling Protocol (CISP).

- **show cisp (IOS command)**
  - Displays CISP information for a specified interface.
To enable the 802.1X critical authentication on a port, use the `dot1x critical` command. To return to the default setting, use the `no dot1x critical` command.

### Syntax Description

This command has no keywords or variables.

### Defaults

Critical authentication is disabled.

### Command Modes

Interface configuration mode

### Examples

This example shows how to enable 802.1x critical authentication:

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

### Related Commands

- `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.
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.

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

**Defaults**
The default is to not send EAPOL success packets.

**Command Modes**
Global configuration mode

**Examples**
This example shows how to enable sending EAPOL success packets:

```
Switch(config-if)# dot1x critical eapol
Switch(config-if)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dot1x critical</code></td>
<td>Enables the 802.1X critical authentication on a port.</td>
</tr>
<tr>
<td><code>dot1x critical recovery delay</code></td>
<td>Sets the time interval between port reinitializations.</td>
</tr>
<tr>
<td><code>dot1x critical vlan</code></td>
<td>Assigns a critically authenticated port to a specific VLAN.</td>
</tr>
<tr>
<td><code>show dot1x</code></td>
<td>Displays dot1x information.</td>
</tr>
</tbody>
</table>
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

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.

**Syntax**

`delay-time`

**Defaults**

Delay time is set to 100 milliseconds.

**Command Modes**

Global configuration mode

**Examples**

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

```bash
Switch(config-if)# dot1x critical recovery delay 500
```

**Related Commands**

- **delay-time**
  - Specifies the interval between port reinitializations when AAA transition occurs; valid values are from 1 to 10,000 milliseconds.

- **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.
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
```

**Syntax Description**

- **Defaults**: Critical authentication is disabled on a ports VLAN.
- **Command Modes**: Interface configuration mode

**Usage Guidelines**

- The type of VLAN specified must match the type of the port. If the port is an access port, the VLAN must be a regular VLAN. If the port is a private-VLAN host port, the VLAN must be the secondary VLAN of a valid private-VLAN domain. If the port is a routed port, no VLAN may be specified.
- This command is not supported on platforms such as Layer 3 switches that do not include the Critical Auth VLAN sub system.

**Examples**

This 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**

- **vlan-id** *(Optional)*: Specifies the VLANs; valid values are from 1 to 4094.
- **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.
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**

This command has no default settings; the guest VLAN feature is disabled.

**Command Modes**

Interface configuration mode

**Usage Guidelines**

Guest VLANs can be configured only on ports that are statically configured as access ports or private VLAN host ports. Statically configured access ports can be configured with regular VLANs as guest VLANs; statically configured private VLAN host ports can be configured with secondary private VLANs as guest VLANs.

**Examples**

This example shows how to enable a guest VLAN on Fast Ethernet interface 4/3:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet4/3
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x guest-vlan 26
Switch(config-if)#
```

**Related Commands**

- `vlan-id` (Specifies a VLAN in the range of 1 to 4094.)
- `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.)
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 dot1x guest-vlan supplicant` form of this command.

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

802.1X-capable hosts are not put into a guest VLAN.

**Command Modes**

Global configuration mode

**Usage Guidelines**

With Cisco Release 12.2(25) EW A, 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) EW A, 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**

This 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)#
```

**Related Commands**

- `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}`

- `dot1x system-auth-control`
  Enables 802.1X authentication on the switch.

- `show dot1x`
  Displays dot1x information.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

dot1x host-mode

[  multi-host
[  single-host | multi-domain

Syntax Description

Defaults

The default is single-host mode.

Command Modes

Interface configuration mode

Usage Guidelines

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

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

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

You can assign both voice and data VLAN dynamically from the ACS server. No additional configuration is required to enable dynamic VLAN assignment on the switch. To enable VLAN assignment, you must configure the Cisco ACS server. For details on configuring the ACS server for voice VLAN assignment, refer to the "Cisco ACS Configuration for VLAN Assignment" section in the Catalyst 4500 Series Switch Software Configuration Guide—Release, 12.2(52)SG.

Examples

This example shows how to enable IEEE 802.1x authentication and to enable multiple-hosts mode:

Switch# 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#

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

Switch# configure t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface 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
dot1x host-mode
Switch(config-if)#
end
Switch#

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

Related Commands
Command Description
show dot1x
Displays dot1x information.
To unauthorize an interface before reinitializing 802.1X, use the `dot1x initialize` command.

**Syntax Description**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Usage Guidelines**

Use this command to initialize state machines and to set up the environment for fresh authentication.

**Examples**

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

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

**Related Commands**

- `interface`
  Number of the interface.
- `show dot1x`
  Displays dot1x information.
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]
```

**Syntax Description**

- **no dot1x mac-auth-bypass [eap]**

**Defaults**
There is no default setting.

**Command Modes**
Interface configuration mode

**Usage Guidelines**
The removal of the `dot1x mac-auth-bypass` configuration from a port does not affect the 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**
This example shows how to enable EAP MAC address authentication:
```
Switch(config-if)# dot1x mac-auth-bypass
Switch(config-if)#
```

(Optional) Specifies using EAP MAC address authentication.
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.

```plaintext
dot1x max-reauth-req count
no dot1x max-reauth-req
```

**Syntax Description**

- `count`: Number of times that the switch retransmits EAP-Request/Identity frames before restarting the authentication process; valid values are from 1 to 10.

**Defaults**

The switch sends a maximum of two retransmissions.

**Command Modes**

- Interface configuration mode

**Usage Guidelines**

You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers. This setting impacts the wait before a non-dot1x-capable client is admitted to the guest VLAN, if one is configured.

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

**Examples**

This example shows how to set 5 as the number of times that the switch retransmits an EAP-Request/Identity frame before restarting the authentication process:

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

**Related Commands**

- `show dot1x`: Displays dot1x information.
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**

- **Defaults**: The switch sends a maximum of two retransmissions.
- **Command Modes**: Interface configuration mode

**Usage Guidelines**

You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers. You can verify your settings by entering the `show dot1x` privileged EXEC command.

**Examples**

This example shows how to set 5 as the number of times that the switch retransmits an EAP-Request frame before restarting the authentication process:

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

This example shows how to return to the default setting:

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

**Related Commands**

- `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.
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 }
```

**Syntax Description**

**Defaults**
The port 802.1X authorization is disabled.

**Command Modes**
Interface configuration mode

**Usage Guidelines**
The 802.1X protocol is supported on both the Layer 2 static-access ports and the Layer 3-routed ports. You can use the `auto` keyword only if the port is not configured as follows:

- **Trunk port**—If you try to enable 802.1X on a trunk port, an error message appears, and 802.1X is not enabled. If you try to change the mode of an 802.1X-enabled port to trunk, the port mode is not changed.
- **Dynamic ports**—A port in dynamic mode can negotiate with its neighbor to become a trunk port. If you try to enable 802.1X on a dynamic port, an error message appears, and 802.1X is not enabled. If you try to change the mode of an 802.1X-enabled port to dynamic, the port mode is not changed.
- **EtherChannel port**—Before enabling 802.1X on the port, you must first remove it from the EtherChannel. If you try to enable 802.1X on an EtherChannel 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.

- **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.
Examples

This 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show dot1x</td>
<td>Displays dot1x information.</td>
</tr>
</tbody>
</table>
To manually initiate a reauthentication of all 802.1X-enabled ports or the specified 802.1X-enabled port, use the `dot1x re-authenticate` command.

```
dot1x re-authenticate [interface interface-id]
```

**Syntax Description**

- **interface interface-id**: (Optional) Module and port number of the interface.

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Usage Guidelines**

You can use this command to reauthenticate a client without waiting for the configured number of seconds between reauthentication attempts (re-authperiod) and automatic reauthentication.

**Examples**

This example shows how to manually reauthenticate the device connected to Gigabit Ethernet interface 1/1:

```
Switch# dot1x re-authenticate interface gigabitethernet1/1
Starting reauthentication on gigabitethernet1/1
Switch#
```
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.

```
adot1x re-authentication

```

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

The periodic reauthentication is disabled.

**Command Modes**

Interface configuration mode

**Usage Guidelines**

You configure the amount of time between the periodic reauthentication attempts by using the `dot1x timeout re-authperiod` command.

**Examples**

This example shows how to disable the periodic reauthentication of the client:

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

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

- `dot1x timeout`: Sets the reauthentication timer.
- `show dot1x`: Displays dot1x information.
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 dot1x system-auth-control` command.

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

**Defaults**
The 802.1X authentication is disabled.

**Command Modes**
Global configuration mode

**Usage Guidelines**
You must enable `dot1x system-auth-control` if you want to use the 802.1X access controls on any port on the switch. You can then use the `dot1x port-control auto` command on each specific port on which you want the 802.1X access controls to be used.

**Examples**
This example shows how to enable 802.1X authentication:

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1x initialize</td>
<td>Unauthorizes an interface before reinitializing 802.1X.</td>
</tr>
<tr>
<td>show dot1x</td>
<td>Displays dot1x information.</td>
</tr>
</tbody>
</table>
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
```

### Syntax Description

#### `reauth-period` {seconds | server}
- **seconds**: Number of seconds between reauthentication attempts; valid values are from 1 to 65535. See the "Usage Guidelines" section for more information.
- **server**: Number of seconds between reauthentication attempts; valid values are from 1 to 65535 as derived from the Session-Timeout RADIUS attribute. See the "Usage Guidelines" section for more information.

#### `quiet-period` seconds
- **seconds**: Number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client; valid values are from 0 to 65535 seconds.

#### `tx-period` seconds
- **seconds**: Number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request; valid values are from 1 to 65535 seconds.

#### `supp-timeout` seconds
- **seconds**: Number of seconds that the switch waits for the retransmission of EAP-Request packets; valid values are from 30 to 65535 seconds.

#### `server-timeout` seconds
- **seconds**: Number of seconds that the switch waits for the retransmission of packets by the back-end authenticator to the authentication server; valid values are from 30 to 65535 seconds.

### Defaults

The default settings are as follows:

- Reauthentication period is 3600 seconds.
- Quiet period is 60 seconds.
- Transmission period is 30 seconds.
- Supplicant timeout is 30 seconds.
- Server timeout is 30 seconds.

### Command Modes

Interface configuration mode

### Usage Guidelines

The periodic reauthentication must be enabled before entering the `dot1x timeout` command. Enter the `dot1x re-authentication` command to enable periodic reauthentication.

### Examples

This example shows how to set 60 as the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request:

```
dot1x timeout reauth-period 60
```
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

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

This example shows how to set up the switch to use a reauthentication timeout derived from a Session-Timeout attribute taken from the RADIUS Access-Accept message received when a host successfully authenticates via 802.1X:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet4/3
Switch(config-if)# dot1x timeout reauth-period server
Switch(config-if)# end
Switch#
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1x initialize</td>
<td>Unauthorizes an interface before reinitializing 802.1X.</td>
</tr>
<tr>
<td>show dot1x</td>
<td>Displays dot1x information.</td>
</tr>
</tbody>
</table>
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}
```

**Syntax Description**

- `auto`: Specifies the autonegotiation operation.
- `full`: Specifies the full-duplex operation.
- `half`: Specifies the half-duplex operation.

**Defaults**

Half-duplex operation

**Command Modes**

Interface configuration mode

**Usage Guidelines**

Table 2-1 lists the supported command options by interface.

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Supported Syntax</th>
<th>Default Setting</th>
<th>Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/100-Mbps module</td>
<td>duplex</td>
<td>half</td>
<td>If the speed is set to <code>auto</code>, you will not be able to set the <code>duplex</code> mode. If the speed is set to <code>10</code> or <code>100</code>, and you do not configure the <code>duplex</code> setting, the duplex mode is set to half-duplex.</td>
</tr>
<tr>
<td>100-Mbps fiber modules</td>
<td>duplex</td>
<td>half</td>
<td></td>
</tr>
<tr>
<td>Gigabit Ethernet</td>
<td>Not supported.</td>
<td>Not supported.</td>
<td>Gigabit Ethernet interfaces are set to full-duplex.</td>
</tr>
<tr>
<td>10/100/1000</td>
<td>duplex</td>
<td>half</td>
<td>If the speed is set to <code>auto</code> or <code>1000</code>, you will not be able to set <code>duplex</code>. If the speed is set to <code>10</code> or <code>100</code>, and you do not configure the <code>duplex</code> setting, the duplex mode is set to half-duplex.</td>
</tr>
</tbody>
</table>
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 reenable the interface during the reconfiguration.

Table 2-2 describes the system performance for different combinations of the duplex and speed modes. The specified duplex command that is configured with the specified speed command produces the resulting action shown in the table.

Examples
This example shows how to configure the interface for full-duplex operation:

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

Related Commands
Table 2-2 Relationship Between duplex and speed Commands

<table>
<thead>
<tr>
<th>duplexer Command</th>
<th>speed Command</th>
<th>Resulting System Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>duplex half</td>
<td>speed auto</td>
<td>Autonegotiates both speed and duplex modes</td>
</tr>
<tr>
<td>duplex half</td>
<td>speed 10</td>
<td>Forces 10 Mbps and half duplex</td>
</tr>
<tr>
<td>duplex full</td>
<td>speed 10</td>
<td>Forces 10 Mbps and full duplex</td>
</tr>
<tr>
<td>duplex half</td>
<td>speed 100</td>
<td>Forces 100 Mbps and half duplex</td>
</tr>
<tr>
<td>duplex full</td>
<td>speed 100</td>
<td>Forces 100 Mbps and full duplex</td>
</tr>
<tr>
<td>duplex full</td>
<td>speed 1000</td>
<td>Forces 1000 Mbps and full duplex</td>
</tr>
</tbody>
</table>

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.
To configure access control, use the `epm access control [open | default]` command.

**Syntax Description**

- `open` specifies open access control.
- `default` specifies default access control.

**Defaults**

If the `epm access control` command is not configured, the behavior defaults to the `epm access control default` command. Nothing is generated.

**Command Modes**

Configuration mode

**Usage Guidelines**

When you enter the `epm access control` command, it is generated. 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**

- `open` Specifies open access control.
- `default` Specifies default access control.
To erase a file system, use the `erase` command.

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

**Syntax Description**

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Usage Guidelines**

**Caution**

When you use the `erase` command to erase a file system, you cannot recover the files in the file system.

In addition to the command options shown above, options with the prefix slave that are used to identify nvram: and flash (such as slavenvram: and slavecat4000_flash:) appear in the command help messages on the dual supervisor engine redundancy switch.

The `erase nvram:` command replaces the `write erase` and the `erase startup-config` commands. This command erases both the startup-config and the private-config 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 non volatile 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:**

erase /all non-default

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: 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

00:01:48: %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram

Erasing the nvram filesystem will remove all files! Continue? [confirm]

Erase of nvram: complete

00:38:10: %SYS-7-NV_BLOCK_INIT: Initalized the geometry of nvram

This example shows how to erase filesyst em cat4000_flash.

Erase of cat4000_flash: complete

Switch#
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>erase</code></td>
<td>Specifies the device and filename of the configuration file.</td>
</tr>
<tr>
<td><code>delete</code></td>
<td>Deletes a file from a flash memory device or NVRAM.</td>
</tr>
<tr>
<td><code>show bootvar</code></td>
<td>Displays BOOT environment variable information.</td>
</tr>
<tr>
<td><code>undelete</code></td>
<td>Recovers a file marked &quot;deleted&quot; on a Class a flash file system.</td>
</tr>
</tbody>
</table>
To enable error-disable detection, use the `errdisable detect` command. To disable the error-disable detection feature, use the `no` form of this command.

```
errdisable detect cause

{ all |
  arp-inspection |
  bpduguard shutdown vlan |
  dhcp-rate-limit |
  dt-p-f lap |
  gbic-invalid |
  l2ptguard |
  link-flap |
  pagp-flap } |

no errdisable detect cause

{ all |
  arp-inspection |
  bpduguard shutdown vlan |
  dhcp-rate-limit |
  dt-p-f lap |
  gbic-invalid |
  l2ptguard |
  link-flap |
  pagp-flap }
```

**Syntax Description**

- `cause` Specifies error-disable detection to detect a specific cause.
- `all` Specifies error-disable detection for all error-disable causes.
- `arp-inspection` Specifies the detection for the ARP inspection error-disable cause.
- `action shutdown vlan` (Optional) Specifies per-VLAN error-disable for ARP inspection and DHCP rate limiting.
- `bpduguard shutdown vlan` Specifies per-VLAN error-disable for BPDU guard.
- `dhcp-rate-limit` Specifies the detection for the DHCP rate-limit error-disable cause.
- `dtp-flap` Specifies the detection for the DTP flap error-disable cause.
- `gbic-invalid` Specifies the detection for the GBIC invalid error-disable cause.
- `l2ptguard` Specifies the detection for the Layer 2 protocol-tunnel error-disable cause.
- `link-flap` Specifies the detection for the link flap error-disable cause.
- `pagp-flap` Specifies the detection for the PAgP flap error-disable cause.

**Defaults**

All error-disable causes are detected.

**Command Modes**

Global configuration mode

**Usage Guidelines**

A cause (dtp-flap, link-flap, pagp-flap) is defined as the reason why the error-disabled state occurred. When a cause is detected on an interface, the interface is placed in error-disabled state (an operational state that is similar to link-down state).

You must enter the `shutdown` command and then the `no shutdown` command to recover an interface manually from the error-disable state.

To prevent the port from shutting down, you can use the `shutdown vlan` option to shut down just the offending VLAN on the port where the violation occurred. This option is available for the following three causes: bpduguard, arp-inspection, and dhcp-rate-limit. You can use the `clear errdisable` command to recover disabled VLANs on a port.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

errdisable detect

Examples

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

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

This example shows how to enable per-VLAN error-disable detection for BPDU guard:

Switch(config)#
errdisable detect cause bpduguard shutdown vlan
Switch(config)#
end
Switch#

show errdisable detect

<table>
<thead>
<tr>
<th>ErrDisable Reason</th>
<th>Detection</th>
</tr>
</thead>
<tbody>
<tr>
<td>arp-inspection</td>
<td>Enabled</td>
</tr>
<tr>
<td>bpduguard</td>
<td>Enabled</td>
</tr>
<tr>
<td>channel-misconfig</td>
<td>Enabled</td>
</tr>
<tr>
<td>dhcp-rate-limit</td>
<td>Enabled</td>
</tr>
<tr>
<td>dtp-flap</td>
<td>Enabled</td>
</tr>
<tr>
<td>gbic-invalid</td>
<td>Enabled</td>
</tr>
<tr>
<td>psecure-violation</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

Related Commands

Command Description

show errdisable detect
Displays the error disable detection status.

show interfaces status
Displays the interface status or a list of interfaces in erro r-disabled state.
To configure the recovery mechanism variables, use the `errdisable recovery` command. To return to the default setting, use the `no` form of this command.

```
cisco(config)# errdisable recovery
```

**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.
- **pesecure-violation** (Optional) Enables the recovery timer for the pesecure violation error-disable cause.
- **security-violation** (Optional) Enables the automatic recovery of ports disabled due to 802.1X security violations.
- **storm-control** (Optional) Enables the 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** (Optional) Specifies the time to recover from a specified error-disable cause; valid values are from 30 to 86400 seconds.
Chapter 2 Cisco IOS Commands for the Catalyst 4500 Series Switches

errdisable recovery

Defaults
Error disable recovery is disabled.
The recovery interval is set to 300 seconds.

Command Modes
Global configuration mode

Usage Guidelines
A cause (bpduguard, dtp-flap, link-flap, pagp-flap, udld) is defined as the reason why the error-disabled state occurred. When a cause is detected on an interface, the interface is placed in error-disabled state (an operational state that is similar to the link-down state). If you do not enable error-disable recovery for the cause, the interface stays in the error-disabled state until a shutdown and no shutdown occurs. If you enable recovery for a cause, the interface is brought out of the error-disabled state and allowed to retry operation again once all the causes have timed out.

You must enter the shutdown command and then the no shutdown command to recover an interface manually from error disable.

Examples
This example shows how to enable the recovery timer for the BPDU guard error disable cause:

Switch(config)#
errdisable recovery cause bpduguard
Switch(config)#

This example shows how to set the timer to 300 seconds:

Switch(config)#
errdisable recovery interval 300
Switch(config)#

This example shows how to enable the errdisable recovery for arp-inspection:

Switch(config)#
errdisable recovery cause arp-inspection
Switch(config)#
end
Switch#
show errdisable recovery

ErrDisable Reason    Timer Status
-----------------    --------------
udld                 Disabled
bpduguard            Disabled
security-violation   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
Timer interval: 300 seconds
Interfaces that will be enabled at the next timeout:
Switch#
Chapter 2 - Cisco IOS Commands for the Catalyst 4500 Series Switches

errdisable recovery

Related Commands
- 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.
To configure a Gigabit Ethernet interface to send or receive pause frames, use the `flowcontrol` command. To disable the flow control setting, use the `no` form of this command.

```
flowcontrol {receive | send} {off | on | desired}
no flowcontrol {receive | send} {off | on | desired}
```

**Syntax Description**
- `receive`: Specifies that the interface processes pause frames.
- `send`: Specifies that the interface sends pause frames.
- `off`: Prevents a local port from receiving and processing pause frames from remote ports or from sending pause frames to remote ports.
- `on`: Enables a local port to receive and process pause frames from remote ports or send pause frames to remote ports.
- `desired`: Obtains predictable results whether a remote port is set to on, off, or desired.

**Defaults**
- The default settings for Gigabit Ethernet interfaces are as follows:
  - Sending pause frames is off—Non-oversubscribed Gigabit Ethernet interfaces.
  - Receiving pause frames is desired—Non-oversubscribed Gigabit Ethernet interfaces.
  - Sending pause frames is on—Oversubscribed Gigabit Ethernet interfaces.
  - Receiving pause frames is desired—Oversubscribed Gigabit Ethernet interfaces.

**Table 2-3 Default Module Settings**

<table>
<thead>
<tr>
<th>Module</th>
<th>Ports</th>
<th>Send</th>
</tr>
</thead>
<tbody>
<tr>
<td>All modules except</td>
<td>All</td>
<td></td>
</tr>
<tr>
<td>WS-X4418-GB and</td>
<td>Ports</td>
<td></td>
</tr>
<tr>
<td>WS-X4416-2GB-TX</td>
<td>Off</td>
<td></td>
</tr>
<tr>
<td>WS-X4418-GB Uplink ports</td>
<td>Off</td>
<td></td>
</tr>
<tr>
<td>WS-X4418-GB Oversubscribed ports</td>
<td>Off</td>
<td></td>
</tr>
<tr>
<td>WS-X4412-2GB-TX Uplink ports</td>
<td>Off</td>
<td></td>
</tr>
<tr>
<td>WS-X4412-2GB-TX Oversubscribed ports</td>
<td>Off</td>
<td></td>
</tr>
<tr>
<td>WS-X4416-2GB-TX Uplink ports</td>
<td>Off</td>
<td></td>
</tr>
<tr>
<td>WS-X4416-2GB-TX Oversubscribed ports</td>
<td>Off</td>
<td></td>
</tr>
</tbody>
</table>
Table 2-4 describes the guidelines for using the different configurations of the `send` and `receive` keywords with the `flowcontrol` command.

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

Examples

This example shows how to enable send flow control:

```
Switch(config-if)# flowcontrol receive on
```

This example shows how to disable send flow control:

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

<table>
<thead>
<tr>
<th>Configuration Description</th>
<th>Interface Type</th>
<th>Configured Speed</th>
<th>Advertised Flow Control</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>send on</code></td>
<td>10/100/1000BASE-TX</td>
<td>Speed 1000</td>
<td>Configured flow control always</td>
</tr>
<tr>
<td><code>send off</code></td>
<td>1000BASE-T</td>
<td>Negotiation always enabled</td>
<td>Configured flow control always</td>
</tr>
<tr>
<td><code>send desired</code></td>
<td>1000BASE-X</td>
<td>No speed negotiation</td>
<td>Configured flow control forced</td>
</tr>
<tr>
<td><code>receive on</code></td>
<td>1000BASE-X</td>
<td>Speed no negotiation</td>
<td>Configured flow control negotiated</td>
</tr>
<tr>
<td><code>receive off</code></td>
<td>1000BASE-X</td>
<td>Speed no negotiation</td>
<td>Configured flow control always</td>
</tr>
<tr>
<td><code>receive desired</code></td>
<td>1000BASE-X</td>
<td>Speed no negotiation</td>
<td>Configured flow control always</td>
</tr>
</tbody>
</table>
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

**flowcontrol**

This example shows how to set receive flow control to desired:

Switch(config-if)#
flowcontrol receive desired
Switch(config-if)#

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface port-channel</td>
<td>Accesses or creates a port-channel interface.</td>
</tr>
<tr>
<td>interface range</td>
<td>Runs a command on multiple ports at the same time.</td>
</tr>
<tr>
<td>show flowcontrol</td>
<td>Displays the per-interface status and statistics related to flow control.</td>
</tr>
<tr>
<td>show running-config</td>
<td>Displays the running-configuration for a switch.</td>
</tr>
<tr>
<td>speed</td>
<td>Configures the interface speed.</td>
</tr>
</tbody>
</table>
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

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.

```
Switch(config)# configure terminal
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip access list</td>
<td>Creates an IP ACL (Access Control List).</td>
</tr>
<tr>
<td>ipv6 access list</td>
<td>Creates an IPv6 ACL.</td>
</tr>
<tr>
<td>mac access-list</td>
<td>Defines the extended MAC access lists.</td>
</tr>
</tbody>
</table>
To control the beacon LED in conjunction with the beacon button, enter the `hw-module beacon` command:

```
hw-module beacon [on | off]
```

**Syntax Description**

No parameters.

**Defaults**

None.

**Command Modes**

Global configuration.

**Usage Guidelines**

Either press the beacon button on the front side of the switch or enter the `hw-module 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
```

```
*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
```

```
*Feb 16 13:12:18.083: %C4K_IOSMODPORTMAN-6-BEACONTURNEDOFF: Beacon has been turned off
```

`on` 
Turns on the LED.

`off` 
Turns off the LED.
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

Defaults
After a boot up, the power is on.

Command Modes
Global configuration mode

Usage Guidelines
After you enter `no hw-module power` command and OIR the linecard, the configuration persists and is valid for any slot in the chassis it is applied to.

Examples
This example shows how to shut off power to a module in slot 5:
```
Switch# no hw-module slot 5 power
Switch#
```

Related Commands
```
slot (Optional) Specifies a slot on a chassis.
module (Optional) Specifies a line module.
number Slot or module number.
```

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

```
no hw-module system max-queue-limit
```

**Syntax Description**

- `max-queue-limit`: Specifies the queue limit for all interfaces. Valid values are from 1024 to 8184. This parameter must be a multiple of 8.

**Defaults**

- Not enabled by default

**Command Modes**

- Global configuration mode

**Usage Guidelines**

- This command allows you to change the queue limit for all interfaces globally rather than apply a policy with a queue limit to all the interfaces.
- This is a global configuration command. It can be overridden by the per port, per class, queue-limit command.
- For a standalone supervisor engine, you must reboot the engine after applying this command. For a redundant supervisor engine, you must enter the `redundancy reload shelf` command to enforce a reboot on both the supervisor engines.

**Examples**

This example shows how to set the queue limit globally to 1024:

```
Switch> enable
Switch# configure terminal
Switch(config)# hw-module system max-queue-limit 1024
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)
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 {vlans vlan-range}
no instance instance-id
```

**Syntax Description**
- **instance-id**: MST instance to which the specified VLANs are mapped; valid values are from 0 to 15.
- **vlans**: Specifies the number of the VLANs to be mapped to the specified instance. The number is entered as a single value or a range; valid values are from 1 to 4094.

**Defaults**
Mapping is disabled.

**Command Modes**
MST configuration mode

**Usage Guidelines**
The mapping is incremental, not absolute. When you enter a range of VLANs, this range is added or removed to the existing ones.

Any unmapped VLAN is mapped to the CIST instance.

**Examples**
- This example shows how to map a range of VLANs to instance 2:
  ```
  Switch(config-mst)# instance 2 vlans 1-100
  Switch(config-mst)#
  ```
- This example shows how to map a VLAN to instance 5:
  ```
  Switch(config-mst)# instance 5 vlans 1100
  Switch(config-mst)#
  ```
- This example shows how to move a range of VLANs from instance 2 to the CIST instance:
  ```
  Switch(config-mst)# no instance 2 vlans 40-60
  Switch(config-mst)#
  ```
- This example shows how to move all the VLANs mapped to instance 2 back to the CIST instance:
  ```
  Switch(config-mst)# no instance 2
  Switch(config-mst)#
  ```

**Related Commands**
- `name`: Sets the MST region name.
- `revision`: Sets the MST configuration revision number.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

instance

show spanning-tree mst
Displays MST protocol information.

spanning-tree mst configuration
Enters the MST configuration submode.

Command Description
To select an interface to configure and to enter interface configuration mode, use the `interface` command.

**Syntax Description**

- **Defaults**: No interface types are configured.

**Command Modes**: Global configuration mode

**Usage Guidelines**

Table 2-6 lists the valid values for `type`.

**Table 2-6 Valid type Values**

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet</td>
<td>Ethernet IEEE 802.3 interface.</td>
</tr>
<tr>
<td>fastethernet</td>
<td>100-Mbps Ethernet interface.</td>
</tr>
<tr>
<td>gigabitethernet</td>
<td>Gigabit Ethernet IEEE 802.3z interface.</td>
</tr>
<tr>
<td>tengigabitethernet</td>
<td>10-Gigabit Ethernet IEEE 802.3ae interface.</td>
</tr>
<tr>
<td>ge-wan</td>
<td>Gigabit Ethernet WAN IEEE 802.3z interface; supported on Catalyst 4500 series switches that are configured with a Supervisor Engine 2 only.</td>
</tr>
<tr>
<td>pos</td>
<td>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.</td>
</tr>
<tr>
<td>atm</td>
<td>ATM interface; supported on Catalyst 4500 series switches that are configured with a Supervisor Engine 2 only.</td>
</tr>
<tr>
<td>vlan</td>
<td>VLAN interface; see the <code>interface vlan</code> command.</td>
</tr>
<tr>
<td>port-channel</td>
<td>Port channel interface; see the <code>interface port-channel</code> command.</td>
</tr>
<tr>
<td>null</td>
<td>Null interface; the valid value is 0.</td>
</tr>
</tbody>
</table>

Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

interface

Examples

This 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.
To access or create a port-channel interface, use the `interface port-channel` command.

### Syntax Description

This command has no default settings.

### Command Modes
Global configuration mode

### Usage Guidelines
You do not have to create a port-channel interface before assigning a physical interface to a channel group. A port-channel interface is created automatically when the channel group gets its first physical interface, if it is not already created. You can also create the port channels by entering the `interface port-channel` command. This will create a Layer 3 port channel. To change the Layer 3 port channel into a Layer 2 port channel, use the `switchport` command before you assign the physical interfaces to the channel group. A port channel cannot be changed from Layer 3 to Layer 2 or vice versa when it contains member ports.

### 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
- `channel-group`: Assigns and configures an EtherChannel interface to an EtherChannel group.
- `show etherchannel`: Displays EtherChannel information for a channel.
To run a command on multiple ports at the same time, use the `interface range` command.

```plaintext
interface range
vlan vlan_id - vlan_id
port-range
macro name
```

### Syntax Description

- **Defaults**
  This command has no default settings.
- **Command Modes**
  - Global configuration mode
  - Interface configuration mode

### Usage Guidelines

- You can use the `interface range` command on the existing VLAN SVIs only. To display the VLAN SVIs, enter the `show running-config` command. The VLANs that are not displayed cannot be used in the `interface range` command.
- The values that are entered with the `interface range` command are applied to all the existing VLAN SVIs.
- Before you can use a macro, you must define a range using the `define interface-range` command.
- All configuration changes that are made to a port range are saved to NVRAM, but the port ranges that are created with the `interface range` command do not get saved to NVRAM.
- You can enter the port range in two ways:
  1. Specifying up to five port ranges
  2. 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 (-):
  ```plaintext
  interface range gigabitethernet 5/1 -20, gigabitethernet4/5 -20
  ```
- Use these formats when entering the `port-range`:
  1. `interface-type {mod} / {first-port} - {last-port}`
  2. `interface-type {mod} / {first-port} - {last-port}`

### Valid values for `interface-type`

- FastEthernet
- GigabitEthernet

### Examples

- `vlan 10 - 20`
- `interface range gigabitethernet 5/1 -20, gigabitethernet4/5 -20`
interface range

You cannot specify both a macro and an interface range in the same command. After creating a macro, you can enter additional ranges. If you have already entered an interface range, the CLI does not allow you to enter a macro.

You can specify a single interface in the port-range value. This makes the command similar to the interface interface-number command.

Examples

This example shows how to use the interface range command to interface to FE 5/18 - 20:

```
Switch(config)#
interface range fastethernet 5/18 - 20
Switch(config-if)#
```

This command shows how to run a port-range macro:

```
Switch(config)#
interface range macro macro1
Switch(config-if)#
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>define interface-range</td>
<td>Creates a macro of interfaces.</td>
</tr>
<tr>
<td>show running config</td>
<td>(refer to Cisco IOS documentation) Displays the running configuration for a switch.</td>
</tr>
</tbody>
</table>
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
```

**Syntax Description**

- `vlan_id`: Number of the VLAN; valid values are from 1 to 4094.

**Defaults**

Fast EtherChannel is not specified.

**Command Modes**

Global configuration mode

**Usage Guidelines**

The SVIs are created the first time that you enter the `interface vlan vlan_id` command for a particular VLAN. The `vlan_id` value corresponds to the VLAN tag that is associated with the data frames on an ISL or 802.1Q-encapsulated trunk or the VLAN ID that is configured for an access port. A message is displayed whenever a VLAN interface is newly created, so you can check that you entered the correct VLAN number.

If you delete an SVI by entering the `no interface vlan vlan_id` command, the associated interface is forced into an administrative down state and marked as deleted. The deleted interface will no longer be visible in a `show interface` command.

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

**Examples**

This example shows the output when you enter the `interface vlan vlan_id` command for a new VLAN number:

```
Switch(config)#
interface vlan 23
% Creating new VLAN interface.
```

[290x374]Catalyst 4500 Series Switch Cisco IOS Command Reference—Release IOS XE 3.3.0XO(15.1(1)XO)

Chapter 2      Cisco IOS Commands for  the Catalyst 4500 Series Switches

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
```

**Syntax Description**

- `vlan_id`: Number of the VLAN; valid values are from 1 to 4094.

**Defaults**

Fast EtherChannel is not specified.

**Command Modes**

Global configuration mode

**Usage Guidelines**

The SVIs are created the first time that you enter the `interface vlan vlan_id` command for a particular VLAN. The `vlan_id` value corresponds to the VLAN tag that is associated with the data frames on an ISL or 802.1Q-encapsulated trunk or the VLAN ID that is configured for an access port. A message is displayed whenever a VLAN interface is newly created, so you can check that you entered the correct VLAN number.

If you delete an SVI by entering the `no interface vlan vlan_id` command, the associated interface is forced into an administrative down state and marked as deleted. The deleted interface will no longer be visible in a `show interface` command.

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

**Examples**

This example shows the output when you enter the `interface vlan vlan_id` command for a new VLAN number:

```
Switch(config)#
interface vlan 23
% Creating new VLAN interface.
```
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

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.

**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

**Defaults**

If you do not enter this command, if any of the customized web-based authentication page files with the file of same name have been changed, you see the old login page rather than the new file.

**Command Modes**

Global configuration mode

**Usage Guidelines**

You should enter this command whenever the customized web-based authentication page has been changed in the system directory.

**Examples**

This example shows how to enter this command:

```
Switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip admission proxy http [success | failure | refresh-all | login]
Switch(config)# end
```

Switch# <The new html page is observed.>

```
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

static
```

### Syntax Description

- **ip arp inspection**
  - `filter arp-acl-name`
  - `vlan vlan-range` (optional)
  - `static` (optional)

### Defaults

No defined ARP ACLs are applied to any VLAN.

### Command Modes

- Global configuration mode

### Usage Guidelines

When an ARP access control list is applied to a VLAN for dynamic ARP inspection, the ARP packets containing only the IP-to-Ethernet MAC bindings are compared against the ACLs. All other packet types are bridged in the incoming VLAN without validation.

This command specifies that the incoming ARP packets are compared against the ARP access control list, and the packets are permitted only if the access control list permits them.

If the access control lists deny the packets because of explicit denies, the packets are dropped. If the packets are denied because of an implicit deny, they are then matched against the list of DHCP bindings if the ACL is not applied statically.

### Examples

This example shows how to apply the ARP ACL static hosts to VLAN 1 for DAI:

```
Switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip arp inspection filter static-hosts vlan 1
Switch(config)#
```

```
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
----     -----------      ------------
```

### Syntax

- **arp-acl-name**
  - Access control list name.
- **vlan-range**
  - VLAN number or range; valid values are from 1 to 4094.
- **static**
  - (Optional) Specifies that the access control list should be applied statically.
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip arp inspection filter vlan</td>
<td>Defines an ARP access list or adds clauses at the end of a predefined list.</td>
</tr>
<tr>
<td>show ip arp inspection</td>
<td>Displays the status of dynamic ARP inspection for a specific range of VLANs.</td>
</tr>
</tbody>
</table>
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

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]
```

**Syntax Description**

- `rate pps`: Specifies an upper limit on the number of incoming packets processed per second. The rate can range from 1 to 10000.
- `none`: Specifies no upper limit on the rate of the incoming ARP packets that can be processed.
- `burst interval seconds`: (Optional) Specifies the consecutive interval in seconds over which the interface is monitored for the high rate of the ARP packets. The interval is configurable from 1 to 15 seconds.

**Defaults**

- The rate is set to 15 packets per second on the untrusted interfaces, assuming that the network is a switched network with a host connecting to as many as 15 new hosts per second.
- The rate is unlimited on all the trusted interfaces.
- The burst interval is set to 1 second by default.

**Command Modes**

- Interface configuration mode

**Usage Guidelines**

- The 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.
ip arp inspection limit (interface)

Examples

This example shows how to limit the rate of the incoming ARP requests to 25 packets per second:

Switch#
config terminal
Switch(config)#
interface 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#

This example shows how to limit the rate of the incoming ARP requests to 20 packets per second and to set the interface monitoring interval to 5 consecutive seconds:

Switch#
config terminal
Switch(config)#
interface 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 number`: Number of entries from the logging buffer; the range is from 0 to 1024.
- `logs number`: Number of entries to be logged in an interval; the range is from 0 to 1024. A 0 value indicates that entries should not be logged out of this buffer.
- `interval seconds`: Logging rate; the range is from 0 to 86400 (1 day). A 0 value indicates an immediate log.

**Defaults**

- When dynamic ARP inspection is enabled, denied, or dropped, the ARP packets are logged.
- The number of entries is set to 32.
- The number of logging entries is limited to 5 per second.
- The interval is set to 1.

**Command Modes**

- Global configuration mode

**Usage Guidelines**

The first dropped packet of a given flow is logged immediately. The subsequent packets for the same flow are registered but are not logged immediately. Registering these packets is done in a log buffer that is shared by all the VLANs. Entries from this buffer are logged on a rate-controlled basis.

**Examples**

This example shows how to configure the logging buffer to hold up to 45 entries:

```
Switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip arp inspection log-buffer entries 45
Switch(config)# end
```

```
Switch# show ip arp inspection log
Total Log Buffer Size : 45
Syslog rate : 5 entries per 1 seconds.
No entries in log buffer.
```

This example shows how to configure the logging rate to 10 logs per 3 seconds:

```
Switch(config)# ip arp inspection log-buffer logs 10 interval 3
Switch(config)# end
```

```
Switch# show ip arp inspection log
Total Log Buffer Size : 45
Syslog rate : 10 entries per 3 seconds.
No entries in log buffer.
```
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

**ip arp inspection log-buffer**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>arp access-list</code></td>
<td>Defines an ARP access list or adds clauses at the end of a predefined list.</td>
</tr>
<tr>
<td><code>show ip arp inspection</code></td>
<td>Displays the status of dynamic ARP inspection for a specific range of VLANs.</td>
</tr>
</tbody>
</table>
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.

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Interface configuration mode

**Examples**

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

```plaintext
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:

```plaintext
Switch# show ip arp inspection interfaces fastEthernet 6/3
Interface        Trust State     Rate (pps)  Burst Interval
---------------  -----------     ----------  ------------
 Fa6/3            Trusted               None        1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip arp inspection</code></td>
<td>Displays the status of dynamic ARP inspection for a specific range of VLANs.</td>
</tr>
</tbody>
</table>
To perform specific checks for ARP inspection, use the `ip arp inspection validate` command. To disable checks, use the `no` form of this command.

```
src-mac
```

```
dst-mac
```

```
ip
```

**Syntax Description**

**Defaults**
Checks are disabled.

**Command Modes**
Global configuration mode

**Usage Guidelines**
When enabling the checks, specify at least one of the keywords (`src-mac`, `dst-mac`, and `ip`) on the command line. Each command overrides the configuration of the previous command. If a command enables `src` and `dst-mac` validations, and a second command enables IP validation only, the `src` and `dst-mac` validations are disabled as a result of the second command.

The `no` form of this command disables only the specified checks. If none of the check options are enabled, all the checks are disabled.

**Examples**
This example shows how to enable the source MAC validation:

```
Switch(config) #
ip arp inspection validate src-mac
Switch(config) #
en
Switch#
show ip arp inspection vlan 1
```

Source Mac Validation : Enabled
Destination Mac Validation : Disabled
IP Address Validation : Disabled

**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.
### Chapter 2      Cisco IOS Commands for  the Catalyst 4500 Series Switches

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Configuration</th>
<th>Operation</th>
<th>ACL Match</th>
<th>Static ACL</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enabled</td>
<td>Active</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Vlan</th>
<th>ACL Logging</th>
<th>DHCP Logging</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Deny</td>
<td>Deny</td>
</tr>
</tbody>
</table>

Switch#  

**Related Commands**

- `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.
To enable dynamic ARP inspection (DAI) on a per-VLAN basis, use the `ip arp inspection` command. To disable DAI, use the `no` form of this command.

```
ip arp inspection vlan

Syntax Description

Defaults
ARP inspection is disabled on all VLANs.

Command Modes
Global configuration mode

Usage Guidelines
You must specify on which VLANs to enable DAI. DAI may not function on the configured VLANs if they have not been created or if they are private.

Examples
This example shows how to enable DAI on VLAN 1:

```
Switch# configure terminal
Switch(config)# ip arp inspection vlan 1
Switch(config)# end
Switch# show ip arp inspection vlan 1
Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

Vlan     Configuration    Operation   ACL Match          Static ACL
----     -------------    ---------   ---------          ----------
1     Enabled          Active

Vlan     ACL Logging      DHCP Logging
----     -----------      ------------
1     Deny             Deny
```

This example shows how to disable DAI on VLAN 1:

```
Switch# configure terminal
Switch(config)# no ip arp inspection vlan 1
```

VLAN number or range; valid values are from 1 to 4094.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip arp inspection vlan</td>
<td>Defines an ARP access list or adds clauses at the end of a predefined list.</td>
</tr>
<tr>
<td>show ip arp inspection</td>
<td>Displays the status of dynamic ARP inspection for a specific range of VLANs.</td>
</tr>
</tbody>
</table>
Chapter 2  

Cisco IOS Commands for the Catalyst 4500 Series Switches

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

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

syntax description

defaults

all denied or dropped packets are logged.

command modes

global configuration mode

usage guidelines

the acl-match and dhcp-bindings keywords merge with each other. when you set an acl match configuration, the dhcp bindings configuration is not disabled. you can use the no form of this command to reset some of the logging criteria to their defaults. if you do not specify either option, all the logging types are reset to log on when the arp packets are denied. the two options that are available to you are as follows:

1. acl-match — logging on acl matches is reset to log on deny
2. dhcp-bindings — logging on dhcp binding compared is reset to log on deny

examples

this example shows how to configure an arp inspection on vlan 1 to add packets to a log on matching against the acl's with the logging keyword:

switch# config terminal

switch(config)#

vlan-range

number of the vlan's 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 acl's 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 ace's. 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.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

ip arp inspection vlan logging
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.
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 | original | tunnel | universal}
```

**Syntax Description**
- **include-ports** Specifies the algorithm that includes the Layer 4 ports.
  - **source** Specifies the source port in the load-balancing hash functions.
  - **destination** 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.

**Defaults**
Default load-sharing algorithm is disabled.

**Note**
This option does not include the source or destination port in the load-balancing hash.

**Command Modes**
Global configuration mode

**Usage Guidelines**
The original algorithm, tunnel algorithm, and universal algorithm are 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**
This example shows how to configure the IP CEF load-sharing algorithm that includes Layer 4 ports:

```
Switch(config) #
ip cef load-sharing algorithm include-ports
Switch(config) #
```
This example shows how to configure the 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.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

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**

- **Defaults**
  - This command has no default settings.

- **Command Modes**
  - Interface configuration mode

**Examples**

This example shows how to enable IP port security with IP-MAC filters on a Layer 2 access port:

```
Switch# configure terminal
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)#
```

You can verify your settings by entering the `show ip verify source` privileged EXEC command.

**Related Commands**

- **number**
  - Specifies the number of bindings created in the IP device tracking table for a port, valid values are from 0 to 2048.
- **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.
To enable DHCP snooping globally, use the `ip dhcp snooping` command. To disable DHCP snooping, use the `no` form of this command.

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

DHCP snooping is disabled.

**Command Modes**

Global configuration mode

**Usage Guidelines**

You must enable DHCP snooping globally before you can use DHCP snooping on a VLAN.

**Examples**

This example shows how to enable DHCP snooping:

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

This example shows how to disable DHCP snooping:

```
Switch(config) #
no ip dhcp snooping
Switch(config) #
```

**Related Commands**

- `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.
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-name expiry seconds
```

**Syntax Description**
- `mac-address`: Specifies a MAC address.
- `vlan`: Specifies a valid VLAN number.
- `ip-address`: Specifies an IP address.
- `interface`: Specifies an interface type and number.
- `expiry`: Specifies the interval (in seconds) after which binding is no longer valid.

**Defaults**
This command has no default settings.

**Command Modes**
Privileged EXEC mode

**Usage Guidelines**
Whenever a binding is added or removed using this command, the binding database is marked as changed and a write is initiated.

**Examples**
This example shows how to generate a DHCP binding configuration on interface gigabitethernet1/1 in VLAN 1 with an expiration time of 1000 seconds:

```
Switch# ip dhcp snooping binding 0001.1234.1234 vlan 1 172.20.50.5 interface gi1/1 expiry 1000
```

**Related Commands**
- `mac-address`
- `vlan vlan-ip`
- `ip-address`
- `interface interface-name`
- `expiry seconds`
- `ip dhcp snooping`
- `ip dhcp snooping information option`
- `ip dhcp snooping trust`
- `ip dhcp snooping vlan`
- `show ip dhcp snooping`
- `show ip dhcp snooping binding`
To store the bindings that are generated by DHCP snooping, use the `ip dhcp snooping database` command. To either reset the timeout, reset the write-delay, or delete the agent specified by the URL, use the `no` form of this command.

```
ip dhcp snooping database
    { url | timeout seconds | write-delay seconds }
no ip dhcp snooping database
    { timeout | write-delay }
```

**Syntax Description**

- `url`: Specifies the URL in one of the following forms:
  - `tftp://<host>/<filename>`
  - `ftp://<user>:<password>@<host>/<filename>`
  - `rcp://<user>@<host>/<filename>`
  - `nvram:/<filename>`
  - `bootflash:/<filename>`

- `timeout seconds`: Specifies when to abort the database transfer process after a change to the binding database.
  - The minimum value of the delay is 15 seconds. 0 is defined as an infinite duration.

- `write-delay seconds`: Specifies the duration for which the transfer should be delayed after a change to the binding database.

**Defaults**

- The timeout value is set to 300 seconds (5 minutes).
- The write-delay value is set to 300 seconds.

**Command Modes**

- Interface configuration mode

**Usage Guidelines**

You need to create an empty file at the configured URL on network-based URLs (such as TFTP and FTP) before the switch can write the set of bindings for the first time at the URL.

**Note**

Because both NVRAM and bootflash have limited storage capacity, using TFTP or network-based files is recommended. If you use flash to store the database file, new updates (by the agent) result in the creation of new files (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.
ip dhcp snooping database

Examples

This example shows how to store a database file with the IP address 10.1.1.1 within a directory called directory. A file 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 Succeded 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.
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.

```
Configure terminal
ip dhcp snooping
ip dhcp snooping vlan 500 555
ip dhcp snooping information option format remote-id hostname
interface GigabitEthernet 5/1
ip dhcp snooping trust
ip dhcp snooping limit rate 100
interface FastEthernet 2/1
format remote-id string customer-555
```

### 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.

### Defaults

DHCP option 82 data insertion is enabled.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

ip dhcp snooping information option

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.

Syntax Description

This command has no arguments or keywords.

Defaults

DHCP packets with option 82 are not allowed on snooping untrusted ports.

Command Modes

Global configuration mode

Examples

This example shows how to allow DHCP packets with option 82 data inserted to be received from a snooping untrusted port:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip dhcp snooping information option allow-untrusted
Switch(config)# end
Switch#
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip dhcp snooping</td>
<td>Globally enables DHCP snooping.</td>
</tr>
<tr>
<td>ip dhcp snooping information option</td>
<td>Enables DHCP option 82 data insertion.</td>
</tr>
<tr>
<td>ip dhcp snooping limit rate</td>
<td>Configures the number of the DHCP messages that an interface can receive per second.</td>
</tr>
<tr>
<td>ip dhcp snooping trust</td>
<td>Enables DHCP snooping on a trusted VLAN.</td>
</tr>
<tr>
<td>ip dhcp snooping vlan</td>
<td>Enables DHCP snooping on a VLAN or a group of VLANs.</td>
</tr>
<tr>
<td>show ip dhcp snooping</td>
<td>Displays the DHCP snooping configuration.</td>
</tr>
<tr>
<td>show ip dhcp snooping binding</td>
<td>Displays the DHCP snooping binding entries.</td>
</tr>
</tbody>
</table>
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.

**Syntax Description**

- `ip dhcp snooping limit rate <rate>`
- `no ip dhcp snooping limit rate`

**Defaults**

DHCP snooping rate limiting is disabled.

**Command Modes**

- Interface configuration mode

**Usage Guidelines**

Typically, the rate limit applies to the untrusted interfaces. If you want to set up rate limiting for the trusted 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**

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

```
Switch(config-if)#
ip dhcp snooping limit rate 150
Switch(config)#
```

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

```
Switch(config-if)#
no ip dhcp snooping limit rate
Switch(config)#
```

**Related Commands**

- `rate`
  - **Number of DHCP messages a switch can receive per second.**
- `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.**
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.

```
Switch(config-if)# ip dhcp snooping trust
Switch(config)#
```

```
Switch(config-if)# no ip dhcp snooping trust
Switch(config)#
```

Syntax Description
This command has no arguments or keywords.

Defaults
DHCP snooping trust is disabled.

Command Modes
Interface configuration mode

Related Commands
- `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.

```
[switch] ip dhcp snooping vlan [number]
```

**Syntax Description**

- `number` (Optional) Single VLAN number or a range of VLANs; valid values are from 1 to 4094.

**Defaults**

DHCP snooping is disabled.

**Command Modes**

Global configuration mode

**Usage Guidelines**

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

**Examples**

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

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

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

```
Switch(config) #
no ip dhcp snooping vlan 10
Switch(config) #
```

This example shows how to enable DHCP snooping on a group of VLANs:

```
Switch(config) #
ip dhcp snooping vlan 10 55
Switch(config) #
```

This example shows how to disable DHCP snooping on a group of VLANs:

```
Switch(config) #
no ip dhcp snooping vlan 10 55
Switch(config) #
```
### Chapter 2      Cisco IOS Commands for  the Catalyst 4500 Series Switches

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip dhcp snooping</code></td>
<td>Globally enables DHCP snooping.</td>
</tr>
<tr>
<td><code>ip dhcp snooping information option</code></td>
<td>Enables DHCP option 82 data insertion.</td>
</tr>
<tr>
<td><code>ip dhcp snooping limit rate</code></td>
<td>Configures the number of the DHCP messages that an interface can receive per second.</td>
</tr>
<tr>
<td><code>ip dhcp snooping trust</code></td>
<td>Enables DHCP snooping on a trusted VLAN.</td>
</tr>
<tr>
<td><code>ip dhcp snooping vlan information</code></td>
<td>Enables circuit-id (a suboption of DHCP snooping option-82) on a VLAN.</td>
</tr>
<tr>
<td><code>show ip dhcp snooping</code></td>
<td>Displays the DHCP snooping configuration.</td>
</tr>
<tr>
<td><code>show ip dhcp snooping binding</code></td>
<td>Displays the DHCP snooping binding entries.</td>
</tr>
</tbody>
</table>
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
```

### Syntax Description

- **number**
  - Specifies single or range of VLANs; valid values are from 1 to 4094.
- **override** (Optional)
  - Specifies an override string.
- **string**
  - Specifies a user-defined string for the circuit ID; range of 3 to 63 ASCII characters with no spaces.

### Defaults

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

### Command Modes

Interface configuration

### 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
```

This example shows how to configure the option-82 circuit-ID override suboption:
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip dhcp snooping</td>
<td>Globally enables DHCP snooping.</td>
</tr>
<tr>
<td>ip dhcp snooping info</td>
<td>Enables DHCP option 82 data insertion.</td>
</tr>
<tr>
<td>ip dhcp snooping limit</td>
<td>Configures the number of DHCP messages an interface can receive per second.</td>
</tr>
<tr>
<td>ip dhcp snooping trust</td>
<td>Enables DHCP snooping on a trusted VLAN.</td>
</tr>
<tr>
<td>ip dhcp snooping vlan</td>
<td>Enables DHCP snooping on a VLAN or a group of VLANs.</td>
</tr>
<tr>
<td>show ip dhcp snooping</td>
<td>Displays the DHCP snooping configuration.</td>
</tr>
<tr>
<td>show ip dhcp snooping binding</td>
<td>Displays the DHCP snooping binding entries.</td>
</tr>
</tbody>
</table>
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**

- **Defaults**: Profiles are not applied.
- **Command Modes**: Interface configuration mode

**Usage Guidelines**

- You can apply IGMP filters only to Layer 2 physical interfaces; you cannot apply IGMP filters to routed ports, switch virtual interfaces (SVIs), or ports that belong to an EtherChannel group.
- An IGMP profile can be applied to one or more switch port interfaces, but one port can have only one profile applied to it.

**Examples**

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

```
Switch(config)#
interface gigabitethernet1/1
Switch(config-if)#
ip igmp filter 22
Switch(config-if)#
```

**Related Commands**

- `profile number` - IGMP profile number to be applied; valid values are from 1 to 429496795.
- `ip igmp profile` - Creates an IGMP profile.
- `show ip igmp profile` - Displays all configured IGMP profiles or a specified IGMP profile.
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
```

**Syntax Description**

- `number`: Maximum number of IGMP groups that an interface can join; valid values are from 0 to 4294967294.

**Defaults**

No maximum limit.

**Command Modes**

Interface configuration mode

**Usage Guidelines**

You can use the `ip igmp max-groups` command only on Layer 2 physical interfaces; you cannot set the IGMP maximum groups for the routed ports, the switch virtual interfaces (SVIs), or the ports that belong to an EtherChannel group.

**Examples**

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

```
Switch(config)#
interface gigabitethernet1/1
Switch(config-if)#
ip igmp max-groups 25
Switch(config-if)
```
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

ip igmp profile

To create an IGMP profile, use the `ip igmp profile` command. To delete the IGMP profile, use the `no` form of this command.

```
ip igmp profile profile number
no ip igmp profile profile number
```

**Syntax Description**

- **profile number**: IGMP profile number being configured; valid values are from 1 to 4294967295.

**Command Modes**

- Global configuration mode
- IGMP profile configuration

**Usage Guidelines**

When entering a range, enter the low IP multicast address, a space, and the high IP multicast address.

You can apply an IGMP profile to one or more Layer 2 interfaces, but each interface can have only one profile applied to it.

**Examples**

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

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

**Related Commands**

- `profile number`: IGMP profile number being configured; valid values are from 1 to 4294967295.
- `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.
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
```

**Syntax Description**

- **seconds**: Frequency, in seconds, at which the IGMP host-query messages are transmitted; valid values depend on the IGMP snooping mode. See the "Usage Guidelines" section for more information.

**Defaults**

The query interval is set to 60 seconds.

**Command Modes**

Interface configuration mode

**Usage Guidelines**

If you use the default IGMP snooping configuration, the valid query interval values are from 1 to 65535 seconds. If you have 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**

This example shows how to change the frequency at which the designated switch sends the IGMP host-query messages:

```
Switch(config-if)#
ip igmp query-interval 120
Switch(config-if)#
```

**Related Commands**

- `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.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

**ip igmp query-interval**

Configures the frequency of Protocol Independent Multicast (PIM) router query messages.

**show ip igmp groups**

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.
To enable IGMP snooping, use the `ip igmp snooping` command. To disable IGMP snooping, use the `no` form of this command.

```plaintext
ip igmp snooping [tcn {flood query count count | query solicit}]
no ip igmp snooping [tcn {flood query count count | query solicit}]
```

**Syntax Description**
- `ip igmp snooping`: Enables IGMP snooping.
- `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 count`: (Optional) Specifies how often the spanning tree table is flooded; valid values are from 1 to 10.
  - `solicit`: (Optional) Specifies an IGMP general query.

**Defaults**
IGMP snooping is enabled.

**Command Modes**
- Global configuration mode
- Interface configuration mode

**Usage Guidelines**
- The `tcn flood` option applies only to Layer 2 switch ports and EtherChannels; it does not apply to routed ports, VLAN interfaces, or Layer 3 channels.
- The `ip igmp snooping` command is disabled by default on multicast routers.

**Note**
You can use the `tcn flood` option in interface configuration mode.

**Examples**
- This example shows how to enable IGMP snooping:
  ```plaintext
  Switch(config)##
pip igmp snooping
  Switch(config)##
  ```
- This example shows how to disable IGMP snooping:
  ```plaintext
  Switch(config)##
  no ip igmp snooping
  Switch(config)##
  ```
- This example shows how to enable the flooding of the spanning tree table to the network after nine topology changes have occurred:
  ```plaintext
  Switch(config)##
ip igmp snooping tcn flood query count 9
  Switch(config)##
  ```
- This example shows how to disable the flooding of the spanning tree table to the network:
  ```plaintext
  Switch(config)##
ip igmp snooping tcn flood query count 9
  ```
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

**ip igmp snooping**

Switch(config)#

```plaintext
no ip igmp snooping tcn flood
```

Switch(config)#

This example shows how to enable an IGMP general query:

Switch(config)#

```plaintext
ip igmp snooping tcn query solicit
```

Switch(config)#

This example shows how to disable an IGMP general query:

Switch(config)#

```plaintext
no ip igmp snooping tcn query solicit
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip igmp snooping vlan immediate-leave</td>
<td>Enable IGMP immediate-leave processing.</td>
</tr>
<tr>
<td>ip igmp snooping vlan mrouter interface</td>
<td>Configures a Layer 2 interface as a multicast router interface for a VLAN.</td>
</tr>
<tr>
<td>ip igmp snooping vlan static</td>
<td>Configures a Layer 2 interface as a member of a group.</td>
</tr>
</tbody>
</table>
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.

Defaults
IGMP snooping report-suppression is enabled.

Command Modes
Global configuration mode

Usage Guidelines
If the `ip igmp snooping report-suppression` command is disabled, all the IGMP reports are forwarded to the multicast devices. If the command is enabled, report suppression is done by IGMP snooping.

Examples
This example shows how to enable report suppression:
```
Switch(config)#
ip igmp snooping report-suppression
Switch(config)#
```

This example shows how to disable report suppression:
```
Switch(config)#
no ip igmp snooping report-suppression
Switch(config)#
```

This example shows how to display the system status for report suppression:
```
Switch#
show ip igmp 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#
```
### Chapter 2: Cisco IOS Commands for the Catalyst 4500 Series Switches

**Command: `ip igmp snooping report-suppression`**

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip igmp snooping vlan immediate-leave</code></td>
<td>Enable IGMP immediate-leave processing.</td>
</tr>
<tr>
<td><code>ip igmp snooping vlan mrouter</code></td>
<td>Configures a Layer 2 interface as a multicast router interface for a VLAN.</td>
</tr>
<tr>
<td><code>ip igmp snooping vlan static</code></td>
<td>Configures a Layer 2 interface as a member of a group.</td>
</tr>
</tbody>
</table>
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.

**Syntax Description**

- **Command**: `ip igmp snooping vlan`  
- **Parameters**: `vlan-id`  

**Defaults**  
IGMP snooping is disabled.

**Command Modes**  
Global configuration mode

**Usage Guidelines**  
This command is entered in VLAN interface configuration mode only.

**Examples**

This example shows how to enable IGMP snooping on a VLAN:

```
Switch(config)#
ip igmp snooping vlan 200
Switch(config)#
```

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

```
Switch(config)#
no ip igmp snooping vlan 200
Switch(config)#
```

**Related Commands**

- `vlan-id`  
  Number of the VLAN; valid values are from 1 to 1001 and from 1006 to 4094.
- `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
- `ip igmp snooping vlan static`  
  Configures a Layer 2 interface as a member of a group.
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.

```plaintext
ip igmp snooping vlan <vlan-id> explicit-tracking
no ip igmp snooping vlan <vlan-id> explicit-tracking
```

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

**Defaults**
- Explicit host tracking is enabled.

**Command Modes**
- Global configuration mode

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

```
Switch(config) #
no ip igmp snooping vlan 200 explicit-tracking
Switch(config) #
end
Switch #
show ip igmp snooping vlan 200 | include explicit tracking
```

```
Global IGMP Snooping configuration:
-----------------------------------
IGMP snooping             : Enabled
IGMPv3 snooping           : Enabled
Report suppression        : Enabled
TCN solicit query         : Disabled
TCN flood query count     : 2
Vlan 2:
--------
IGMP snooping                  : Enabled
IGMPv2 immediate leave         : Disabled
Explicit host tracking         : Disabled
Multicast router learning mode : pim-dvmrp
CGMP interoperability mode     : IGMP_ONLY
Explicit host tracking         : Disabled
```

**Related Commands**
- `vlan_id`

**Command Description**
- `ip igmp snooping vlan immediate-leave`: Enables IGMP immediate-leave processing.
- `ip igmp snooping vlan mrouter`: Configures a Layer 2 interface as a multicast router interface for a VLAN.
- `ip igmp snooping vlan static`: Configures a Layer 2 interface as a member of a group.
- `show ip igmp snooping membership`: Displays host membership information.
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.

**Syntax Description**

**Defaults**

Immediate leave processing is disabled.

**Command Modes**

Global configuration mode

**Usage Guidelines**

You enter this command in global configuration mode only. Use the immediate-leave feature only when there is a single receiver for the MAC group for a specific VLAN. The immediate-leave feature is supported only with IGMP version 2 hosts.

**Examples**

This example shows how to enable IGMP immediate-leave processing on VLAN 4:

```
Switch(config) #
ip igmp snooping vlan 4 immediate-leave
Switch(config) #
```

This example shows how to disable IGMP immediate-leave processing on VLAN 4:

```
Switch(config) #
no ip igmp snooping vlan 4 immediate-leave
Switch(config) #
```

**Related Commands**

- `vlan_num`: Number of the VLAN; valid values are from 1 to 4094.
- `immediate-leave`: Enables immediate leave processing.
- `ip igmp snooping`: Enables IGMP snooping.
- `ip igmp snooping vlan mrouter`: Configures a Layer 2 interface as a multicast router interface for a VLAN.
- `ip igmp snooping vlan static`: Configures a Layer 2 interface as a member of a group.
- `show ip igmp interface`: Displays the information about the IGMP-interface status and configuration.
- `show mac-address-table multicast`: Displays information about the multicast MAC address table.
To statically configure a 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}}
```

**Syntax Description**

- `vlan vlan-id`: Specifies the VLAN ID number to use in the command; valid values are from 1 to 4094.
- `interface`: Specifies the next-hop interface to a multicast switch.
  - `fastethernet slot/port`: Specifies the Fast Ethernet interface; number of the slot and port.
  - `gigabitethernet slot/port`: Specifies the Gigabit Ethernet interface; number of the slot and port.
  - `tengigabitethernet slot/port`: Specifies the 10-Gigabit Ethernet interface; number of the slot and port.
  - `port-channel number`: Port-channel number; valid values are from 1 to 64.
- `learn`: Specifies the multicast switch learning method.
  - `cgmp`: Specifies the multicast switch snooping CGMP packets.
  - `pim-dvmrp`: Specifies the multicast switch snooping PIM-DVMRP packets.

**Defaults**

Multicast switch snooping PIM-DVMRP packets are specified.

**Command Modes**

Interface configuration mode

**Usage Guidelines**

You enter this command in VLAN interface configuration mode only.

The interface to the switch must be in the VLAN where you are entering the command. It must be both administratively up and line protocol up.

The CGMP learning method can decrease control traffic.

The learning method that you configure is saved in NVRAM.

The static connections to multicast interfaces are supported only on switch interfaces.

**Examples**

This example shows how to specify the next-hop interface to a multicast switch:

```
Switch(config-if) #
ip igmp snooping 400 mrouter interface fastethernet 5/6
Switch(config-if) #
```
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

`ip igmp snooping vlan mrouter`  
This example shows how to specify the multicast switch learning method:

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

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip igmp snooping</code></td>
<td>Enable IGMP snooping.</td>
</tr>
<tr>
<td><code>ip igmp snooping vlan immediate-leave</code></td>
<td>Enable IGMP immediate-leave processing.</td>
</tr>
<tr>
<td><code>ip igmp snooping vlan static</code></td>
<td>Configures a Layer 2 interface as a member of a group.</td>
</tr>
<tr>
<td><code>show ip igmp snooping</code></td>
<td>Displays information on dynamically learned and manually configured VLAN switch interfaces.</td>
</tr>
<tr>
<td><code>show ip igmp snooping mrouter</code></td>
<td>Displays information on the dynamically learned and manually configured multicast switch interfaces.</td>
</tr>
</tbody>
</table>
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 slot/port |
  port-channel number |
```

**Syntax Description**

- **Defaults**: This command has no default settings.
- **Command Modes**: Global configuration mode.

**Examples**

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

```
Switch(config)#
ip igmp snooping vlan 4 static 0100.5e02.0203 interface fastethernet 5/11
```

Configuring port FastEthernet5/11 on group 0100.5e02.0203 vlan 4

```
Switch(config)#
```

**Related Commands**

- `vlan_num`: Number of the VLAN.
- `mac-address`: Group MAC address.
- `interface`: Specifies the next-hop interface to multicast switch.
- `fastethernet`: Number of the slot and port.
- `gigabitethernet`: Specifies the Gigabit Ethernet interface; number of the slot and port.
- `tengigabitethernet`: Specifies the 10-Gigabit Ethernet interface; number of the slot and port.
- `port-channel`: Port-channel number; valid values are from 1 through 64.

**Command Description**

- **ip igmp snooping**: Enable IGMP snooping.
- **ip igmp snooping vlan immediate-leave**: Enable IGMP immediate-leave processing.
- **ip igmp snooping vlan mrouter**: Configures a Layer 2 interface as a multicast router interface for a VLAN.
- **show mac-address-table multicast**: Displays information about the multicast MAC address table.
To enable the local proxy ARP feature, use the `ip local-proxy-arp` command. To disable the local proxy ARP feature, use the `no ip local-proxy-arp` command.

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

Local proxy ARP is disabled.

**Command Modes**

Interface configuration mode

**Usage Guidelines**

Use this feature only on subnets where hosts are intentionally prevented from communicating directly to the switch on which they are connected. ICMP redirect is disabled on interfaces where the local proxy ARP feature is enabled.

**Examples**

This example shows how to enable the local proxy ARP feature:
```
Switch(config-if) #
ip local-proxy-arp
Switch(config-if) #
```
To enable MFIB fast drop, use the `ip mfib fastdrop` command. To disable MFIB fast drop, use the `no` form of this command.

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

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

### Defaults
MFIB fast drop is enabled.

### Command Modes
Privileged EXEC mode

### Examples
This example shows how to enable MFIB fast drops:
```
Switch# ip mfib fastdrop
Switch#
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip mfib fastdrop</td>
<td>Clears all the MFIB fast-drop entries.</td>
</tr>
<tr>
<td>show ip mfib fastdrop</td>
<td>Displays all currently active fast-drop entries and shows whether fast drop is enabled.</td>
</tr>
</tbody>
</table>
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 ip multicast multipath` command.

**Syntax Description**

**Command Default**

If multiple equal-cost paths exist, multicast traffic will not be load-split across those paths.

**Command Modes**

Global configuration (config)

**Usage Guidelines**

The `ip multicast multipath` command does not work with bidirectional Protocol Independent Multicast (PIM).

Use the `ip multicast multipath` command to enable load splitting of IP multicast traffic across multiple equal-cost paths.

If two or more equal-cost paths from a source are available, unicast traffic will be load-split across those paths. However, by default, multicast traffic is not load-split across multiple equal-cost paths. In general, multicast traffic flows down from the reverse path forwarding (RPF) neighbor. According to the PIM specifications, this neighbor must have the highest IP address if more than one neighbor has the same metric.

When you configure load splitting with the `ip multicast multipath` command, the system splits multicast traffic across multiple equal-cost paths based on source address using the S-hash algorithm. When the `ip multicast multipath` command is configured and multiple equal-cost paths exist, the path in which multicast traffic will travel is selected based on the source IP address. Multicast traffic from different sources will be load-split across the different equal-cost paths. Load splitting will not occur across equal-cost paths for multicast traffic from the same source sent to different multicast groups.

**Note**

The `ip multicast multipath` command load splits the traffic but does not load balance the traffic. Traffic from a source will use only one path, even if the traffic greatly exceeds traffic from other sources.

**vrf**

(Optional) Enables ECMP multicast load splitting for IP multicast traffic associated with the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the `vrf-name` argument.

**s-g-hash**

`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.
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
```
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

vl an

interface

interface-name
```

**Syntax Description**

This command has no default settings.

**Command Modes**

Global configuration mode

**Usage Guidelines**

The `ip source binding` command is used to add a static IP source binding entry only. The `no` form of this command deletes the corresponding IP source binding entry. For the deletion to succeed, all required parameters must match.

Each static IP binding entry is keyed by a MAC address and VLAN number. If the CLI contains an existing MAC and VLAN, the existing binding entry will be updated with the new parameters; a separate binding entry will not be created.

**Examples**

This example shows how to configure the static IP source binding:

```
Switch# config terminal
Switch(config)# ip source binding 11.0.0.1 0000.000A.000B vlan 10 interface fastethernet6/10
Switch(config)#
```

**Related Commands**

- `ip-address`
- `mac-address`
- `vlan`
- `interface`
- `interface-name`

**Command Description**

`show ip source binding`
Displays IP source bindings that are configured on the system.
To enable sticky ARP, use the `ip sticky-arp` command. Use the `no` form of this command to disable sticky ARP.

Syntax Description
This command has no arguments or keywords.

Defaults
Enabled

Command Modes
Global configuration mode

Usage Guidelines
This command is supported on PVLANs only.
ARP entries that are learned on Layer 3 PVLAN interfaces are sticky ARP entries. (You should display and verify ARP entries on the PVLAN interface using the `show arp` command).
For security reasons, sticky ARP entries on the PVLAN interface do not age out. Connecting new equipment with the same IP address generates a message and the ARP entry is not created. Because the ARP entries on the PVLAN interface do not age out, you must manually remove ARP entries on the PVLAN interface if a MAC address changes.
Unlike static entries, sticky-ARP entries are not stored and restored when you enter the `reboot` and `restart` commands.

Examples
This example shows how to enable sticky ARP:
```console
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config) ip sticky-arp
Switch(config)#
```
This example shows how to disable sticky ARP:
```console
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config) no ip sticky-arp
Switch(config)#
```
### ip sticky-arp

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>arp</td>
<td>Enables Address Resolution Protocol (ARP) entries for static routing over the Switched Multimegabit Data Service (SMDS) network.</td>
</tr>
<tr>
<td>show arp</td>
<td>Displays ARP information.</td>
</tr>
</tbody>
</table>
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.

### Syntax Description

This command has no default settings.

### Defaults

The IP header is validated for bridged and routed IPv4 packets.

### Command Modes

Global configuration mode

### Usage Guidelines

This command does not apply to Layer 3-switched (routed) packets.

The Catalyst 4500 series switch checks the validity of the following fields in the IPv4 header for all switched IPv4 packets:

1. The version must be 4.
2. The header length must be greater than or equal to 20 bytes.
3. The total length must be greater than or equal to four times the header length and greater than the Layer 2 packet size minus the Layer 2 encapsulation size.

If an IPv4 packet fails the IP header validation, the packet is dropped. If you disable the header validation, the packets with the invalid IP headers are bridged but are not routed even if routing was intended. The IPv4 access lists also are not applied to the IP headers.

### Examples

This example shows how to disable the IP header validation for the Layer 2-switched IPv4 packets:

```
Switch# config terminal
Switch(config)# no ip verify header vlan all
Switch(config)# end
Switch#
```
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**

**Defaults**
IP source guard is disabled.

**Command Modes**
Global configuration mode

**Examples**
This example shows how to enable IP source guard on VLANs 10 through 20 on a per-port basis:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip dhcp snooping
Switch(config)# 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#
```

This example shows how to enable IP port security with IP-MAC filters on a Layer 2 access port:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip device tracking
Switch(config)# interface fastEthernet 4/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 1
Switch(config-if)# 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
```

**Related Commands**

- `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.
You can verify your settings by entering the `show ip verify source` privileged EXEC command.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip device tracking maximum</code></td>
<td>Enables IP port security binding tracking on a Layer 2 port.</td>
</tr>
<tr>
<td><code>ip dhcp snooping</code></td>
<td>Globally enables DHCP snooping.</td>
</tr>
<tr>
<td><code>ip dhcp snooping information option</code></td>
<td>Enables DHCP option 82 data insertion.</td>
</tr>
<tr>
<td><code>ip dhcp snooping limit rate</code></td>
<td>Configures the number of DHCP messages that an interface can receive per second.</td>
</tr>
<tr>
<td><code>ip dhcp snooping trust</code></td>
<td>Enables DHCP snooping on a trusted VLAN.</td>
</tr>
<tr>
<td><code>ip source binding</code></td>
<td>Adds or deletes a static IP source binding entry.</td>
</tr>
<tr>
<td><code>show ip dhcp snooping</code></td>
<td>Displays the DHCP snooping configuration.</td>
</tr>
<tr>
<td><code>show ip dhcp snooping binding</code></td>
<td>Displays the DHCP snooping binding entries.</td>
</tr>
<tr>
<td><code>show ip source binding</code></td>
<td>Displays IP source bindings that are configured on the system.</td>
</tr>
<tr>
<td><code>show ip verify source</code></td>
<td>Displays the IP source guard configuration and filters on a particular interface.</td>
</tr>
</tbody>
</table>
To enable and configure unicast RPF checks on an IPv4 interface, use the `ip verify unicast source reachable-via` command. To disable unicast RPF, use the `no` form of this command.

```
no ip verify unicast source reachable-via
```

### Syntax Description

**Defaults**

Disabled

**Command Modes**

Interface configuration mode

### 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

This example shows how to enable unicast RPF exist-only checking mode:

```
Switch# configure terminal
Switch(config) interface gigabitethernet1/1
Switch(config-if) ip verify unicast source reachable-via rx allow-default
Switch(config-if) end
Switch#
```

### Related Commands

- `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 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.
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]
```

**Syntax Description**

**Command Default**

WCCP services are not enabled on the router.

**Command Modes**

Global configuration (config)

**web-cache**

Specifies the web-cache service.

**service-number**

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**

multicast-address

(Optional) Multicast IP address that communicates with the WCCP service group. The multicast address is used by the router to determine which cache engine should receive redirected messages.

**redirect-list**

access-list

(Optional) Access list that controls traffic redirected to this service group. The `access-list` argument should consist of a string of no more than 64 characters (name or number) that specifies the access list.

**group-list**

access-list

(Optional) Access list that determines which cache engines are allowed to participate in the service group. The `access-list` argument specifies either the number or the name of a standard or extended access list.

**password**

[0 | 7] password

(Optional) Message digest algorithm 5 (MD5) authentication for messages received from the service group. Messages that are not accepted by the authentication are discarded. The encryption type can be 0 or 7, with 0 specifying not yet encrypted and 7 for proprietary. The `password` argument can be up to eight characters in length.
ip wccp
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
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
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
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip wccp check services all</td>
<td>Enables all WCCP services.</td>
</tr>
<tr>
<td>ip wccp version</td>
<td>Specifies which version of WCCP you wish to use on your router.</td>
</tr>
<tr>
<td>show ip wccp</td>
<td>Displays global statistics related to WCCP.</td>
</tr>
</tbody>
</table>
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 ip wccp check services all` command.

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

WCCP services are not enabled on the router.

**Command Modes**

Global configuration (config)

**Usage Guidelines**

With the `ip wccp check services all` command, WCCP can be configured to check all configured services for a match and perform redirection for those services if appropriate. The caches to which packets are redirected can be controlled by a redirect ACL access control list (ACL) as well as by the priority value of the service.

It is possible to configure an interface with more than one WCCP service. When more than one WCCP service is configured on an interface, the precedence of a service depends on the relative priority of the service compared to the priority of the other configured services. Each WCCP service has a priority value as part of its definition.

If no WCCP services are configured with a redirect ACL, the services are considered in priority order 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
```
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

ip wccp check services all

Related Commands

- 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.
- `service-number`: WCCP service number; valid values are from 0 to 254.

**Defaults**

This command is disabled by default.

**Command Modes**

- Interface configuration (config-if)

**Usage Guidelines**

On routers that are to be members of a Service Group when IP multicast is used, the following configuration is required:

- Configure the IP multicast address for use by the WCCP Service Group.
- Configure the interfaces on which the router wishes to receive the IP multicast address with the `ip wccp {web-cache | service-number} group-listen` interface configuration command.

**Examples**

The following example shows how to enable the multicast packets for a web cache with a multicast address of 224.1.1.100:

```
Switch# 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**

- `web-cache`: The web cache service.
- `service-number`: WCCP service number; valid values are from 0 to 254.

**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 group-listen

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.
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**

**Command Default**
Redirection checking on the interface is disabled.

**Command Modes**
Interface configuration (config-if)

**Usage Guidelines**
The `ip wccp {web-cache | service-number} redirect in` command allows you to configure WCCP redirection on an interface receiving inbound network traffic. When the command is applied to an interface, all packets arriving at that interface will be compared against the criteria defined by the specified WCCP service. If the packets match the criteria, they will be redirected.

Likewise, the `ip wccp {web-cache | service-number} redirect out` command allows you to configure the WCCP redirection check at an outbound interface.

**Tips**
Be careful not to confuse the `ip wccp {web-cache | service-number} redirect {in | out}` 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

<table>
<thead>
<tr>
<th>Command Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip wccp check services all</td>
</tr>
<tr>
<td>ip wccp group-listen</td>
</tr>
<tr>
<td>ip wccp redirect exclude in</td>
</tr>
<tr>
<td>show ip interface</td>
</tr>
<tr>
<td>show ip wccp</td>
</tr>
</tbody>
</table>
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.

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Redirection exclusion is disabled.

**Command Modes**

Interface configuration (config-if)

**Usage Guidelines**

This configuration command instructs the interface to exclude inbound packets from any redirection check. Note that the command is global to all the services and should be applied to any inbound interface that will be excluded from redirection.

This command is intended to be used to accelerate the flow of packets from a cache engine to the Internet as well as allow 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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip wccp enable</code></td>
<td>Enables support of the WCCP service for participation in a service group.</td>
</tr>
<tr>
<td><code>ip wccp redirect enable</code></td>
<td>Enables packet redirection on an inbound or outbound interface using Web Cache Communication Protocol (WCCP).</td>
</tr>
<tr>
<td><code>ip wccp redirect out</code></td>
<td>Configures redirection on an interface in the outgoing direction.</td>
</tr>
<tr>
<td><code>ip wccp check services all</code></td>
<td>Configures an interface on a router to enable or disable the reception of IP multicast packets for Web Cache Communication Protocol (WCCP).</td>
</tr>
<tr>
<td><code>ip wccp group-listen</code></td>
<td>Configures an interface on a router to enable or disable the reception of IP multicast packets for Web Cache Communication Protocol (WCCP).</td>
</tr>
<tr>
<td><code>ip wccp redirect exclude in</code></td>
<td>Enables redirection exclusion on an interface.</td>
</tr>
<tr>
<td><code>show ip interface</code></td>
<td>Displays the usability status of interfaces that are configured for IP.</td>
</tr>
<tr>
<td><code>show ip wccp</code></td>
<td>Displays the WCCP global configuration and statistics.</td>
</tr>
</tbody>
</table>
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

ipv6 mld snooping

To enable IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping globally or on the specified VLAN, use the `ipv6 mld snooping` command without keywords. To disable MLD snooping on a switch or the VLAN, use the `no` form of this command.

```
ipv6 mld snooping [vlan vlan-id]
no ipv6 mld snooping [vlan vlan-id]
```

Syntax Description

- `vlan vlan-id` (Optional) Enables or disables IPv6 MLD snooping on the specified VLAN.

Defaults

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

Usage Guidelines

- When MLD snooping is globally disabled, it is disabled on all the existing VLAN interfaces. When you globally enable MLD snooping, it is enabled on all VLAN interfaces that are in the default state (enabled). VLAN configuration overrides global configuration on interfaces on which MLD snooping has been disabled.
- If MLD snooping is globally disabled, you cannot enable it on a VLAN. If MLD snooping is globally enabled, you can disable it on individual VLANs.
- VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in MLD snooping.

Examples

This example shows how to globally enable MLD snooping:

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

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

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

You can verify your settings by entering the `show ipv6 mld snooping` user EXEC command.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipv6 mld snooping</td>
<td>Displays IP version 6 (IPv6) Multicast Listener Discovery</td>
</tr>
<tr>
<td></td>
<td>(MLD) snooping configuration of the switch or the VLAN.</td>
</tr>
</tbody>
</table>
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
```

**Syntax Description**

- **Command Default**: The default global count is 2.
- **The default VLAN count is 0 (the global count is used).**

**Command Modes**: Global configuration mode

**Usage Guidelines**

In MLD snooping, the IPv6 multicast switch periodically sends out queries to hosts belonging to the multicast group. If a host wants to leave a multicast group, it can silently leave or it can respond to the query with a Multicast Listener Done message (equivalent to an IGMP Leave message). When Immediate Leave is not configured (it should not be configured if multiple clients for a group exist on the same port), the configured last-listener query count determines the number of MASQs that are sent before an MLD client is aged out.

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

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

**Examples**

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

```
Switch# 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#
```

This example shows how to set the last-listener query count for VLAN 10:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ipv6 mld snooping vlan 10 last-listener-query-count 3
Switch(config)# end
Switch#
```
You can verify your settings by entering the `show ipv6 mld snooping` command.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 mld snooping</td>
<td>Configures IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping on the switch or on a VLAN.</td>
</tr>
<tr>
<td>show ipv6 mld snooping</td>
<td>Displays IP version 6 (IPv6) MLD snooping configuration of the switch or the VLAN.</td>
</tr>
<tr>
<td>show ipv6 mld snooping querier</td>
<td>Displays IP version 6 (IPv6) MLD snooping querier-related information most recently received by the switch or the VLAN.</td>
</tr>
</tbody>
</table>
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.

`ip v6 mld snooping [vlan vlan-id] last-listener-query-interval integer_value`

### Syntax Description

- `vlan` (Optional) Configures last-listener query interval on the specified VLAN.
- `integer_value` 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

### Usage Guidelines
- The last-listener-query-interval time is the maximum time that a multicast switch waits after issuing a Multicast Address Specific Query (MASQ) before deleting a port from the multicast group.
- In MLD snooping, when the IPv6 multicast switch receives an MLD leave message, it sends out queries to hosts belonging to the multicast group. If there are no responses from a port to a MASQ for a length of time, the switch deletes the port from the membership database of the multicast address. The last listener query interval is the maximum time that the switch waits before deleting a nonresponsive port from the multicast group.
- When a VLAN query interval is set, the global query interval is overridden. When the VLAN interval is set at 0, the global value is used.
- VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in MLD snooping.

### Examples

This example shows how to globally set the last-listener query interval to 2 seconds:

```
Switch# 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
```

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

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ipv6 mld snooping vlan 1 last-listener-query-interval 5500
```
ipv6 mld snooping last-listener-query-interval

Switch(config)#
end
Switch#

You can verify your settings by entering the `show ipv6 mld snooping` command.

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 mld snooping</td>
<td>Configures IP version 6 (IPv6) Multicast Listener Discovery Multicast Address Specific Queries (MASQs) that will be sent before aging out a client.</td>
</tr>
<tr>
<td>show ipv6 mld snooping querier</td>
<td>Displays IP version 6 (IPv6) MLD snooping querier-related information most recently received by the switch or the VLAN.</td>
</tr>
</tbody>
</table>
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.

```
Switch(config)＃
ipv6 mld snooping listener-message-suppression
Switch(config)＃
```

You can verify your settings by entering the `show ipv6 mld snooping [vlan vlan-id]` user EXEC command.

**Related Commands**

- `ip v6 mld snooping`: Enables IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping globally or on the specified VLAN.
- `show ipv6 mld snooping [vlan vlan-id]`: 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
```

**Syntax Description**

- **Command Default**
  - The default global robustness variable (number of queries before deleting a listener) is 2.
  - The default VLAN robustness variable (number of queries before aging out a multicast address) is 0, which means that the system uses the global robustness variable for aging out the listener.

- **Command Modes**
  - Global configuration mode

- **Usage Guidelines**
  - Robustness is measured by the number of MLDv1 queries sent with no response before a port is removed from a multicast group. A port is deleted when there are no MLDv1 reports received for the configured number of MLDv1 queries. The global value determines the number of queries that the switch waits before deleting a listener that does not respond, and it applies to all VLANs that do not have a VLAN value set.
  - The robustness value configured for a VLAN overrides the global value. If the VLAN robustness value is 0 (the default), the global value is used.
  - VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in MLD snooping.

- **Examples**
  - This example shows how to configure the global robustness variable so that the switch sends out three queries before it deletes a listener port that does not respond:
    ```
    Switch# configure terminal
    Enter configuration commands, one per line. End with CNTL/Z.
    Switch(config)# ipv6 mld snooping robustness-variable 3
    Switch(config)# end
    ```
  - This 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
    ```
You can verify your settings by entering the `show ipv6 mld snooping` [vlan vlan-id] user EXEC command.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ip v6 mld snooping</strong></td>
<td>Configures IP version 6 (IPv6) Multicast Listener Discovery Multicast Address Specific Queries (MASQs) that will be sent before aging out a client.</td>
</tr>
<tr>
<td><strong>show ipv6 mld snooping</strong></td>
<td>Displays IP version 6 (IPv6) MLD snooping configuration of the switch or the VLAN.</td>
</tr>
</tbody>
</table>
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}
```

### Syntax Description

- **Command Default**: TCN query soliciting is disabled.
- **When enabled**, the default flood query count is 2.

### Command Modes

- Global configuration mode

### Examples

This example shows how to enable TCN query soliciting:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ipv6 mld snooping tcn query solicit.
Switch(config)# end
```

This example shows how to set the flood query count to 5:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ipv6 mld snooping tcn flood query count 5.
Switch(config)# end
```

You can verify your settings by entering the `show ipv6 mld snooping` [vlan vlan-id] user EXEC command.

### Related Commands
- `flood query count integer_value`: Sets the flood query count, which is the number of queries that are sent before forwarding multicast data to only those ports requesting it. The range is 1 to 10.
- `query solicit`: Enables soliciting of TCN queries.
- `show ipv6 mld snooping [vlan vlan-id]`: Displays IP version 6 (IPv6) MLD snooping configuration of the switch or the 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.

### Syntax Description

<table>
<thead>
<tr>
<th>Command Default</th>
<th>Syntax</th>
</tr>
</thead>
</table>
| MLD snooping Immediate-Leave processing is disabled. | `ipv6 mld snooping vlan` [immediate-leave | mrouter | interface | interface-id | static]
| By default, there are no static IPv6 multicast groups. | `[ipv6-multicast-address | interface | interface-id]` |
| By default, there are no multicast switch ports. | |

### Command Modes

- Global configuration mode

### Usage Guidelines

- You should only configure the Immediate-Leave feature when there is only one receiver on every port in the VLAN. The configuration is saved in NVRAM.
- The `static` keyword is used for configuring the MLD member ports statically.
- The configuration and the static ports and groups are saved in NVRAM.
- VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in MLD snooping.

### Examples

This example shows how to enable MLD Immediate-Leave processing on VLAN 1:

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping vlan 1 immediate-leave
Switch(config)# end
Switch#
```
This example shows how to disable MLD Immediate-Leave processing on VLAN 1:

```
Switch#
configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
no ipv6 mld snooping vlan 1 immediate-leave
Switch(config)#
end
Switch#
```

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

```
Switch#
configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
ipv6 mld snooping vlan 1 mrouter interface GigabitEthernet1/1
Switch(config)#
end
Switch#
```

This example shows how to configure a static multicast group:

```
Switch#
configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
ipv6 mld snooping vlan 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` command.

---

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 mld snooping</td>
<td>Enables IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping globally or on the specified VLAN.</td>
</tr>
<tr>
<td>show ipv6 mld snooping vlan</td>
<td>Displays IP version 6 (IPv6) MLD snooping configuration of the switch or the VLAN.</td>
</tr>
</tbody>
</table>
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.

**Syntax Description**

There are no default settings

**Command Modes**

Privileged EXEC mode

**Usage Guidelines**

You can use the `issu abortversion` command at any time to stop the ISSU process. To complete the process enter the `issu commitversion` command. Before any action is taken, a check ensures that both supervisor engines are either in the run version (RV) or load version (LV) state. When the `issu abortversion` command is entered before the `issu runversion` command, the standby supervisor engine is reset and reloaded with the old image. When the `issu abortversion` command is entered after the `issu runversion` command, a change takes place and the new standby supervisor engine is reset and reloaded with the old image.

**Examples**

This example shows how you can reset and reload the standby supervisor engine:

Switch# issu abortversion 2
Switch#

**Related Commands**

- `active-slot`: Specifies the slot number for the current standby supervisor engine.
- `active-image-new`: (Optional) Name of the new image present in the current standby supervisor engine.
- `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.
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.

**Syntax Description**

**Defaults**
Rollback timer resets automatically 45 minutes after you enter the `issu runversion` command.

**Command Modes**
Privileged EXEC mode

**Usage Guidelines**
After you are satisfied with the new image and have confirmed the new supervisor engine is reachable 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**
This example shows how to halt the rollback timer and allow the ISSU process to continue:

```
Switch# issu acceptversion 2
```

**Related Commands**

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

**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.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

 Issu acceptversion
 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 runversion
 Configures the In Service Software Upgrade (ISU) rollback timer value.

 Show issu state
 Displays the ISSU state and current booted image name during the ISSU process.
To load the new Cisco IOS software image into the new standby supervisor engine, use the `issu commitversion` command.

### Syntax Description

#### Command Mode
- **Privileged EXEC mode**

### Defaults
- Enabled by default.

### 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

This example shows how you can configure the standby supervisor engine to be reset and reloaded with the new Cisco IOS software version:

```
Switch# issu commitversion 1
Switch# ...
```

### Related Commands

- **standby-slot**
  - Specifies the slot number for the currently active supervisor engine.
- **standby-image-new**
  - (Optional) Name of the new image on the currently active supervisor engine.
- **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.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

issu commitversion
Forces a change from the active supervisor engine to the standby supervisor engine and causes the newly active supervisor engine to run the new image specified.

show issu state
Displays the ISSU state and current booted image name during the ISSU process.
To start the ISSU process, use the `issu loadversion` command.

`issu loadversion active-slot active-image-new standby-slot standby-image-new [force]`

**Syntax Description**

- **active-slot**: Specifies the slot number for the currently active supervisor engine.
- **active-image-new**: Specifies the name of the new image on the currently active supervisor engine.
- **standby-slot**: Specifies the standby slot on the networking device.
- **standby-image-new**: Specifies the name of the new image on the standby supervisor engine.
- **force**: (Optional) Overrides the automatic rollback when the new Cisco IOS software version is detected to be incompatible.

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Usage Guidelines**

The `issu loadversion` command causes the standby supervisor engine to be reset and booted with the new Cisco IOS software image specified by the command. If both the old image and the new image are ISSU capable, ISSU compatible, and have no configuration mismatches, the standby supervisor engine moves into Stateful Switchover (SSO) mode, and both supervisor engines move into the load version (LV) state.

It will take several seconds after the `issu loadversion` command is entered for Cisco IOS software to load onto the standby supervisor engine and the standby supervisor engine to transition to SSO mode.

**Examples**

This example shows how to initiate the ISSU process:

```
Switch# issu loadversion 1 bootflash:new-image 2 slavebootflash:new-image
Switch#
```

**Related Commands**

- `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.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

issu loadversion
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 runversion

show issu state
Displays the ISSU state and current booted image name during the ISSU process.
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**

**Syntax Description**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Usage Guidelines**

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

This example shows how to force a change of the active-supervisor engine to standby-supervisor engine:

```
Switch# issu runversion 2
Switch#
```

**Related Commands**

- `standby-slot` (Specifies the standby slot on the networking device.
- `standby-image-new` (Optional) Specifies the name of the new image on the standby supervisor engine.

**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.
- `show issu state` (Displays the ISSU state and current booted image name during the ISSU process.)
To configure the In Service Software Upgrade (ISSU) rollback timer value, use the `issu set rollback-timer` command.

### Syntax Description

**Seconds**

Specfies the rollback timer value, in seconds. The valid timer value range is from 0 to 7200 seconds (2 hours). A value of 0 seconds disables the rollback timer.

### Defaults

Rollback timer value is 2700 seconds.

### Command Modes

Global configuration mode

### Usage Guidelines

Use the `issu set rollback-timer` command to configure the rollback timer value. You can only enable this command when the supervisor engines are in the init state.

### Examples

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

```
Switch# configure terminal
Switch(config)# issu set rollback-timer 3600
Switch(config)# end
Switch#
```

### Related Commands

- `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.
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]]
```

**Syntax Description**

- `cdp` (Optional) Enables tunneling of CDP.
- `stp` (Optional) Enables tunneling of STP.
- `vtp` (Optional) Enables tunneling of VTP.

**Defaults**

The default is that no Layer 2 protocol packets are tunneled.

**Command Modes**

Interface configuration mode

**Usage Guidelines**

You must enter this command, with or without protocol 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**

This example shows how to enable protocol tunneling for the CDP packets:

```
Switch(config-if) #
l2protocol-tunnel cdp
Switch(config-if)#
```

**Related Commands**

- `cdp` (Optional) Enables tunneling of CDP.
- `stp` (Optional) Enables tunneling of STP.
- `vtp` (Optional) Enables tunneling of VTP.

**Command Description**

- `l2protocol-tunnel cos` Configures the class of service (CoS) value for all tunneled Layer 2 protocol packets.
- `l2protocol-tunnel drop-threshold` Sets a drop threshold for the maximum rate of Layer 2 protocol packets per second to be received before an interface drops packets.
- `l2protocol-tunnel shutdown-threshold` Configures the protocol tunneling encapsulation rate.
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.

**Syntax**

```
l2protocol-tunnel cos value
no l2protocol-tunnel cos
```

**Syntax Description**

- **value**: Specifies the CoS priority value for tunneled Layer 2 protocol packets. The range is 0 to 7, with 7 being the highest priority.

**Defaults**

The default is to use the CoS value that is configured for data on the interface. If no CoS value is configured, the default is 5 for all tunneled Layer 2 protocol packets.

**Command Modes**

- Global configuration mode

**Usage Guidelines**

- When enabled, the tunneled Layer 2 protocol packets use this CoS value.
- The value is saved in NVRAM.

**Examples**

This example shows how to configure a Layer 2 protocol tunnel CoS value of 7:

```
Switch(config)\# l2protocol-tunnel cos 7
Switch(config)\#
```

**Related Commands**

- `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.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>l2protocol-tunnel</td>
<td>Enables protocol tunneling on an interface.</td>
</tr>
<tr>
<td>l2protocol-tunnel</td>
<td>Configures the class of service (CoS) value for all tunneled Layer 2 protocol packets.</td>
</tr>
<tr>
<td>l2protocol-tunnel</td>
<td>Configures the protocol tunneling encapsulation rate.</td>
</tr>
</tbody>
</table>

**Defaults**

The default is no drop threshold for the number of the Layer 2 protocol packets.

**Command Modes**

Interface configuration mode

**Usage Guidelines**

The `l2protocol-tunnel drop-threshold` command controls the number of protocol packets per second that are received on an interface before it drops packets. When no protocol option is specified with a keyword, the threshold is applied to each of the tunneled Layer 2 protocol types. If you also set a shutdown threshold on the interface, the drop-threshold value must be less than or equal to the shutdown-threshold value.

When the drop threshold is reached, the interface drops the Layer 2 protocol packets until the rate at which they are received is below the drop threshold.

**Examples**

This example shows how to configure the drop threshold rate:

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

**Related Commands**

- `cdp` (Optional) Specifies a drop threshold for CDP.
- `stp` (Optional) Specifies a drop threshold for STP.
- `vtp` (Optional) Specifies a drop threshold for VTP.
- `value` Specifies a threshold in packets per second to be received for encapsulation before the interface shuts down, or specifies the threshold before the interface drops packets. The range is 1 to 4096. The default is no threshold.
Chapter 2
Cisco IOS Commands for the Catalyst 4500 Series Switches

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 l2protocol-tunnel shutdown-threshold` command.

**Syntax Description**

- **cdp** (Optional) Specifies a shutdown threshold for CDP.
- **stp** (Optional) Specifies a shutdown threshold for STP.
- **vtp** (Optional) Specifies a shutdown threshold for VTP.
- **value** Specifies a threshold in packets per second to be received for encapsulation before the interface shuts down. The range is 1 to 4096. The default is no threshold.

**Command Modes**

- Interface configuration mode

**Usage Guidelines**

The `l2protocol-tunnel shutdown-threshold` command controls the number of protocol packets per second that are received on an interface before it shuts down. When no protocol 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**

This example shows how to configure the maximum rate:

```
Switch(config-if) #
l2protocol-tunnel shutdown-threshold cdp 50
Switch(config-if) #
```
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

l2protocol-tunnel shutdown-threshold

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.
To set the LACP priority for the physical interfaces, use the `lacp port-priority` command.

**Syntax Description**

- **Priority**: Set to 32768.

**Command Modes**

- Interface configuration mode

**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**

This example shows how to set the priority for the interface:

```
Switch(config-if)# lacp port-priority 23748
Switch(config-if)#
```

**Related Commands**

- `priority`: Priority for the physical interfaces; valid values are from 1 to 65535.
- `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.
To set the priority of the system for LACP, use the **lacp system-priority** command.

**Syntax Description**

**Priority** is set to 32768.

**Command Modes**

Global configuration mode

**Usage Guidelines**

You must assign each switch that is running LACP a system priority that can be specified automatically or by entering the **lacp system-priority** command. The system priority is used with the switch MAC address to form the system ID and is also used during negotiation with other systems.

Although this command is a global configuration command, the priority value is supported on port channels with LACP-enabled physical interfaces.

When setting the priority, the higher numbers indicate lower priorities.

You can also enter the **lacp system-priority** command in interface configuration mode. After you enter the command, the system defaults to global configuration mode.

**Examples**

This example shows how to set the system priority:

```
Switch(config)#
lacp system-priority 23748
Switch(config)#
```

**Related Commands**

- **priority**
  - Priority of the system; valid values are from 1 to 65535.
- **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.
To enable power negotiation through LLDP, use the `lldp tlv-select power-management` command.

**Syntax Description**

**Defaults**

Enabled on POEP ports

**Command Modes**

Interface level

**Command History**

**Usage Guidelines**

You need to disable this feature if you do not want to perform power negotiation through LLDP.

This feature is not supported on non-POEP ports; the CLI is suppressed on such ports and TLV is not exchanged.

**Examples**

This example shows how to enable LLDP power negotiation on interface Gigabit Ethernet 3/1:

```
Switch#
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
```

**Related Commands**

This command has no arguments or keywords.

**Release Modification**

12.2(54)SG Support was introduced on the Catalyst 4500 series switch.
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.

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

The global link-status messaging is disabled.

**Command Modes**

Global configuration mode

**Usage Guidelines**

If link-status logging event is not configured at the interface level, this global link-status setting takes effect for each interface.

**Examples**

This example shows how to globally enable link status message on each interface:

```
Switch# 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**

- `logging event link-status (interface configuration)`
  Enables the link-status event messaging on an interface.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

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.

Defaults
Global link-status messaging is enabled.

Command Modes
Interface configuration mode

Usage Guidelines
To enable system logging of interface state-change events on a specific interface, enter the `logging event link-status` command in interface configuration mode. To enable system logging of interface state-change events on all interfaces in the system, enter the `logging event link-status global` command in global configuration mode. All interfaces without the state change event configuration use the global setting.

Examples
This example shows how to enable logging event state-change events on interface 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
Switch(config-if)#
```

This 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 gi11/1
Switch(config-if)# no logging event link-status
Switch(config-if)#
```

This 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)#
```
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

Logging event link-status interface configuration

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>logging event link-status</td>
<td>Changes the default switch-wide global link-status event messaging settings.</td>
</tr>
</tbody>
</table>
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

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
```

Syntax Description

This command has no arguments or keywords.

Defaults

Global trunk-status messaging is disabled.

Command Modes

Global configuration mode

Usage Guidelines

If trunk-status logging event is not configured at the interface level, the global trunk-status setting takes effect for each interface.

Examples

This example shows how to globally enable link status messaging on each interface:

```
Switch# 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

- `logging event trunk-status global` (global configuration): Enables the trunk-status event messaging on an interface.

Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

logging event trunk-status (interface configuration)

To enable the trunk-status event messaging on an interface, use the `logging event trunk-status` command. Use the `no` form of this command to disable the trunk-status event messaging. Use the `logging event trunk-status use-global` command to apply the global trunk-status setting.

```
logging event trunk-status
no logging event trunk-status
logging event trunk-status use-global
```

**Defaults**
Global trunk-status messaging is enabled.

**Command Modes**
Interface configuration mode

**Usage Guidelines**
To enable system logging of interface state-change events on a specific interface, enter the `logging event trunk-status` command in interface configuration mode.

To enable system logging of interface state-change events on all interfaces in the system, enter the `logging event trunk-status use-global` command in global configuration mode. All interfaces without the state change event configuration use the global setting.

**Examples**
This example shows how to enable logging event state-change events on interface gi11/1:

```
Switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gi11/1
Switch(config-if)# logging event trunk-status
Switch(config-if)# end
Switch#
```

This example shows how to turn off logging event trunk status regardless of the global setting:

```
Switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gi11/1
Switch(config-if)# no logging event trunk-status
Switch(config-if)# end
Switch#
```

This example shows how to enable the global event trunk-status setting on interface gi11/1:

```
Switch# 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#
```
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

logging event trunk-status (interface configuration)

Related Commands

Command Description

logging event trunk-status global (global configuration)
Enables the trunk-status event messaging on an interface.
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]
```

**Note**
The `mab` command is totally independent of the effect of the `dot1x system-auth control` command.

**Syntax Description**
- `Command Default`: Disabled
- `Command Modes`: Interface configuration mode

**Usage Guidelines**
When a port is configured for MAB as a fallback method, it operates in a typical dot1X method until a configurable number of failed attempts to request the identity of the host. The 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
```
The following example shows how to enable and configure MAB on a port:
```
Switch(config-if)# mab eap
```
The following example shows how to disable MAB on a port:
```
Switch(config-if)# no mab
```

**Related Commands**
- `show authentication`: Displays Authentication Manager information.
- `show mab`: Displays MAB information.
- `show running-config`: Displays the running configuration information.
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
```

**Syntax Description**

- **Defaults**
  - MAC access lists are not defined.
- **Command Modes**
  - Global configuration mode
- **Usage Guidelines**
  - When you enter the ACL name, follow these naming conventions:
    - Maximum of 31 characters long and can include a-z, A-Z, 0-9, the dash character (-), the underscore character (_), and the period character (.)
    - Must start with an alpha character and must be unique across all ACLs of all types
    - Case sensitive
    - Cannot be a number
    - Must not be a keyword; keywords to avoid are all, default-action, map, help, and editbuffer
  - When you enter the `mac access-list extended name` command, you use the following 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 2-7** describes the syntax of the `mac access-list extended` subcommands.

<table>
<thead>
<tr>
<th>Subcommand</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>any</td>
<td>Specifies any source-host or destination-host.</td>
</tr>
<tr>
<td>arbitrary ethertype</td>
<td>(Optional) Specifies an arbitrary ethertype in the range 1536 to 65535 (Decimal or Hexadecimal)</td>
</tr>
<tr>
<td>deny</td>
<td>Prevents access if the conditions are matched.</td>
</tr>
<tr>
<td>dest-mac mask</td>
<td>(Optional) Specifies a destination MAC address of the form: dest-mac-address dest-mac-address-mask.</td>
</tr>
</tbody>
</table>
Table 2-8 Mapping an Ethernet Packet to a Protocol Family

<table>
<thead>
<tr>
<th>Protocol Family</th>
<th>Ethertype in Packet Header</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appletalk</td>
<td>0x809B, 0x80F3</td>
</tr>
<tr>
<td>Arp-Non-Ipv4</td>
<td>0x0806 and protocol header of Arp is a non-Ipv4 protocol family</td>
</tr>
<tr>
<td>Decnet</td>
<td>0x6000-0x6009, 0x8038-0x8042</td>
</tr>
<tr>
<td>Ipx</td>
<td>0x8137-0x8138</td>
</tr>
</tbody>
</table>
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

This example shows how to create a MAC layer access list named mac_layer that denies traffic from 0000.4700.0001, which is going to 0000.4700.0009, 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#
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
```

**Syntax Description**

- **seconds**
  - Aging time in seconds; valid values are 0 and from 10 to 1000000 seconds.

- **vlan vlan_id**
  - (Optional) Single VLAN number or a range of VLANs; valid values are from 1 to 4094.

**Defaults**

Aging time is set to 300 seconds.

**Command Modes**

Global configuration mode

**Usage Guidelines**

If you do not enter a VLAN, the change is applied to all routed-port VLANs.

Enter 0 seconds to disable aging.

**Examples**

This example shows how to configure the aging time to 400 seconds:

```
Switch(config) #
mac-address-table aging-time 400
Switch(config) #
```

This example shows how to disable aging:

```
Switch(config) #
mac-address-table aging-time 0
Switch(config) #
```

**Related Commands**

- `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}
```

**Syntax Description**

- **Defaults**
  - The group learning feature is disabled.

**Command Modes**

- Global configuration mode

**Usage Guidelines**

The entries within the "ip" and "other" protocol buckets are created according to the protocol of the incoming traffic.

When you use the `mac-address-table dynamic group protocols` command, an incoming MAC address that might belong to either the "ip" or the "other" protocol bucket, is learned on both protocol buckets. Therefore, any traffic destined to this MAC address and belonging to any of the protocol buckets is unicasted to that MAC address, rather than flooded. This reduces the unicast Layer 2 flooding that might be caused if the incoming traffic from a host belongs to a different protocol bucket than the traffic that is destined to the sending host.

**Examples**

This example shows that the MAC addresses are initially assigned to either the "ip" or the "other" protocol bucket:

```
Switch# show mac-address-table dynamic
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  
```
This example shows how to assign MAC addresses that belong to either the "ip" or the "other" bucket to both buckets:

Switch(config)##
mac-address-table dynamic group protocols ip other
Switch(config)##
exit
Switch##
show mac address-table dynamic

Unicast Entries

<table>
<thead>
<tr>
<th>vlan</th>
<th>mac address</th>
<th>type</th>
<th>protocols</th>
<th>port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0000.0000.5000</td>
<td>dynamic ip,other</td>
<td></td>
<td>GigabitEthernet1/1</td>
</tr>
<tr>
<td>1</td>
<td>0001.0234.6616</td>
<td>dynamic ip,other</td>
<td></td>
<td>GigabitEthernet3/1</td>
</tr>
<tr>
<td>1</td>
<td>0003.4700.24c3</td>
<td>dynamic ip,other</td>
<td></td>
<td>GigabitEthernet3/1</td>
</tr>
<tr>
<td>1</td>
<td>0003.4716.f475</td>
<td>dynamic ip,other</td>
<td></td>
<td>GigabitEthernet3/1</td>
</tr>
<tr>
<td>1</td>
<td>0003.4748.75c5</td>
<td>dynamic ip,other</td>
<td></td>
<td>GigabitEthernet3/1</td>
</tr>
<tr>
<td>1</td>
<td>0003.47c4.06c1</td>
<td>dynamic ip,other</td>
<td></td>
<td>GigabitEthernet3/1</td>
</tr>
<tr>
<td>1</td>
<td>0003.47f0.d6a3</td>
<td>dynamic ip,other</td>
<td></td>
<td>GigabitEthernet3/1</td>
</tr>
<tr>
<td>1</td>
<td>0003.47f6.a91a</td>
<td>dynamic ip,other</td>
<td></td>
<td>GigabitEthernet3/1</td>
</tr>
<tr>
<td>1</td>
<td>0003.ba0e.24a1</td>
<td>dynamic ip,other</td>
<td></td>
<td>GigabitEthernet3/1</td>
</tr>
<tr>
<td>1</td>
<td>0003.fd63.3eb4</td>
<td>dynamic ip,other</td>
<td></td>
<td>GigabitEthernet3/1</td>
</tr>
<tr>
<td>1</td>
<td>0004.2326.18a1</td>
<td>dynamic ip,other</td>
<td></td>
<td>GigabitEthernet3/1</td>
</tr>
<tr>
<td>1</td>
<td>0004.5a5d.de53</td>
<td>dynamic ip,other</td>
<td></td>
<td>GigabitEthernet3/1</td>
</tr>
<tr>
<td>1</td>
<td>0004.5a5d.de55</td>
<td>dynamic ip,other</td>
<td></td>
<td>GigabitEthernet3/1</td>
</tr>
<tr>
<td>1</td>
<td>0004.5a5e.6ecc</td>
<td>dynamic ip,other</td>
<td></td>
<td>GigabitEthernet3/1</td>
</tr>
<tr>
<td>1</td>
<td>0004.5a5e.f60e</td>
<td>dynamic ip,other</td>
<td></td>
<td>GigabitEthernet3/1</td>
</tr>
<tr>
<td>1</td>
<td>0004.5a5f.08f6</td>
<td>dynamic ip,other</td>
<td></td>
<td>GigabitEthernet3/1</td>
</tr>
<tr>
<td>1</td>
<td>0004.5a5f.090b</td>
<td>dynamic ip,other</td>
<td></td>
<td>GigabitEthernet3/1</td>
</tr>
<tr>
<td>1</td>
<td>0004.5a64.f813</td>
<td>dynamic ip,other</td>
<td></td>
<td>GigabitEthernet3/1</td>
</tr>
<tr>
<td>1</td>
<td>0004.5a66.1a77</td>
<td>dynamic ip,other</td>
<td></td>
<td>GigabitEthernet3/1</td>
</tr>
<tr>
<td>1</td>
<td>0004.5a6b.56b2</td>
<td>dynamic ip,other</td>
<td></td>
<td>GigabitEthernet3/1</td>
</tr>
<tr>
<td>1</td>
<td>0004.5a6c.6a07</td>
<td>dynamic ip,other</td>
<td></td>
<td>GigabitEthernet3/1</td>
</tr>
<tr>
<td>1</td>
<td>0004.5a88.b075</td>
<td>dynamic ip,other</td>
<td></td>
<td>GigabitEthernet3/1</td>
</tr>
<tr>
<td>Number</td>
<td>MAC Address</td>
<td>Protocol</td>
<td>Interface</td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>-----------------</td>
<td>-------------------</td>
<td>-------------------</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0004.c1bd.1b40</td>
<td>dynamic ip,other</td>
<td>GigabitEthernet3/1</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0004.c1d8.b3c0</td>
<td>dynamic ip,other</td>
<td>GigabitEthernet3/1</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0004.c1d8.bd00</td>
<td>dynamic ip,other</td>
<td>GigabitEthernet3/1</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0005.dce0.7c0a</td>
<td>dynamic assigned</td>
<td>GigabitEthernet3/1</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0007.e997.74dd</td>
<td>dynamic ip,other</td>
<td>GigabitEthernet3/1</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0007.e997.7e8f</td>
<td>dynamic ip,other</td>
<td>GigabitEthernet3/1</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0007.e9ad.5e24</td>
<td>dynamic ip,other</td>
<td>GigabitEthernet3/1</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0007.e9c9.0bc9</td>
<td>dynamic ip,other</td>
<td>GigabitEthernet3/1</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>000b.5f0a.f1d8</td>
<td>dynamic ip,other</td>
<td>GigabitEthernet3/1</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>000b.fdf3.c498</td>
<td>dynamic ip,other</td>
<td>GigabitEthernet3/1</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0012.436f.c07f</td>
<td>dynamic ip,other</td>
<td>GigabitEthernet3/1</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0050.0407.5fe1</td>
<td>dynamic ip,other</td>
<td>GigabitEthernet3/1</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0050.6901.65af</td>
<td>dynamic ip,other</td>
<td>GigabitEthernet3/1</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0050.da6c.81cb</td>
<td>dynamic ip,other</td>
<td>GigabitEthernet3/1</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0050.dad0.af07</td>
<td>dynamic ip,other</td>
<td>GigabitEthernet3/1</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>00a0.ccd7.20ac</td>
<td>dynamic ip,other</td>
<td>GigabitEthernet3/1</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>00b0.64fd.1b84</td>
<td>dynamic assigned</td>
<td>GigabitEthernet3/1</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>00d0.b775.c8bc</td>
<td>dynamic ip,other</td>
<td>GigabitEthernet3/1</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>00d0.b775.c8ee</td>
<td>dynamic ip,other</td>
<td>GigabitEthernet3/1</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>00d0.b79e.de1d</td>
<td>dynamic ip,other</td>
<td>GigabitEthernet3/1</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>00e0.4c79.1939</td>
<td>dynamic ip,other</td>
<td>GigabitEthernet3/1</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>00e0.4c7b.d765</td>
<td>dynamic ip,other</td>
<td>GigabitEthernet3/1</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>00e0.4c82.66b7</td>
<td>dynamic ip,other</td>
<td>GigabitEthernet3/1</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>00e0.4c8b.f83e</td>
<td>dynamic ip,other</td>
<td>GigabitEthernet3/1</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>00e0.4c8c.0861</td>
<td>dynamic ip,other</td>
<td>GigabitEthernet3/1</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0800.20d1.bf09</td>
<td>dynamic ip,other</td>
<td>GigabitEthernet3/1</td>
<td></td>
</tr>
</tbody>
</table>
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
vl an-id
```

**Syntax Description**

- `vlan-id`: Specifies a single VLAN ID or a range of VLAN IDs separated by a hyphen or comma. Valid VLAN IDs are 1 to 4094.

**Defaults**

Enabled on all VLANs

**Command Modes**

Global configuration

**Usage Guidelines**

When you control MAC address learning on a VLAN, you can manage the available table space by controlling which VLANs, and which ports can learn MAC addresses.

You can disable MAC address learning on a single VLAN ID (for example, by entering `no mac address-table learning vlan 223`) or on a range of 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 reject 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.
Chapter 2: Cisco IOS Commands for the Catalyst 4500 Series Switches

mac address-table learning vlan

Examples

This example shows how to disable MAC address learning on VLAN 2003:

Switch(config)#
no mac address-table learning vlan 2003

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mac address-table learning</td>
<td>Displays the MAC address learning status on all VLANs or on the specified VLAN.</td>
</tr>
</tbody>
</table>
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.

**Syntax Description**

- `change` (Optional) Specifies enabling MAC change notification.
- `history-size hs_value` (Optional) Sets a maximum number of entries in the MAC change notification history table. The range is 0 to 500 entries.
- `interval intv_value` (Optional) Sets a notification trap interval: the set interval time between two consecutive traps. The range is 0 to 2,147,483,647 seconds.
- `mac-move` (Optional) Specifies enabling MAC move notification.
- `threshold` (Optional) Specifies enabling MAC threshold notification.
  - `limit percentage` (Optional) Specifies the percentage of MTU utilization threshold; valid values are from 1 to 100 percent.
  - `interval time` (Optional) Specifies the time between MAC threshold notifications; valid values are greater than or equal to 120 seconds.
- `learn-fail` (Optional) Specifies syslog (level 6) notifications of failures to install MAC addresses learned in software into hardware. Disabled by default.
  - `interval time` (Optional) Specifies the syslog interval between hardware MAC learning failure notifications. The default value is 150 seconds. The range is between 1 to 100000 seconds.
  - `limit num_fail` (Optional) Specifies the number of hardware MAC learning failures to be allowed in a notification interval.

**Defaults**

- The 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.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

mac-address-table notification

Command Modes
Global configuration mode

Usage Guidelines
You can enable the MAC change notification feature using the `mac-address-table notification change` command. If you do this, you must also enable MAC notification traps on an interface using the `snmp trap mac-notification change interface` configuration command and configure the switch to send MAC change traps to the NMS using the `snmp-server enable traps mac-notification global` command.

When the `history-size` option is configured, the existing MAC change history table is deleted, and a new table is created.

Examples
This example shows how to set the MAC address notification history table size to 300 entries:
```
Switch(config)#
mac-address-table notification change history-size 300
```

This example shows how to set the MAC address notification interval time to 1250 seconds:
```
Switch(config)#
mac-address-table notification change interval 1250
```

This example shows how to enable hardware MAC address learning failure syslog notification:
```
Switch(config)#
mac address-table notification learn-fail
```

This example shows how to set the interval of hardware MAC address learning failure syslog notification to 30 seconds:
```
Switch(config)#
mac address-table notification learn-fail interval 30
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear mac-address-table</td>
<td>Clears the global counter entries from the Layer 2 MAC address table.</td>
</tr>
<tr>
<td>mac-address-table notification</td>
<td>Enables MAC address notification on a switch.</td>
</tr>
<tr>
<td>snmp-server enable traps</td>
<td>Enables SNMP notifications.</td>
</tr>
<tr>
<td>snmp trap mac-notification change</td>
<td>Enables SNMP MAC address notifications.</td>
</tr>
</tbody>
</table>
mac-address-table static

To configure the static MAC addresses for a VLAN interface or drop unicast traffic for a MAC address on 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
```

### Syntax Description

- **Defaults**: This command has no default settings.
- **Command Modes**: Global configuration mode
- **Usage Guidelines**: When a static MAC address is installed, it is associated with a port. The output interface specified must be a Layer 2 interface and not an SVI. If you do not enter a protocol type, an entry is automatically created for each of the four protocol types. Entering the `no` form of this command does not remove the system MAC 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**

This example shows how to add the static entries to the MAC address table:

```
Switch(config)#
mac-address-table static 0050.3e8d.6400 vlan 100 interface fastethernet5/7
Switch(config)#
```

### Related Commands

- **show mac-address-table static**: Displays the static MAC address table entries only.
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.

### Syntax Description

```plaintext
macro apply cisco-desktop $AVID
```

### Defaults

This command has no default settings.

### Command Modes

Interface configuration mode

### Usage Guidelines

This command can only be viewed and applied; it cannot be modified. Ensure that the existing configuration on the interface does not conflict with the intended macro configuration. Before you apply the macro, clear the configuration on the interface with the `default interface` command.

### Examples

This example shows how to enable the Cisco-recommended features and settings on port fa2/1:

```
Switch(config)#
interface FastEthernet2/1
Switch(config-if)#
macro apply cisco-desktop $AVID 50
Switch(config-if)#
```

The contents of this macro are as follows:

- **Basic interface - Enable data VLAN only**
- **Recommended value for access vlan (AVID) should not be 1**
  ```plaintext
  switchport access vlan $AVID [access_vlanid]
  ```
- **Enable port security limiting port to a single MAC address -- that of desktop**
  ```plaintext
  switchport port-security
  ```
- **Ensure port-security age is greater than one minute and use inactivity timer**
  ```plaintext
  switchport port-security violation restrict
  switchport port-security aging time 2
  switchport port-security aging type inactivity
  ```
- **Configure port as an edge network port**
  ```plaintext
  spanning-tree portfast
  spanning-tree bpduguard enable
  ```
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

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 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.
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**

- `$AVID` specifies an access VLAN ID.
- `$VVID` specifies a voice VLAN ID.

**Defaults**

This command has no default settings.

**Command Modes**

- Interface configuration mode

**Usage Guidelines**

- This command can only be viewed and applied; it cannot be modified.
- Ensure that the existing configuration on the interface does not conflict with the intended macro configuration. Before you apply the macro, clear the configuration on the interface with the `default interface` command.

**Examples**

This example shows how to enable the Cisco-recommended features and settings on port fa2/1:

```
Switch(config)#
interface FastEthernet2/1
Switch(config-if)#
macro apply cisco-phone $AVID 10 $VVID 50
```

The contents of this macro are as follows:

- **VoIP enabled interface - Enable data VLAN and voice VLAN (VVID)**
  ```
  switchport access vlan $AVID [access_vlan_id]
  switchport mode access
  ```
- **Update the Voice VLAN (VVID) value which should be different from data VLAN**
  ```
  switchport voice vlan $VVID [voice_vlan_id]
  ```
- **Enable port security limiting port to a 3 MAC addresses -- One for desktop and two for phone**
  ```
  switchport port-security
  switchport port-security maximum 3
  ```
- **Ensure port-security 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-qos 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
  ```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>macro apply cisco-phone</td>
<td>Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a standard desktop.</td>
</tr>
<tr>
<td>macro apply cisco-router</td>
<td>Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a router.</td>
</tr>
<tr>
<td>macro apply cisco-switch</td>
<td>Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to another switch.</td>
</tr>
</tbody>
</table>
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**

This command has no default settings.

**Command Modes**

Interface configuration mode

**Usage Guidelines**

This command can only be viewed and applied; it cannot be modified. Ensure that the existing configuration on the interface does not conflict with the intended macro configuration. Before you apply the `macro apply cisco-router` command, clear the configuration on the interface with the `default interface` command.

**Examples**

This example shows how to enable the Cisco-recommended features and settings on port fa2/1:

```
Switch(config)#
interface FastEthernet2/1
Switch(config-if)#
macro apply cisco-router $NVID 80
```

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.
spanning-tree portfast
spanning-tree bpduguard enable
```

$NVID

Specifies a native VLAN ID.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>macro apply cisco-router</td>
<td>Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a router.</td>
</tr>
<tr>
<td>macro apply cisco-desktop</td>
<td>Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a standard desktop.</td>
</tr>
<tr>
<td>macro apply cisco-phone</td>
<td>Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a standard desktop and a Cisco IP phone.</td>
</tr>
<tr>
<td>macro apply cisco-switch</td>
<td>Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to another switch.</td>
</tr>
</tbody>
</table>
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**: Specifies a native VLAN ID.

**Defaults**

This command has no default settings.

**Command Modes**

Interface configuration mode

**Usage Guidelines**

This command can only be viewed and applied; it cannot be modified.

Ensure that the existing configuration on the interface does not conflict with the intended macro configuration. Before you apply this macro, clear the configuration on the interface with the `default interface` command.

**Examples**

This example shows how to enable the Cisco-recommended features and settings on port fa2/1:

```
Switch(config)#
interface FastEthernet2/1
Switch(config-if)#
macro apply cisco-switch 45
Switch(config-if)#
```

The contents of this macro are as follows:

```shell
# 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
```

$NVID native_vlanid

Specifies a native VLAN ID.
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>macro apply cisco-switch</td>
<td>Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a standard desktop.</td>
</tr>
<tr>
<td>macro apply cisco-phone</td>
<td>Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a standard desktop and a Cisco IP phone.</td>
</tr>
<tr>
<td>macro apply cisco-router</td>
<td>Enables the Cisco-recommended features and settings that are suitable for connecting a switch port to a router.</td>
</tr>
</tbody>
</table>
Use the `macro auto device` command to simplify changing the parameters for 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**
- `device_type` (Optional)
- `params values` (Optional)
- `param name=value` (Optional)

**Command Modes**
- Global configuration

**Usage Guidelines**
- Although you can use the `macro auto execute` command to produce the same effect as the `macro auto device` command, the latter is simpler.

**Examples**
This example shows how to change the access VLAN and voice VLAN from their default value to user-defined values for phone devices.

```
(config)# macro auto device phone ACCESS_VLAN=10 VOICE_VLAN=20
```

**Related Commands**
- `device_type`—Specifies the device type.
- `phone—Apply interface configs on detecting a phone
- `switch—Apply interface configs on detecting a switch
- `router—Apply interface configs on detecting a router
- `ap—Apply interface configs on detecting an ap
- `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

**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 function.
- `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.
Chapter 2      Cisco IOS Commands for  the Catalyst 4500 Series Switches

macro auto device

- Specifies not to remove configurations applied by ASP across link flaps and device removal.

shell trigger

- Creates a user defined trigger.
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]`

**Syntax Description**

- **Defaults**
  - Auto Smartports is disabled.

- **Command Modes**
  - Global configuration

- **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: $NA TIVE_VLAN=(1).
    - `CISCO_ROUTER_AUTO_SMARTPORT` (Optional) Specify the parameter values: $NA TIVE_VLAN=(1).
    - `CISCO_AP_AUTO_SMARTPORT` (Optional) Specify the parameter values: $NA TIVE_VLAN=(1).
    - `CISCO_LW AP_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.
Chapter 2  
Cisco IOS Commands for the Catalyst 4500 Series Switches

macro auto execute (built-in function)

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

This 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)# !!! 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 to another Cisco Switch after the Macro is applied
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
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>macro auto execute</code></td>
<td>Simplifies changing the parameters for a built-in functions for a device type.</td>
</tr>
<tr>
<td><code>macro auto execute (remotely-defined trigger)</code></td>
<td>Maps a trigger to a remotely defined function.</td>
</tr>
<tr>
<td><code>macro auto execute (user-defined function)</code></td>
<td>Maps a trigger to a user-defined function.</td>
</tr>
<tr>
<td><code>macro auto global processing</code></td>
<td>Enables Auto Smartports on a switch.</td>
</tr>
<tr>
<td><code>macro auto processing</code></td>
<td>Enables Auto SmartPorts macros on a specific interface.</td>
</tr>
<tr>
<td><code>macro auto sticky</code></td>
<td>Specifies not to remove configurations applied by ASP across link flaps and device removal.</td>
</tr>
<tr>
<td><code>shell trigger</code></td>
<td>Creates a user defined trigger.</td>
</tr>
</tbody>
</table>
Use the `macro auto execute (remotely-defined trigger)` command to map a trigger to a remotely defined function.

Use the `no macro auto execute` command to unmap the trigger.

**Syntax Description**

- `trigger_name` specifies the trigger name.
- `remote url` specifies the remotely-defined URL.

**Defaults**

None

**Command Modes**

Global configuration

**Usage Guidelines**

This command enables you to store shell functions in a central location and utilize them by ASP on many switches. This alleviates the problem of updating functions on every switch for each modification.

Triggering of the remotely defined function requires network connectivity to the URL, which is accessed for each execution of the function.

**Examples**

This example shows how to map a trigger to the remotely defined function `myfunction`—the filename that contains the function body:

```
Switch(config) #
macro auto execute mytrigger remote tftp://dirt/tftpboot/myfunction
```

**Related Commands**

- `trigger_name`
  
  Specifies the trigger name.

- `url`
  
  Specifies the remotely-defined URL.
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] 

[params name=value] 

{ 

function body 

}
```

**Syntax Description**

**Defaults**

None

**Command Modes**

Global configuration

**Usage Guidelines**

Because the function defined in this command does not have a name, you cannot use it to map to another trigger. This is the only way that you can map a trigger to a user defined function. Shell functions defined in the non-configure mode can not be used to map triggers.

**Examples**

This example shows how to map the user-defined event trigger Cisco Digital Media Player (DMP) to a user-defined macro.

1. Connect the DMP to an 802.1x- or MAB-enabled switch port.
2. On the RADIUS server, set the attribute-value pair to `auto-smart-port=CISCO_DMP_EVENT`.
3. On the switch, create the event trigger `CISCO_DMP_EVENT`, and enter the user-defined macro commands shown below.
4. 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
```

**trigger_name**

Specifies the trigger name.

**params name=value**

(Optional) Specifies values for the parameters that are to be used in the function body.

**function_body**

Shell functions with CLIs.
 Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

macro auto execute (user-defined function)

exit

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
fi

Switch(config)#

end

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>macro auto device</td>
<td>Simplifies changing the parameters for a built-in function for a device type.</td>
</tr>
<tr>
<td>macro auto execute</td>
<td>Changes built-in function default values or to map user-defined triggers to built-in functions, and to pass the parameter values.</td>
</tr>
<tr>
<td>macro auto execute</td>
<td>Maps a trigger to a remotely defined function.</td>
</tr>
<tr>
<td>macro auto global processing</td>
<td>Enables Auto Smartports on a switch.</td>
</tr>
<tr>
<td>macro auto processing</td>
<td>Enables Auto SmartPorts macros on a specific interface.</td>
</tr>
<tr>
<td>macro auto sticky</td>
<td>Specifies not to remove configurations applied by ASP across link flaps and device removal.</td>
</tr>
<tr>
<td>shell trigger</td>
<td>Creates a user-defined trigger.</td>
</tr>
</tbody>
</table>
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
```

```
no macro auto global
```

**Note**
Starting with Release 15.0(2)SG, the `fallback` option has been deprecated.

**Syntax Description**

**Defaults**
Auto Smartports is disabled.

**Command Modes**
Global configuration

**Usage Guidelines**
Use the `macro auto global processing` global configuration command to globally enable Auto Smartports macros on the switch. To disable ASP macros on a specific port, use the `no` macro auto 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.
Chapter 2  Cisco IOS Commands for the Catalyst 4500 Series Switches

The `macro auto global processing` command enables ASP globally if it is not already enabled, and sets 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

This example shows how enable ASP on a switch and to disable the feature on Gi1/0/1:

Switch(config)\
  interface interface Gi1/0/1\
Switch(config-if)\
  no macro auto processing\
Switch(config)\
  macro auto global processing\

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>macro auto device</code></td>
<td>Simplifies changing the parameters for a built-in function for a device type.</td>
</tr>
<tr>
<td><code>macro auto execute (built-in function)</code></td>
<td>Changes built-in function default values or to map user-defined triggers to built-in functions, and to pass the parameter values.</td>
</tr>
<tr>
<td><code>macro auto execute (remotely-defined trigger)</code></td>
<td>Maps a trigger to a remotely defined function.</td>
</tr>
<tr>
<td><code>macro auto execute (user-defined function)</code></td>
<td>Maps a trigger to a user-defined function.</td>
</tr>
<tr>
<td><code>macro auto processing</code></td>
<td>Enables ASP macros on a specific interface.</td>
</tr>
<tr>
<td><code>macro auto sticky</code></td>
<td>Enables a user to not remove configurations applied by ASP across link flaps and device removal.</td>
</tr>
<tr>
<td><code>shell trigger</code></td>
<td>Creates a user defined trigger.</td>
</tr>
</tbody>
</table>
Chapter 2  Cisco IOS Commands for the Catalyst 4500 Series Switches

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.

**Syntax Description**
- `macro auto mac-address-group` **grp_name**
- `no macro auto mac-address-group` **grp_name**

**Command Modes**
- Global configuration

**Usage Guidelines**
This command changes the mode to config-mac-addr-grp, in which you can add or remove a MAC address or OUI from the group.

**Examples**
This 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)#
```

**Related Commands**
- **grp_name**
  - Specifies the group name.

---

**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.
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.

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

**Command Default**
Device classifier is enabled.

**Command Modes**
Global configuration

**Usage Guidelines**
Use the `no` `macro auto monitor` global configuration command to disable the device classifier. You cannot disable the device classifier while it is being used by features such as ASP.

**Examples**
This example shows how to enable the ASP device classifier on a switch:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# macro auto monitor
Switch(config)#
```

**Related Commands**
- `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.
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**
- **Defaults**
  - Fallback mechanism is CDP.
- **Command Modes**
  - Interface level configuration
- **Usage Guidelines**
  - The `no macro auto processing` command should be configured on all interfaces where ASP is not desirable (such as Layer 3 and EtherChannel interfaces) before ASP is enabled globally.
  - At the interface level, the default fallback mechanism is CDP. To change the mechanism to LLDP, enter the `no macro auto processing fallback cdp` command, followed by the `macro auto processing fallback lldp` command.

**Examples**

This example shows how to enable the feature on an interface:

```
Switch(config)#
interface Gi3/1
Switch(config-if)#
macro auto processing
```

**Related Commands**

- `fallback cdp` - Specifies CDP as the fallback mechanism.
- `fallback lldp` - Specifies LLDP as the fallback mechanism.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

macro auto processing

Maps a trigger to a remotely defined function.

macro auto execute

Maps a trigger to a user-defined function.

macro auto global processing

Enables Auto Smartports on a switch.
Use the `macro auto sticky` configuration to specify not to remove configurations applied by ASP across link flaps and device removal.

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

Not sticky (macros are removed)

**Command Modes**

Global configuration

**Usage Guidelines**

This command enables you to avoid unnecessary removal of ASP 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**

This example shows how to specify not to remove configurations:

```
Switch(config)＃
macro auto sticky
```

**Related Commands**

This command has no arguments or keywords.

**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.
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.

**Syntax Description**

This command has no keywords or variables.

**Defaults**

This command has no default setting.

**Command Modes**

Global configuration mode

**Examples**

These examples show how to apply the system-defined default to the switch:

Switch(config)#

macro global apply cisco-global

Changing VTP domain name from gsg-vtp to [smartports] Device mode already VTP TRANSPARENT.

Switch(config)#
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.

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

**Defaults**
This command has no default setting.

**Command Modes**
Global configuration mode

**Examples**
This example shows how to apply the system-defined default to the switch:

```
Switch (config)#
macro global apply system-cpp
Switch (config)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>macro global apply cisco-global</code></td>
<td>Applies the system-defined default template to the switch.</td>
</tr>
<tr>
<td><code>macro global description</code></td>
<td>Enters a description about the macros that are applied to the switch.</td>
</tr>
</tbody>
</table>
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 udld aggressive mode enabled
```

You can verify your settings by entering the `show parser macro description` privileged EXEC command.

**Related Commands**

<table>
<thead>
<tr>
<th>Command Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>macro global apply cisco-global</code></td>
</tr>
</tbody>
</table>
To enter the main CPU submode and manually synchronize the configurations on the two supervisor engines, use the `main-cpu` command.

**Command Syntax**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Redundancy mode

**Usage Guidelines**

The main CPU submode is used to manually synchronize the configurations on the two supervisor engines. From the main CPU submode, use the `auto-sync` command to enable automatic synchronization of the configuration files in NVRAM.

**Note**

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**

This example shows how to re-enable 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#
```

```
Switch# copy running-config startup-config
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>auto-sync</code></td>
<td>Enables automatic synchronization of the configuration files in NVRAM.</td>
</tr>
</tbody>
</table>
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}
```

**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 {acl-number | acl-name}`: Selects one or more IP ACLs for a VLAN access-map sequence; valid values are from 1 to 199 and from 1300 to 2699.
- `mac address acl-name`: Selects one or more MAC ACLs for a VLAN access-map sequence.

**Defaults**

This command has no default settings.

**Command Modes**

VLAN access-map mode

**Usage Guidelines**

The match clause specifies the IP or MAC ACL for traffic filtering.

The MAC sequence is not effective for IP packets. IP packets should be access controlled by IP match clauses.

Refer to the *Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide* for additional configuration guidelines and restrictions.

Refer to the *Cisco IOS Command Reference* publication for additional match command information.

**Examples**

This example shows how to define a match clause for a VLAN access map:

```
Switch(config)#
vlan access-map ganymede 10
Switch(config-access-map)#
match ip address 13
```

**Related Commands**

- `ip address acl-number`: Selects one or more IP ACLs for a VLAN access-map sequence; valid values are from 1 to 199 and from 1300 to 2699.
- `ip address acl-name`: Selects an IP ACL by name.
- `mac address acl-name`: Selects one or more MAC ACLs for a VLAN access-map sequence.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

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.

```
macth {
  access-group acl-index-or-name
  cos cos-list
  [lp] dscp dscp-list
  [lp] precedence ip-precedence-list
  qos-group value
  protocol [ip|ipv6|arp]
  no match {
    access-group acl-index-or-name
    cos cos-list
    [lp] dscp dscp-list
    [lp] precedence ip-precedence-list
    qos-group value
    protocol [ip|ipv6|arp]
  }
```

**Syntax Description**

**Defaults**
No match criteria are defined.

**Command Modes**
Class-map configuration mode

**access-group acl-index-or-name**
Number or name of an IP standard or extended access control list (ACL) or MAC ACL. For an IP standard ACL, the ACL index range is 1 to 99 and 1300 to 1999. For an IP extended ACL, the ACL index range is 100 to 199 and 2000 to 2699.

**cos cos-list**
Lists up to four Layer 2 class of service (CoS) values to match against a packet. Separate each value with a space. The range is 0 to 7.

**[lp] dscp dscp-list**
(Optional) IP keyword. It specifies that the match is for IPv4 packets only. If not used, the match is for both IPv4 and IPv6 packets. Lists up to eight IP Differentiated Services Code Point (DSCP) values to match against a packet. Separate each value with a space. The range is 0 to 63. You also can enter a mnemonic name for a commonly used value.

**[lp] precedence ip-precedence-list**
(Optional) IP keyword. It specifies that the match is for IPv4 packets only. If not used, the match is for both IPv4 and IPv6 packets. Lists up to eight IP-precedence values to match against a packet. Separate each value with a space. The range is 0 to 7. You also can enter a mnemonic name for a commonly used value.

**qos-group value**
Specifies the internally generated qos-group value assigned to a packet on the input qos classification.

**protocol ip**
Specifies 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.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

match (class-map configuration)

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 2-84.

Examples

This 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
```

This 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
```

This 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#
This example shows how to specify a class-map that applies only to IPv6 traffic on a Supervisor Engine 6-E:

Switch# configure terminal
Switch(config)\# class-map match all ipv6 only
Switch(config-cmap)# match dscp 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.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>class-map</td>
<td>Creates a class map to be used for matching packets to the class whose name you specify and to enter class-map configuration mode.</td>
</tr>
<tr>
<td>show class-map</td>
<td>Displays class map information.</td>
</tr>
</tbody>
</table>
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
}
```

### Syntax Description

- `source-address` Establishes a new flow from a flow with a unique IP source address.
- `ip destination-address` Establishes a new flow from a flow with a unique IP destination address.
- `ip protocol` (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.

### Defaults

This command has no default settings.

### Command Modes

`class-map configuration submode`

### Usage Guidelines

- When you specify the `source-address` keyword, each flow with a unique source address is treated as a new flow.
- When you specify the `destination-address` keyword, each flow with a unique destination address is treated as a new flow.
- A policy 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.

### Examples

This example shows how to create a flow-based class map associated with a source address:

```
Switch(config)#
class-map match-all c1
Switch(config-cmap)#
macth flow ip source-address
Switch(config-cmap)#
end
```

```
Switch# show class-map c1
Class Map match-all c1 (id 2)
Match flow  ip source-address
```

Note

The `match flow` command is available on the Catalyst 4500 series switch only when Supervisor Engine VI (WS-X4516-10GE) is present.
Chapter 2  Cisco IOS Commands for the Catalyst 4500 Series Switches

match flow ip
destination-address

Switch(config-cmap)#
destination-address

Switch(config-pmap-c)#
police 1000000 9000

Switch(config-if)#
service-policy input p1

write memory
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

match flow ip

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:

<table>
<thead>
<tr>
<th>SrcIp</th>
<th>DstIp</th>
<th>IpProt</th>
<th>SrcL4Port</th>
<th>DstL4Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.10.10</td>
<td>192.168.20.20</td>
<td>20</td>
<td>6789</td>
<td>81</td>
</tr>
<tr>
<td>192.168.10.10</td>
<td>192.168.20.20</td>
<td>20</td>
<td>6789</td>
<td>21</td>
</tr>
</tbody>
</table>

With the following configuration, each flow is policed to a 1000000 bps with an allowed 9000-byte burst value.

Switch# conf terminal
Switch(config)#
class-map c1
Switch(config-cmap)#
m_match flow ip source-address ip destination-address ip protocol l4 source-port l4 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)#
ext
Switch(config-pmap)#
ext
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 l4 source-port l4 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
match flow ip

Switch#
show class-map c1
Class Map match-all c1 (id 2)
Match flow ip source-address ip destination-address ip protocol l4 source-port l4 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)

Switch#

15432182 packets
Match: flow ip source-address ip destination-address ip protocol l4 source-port l4 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.
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.

### Syntax Description

This command has no arguments or keywords.

### Defaults

Auto-MDIX is enabled.

### Command Modes

Interface configuration mode

### 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,
- 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,
- 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,
- WS-X4232-GB-RJ.

When you enable auto-MDIX on an interface, you must also set the interface speed to be autonegotiated so that the feature operates correctly.

When auto-MDIX (and autonegotiation of speed) is enabled on one or both of connected interfaces, link up occurs even if the cable type (straight-through or crossover) is incorrect.

### Examples

This example shows how to enable auto MDIX on a port:

```
Switch# configure terminal
Switch(config)# interface FastEthernet6/3
Switch(config-if)# speed auto
Switch(config-if)# mdix auto
Switch(config-if)# end
```
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

- mdix auto
- show interfaces capabilities
  Displays the interface capabilities for an interface or for all the interfaces on a switch.
- show interfaces status
  Displays the interface status.
To select the connector for a dual-mode capable port, use the `media-type` command.

```
media-type {rj45 | sfp}
```

**Syntax Description**

**Defaults**

- `sfp`

**Command Modes**

- **Interface configuration mode**

**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**

This 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
```

- `rj45` Uses the RJ-45 connector.
- `sfp` Uses the SFP connector.
To set the redundancy mode, use the `mode` command.

```
mode {rpr | sso}
```

**Syntax Description**

**Defaults**

If you are upgrading the current supervisor engine from Cisco IOS Release 12.2(18)EW or an earlier release to 12.2(20)EW A, 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

**Usage Guidelines**

- RPR and SSO mode are not supported on Catalyst 4500 series switches that are configured with Supervisor Engine 2.
- The `mode` command can be entered only from within redundancy configuration mode.
- Follow these guidelines when configuring your system to RPR or SSO mode:
  1. You must use identical Cisco IOS images and supervisor engines to support RPR and SSO mode.
  2. Redundancy may not work due to differences between the Cisco IOS release and supervisor engine capabilities.
  3. Any modules that are not online at the time of a switchover are reset and reloaded on a switchover.
  4. 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.
  5. The FIB tables are cleared on a switchover. Routed traffic is interrupted until route tables reconverge.

**Examples**

This example shows how to set the redundancy mode to SSO:

```
Switch(config)#
redundancy
Switch(config-red)#
mode sso
Switch(config-red)#
```

**Related Commands**

- `rpr` Specifies RPR mode.
- `sso` Specifies SSO mode.

**Command Description**

- `redundancy` Enters the redundancy configuration mode.
- `redundancy force-switchover` Forcibly switches from the active to the standby supervisor engine.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

mode

show redundancy
Displays redundancy facility information.

show running-config
Displays the running configuration of a switch.

Command Description
monitor capture {access-list | class-map}

To specify an access list or class map as the core filter, use the `monitor capture {access-list | class-map}` command. To remove the filter, use the `no` form of this command.

```
monitor capture name {access-list name | class-map name}
no monitor capture name {access-list name | class-map name}
```

**Syntax Description**
- **name** Specifies a capture point.
- **access-list name** Specifies access list name
- **class-map name** Specifies class map name

**Defaults**
- None

**Command Modes**
- Privileged EXEC mode

**Usage Guidelines**
- The access list or class 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 filename]

Syntax Description
- **Defaults**: none
- **Command Modes**: Privileged EXEC mode

**Usage Guidelines**
- The **clear** option empties the capture buffer and the **export** option stores the packets in the capture buffer to a .pcap 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**

- **name**: Specifies a capture point.
- **interface name**: Specifies an interface. Interface range is allowed.
- **vlan num**: Specifies a VLAN.
- **control-plane**: Specifies control plane.
- **input | output | both**: Specific traffic direction.

**Defaults**

None

**Command Modes**

Privileged EXEC mode

**Usage Guidelines**

Specifies one or more attachment points with direction. We can specify a range of interfaces also. The command can be repeated as many times as needed to add multiple attachment points.

We need to mention at least one attachment point. For VLAN, the direction has to be set to both.

**Examples**

The following example shows how to add an attachment point:

Switch# monitor capture mycap interface gigabitEthernet 3/1 in

The following example shows how to remove an attachment point:

Switch# no monitor capture mycap interface gigabitEthernet 3/1 in
monitor capture file location buffer-size

To specify the capture destination, use the `monitor capture` command. To remove the details, use the `no` form of this command.

```
monitor capture name [file location] filename [buffer-size <1-100>] [ring <2-10>] [size <1-100>] | [buffer [circular] size <1-100>]
```

**Syntax Description**

- `file location` | `filename` specifies filename of location.
- `buffer-size <1-100>` specifies buffer size in MB.
- `ring <2-10>` specifies number of files.
- `size <1-100>` specifies the file size.
- `buffer [circular] size <1-100>` specifies that the capture destination is a buffer. By default, the mode is linear. The keyword `circular` sets the buffer mode to circular. The keyword `size` specifies the buffer size.

**Defaults**

The default buffer size is one MB.

**Command Modes**

Privileged EXEC mode

**Usage Guidelines**

The capture destination can be a file in storage disk or a memory buffer. This command specifies the parameters related to packet storage.

- The `file` option specifies that the packets must be stored 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 1000000 file 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# sh monitor capture mycap buffer
```

```
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]
```

```
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)
```

```
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)
```
Switch#
sh monitor capture mycap buffer dump
0.000000   10.1.1.164 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002

Switch#
sh monitor capture mycap buffer detailed

Switch#
monitor capture mycap stop
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

- `name`: Specifies a capture point.
- `duration`: seconds
- `packet-length`: size
  - Specifies packet length. If the actual packet is longer, only the first size bytes are stored.
- `packets`: num
  - Specifies number of packets to be processed.

### Defaults
- Entire packet is processed if packet-length is not specified.

### Command Modes
- Privileged EXEC mode

### Usage Guidelines
- Specifies session duration, packet segment length and number of packets to be stored.

### Examples

The following example shows how to associate/disassociate a capture file:

```
Switch# monitor capture mycap limit duration 10
Switch# monitor capture mycap limit packet-length 128
Switch# monitor capture mycap limit packets 100
Switch# no monitor capture mycap limit duration packet-length packets
Switch# monitor capture mycap limit duration 10 packet-length 128 packets 100
Switch# no monitor capture mycap limit
```
To define an explicit in-line core filter, use the `monitor capture` 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
|

For IPv4/IPv6, use one of the formats below

Switch# [no] monitor capture mycap match
{ipv4 | ipv6}
[src-prefix
src-prefix/length | any | host src-ip-addr] 
[dest-prefix
dest-prefix/length | any | host dest-ip-addr]

Switch# [no] monitor capture mycap match
{ipv4 | ipv6}
proto {tcp | udp}
[src-prefix
src-prefix/length | any | host src-ip-addr] 
[dest-prefix
dest-prefix/length | any | host dest-ip-addr] 
[eq | gt | lt | neq 0-65535]

Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

monitor capture mycap match

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**

- **name** Specifies a capture point.
- **start** Starts the Wireshark session and captures live traffic.
- **capture-filter filter-string** Specifies the capture filter.
- **display [display-filter filter-string]** Decodes and displays the filter. Optionally, specifies the display filter.
- **[brief | detailed | dump | stop]** Specifies the display mode. Default is brief.

**Defaults**

The default display mode is **brief**.

**Command Modes**

Privileged EXEC mode

**Usage Guidelines**

These commands start or stop a capture session, assuming all mandatory parameters are specified. We must ensure that 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# 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]
Switch# monitor capture mycap start capture-filter "udp.port == 20001" display

%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]

Switch# 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]
Ethernet II, Src: 00:00:00:00:03:01 (00:00:00:00:03:01), Dst: 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)
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

monitor capture start

.... ..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

Switch# m
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 f6 0a 01 01 75 14 01   ......@.Y....u..
monitor capture start

no monitor capture mycap file

monitor capture mycap start display display-filter "udp.port == 20002" dump

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)

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#
one or more source or destination interfaces from a SPAN session, or a source VLAN from a SPAN.

To enable the SPAN sessions on interfaces or VLANs, use the

(Optional) Indicates whether the ingress option is enabled.
(Optional) Specifies dot1q encapsulation.
(Optional) Specifies the encapsulation type of the destination

Number of a SPAN session; valid values are from 1 to 6.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

monitor session

learning

(Optional) Enables host learning on ingress-enabled destination ports.

remote

vlan

vlan_id

Specifies an RSPAN source or destination session on a switch.

source

Port-channel

interface-number

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

queue_id

(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 a high priority.

3

Specifies packets with a medium priority.

4

Specifies packets with a low priority.

ucast-rpf-fail


all

(Optional) all queues.
Chapter 2Cisco IOS Commands for the Catalyst 4500 Series Switches

monitor session

Defaults

Received and transmitted traffic, as well as all VLANs, packet types, and address types are monitored on a trunking interface. Packets are transmitted untagged 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

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

vlan_id
(Optional) Specifies the VLAN to be filtered. The number is entered as a single value or a range; valid values are from 1 to 4094.

packet-type
Limits SPAN source traffic to packets of a specified type.

good
Specifies a good packet type.

bad
Specifies a bad packet type.

address-type

unicast
| multicast
| broadcast

Limits SPAN source traffic to packets of a specified address type. Valid types are unicast, multicast, and broadcast.
**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 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**

This 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
```

This 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
```

```
This 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

This 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

This 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

This example shows how to configure RSPAN VLAN 20 as the destination:

Switch#
configure terminal
Switch(config)#
monitor session 2 destination remote vlan 20
Switch(config)#
end

This example shows how to use queue 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.
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
```

**Syntax Description**

The default settings are as follows:
- Jumbo frames are disabled
- 1500 bytes for all ports

**Defaults**

```
Jumbo frames are disabled
1500 bytes for all ports
```

**Command Modes**

Interface configuration mode

**Usage Guidelines**

Jumbo frames are supported on nonblocking Gigabit Ethernet ports, switch virtual interfaces (SVI), and EtherChannels. Jumbo frames are not available for 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**

This example shows how to specify an MTU of 1800 bytes:

```
Switch(config)>
interface GigabitEthernet 1/1
Switch(config-if)>
mtu 1800
```

**Related Commands**

- `system mtu`: Sets the maximum Layer 2 or Layer 3 payload size.
To set the MST region name, use the `name` command. To return to the default name, use the `no name` form of this command.

**Syntax Description**

**Defaults**

The MST region name is not set.

**Command Modes**

MST configuration mode

**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**

This example shows how to name a region:

```
Switch(config-mst)#
name Cisco
Switch(config-mst)#
```

**Related Commands**

- `name`: Specifies the name of the MST region. The name can be any string with a maximum length of 32 characters.
- `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.
To configure Network Mobility Services Protocol (NMSP) on the switch, use the `nmsp` command. This command is available only when your switch is running the cryptographic (encrypted) software image. Use the `no` form of this command to return to the default setting.

```
{nmsp {enable | {notification interval {attachment | location} interval-seconds}}}
{no nmsp {enable | {notification interval {attachment | location} interval-seconds}}}
```

**Syntax Description**

- `enable`: Enables the NMSP features on the switch.
- `notification interval`: Specifies the NMSP notification interval.
- `attachment`: Specifies the attachment notification interval.
- `location`: Specifies the location notification interval.
- `interval-seconds`: Duration in seconds before a switch sends the location or attachment updates to the MSE. The range is 1 to 30; the default is 30.

**Defaults**

NMSP is disabled, NMSP notification interval attachment and NMSP notification interval location defaults are 30 seconds.

**Command Modes**

Global configuration mode

**Usage Guidelines**

Use the `nmsp` global configuration command to enable the switch to send encrypted NMSP location and attachment notifications to a Cisco Mobility Services Engine (MSE).

**Examples**

This example shows how to enable NMSP on a switch and set the location notification time to 10 seconds:

```
Switch(config)#
nmsp enable
Switch(config)#
nmsp notification interval location 10
Switch(config)#
```

**Related Commands**

- `clear nmsp statistics`: Clears the NMSP statistic counters.
- `nmsp attachment suppress`: Suppress reporting attachment information from a specified interface.
- `show nmsp`: Displays the NMSP information.
To suppress reporting attachment information from a specified interface, use the `nmsp attachment suppress` 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.

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

Attachment information is reported.

**Command Modes**

Interface configuration mode

**Usage Guidelines**

Use the `nmsp attachment suppress` command to configure an interface to not send attachment notifications to a Cisco Mobility Services Engine (MSE).

**Examples**

This example shows how to configure an interface to not send attachment information to the MSE:

```
Switch(config)#
switch interface gigabitethernet1/2
Switch(config-if)#
no nmsp attachment suppress
```

**Related Commands**

- `nmsp`: Configures Network Mobility Services Protocol (NMSP) on the switch.
- `show nmsp`: Displays the NMSP information.
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}
```

### Syntax Description
- **Defaults**: Aggregation port is enabled.
- **Command Modes**: Interface configuration mode

### Examples
- This example shows how to enable physical port address learning within the bundle:

  ```
  Switch(config-if) #
  pagp learn-method physical-port
  Switch(config-if) #
  ```

- This example shows how to enable aggregation port address learning within the bundle:

  ```
  Switch(config-if) #
  pagp learn-method aggregation-port
  Switch(config-if) #
  ```

### Related Commands
- **aggregation-port**: Specifies learning the address on the port channel.
- **physical-port**: Specifies learning the address on the physical port within the bundle.

### Command Description
- **show pagp**: Displays information about the port channel.
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
```

**Syntax Description**

- **priority**: Port priority number; valid values are from 1 to 255.

**Defaults**

Port priority is set to 128.

**Command Modes**

Interface configuration mode

**Usage Guidelines**

The higher the priority, the better the chances are that the port will be selected in the hot standby mode.

**Examples**

This example shows how to set the port priority:

```
Switch(config-if) #
pagp port-priority 45
Switch(config-if) #
```

**Related Commands**

- `priority`
- `pagp learn-method`
- `show pagp`
To disable sending routing updates on an interface, use the `passive-interface` command. To reenable the sending of routing updates, use the `no` form of this command.

```
[[default] {interface-type interface-number} | {range interface-type interface-number-interface-type interface-number}]
```

**Syntax Description**

**Defaults**
Routing updates are sent on the interface.

**Command Modes**
Router configuration mode

**Usage Guidelines**
You can use the `passive-interface range` command on the following interfaces: FastEthernet, GigabitEthernet, VLAN, Loopback, Port-channel, 10-GigabitEthernet, and Tunnel. When you use the `passive-interface range` command on a VLAN interface, the interface should be the existing VLAN SVIs. To display the VLAN SVIs, enter the `show running config` command. The VLANs that are not displayed cannot be used in the `passive-interface range` command.

The 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:

1. Specifying up to five interface ranges
2. 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`:

1. `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 value. This makes the command similar to the \texttt{passive-interface} interface-number command.

Note The \texttt{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 \texttt{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 \texttt{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:

\begin{verbatim}
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
\end{verbatim}

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):

\begin{verbatim}
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
\end{verbatim}

The following example sets all interfaces as passive, then activates Ethernet interface 0:

\begin{verbatim}
Switch(config-if)\# router ospf 100
Switch(config-router)\# passive-interface default
\end{verbatim}
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) 
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]
```

**Syntax Description**

- **Defaults**
  This command has no default settings.

- **Command Modes**
  arp-nacl configuration mode

- **request**
  (Optional) Requests a match for the ARP request. When `request` is not specified, matching is performed against all ARP packets.

- **ip**
  Specifies the sender IP address.
  - `any` Specifies that any IP or MAC address will be accepted.
  - `host sender-ip` Specifies that only a specific sender IP address will be accepted.
  - `sender-ip sender-ip-mask` Specifies that a specific range of sender IP addresses will be accepted.

- **mac**
  Specifies the sender MAC address.
  - `host sender-mac` Specifies that only a specific sender MAC address will be accepted.
  - `sender-mac sender-mac-mask` Specifies that a specific range of sender MAC addresses will be accepted.

- **response**
  Specifies a match for the ARP responses.
  - `ip` Specifies the IP address values for the ARP responses.
  - `host target-ip` (Optional) Specifies that only a specific target IP address will be accepted.
  - `target-ip target-ip-mask` (Optional) Specifies that a specific range of target IP addresses will be accepted.

- **mac**
  Specifies the MAC address values for the ARP responses.
  - `host target-mac` (Optional) Specifies that only a specific target MAC address will be accepted.
  - `target-mac target-mac-mask` (Optional) Specifies that a specific range of target MAC addresses will be accepted.

- **log**
  (Optional) Logs a packet when it matches the access control entry (ACE).
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

permit

Usage Guidelines
Permit clauses can be added to forward or drop ARP packets based on some matching criteria.

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

Switch(config)#
arp access-list static-hosts
Switch(config-arp-nacl)#
permit ip host 1.1.1.1 mac host 0000.0000.abcd
Switch(config-arp-nacl)#
en
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.
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 police` command.

```
police {bps | kbps | mbps | gbps} [burst-normal] [burst-max] [conform-action] [exceed-action] [violate-action] action [violate-action] action

Syntax Description
```

- `bps`: Average rate, in bits per second. Valid values are 32,000 to 32,000,000,000.
- `kbps`: Average rate, in kilobytes per second. Valid values are 32 to 32,000,000.
- `mbps`: Average rate, in megabits per second. Valid values are 1 to 32,000.
- `gbps`: Average rate, in gigabits per second. Valid values are 1 to 32.
- `burst-normal`: (Optional) Normal burst size, in bytes. Valid values are 64 to 2,596,929,536.
- `burst-max`: (Optional) Excess burst size, in bytes. Valid values are 64 to 2,596,929,536.
- `conform-action`: Action to take on packets that conform to the rate limit.
- `exceed-action`: Action to take on packets that exceed the rate limit.
- `violate-action`: (Optional) Action to take on packets that violate the normal and maximum burst sizes.
- `action`: Action to take on packets. Specify one of the following keywords:
  - `drop`: Drops the packet.
  - `set-cos-transmit new-ios`: Sets the class of services (CoS) value to a new value and send the packet. The range is 0 to 7.
  - `set-dscp-transmit value`: Sets the IP differentiated services code point (DSCP) value and transmits the packet with the new IP DSCP value setting.
  - `set-prec-transmit value`: Sets the IP precedence and transmits the packet with the new IP precedence value setting.
  - `transmit`: Transmits the packet. The packet is not altered.

Defaults

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)

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:
  \[(\text{time between packets} \times 8 \text{ bytes}) / 8 \text{ bytes}\]

- 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 Tokens 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:

\[
\text{time between packets} \times \text{policer rate} / 8 \text{ bytes}
\]

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 exceed 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.

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 \((0.25 \times 8000)/8\), 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.

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, 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
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>police (percent)</td>
<td>Configures traffic policing on the basis of a percentage of bandwidth available on an interface.</td>
</tr>
<tr>
<td>police (two rates)</td>
<td>Configures traffic policing using two rates, the committed information rate (CIR) and the peak information rate (PIR).</td>
</tr>
<tr>
<td>policy-map</td>
<td>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.</td>
</tr>
<tr>
<td>service-policy (policy-map class)</td>
<td>Creates a service policy that is a quality of service (QoS) policy within a policy map.</td>
</tr>
<tr>
<td>show policy-map</td>
<td>Displays information about the policy map.</td>
</tr>
<tr>
<td>show policy-map interface</td>
<td>Displays the statistics and configurations of the input and output policies that are attached to an interface.</td>
</tr>
</tbody>
</table>
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
```
police (percent)

Command Modes
Policy-map class configuration mode

Usage Guidelines
This command calculates the CIR and PIR on the basis of a percentage of the maximum amount of bandwidth available on the interface. When a policy map is attached to the interface, the equivalent CIR and PIR values in bits per second (bps) are calculated on the basis of the interface bandwidth and the percent value entered with this command. The show policy-map interface command can then be used to verify the bps rate calculated.

The calculated CIR and PIR bps rates must be in the range of 32,000 and 32,000,000,000 bps. If the rates are outside this range, the associated policy map cannot be attached to the interface. If the interface bandwidth changes (for example, more is added), the bps values of the CIR and the PIR are recalculated on the basis of the revised amount of bandwidth. If the CIR and PIR percentages are changed after the policy map is attached to the interface, the bps values of the CIR and PIR are recalculated.

This command also allows you to specify the values for the conform burst size and the peak burst size in milliseconds. If you want bandwidth to be calculated as a percentage, the conform burst size and the peak burst size must be specified in milliseconds (ms).

Examples
This example shows how to configure traffic policing using a CIR and a PIR based on a percentage of bandwidth on Gigabit interface 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
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

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] [peak-burst peak-burst-in-bytes bytes]
```

```
no police rate units bps [burst burst-in-bytes bytes] [peak-rate peak-rate-in-bps bps] [peak-burst peak-burst-in-bytes bytes]
```

Syntax Description

- **Command Default**: This command is disabled by default.
- **units**: Specifies the traffic police rate in bits per second. Valid range is 32,000 to 32,000,000,000.
- **bps**: (Optional) Bits per second (bps) will be used to determine the rate at which traffic is policed. Note: If a rate is not specified, traffic is policed via bps.
- **burst**: (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**: (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**: (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.
- **percentage**: (Optional) Bandwidth percentage. Valid range is a number from 1 to 100.
- **burst**: (Optional) Burst rate, in milliseconds, will be used for policing traffic. Valid range is a number from 1 to 2,000.
- **peak-rate percent**: (Optional) A percentage of interface bandwidth will be used to determine the PIR. Valid range is a number from 1 to 100.
- **peak-burst**: (Optional) Peak burst rate, in milliseconds, will be used for policing traffic. Valid range is a number from 1 to 2,000.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

police rate

Command Modes
Policy-map configuration mode

Usage Guidelines
Use the **police rate** command to limit traffic on the basis of pps, bps, or a percentage of interface bandwidth.

If the **police rate** command is issued, but the a rate is not specified, traffic that is destined will be policed on the basis of bps.

Examples

This example shows how to configure policing on a class to limit traffic to an average rate of 1,500,000 bps:

```
Switch(config)#
class-map c1
Switch(config-cmap)#
match access-group 140
Switch(config-cmap)#
exit
Switch(config)#
policy-map p1
Switch(config-pmap)#
class c1
Switch(config-pmap-c)#
police rate 1500000  burst 500000
Switch(config-pmap-c)#
exit
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>policy-map</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>show policy-map</strong></td>
<td>Displays information about the policy map.</td>
</tr>
</tbody>
</table>
To configure traffic policing using two rates, the committed information rate (CIR) and the peak information rate (PIR), use the `police` command in policy-map configuration mode. To remove two-rate traffic policing from the configuration, use the `no` form of this command.

```
police cir [bc conform-burst] pir [be peak-burst] [conform-action] [exceed-action] [violate-action]
```

**Syntax Description**

**Command Default**
This command is disabled by default.

**Command Modes**
Policy-map configuration mode

**cir**
Committed information rate (CIR) at which the first token bucket is updated.

**cir**
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.

**conform-burst**
(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.

**pir**
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.

**peak-burst**
(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.

**action**
(Optional) Action to take on packets. Specify one of the following keywords:

- **drop** — Drops the packet.
- **set-cos-transmit** new-ios — Sets the class of services (CoS) value to a new value and send the packet. The range is 0 to 7.
- **set-dscp-transmit** new-dscp — Sets the IP differentiated services code point (DSCP) value and sends the packet with the new IP DSCP value setting.
- **set-prec-transmit** new-prec — Sets the IP precedence and sends the packet with the new IP precedence value setting.
- **transmit** — Sends the packet with no alteration.
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:

1. The Tc token bucket is updated at the CIR value each time a packet arrives at the two-rate policer. The Tc token bucket can contain up to the confirm burst (Bc) value.
2. 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:

\[
Tc(t) = \min(CIR \times (t-t1) + Tc(t1), Bc)
\]
\[
Tp(t) = \min(PIR \times (t-t1) + Tp(t1), Be)
\]

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:

1. If B > Tp(t), the packet is marked as violating the specified rate.
2. 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.
3. 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:

1. 100 kbps would be marked as conforming to the rate.
2. 100 kbps would be marked as exceeding the rate.
3. 50 kbps would be marked as violating the rate.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

Figure 2-1  Marking Packets and Assigning Actions with the Two-Rate Policer

Examples

This example shows how to configure two-rate traffic policing on a class to limit traffic to an average committed rate of 500 kbps and a peak rate of 1 Mbps:

Switch#  
configure terminal

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

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

<table>
<thead>
<tr>
<th>PIR</th>
<th>B &gt; Tp</th>
<th>Violate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Action</th>
<th>B &gt; Tc</th>
<th>Conform</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Conform</td>
</tr>
</tbody>
</table>

CIR | Bc | 60515
police (two rates)
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.
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
```

### Syntax Description

- **policy-map-name**: Name of the policy map.

### Defaults

No policy maps are defined.

### Command Modes

- **Global configuration mode**

### Usage Guidelines

Before configuring policies for classes whose match criteria are defined in a class map, use the `policy-map` command to specify the name of the policy map to be created or modified. After you enter the `policy-map` command, the switch enters policy-map configuration mode. You can configure or modify the class policies for that policy map and decide how to treat the classified traffic.

These configuration commands are available in policy-map configuration mode:

- **class**: Defines the classification match criteria for the specified class map. For more information, see the "class" section on page 2-84.
- **description**: Describes the policy map (up to 200 characters).
- **exit**: Exits policy-map configuration mode and returns you to global configuration mode.
- **no**: Removes a previously defined policy map.

To return to global configuration mode, use the `exit` command. To return to privileged EXEC mode, use the `end` command.

You can configure class policies in a policy map only if the classes have match criteria defined for them. To configure the match criteria for a class, use the `class-map` global configuration and `match` class-map configuration commands.

### Examples

This example shows how to configure multiple classes in a policy map called policymap2:

```
Switch# configure terminal
Switch(config)# policy-map policymap2
Switch(config-pmap)# class class1
Switch(config-pmap-c)# police 100000 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
```
This example shows how to delete the policy map called policymap2:

```
Switch#
configure terminal
Switch(config)#
no policy-map policymap2
Switch#
```

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

---

**Related Commands**

- **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.
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
```

**Syntax Description**

```
Syntax Description

Defaults
Load distribution on the source XOR destination IP address is enabled.

Command Modes
Global configuration mode

Usage Guidelines

The following values are valid for the load-distribution method:

- `dst-ip` — Load distribution on the destination IP address
- `dst-mac` — Load distribution on the destination MAC address
- `dst-port` — Load distribution on the destination TCP/UDP port
- `src-dst-ip` — Load distribution on the source XOR destination IP address
- `src-dst-mac` — Load distribution on the source XOR destination MAC address
- `src-dst-port` — Load distribution on the source XOR destination TCP/UDP port
- `src-ip` — Load distribution on the source IP address
- `src-mac` — Load distribution on the source MAC address
- `src-port` — Load distribution on the source port

Examples

This example shows how to set the load-distribution method to the destination IP address:

```
Switch(config)#
port-channel load-balance dst-ip
```

This example shows how to set the load-distribution method to the source XOR destination IP address:

```
Switch(config)#
port-channel load-balance src-dst-port
```

**Related Commands**

```
method
Specifies the load distribution method. See the "Usage Guidelines" section for more information.
```

<table>
<thead>
<tr>
<th>Command Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface port-channel</td>
<td>Accesses or creates a port-channel interface.</td>
</tr>
<tr>
<td>show etherchannel</td>
<td>Displays EtherChannel information for a channel.</td>
</tr>
</tbody>
</table>
To disable the EtherChannel standalone option in a port channel, use the `port-channel standalone-disable` command in interface configuration mode. To enable this option, use the `no` form of this command.

```
port-channel standalone-disable
no port-channel standalone-disable
```

### Syntax Description

This command has no arguments or keywords.

### Defaults

The standalone option is disabled.

### Command Modes

Interface configuration mode

### Usage Guidelines

This command can only be used when the port channel protocol type is Link Aggregation Control Protocol (LACP). It allows you to change the current behavior when a physical port cannot bundle with an LACP EtherChannel.

### Examples

The following example shows how to enable the EtherChannel standalone option in a port channel:

```
Switch(config-if)#
no port-channel standalone-disable
```
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

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.

Syntax Description

- `mac_address`: The MAC address that needs to be secured.

Command Modes

VLAN-range interface submode

Usage Guidelines

Layer 2 interfaces can be part of multiple VLANs (for example, a typical trunk port). In conjunction with the `vlan` command, you can use the `port-security mac-address` command to specify different addresses on different VLANs.

Examples

This example shows how to configure the secure address 1.1.1 on interface Gigabit Ethernet 1/1 for VLANs 2-3:

```
Switch# configure terminal
Switch(config)#!
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

- `mac_address`: The MAC address that needs to be secured.
- `port-security mac-address`: 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.
To configure a sticky address on an interface for a specific VLAN or VLAN range, use the `port-security mac-address sticky` command.

**Syntax Description**

- **Syntax:**
  
  ```
  port-security mac-address sticky mac_address
  ```

**Command Modes**

- **VLAN-range interface submode**

**Usage Guidelines**

- The Sticky feature must be enabled on an interface before you can configure the `port-security mac-address sticky` command.
- 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.
- Sticky MAC addresses are addresses that persist across switch reboots and link flaps.

**Examples**

This example shows how to configure the sticky address 1.1.1 on interface Gigabit Ethernet 1/1 for VLANs 2-3:

```
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**
  
  ```
  mac_address
  ```

  The MAC-address that needs to be secured.

  ```
  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.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>max_value</td>
<td>The maximum number of MAC-addresses.</td>
</tr>
</tbody>
</table>

**Command Modes**

VLAN-range interface submode

**Usage Guidelines**

Layer 2 interfaces can be part of multiple VLANs (for example, a typical trunk port). In conjunction with the `vlan` command, you can use the `port-security maximum` command to specify the maximum number of secure addresses on different VLANs.

If a specific VLAN on a port is not configured with a maximum value, the maximum configured for the port is used for that VLAN. In this situation, the maximum number of addresses that can be secured on this VLAN is limited to the maximum value configured on the port.

Each VLAN can be configured with a maximum count that is greater than the value configured on the port. Also, the sum total of the maximum configured values for all the VLANs can exceed the maximum configured for the port. In either of these situations, the number of MAC addresses secured on each VLAN is limited to the lesser of the VLAN configuration maximum and the port configuration maximum.

**Examples**

This example shows how to configure a maximum number of addresses (5) on interface 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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>port-security mac-address</td>
<td>Configures a secure address on an interface for a specific VLAN or VLAN range.</td>
</tr>
<tr>
<td>port-security mac-address sticky</td>
<td>Configures a sticky address on an interface for a specific VLAN or VLAN range.</td>
</tr>
</tbody>
</table>
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
```

**Syntax Description**

Sets the total capacity of the external DC source in watts; valid values are from 300 to 8500.

**Defaults**

DC power input is 2500 W.

**Command Modes**

Global configuration mode

**Usage Guidelines**

If your interface is not capable of supporting Power over Ethernet, you will receive this message:

```
Power over Ethernet not supported on interface Admin
```

**Examples**

This example shows how to set the total capacity of the external DC power source to 5000 W:

```
Switch(config)＃
power dc input 5000
Switch(config)＃
```

**Related Commands**

- **watts**
  - Sets the total capacity of the external DC source in watts; valid values are from 300 to 8500.
- **show power**
  - Displays information about the power status.
To enable EEE, use the `power efficient-ethernet auto` command. To disable EEE, use the `no` form of this command.

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

EEE is disabled

**Command Modes**

Global configuration mode

**Usage Guidelines**

EEE is supported on WS-X4748-UPOE+E and WS-X4748-RJ45-E.

EEE defines support for physical layer devices (PHYs) to operate in Low Power Idle (LPI) mode. When enabled, EEE supports QUIET times during low link utilization allowing both sides of a link to disable portions of each PHY'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**

This example shows how to enable EEE:

```
Switch# configure terminal
Switch(config) interface gigabitethernet 1/1
Switch(config-if) power efficient-ethernet auto
Switch(config-if) exit
```
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}
```

**Defaults**

- The default settings are as follows:
  - Auto mode for Power over Ethernet is set.
  - Maximum mW mode is set to 15400. For the WS-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

**Usage Guidelines**

If your interface is not capable of supporting Power over Ethernet, you will receive this message:

```
Power over Ethernet not supported on interface Admin
```

**Examples**

This example shows how to set the inline-power detection and power for the inline-power-capable interfaces:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config) #
interface fastethernet 4/1
Switch(config-if) #
power inline auto
Switch(config-if) #
end
Switch#
```
This example shows how to disable the inline-power detection and power for the inline-power-capable interfaces:

Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 4/1
Switch(config-if)# power inline never
Switch(config-if)# end
Switch#

This example shows how to set the permanent Power over Ethernet allocation to 8000 mW for Fast Ethernet interface 4/1 regardless what is mandated either by the 802.3af class of the discovered device or by any CDP packet that is received from the powered device:

Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 4/1
Switch(config-if)# power inline consumption 8000
Switch(config-if)# end
Switch#

This example shows how to pre-allocate Power over Ethernet to 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.
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 power inline consumption default` form of this command.

```
Switch(config)# power inline consumption default 8000

Switch(config)#
```

**Syntax Description**

- **Defaults**
  - Milliwatt mode is set to 15400.

- **Command Modes**
  - Global configuration mode

**Usage Guidelines**

The `inline power consumption` command overrides the power allocated to the port through IEEE/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**

This example shows how to set the Power over Ethernet allocation to use 8000 mW, regardless of any CDP packet that is received from the powered device:

```
Switch# configure terminal
Switch(config)# power inline consumption default 8000
Switch(config)#
```

**Related Commands**

- `default` - Specifies the switch to use the default allocation.
- `milliwatts` - 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.

- `power inline` - Sets the inline-power state for the inline-power-capable interfaces.
- `show power` - Displays information about the power status.
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.

### Syntax Description

This command has no arguments or keywords.

### Defaults

None

### Command Modes

Interface configuration mode

### Usage Guidelines

Although IEEE 802.at 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 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.
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.

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

Disabled

**Command Modes**

Global configuration mode

**Usage Guidelines**

Be aware of the potential for console flooding if this command is used on a switch connected to several PoE devices.

**Examples**

This example shows how to globally enable PoE status messaging on each interface:

To enable PoE event logging, you 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)# no shut
Switch(config-if)# *Oct 17 12:02:54.915: %ILPOWER-7-DETECT: Interface Gi5/5: Power Device detected: IEEE PD
```

**Related Commands**

- `logging event link-status global` (global configuration)
  Changes the default switch-wide global link-status event messaging settings.
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]]
```

**Syntax Description**

- **Defaults**: PoE policing is disabled.
- **Command Modes**: Interface configuration mode
- **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**

This 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 Oper Admin Oper Cutoff Oper
State State Police Police Power 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 Oper Admin Oper Cutoff Oper
State State Police Police Power Power
--------- ------ ---------- ---------- ---------- ------ -----
Gi2/1 auto on log ok 17.4 9.6
```

- **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.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

power inline police

Related Commands

- 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.
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
```

Syntax Description

- `redundant`
- `combined`

**Defaults**

- Redundant power management mode

**Command Modes**

- Global configuration mode

**Usage Guidelines**

The two power supplies must be the same type and wattage.

- **Caution**
  - If you have power supplies with different types or wattages installed in your switch, the switch will not recognize one of the power supplies. A switch set to redundant mode will not have power redundancy. A switch set to combined mode will use only one power supply.
  - In redundant mode, the power from a single power supply must provide enough power to support the switch configuration.

**Table 2-9 Available Power**

<table>
<thead>
<tr>
<th>Power Supply Redundant Mode (W)</th>
<th>Combined Mode (W)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000 W AC System</td>
<td>1 = 1000</td>
</tr>
<tr>
<td></td>
<td>Inline = 0</td>
</tr>
<tr>
<td>2800 W AC System</td>
<td>1 = 1360</td>
</tr>
<tr>
<td></td>
<td>Inline = 1400</td>
</tr>
<tr>
<td></td>
<td>2 = 2473</td>
</tr>
<tr>
<td></td>
<td>Inline = 2333</td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to set the power management mode to combined:

```
Switch(config)#
power redundancy-mode combined
Switch(config)#
```

**Related Commands**

- `redundant`
  - Configures the switch to redundant power management mode.
- `combined`
  - Configures the switch to combined power management mode.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

command syntax:  

power redundancy-mode

Command Description

show power
Displays information about the power status.
Chapter 2  Cisco IOS Commands for the Catalyst 4500 Series Switches

pppoe intermediate-agent (global)

To enable the PPPoE Intermediate Agent feature on a switch, use the `pppoe intermediate-agent` command. To disable the feature, use the `no` form of this command.

Syntax Description
This command has no arguments or keywords.

Defaults
`disabled`

Command Modes
Global configuration mode

Usage Guidelines
You must enable PPPoE Intermediate Agent globally on a switch before you can use PPPoE Intermediate Agent on an interface or interface VLAN.

Examples
This example shows how to enable PPPoE Intermediate Agent on a switch:

```
Switch(config)#
pppoe intermediate-agent
```

This example shows how to disable PPPoE Intermediate Agent on a switch:

```
Switch(config)#
no pppoe intermediate-agent
```
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.

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

Disabled on all interfaces.

**Command Modes**

Interface configuration mode

**Usage Guidelines**

PPPoE Intermediate Agent is enabled on an interface provided the PPPoE Intermediate Agent is enabled both on the switch and the interface.

**Examples**

This example shows how to enable the PPPoE Intermediate Agent on an interface:

```
Switch(config-if)#
pppoe intermediate-agent
```

This example shows how to disable the PPPoE Intermediate Agent on an interface:

```
Switch(config-if)#
no pppoe intermediate-agent
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pppoe intermediate-agent</td>
<td>Sets circuit ID or remote ID for an interface.</td>
</tr>
<tr>
<td>pppoe intermediate-agent limit rate</td>
<td>Limits the rate of the PPPoE Discovery packets coming on an interface.</td>
</tr>
<tr>
<td>pppoe intermediate-agent trust</td>
<td>Sets the trust configuration of an interface.</td>
</tr>
<tr>
<td>pppoe intermediate-agent vendor-tag strip</td>
<td>Enables vendor-tag stripping on PPPoE Discovery packets from PPPoE Server (or BRAS).</td>
</tr>
</tbody>
</table>
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.

Syntax Description
This command has no arguments or keywords.

Defaults
Disabled on all VLANs on all interfaces

Command Modes
Interface vlan-range configuration mode

Usage Guidelines
Although this command takes effect irrespective of the pppoe intermediate-agent (interface configuration mode) command, you must enable the pppoe intermediate-agent (global configuration mode) command.

Examples
This example shows how to enable PPPoE Intermediate Agent on a range of VLANs:

Switch(config-if)#
vlan-range 167-368
Switch(config-if-vlan-range)#
pppoe intermediate-agent

This example shows how to disable PPPoE Intermediate Agent on a single VLAN:

Switch(config-if)#
vlan-range 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
pppoe intermediate-agent format-type generic-error-message string
pppoe intermediate-agent format-type identifier-string string
```

**Syntax Description**

- `access-node-identifier` has a default value of 0.0.0.0.
- `generic-error-message`, `identifier-string`, `option`, and `delimiter` have no default values.

**Command Modes**

Global configuration mode

**Usage Guidelines**

Use the `access-node-identifier` and `identifier-string` commands to enable the switch to generate the circuit-id parameters automatically. The `no` form of `identifier-string` command unsets the option and delimiter.

Use the `generic-error-message` command to set an error message notifying the sender that the PPPoE Discovery packet was too large.

**access-node-identifier**

- **string**
  - ASCII string literal value for the access-node-identifier.

**generic-error-message**

- **string**
  - ASCII string literal value for the generic-error-message.

**identifier-string**

- **string**
  - 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.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

pppoe intermediate-agent format-type (global)

Examples

This example shows how to set an access-node-identifier:

Switch(config)#
pppoe intermediate-agent format-type access-node-identifier string
switch-abc-123

This example shows how to unset a generic-error-message:

Switch(config)#
no pppoe intermediate-agent format-type generic-error-message

Related Commands Command Description

show pppoe intermediate-agent interface
Displays the PPPoE Intermediate Agent configuration and
statistics (packet counters).
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
```

### Syntax Description
- **circuit-id**
  - string: ASCII string literal value for circuit-id.
- **remote-id**
  - string: ASCII string literal value for remote-id.

### Command Modes
- Interface configuration mode

### Usage Guidelines
Use the `pppoe intermediate-agent format-type` command to set interface-specific circuit-id and remote-id values. If an interface-specific circuit-id is not set, the system's automatic generated circuit-id value is used.

### Examples
This example shows how to set remote-id for an interface:
```
Switch(config-if)#
pppoe intermediate-agent format-type remote-id string user5551983
```
This example shows how to unset circuit-id for an interface:
```
Switch(config)#
no pppoe intermediate-agent format-type circuit-id
```

### Related Commands
- `circuit-id string`
  - string: ASCII string literal value for circuit-id.
- `remote-id string`
  - string: ASCII string literal value for remote-id.
- `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.
Note
This command takes effect only if you enable the `pppoe intermediate-agent` 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

`no pppoe intermediate-agent format-type` {
    circuit-id |
    remote-id
} string

Syntax Description
No default values for circuit-id and remote-id.

Command Modes
Interface vlan-range configuration mode

Usage Guidelines
Use these commands to set circuit-id or remote-id on an interface vlan-range. If the circuit-id is not set, the system’s automatically generated circuit-id is used.

Examples
This example shows how to set remote-id on an interface VLAN:
```
Switch(config-if)#
vlan-range 268
Switch(config-if-vlan-range)#
pppoe intermediate-agent format-type remote-id string user5551983-cabletv
```
This 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
`circuit-id string`
ASCII string literal value to be set for circuit-id.

`remote-id string`
ASCII string literal value to be set for remote-id.

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
```

**Syntax Description**

- `number`: Specifies the threshold rate of PPPoE Discovery packets received on this interface in packets-per-second.

**Defaults**

This command has no default settings.

**Command Modes**

Interface configuration mode

**Usage Guidelines**

If this command is used and the PPPoE Discovery packets that are received exceeds the rate set, the interface will be error-disabled (shutdown).

**Examples**

This example shows how to set a rate limit for an interface:

```
Switch(config-if)# pppoe intermediate-agent limit rate 50
```

This example shows how to disable rate limiting for an interface:

```
Switch(config-if)# no pppoe intermediate-agent limit rate
```

**Related Commands**

- `pppoe intermediate-agent (interface)`: Enables the PPPoE Intermediate Agent feature on an interface.
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.

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

**Defaults**
All interfaces are untrusted.

**Command Modes**
Interface configuration mode

**Usage Guidelines**
At least one trusted interface must be present on the switch for PPPoE Intermediate Agent feature to work. Set the interface connecting the switch to the PPPoE Server (or BRAS) as trusted.

**Examples**
This example shows how to set an interface as trusted:
```
Switch(config-if)# pppoe intermediate-agent trust
```
This example shows how to disable the trust configuration for an interface:
```
Switch(config-if)# no pppoe intermediate-agent trust
```

**Related Commands**
- `pppoe intermediate-agent vendor-tag strip`: Enables vendor-tag stripping on PPPoE Discovery packets from a PPPoE Server (or BRAS).
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.

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

Vendor-tag stripping is turned off.

**Command Modes**

Interface configuration mode

**Usage Guidelines**

This command has no effect on untrusted interfaces.

Use this command on a PPPoE Intermediate Agent trusted interface to strip off the vendor-specific tags in PPPoE Discovery packets that arrive downstream from the PPPoE Server (or BRAS), if any.

**Examples**

This example shows how to set vendor-tag stripping on an interface:

```
Switch(config-if) #
pppoe intermediate-agent vendor-tag strip
```

This example shows how to disable vendor-tag stripping on an interface:

```
Switch(config-if) #
no pppoe intermediate-agent vendor-tag strip
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>pppoe intermediate-agent</strong> (interface)</td>
</tr>
<tr>
<td><strong>pppoe intermediate-agent trust</strong></td>
</tr>
</tbody>
</table>
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.

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

The strict priority queue is disabled.

**Command Modes**

Policy-map class configuration mode

**Usage Guidelines**

Use the `priority` command only in a policy map attached to a physical port. You can use this command only in class-level classes, you cannot use this command in class 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**

This 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.
## Chapter 2: Cisco IOS Commands for the Catalyst 4500 Series Switches

### priority

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bandwidth</td>
<td>Specifies or modifies the minimum bandwidth provided to a class belonging to a policy map attached to a physical port.</td>
</tr>
<tr>
<td>class</td>
<td>Specifies the name of the class whose traffic policy you want to create or change.</td>
</tr>
<tr>
<td>dbl</td>
<td>Enables dynamic buffer limiting for traffic hitting this class.</td>
</tr>
<tr>
<td>policy-map</td>
<td>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.</td>
</tr>
<tr>
<td>service-policy (policy-map class)</td>
<td>Creates a service policy that is a quality of service (QoS) policy within a policy map.</td>
</tr>
<tr>
<td>shape (class-based queueing)</td>
<td>Enables traffic shaping a class of traffic in a policy map attached to a physical port.</td>
</tr>
<tr>
<td>show policy-map</td>
<td>Displays information about the policy map.</td>
</tr>
</tbody>
</table>
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**

**Defaults**
Private VLANs are not configured.

**Command Modes**
VLAN configuration mode

**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.

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.

secondary-vlan-list
Specifies the number of the secondary VLAN. The list can contain only one isolated VLAN ID; it can also contain multiple community or twoway-community VLAN IDs.

**add** (Optional) Associates a secondary VLAN to a primary VLAN.

**remove** (Optional) Clears the association between a secondary VLAN and a primary VLAN.
An isolated VLAN is a VLAN that is used by the isolated ports to communicate with the promiscuous ports. The isolated VLAN traffic is blocked on all other private ports in the same VLAN and can be received only by the standard trunking ports and the promiscuous ports that are assigned to the corresponding primary VLAN.

A community VLAN is the VLAN that carries the traffic among the community ports and from the community ports to the promiscuous ports on the corresponding primary VLAN. A community VLAN is not allowed on a private VLAN trunk.

A promiscuous port is a private port that is assigned to a primary VLAN.

A primary VLAN is a VLAN that is used to convey the traffic from the switches to the customer end stations on the private ports.

You can specify only one isolated VLAN ID value, while multiple community VLANs are allowed. You can only associate isolated and community VLANs to one VLAN. The associated VLAN list may not contain primary VLANs. Similarly, a VLAN that is already associated to a primary VLAN cannot be configured as a primary VLAN.

The `private-vlan` commands do not take effect until you exit the config-VLAN submode.

If you delete either the primary or secondary VLAN, the ports that are associated with the VLAN become inactive.

Refer to the `Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide` for additional configuration guidelines.

Examples

This example shows how to configure VLAN 202 as a primary VLAN and verify the configuration:

```
Switch# 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
```

This 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
```

This 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
```
This example shows how to create a private VLAN relationship among the primary VLAN 14, the isolated VLAN 19, and community VLANs 20 and 21:

Switch(config)#
vlan 19
Switch(config-vlan) #
private-vlan isolated
Switch(config-vlan) #
vlan 14
Switch(config-vlan) #
private-vlan primary
Switch(config-vlan) #
private-vlan association 19

This example shows how to remove a private VLAN relationship and delete the primary VLAN. The associated secondary VLANs are not deleted.

Switch(config-vlan)#
no private-vlan 14
Switch(config-vlan)#

This example shows how to configure VLAN 550 as a two-way-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     303       community
202     304       community
202     305       community
202     306       community
202     307       community
202     309       community
202     440       isolated
308       community

This example shows how to associate community VLANs 303 through 307 and 309 and isolated VLAN 440 with primary VLAN 202 and verify the configuration:

Switch#
configure terminal
Switch(config)#
vlan 202
Switch(config-vlan) #
private-vlan association 303-307,309,440
Switch(config-vlan) #
end
Switch#
show vlan private-vlan

Primary Secondary Type              Interfaces
------- --------- ----------------- ------------------------------------------
202     303       community
202     304       community
202     305       community
202     306       community
202     307       community
202     309       community
202     440       isolated
308       community

Note
The secondary VLAN 308 has no associated primary VLAN.

This example shows how to remove an isolated VLAN from the private VLAN association:

Switch(config)#
vlan 14
Switch(config-vlan) #
private-vlan association remove 18
Switch(config-vlan) #
This example shows how to configure interface FastEthernet 5/1 as a PVLAN host port and verify the configuration:

Switch# 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.
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 private-vlan mapping` form of this command.

```
private-vlan mapping primary-vlan-id { [secondary-vlan-list] | { add secondary-vlan-list } | { remove secondary-vlan-list } }
```

**Syntax Description**

- `primary-vlan-id`: VLAN ID of the primary VLAN of the PVLAN relationship.
- `secondary-vlan-list` (Optional): VLAN ID of the secondary VLANs to map to the primary VLAN.
- `add` (Optional): Maps the secondary VLAN to the primary VLAN.
- `remove` (Optional): Removes the mapping between the secondary VLAN and the primary VLAN.

**Defaults**

All PVLAN mappings are removed.

**Command Modes**

Interface configuration mode

**Usage Guidelines**

- The `secondary_vlan_list` parameter cannot contain spaces. It can contain multiple, comma-separated items. Each item can be a single PVLAN ID or a range of PVLAN IDs separated by hyphens.
- This command is valid in the interface configuration mode of the primary VLAN.
- The SVI of the primary VLAN is created at Layer 3.
- The traffic that is received on the secondary VLAN is routed by the SVI of the primary VLAN.
- The SVIs of the existing secondary VLANs do not function and are considered down after this command is entered.
- A secondary SVI can be mapped to only one primary SVI. If the configured PVLANs association is different from what is specified in this command (if the specified `primary-vlan-id` is configured as a secondary VLAN), all the SVIs that are specified in this command are brought down.
- If you configure a mapping between two VLANs that do not have a valid Layer 2 association, the mapping configuration does not take effect.

**Examples**

This example shows how to map the interface of VLAN 20 to the SVI of VLAN 18:

```
Switch(config) #
interface vlan 18
Switch(config-if) #
private-vlan mapping 18 20
```

This example shows how to permit the routing of the secondary VLAN ingress traffic from PVLANs 303 through 307, 309, and 440 and how to verify the configuration:

```
Switch#
config terminal
```
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

private-vlan mapping

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

<table>
<thead>
<tr>
<th>Interface</th>
<th>Secondary VLAN</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan202</td>
<td>303</td>
<td>isolated</td>
</tr>
<tr>
<td>vlan202</td>
<td>304</td>
<td>isolated</td>
</tr>
<tr>
<td>vlan202</td>
<td>305</td>
<td>isolated</td>
</tr>
<tr>
<td>vlan202</td>
<td>306</td>
<td>isolated</td>
</tr>
<tr>
<td>vlan202</td>
<td>307</td>
<td>isolated</td>
</tr>
<tr>
<td>vlan202</td>
<td>309</td>
<td>isolated</td>
</tr>
<tr>
<td>vlan202</td>
<td>440</td>
<td>isolated</td>
</tr>
</tbody>
</table>

Switch# This example shows the displayed message that you will see if the VLAN that you are adding is already mapped to the SVI of VLAN 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 a secondary.
Switch(config-if)\# This example shows how to remove all PVLAN mappings from the SVI of VLAN 19:
Switch(config)\# interface vlan 19
Switch(config-if)\# no private-vlan mapping
Switch(config-if)\# Switch#

configure terminal
Switch(config)\# interface vlan 202
Switch(config-if)\# private-vlan mapping add 303-307,309,440
Switch(config-if)\# end
Switch#

show interfaces private-vlan mapping

<table>
<thead>
<tr>
<th>Interface</th>
<th>Secondary VLAN</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan202</td>
<td>303</td>
<td>community</td>
</tr>
<tr>
<td>vlan202</td>
<td>304</td>
<td>community</td>
</tr>
<tr>
<td>vlan202</td>
<td>305</td>
<td>community</td>
</tr>
<tr>
<td>vlan202</td>
<td>306</td>
<td>community</td>
</tr>
<tr>
<td>vlan202</td>
<td>307</td>
<td>community</td>
</tr>
<tr>
<td>vlan202</td>
<td>309</td>
<td>community</td>
</tr>
<tr>
<td>vlan202</td>
<td>440</td>
<td>isolated</td>
</tr>
</tbody>
</table>

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.
To map the secondary VLANs to the same instance as the primary VLAN, use the `private-vlan synchronize` command.

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

MST configuration mode

**Usage Guidelines**

If you do not map the VLANs 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**

This example shows how to initialize PVLAN synchronization:

```
Switch(config-mst)#
private-vlan synchronize
Switch(config-mst)#
```

This example assumes that a primary VLAN 2 and a secondary VLAN 3 are associated to VLAN 2, and that all VLANs are mapped to the 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**

- `show spanning-tree mst`
  Displays MST protocol information.
To enter profile call-home configuration submode, use the `profile profile_name` command in call-home configuration mode.

**Syntax Description**

This command has no default settings.

**Command Modes**

cfg-call-home

**Usage Guidelines**

When you enter the `profile profile_name` command in call-home mode, the prompt changes to `Switch(cfg-call-home-profile)#`, and you have access to the following profile configuration commands:

- active
- destination address
- destination message-size-limit bytes
- destination preferred-msg-format
- destination transport-method
- end
- exit
- subscribe-to-alert-group all
- subscribe-to-alert-group configuration
- subscribe-to-alert-group diagnostic severity normal
- subscribe-to-alert-group environment severity notification
- subscribe-to-alert-group syslog severity notification pattern "UPDOWN"
- subscribe-to-alert-group inventory periodic daily 21:12

**Examples**

This 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
```
# Cisco IOS Commands for the Catalyst 4500 Series Switches

## Profile

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>destination_address</td>
<td>Configures the destination e-mail address or URL to which Call Home messages will be sent.</td>
</tr>
<tr>
<td>destination_message-size-limit bytes</td>
<td>Configures a maximum destination message size for the destination profile.</td>
</tr>
<tr>
<td>destination_preferred-msg-format</td>
<td>Configures a preferred message format.</td>
</tr>
<tr>
<td>destination_transport-method</td>
<td>Enables the message transport method.</td>
</tr>
<tr>
<td>subscribe-to-alert-group all</td>
<td>Subscribes to all available alert groups.</td>
</tr>
<tr>
<td>subscribe-to-alert-group configuration</td>
<td>Subscribes this destination profile to the Configuration alert group.</td>
</tr>
<tr>
<td>subscribe-to-alert-group diagnostic</td>
<td>Subscribes this destination profile to the Diagnostic alert group.</td>
</tr>
<tr>
<td>subscribe-to-alert-group environment</td>
<td>Subscribes this destination profile to the Environment alert group.</td>
</tr>
<tr>
<td>subscribe-to-alert-group inventory</td>
<td>Subscribes this destination profile to the Inventory alert group.</td>
</tr>
<tr>
<td>subscribe-to-alert-group syslog</td>
<td>Subscribes this destination profile to the Syslog alert group.</td>
</tr>
</tbody>
</table>
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.

**Defaults**

Policers account only for the Layer 2 header length in policing features. In contrast, shapers account for header length as well as IPG in rate calculations.

**Command Modes**

Global configuration

**Usage Guidelines**

Supervisor Engine 6-E, Supervisor Engine 6L-E, Catalyst 4900M, and Catalyst 4948E use the `qos account layer-all encapsulation` command to account for Layer 1 header of 20 bytes (preamble + IPG) and Layer 2 header in policing features. When this command is configured, policer statistics (in bytes) observed in the output of the `show policy-map interface` command reflect the Layer 1 header length as well (20 bytes per packet).

**Examples**

This example shows how to include IPG in policing:

```
Switch)#
cfg t
Switch(config)#
qos account layer-all encapsulation
Switch(config)#
en
Switch#
```

**Related Commands**

- `show policy-map interface`: Displays policer statistics on a specific interface.
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**

**Defaults**

The length that is specified in the Ethernet header is considered for both IP and non-IP packets. The Layer 2 length includes the VLAN tag overhead.

**Command Modes**

Global configuration mode

**Usage Guidelines**

Shaping and sharing always use Ethernet ARPA length to which 20 bytes of IPv6 overhead is always added for policing. However, only Layer 2 length including VLAN tag overhead is considered.

**Note**

The given length is included when policing all IP packets irrespective of the encapsulation with which it was received. When `qos account layer2 encapsulation 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**

This 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#
```

This 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#
```

**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**

Specifies the additional packet length to account for; the valid range is from 0 to 64 bytes.
## qos account layer2 encapsulation

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show interfaces</td>
<td>Displays traffic on a specific interface.</td>
</tr>
<tr>
<td>switchport</td>
<td>Modifies the switching characteristics of a Layer 2 switch interface.</td>
</tr>
<tr>
<td>switchport block</td>
<td>Prevents the unknown multicast or unicast packets from being forwarded.</td>
</tr>
</tbody>
</table>
To set the trusted state of an interface (for example, whether the packets arriving at an interface are trusted to carry the correct CoS, ToS, and DSCP classifications), use the `qos trust` command. To set an interface to the untrusted state, use the `no` form of this command.

```
qos trust {cos | device cisco-phone | dscp | extend [cos priority]}

no qos trust {cos | device cisco-phone | dscp | extend [cos priority]}
```

### Syntax Description

- **cos**: Specifies that the CoS bits in incoming frames are trusted and derives the internal DSCP value from the CoS bits.
- **device cisco-phone**: Specifies the Cisco IP phone as the trust device for a port.
- **dscp**: Specifies that the ToS bits in the incoming packets contain a DSCP value.
- **extend**: Specifies to extend the trust to Port VLAN ID (PVID) packets coming from the PC.
- **cos priority** (Optional): Specifies that the CoS priority value is set to PVID packets; valid values are from 0 to 7.

### Defaults

The default settings are as follows:

- If global QoS is enabled, trust is disabled on the port.
- If global QoS is disabled, trust DSCP is enabled on the port.
- The CoS priority level is 0.

### Command Modes

- **Interface configuration mode**

### Usage Guidelines

- This command is not supported on the Supervisor Engine 6-E and Catalyst 4900M chassis.
- You can only configure the trusted state on physical LAN interfaces.
- By default, the trust state of an interface when QoS is enabled is untrusted; when QoS is disabled on the interface, the trust state is reset to trust DSCP.
- When the interface trust state is `qos trust cos`, the transmit CoS is always the incoming packet CoS (or the default CoS for the interface, if the packet is not tagged).
- When the interface trust state is not `qos trust dscp`, the security and QoS ACL classification will always use the interface DSCP and not the incoming packet DSCP.
- Trusted boundary should not be configured on the ports that are part of an EtherChannel (that is, a port channel).

### Examples

This example shows how to set the trusted state of an interface to CoS:

```
Switch(config-if)#
quos trust cos
Switch(config-if)#
```
This example shows how to set the trusted state of an interface to DSCP:

Switch(config-if)# qos trust dscp

This example shows how to set the PVID CoS level to 6:

Switch(config-if)# qos trust extend cos 6

This example shows how to set the Cisco phone as the trust device:

Switch(config-if)# qos trust device cisco-phone

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>queue-limit</td>
<td>Defines per-VLAN QoS for a Layer 2 interface.</td>
</tr>
<tr>
<td>show qos interface</td>
<td>Displays QoS information for an interface.</td>
</tr>
</tbody>
</table>
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
```

**Syntax Description**

- `number-of-packets`: 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.

**Defaults**

By default, each physical interface on a Catalyst 4500 switch has a default queue based on the number of slots in a chassis and the number of ports on the linecards.

**Command Modes**

QoS policy-map class configuration mode

**Usage Guidelines**

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.

**Examples**

This 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#
```
Chapter 2  Cisco IOS Commands for the Catalyst 4500 Series Switches

queue-limit

Related Commands

- **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 queueing)**
  Enables traffic shaping a class of traffic in a policy map attached to a physical port.
To enter the redundancy configuration mode, use the `redundancy` command in the global configuration mode.

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Global configuration mode

**Usage Guidelines**

The redundancy configuration mode is used to enter the main CPU submode. To enter the main CPU submode, use the `main-cpu` command in the redundancy configuration mode. The main CPU submode is used to manually synchronize the configurations on the two supervisor engines. From the main CPU submode, use the `auto-sync` command to enable automatic synchronization of the configuration files in NVRAM. Use the `no` command to disable redundancy. If you disable redundancy, then re-enable redundancy, the switch returns to default redundancy settings. Use the `exit` command to exit the redundancy configuration mode.

**Examples**

This example shows how to enter redundancy mode:

```
Switch(config)#
redundancy
Switch(config-red)#
```

This example shows how to enter the main CPU submode:

```
Switch(config)#
redundancy
Switch(config-red)#
main-cpu
Switch(config-r-mc)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>auto-sync</code></td>
<td>Enables automatic synchronization of the configuration files in NVRAM.</td>
</tr>
<tr>
<td><code>main-cpu</code></td>
<td>Enters the main CPU submode and manually synchronize the configurations on the two supervisor engines.</td>
</tr>
</tbody>
</table>
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

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.

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Usage Guidelines**

The following is a log entry example for mismatched commands:

```
00:06:31: 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 engines 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
This 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).
To force a switchover from the active to the standby supervisor engine, use the `redundancy force-switchover` command.

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Usage Guidelines**

Before using this command, refer to the “Performing a Software Upgrade” section of the Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide for additional information.

The `redundancy force-switchover` command conducts a manual switchover to the redundant supervisor engine. The redundant supervisor engine becomes the new active supervisor engine running the Cisco IOS image. The modules are reset. The old active supervisor engine reboots with the new image and becomes the standby supervisor engine.

**Examples**

This example shows how to switch over manually from the active to the standby supervisor engine:

```
Switch# redundancy force-switchover
Switch#
```

**Related Commands**

- `redundancy`: Enters the redundancy configuration mode.
- `show redundancy`: Displays redundancy facility information.
To force a reload of one or both supervisor engines, use the `redundancy reload` command.

```
redundancy reload {peer | shelf}
```

**Syntax Description**

- **peer**: Reloads the peer unit.
- **shelf**: Reboots both supervisor engines.

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Usage Guidelines**

Before using this command, refer to the "Performing a Software Upgrade" section of the Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide for additional information.

The `redundancy reload shelf` command conducts a reboot of both supervisor engines. The modules are reset.

**Examples**

This example shows how to manually reload one or both supervisor engines:

```
Switch# redundancy reload shelf
Switch#
```

**Related Commands**

- `peer`: Reloads the peer unit.
- `shelf`: Reboots both supervisor engines.
- `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.

**Syntax Description**

- **Defaults**: This command has no default settings.
- **Command Modes**: Privileged EXEC mode
- **Usage Guidelines**: This command applies only to the Access Gateway Module on Catalyst 4500 series switches.
  
  The valid values for `mod` depends on the chassis used. For example, if you have a Catalyst 4506 chassis, valid values for the module are from 2 to 6. If you have a 4507R chassis, valid values are from 3 to 7.

  When you execute the `remote login module` command, the prompt changes to Gateway#.

  The `remote login module` command is identical to the `session module` and the `attach module` commands.

**Examples**

This 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**

- `attach module`: Remotely connects to a specific module.
- `session module`: Logs in to the standby supervisor engine using a virtual console.
To convert a VLAN into an RSPAN VLAN, use the `remote-span` command. To convert an RSPAN VLAN to a VLAN, use the `no` form of this command.

```
remote-span
no remote-span
```

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

RSPAN is disabled.

**Command Modes**

VLAN configuration mode

**Examples**

This example shows how to convert a VLAN into an RSPAN VLAN:

```
Switch# config terminal
Switch(config)# vlan 20
Switch(config-vlan)# remote-span
Switch(config-vlan)# end
Switch# monitor session
```
To renew the DHCP binding database, use the `renew ip dhcp snooping database` command.

**Syntax Description**

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Usage Guidelines**

If the URL is not provided, the switch tries to read the file from the configured URL.

**Examples**

This example shows how to renew the DHCP binding database while bypassing the CRC checks:

```
Switch# renew ip dhcp snooping database validation none
Switch#
```

**Related Commands**

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

### Syntax Description

- **Defaults**: The administrative VLAN is VLAN 1.
- **Command Modes**: Global configuration

### Usage Guidelines

- If the VLAN does not already exist, this command does not create the VLAN.
- To avoid the delay introduced by relaying messages in software for link-failure or VLAN-blocking notification during load balancing, REP floods packets at the hardware flood layer (HFL) to a regular multicast address. These messages are flooded to the whole network, not just the REP segment. Switches that do not belong to the segment treat them as data traffic. Configuring an administrative VLAN for the whole domain can control flooding of these messages.
- If no REP administrative VLAN is configured, the default is VLAN 1.
- There can be only one administrative VLAN on a switch and on a segment.
- The administrative VLAN cannot be the RSPAN VLAN.

### Examples

This example shows how to configure VLAN 100 as the REP administrative VLAN:

```
Switch(config) # rep admin vlan 100
```

You can verify your settings by entering the `show interface rep detail` privileged EXEC command.

### Related Commands

- **Command Description**
  - `show interfaces rep detail` (IOS command): Displays detailed REP configuration and status for all interfaces or the specified interface, including the administrative VLAN.
rep block port

Use the rep block port interface configuration command on the REP primary edge port to configure Resilient Ethernet Protocol (REP) VLAN 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}

Syntax Description

- **id** port-id
  - 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.

- **neighbor_offset**
  - 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.

  - **vlan-list**
    - 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.

Defaults

The default behavior after you enter the rep preempt segment privileged EXEC command (for manual preemption) is to block all VLANs at the primary edge port. This behavior remains until you configure the rep block port command.

If the primary edge port cannot determine which port is to be the alternate port, the default action is no preemption and no VLAN load balancing.

Command Modes

Interface configuration

Usage Guidelines

You must enter this command on the REP primary edge port.

When you select an alternate port by entering an offset number, this number identifies the downstream neighbor port of an edge port. The primary edge port has an offset number of 1; positive numbers above 1 identify downstream neighbors of the primary edge port. Negative numbers identify the secondary edge port (offset number -1) and its downstream neighbors. See Neighbor Offset Numbers in a REP Segment Figure 2-2.
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

This 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: 007F001647FB17800EEE

Switch A
Uplink switch B gi2/0/6 Forwarding (1-50)
Uplink switch C gi2/0/8 Forwarding (51-100)
201398
This 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: 007F001647FB178009C3
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

- `rep preempt delay` Configures a waiting period after a segment port failure and recovery before REP VLAN load balancing is triggered.
- `rep preempt segment` Manually starts REP VLAN load balancing on a segment.
- `show interfaces rep detail` (IOS command) Displays REP detailed configuration and status for all interfaces or the specified interface, including the administrative 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**

**Defaults**
The REP link shuts down if it does not receive a hello message from a neighbor within 5000 ms.

**Command Modes**
Interface configuration

**Usage Guidelines**
The LSL hello timer is set to the age-timer value 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**
This 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**

<table>
<thead>
<tr>
<th>Command Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show interfaces rep [detail]</code> (IOS command)</td>
</tr>
</tbody>
</table>

Displays REP configuration and status for all interfaces or the specified interface, including the configured LSL age-out timer value.
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

Defaults
No preemption delay is set. If you do not enter the rep preempt delay command, the default is manual preemption with no delay.

Command Modes
Interface configuration

Usage Guidelines
You must enter this command on the REP primary edge port.
You must enter this command and configure a preempt time delay if you want VLAN load balancing to automatically trigger after a link failure and recovery.
If VLAN load balancing is configured, after a segment port failure and recovery, the REP primary edge port starts a delay timer before VLAN load balancing occurs. Note that the timer restarts after each link failure. When the timer expires, the REP primary edge alerts the alternate port to perform VLAN load balancing (configured by using the rep block port interface configuration command) and prepares the segment for the new topology. The configured VLAN list is blocked at the alternate port, and all other VLANs are blocked at the primary edge port.
Do not configure VLAN load balancing on an interface that carries Ethernet over multiprotocol label switching (EoMPLS) traffic. VLAN load balancing across the REP ring might cause some of the EoMPLS traffic to not be forwarded.

Examples
This example shows how to configure REP preemption time delay of 100 seconds on the primary edge port:
Switch(config)#
interface gigabitethernet 1/0/1
Switch(config-if)#
rep preempt delay 100
Switch(config-if)#
exit
You can verify your settings by entering the show interfaces rep privileged EXEC command.

Related Commands

rep block port
Configures VLAN load balancing.

show interfaces rep [detail]
Displays REP configuration and status for all interfaces or the specified interface.
Chapter 2    Cisco IOS Commands for the Catalyst 4500 Series Switches

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**

**Defaults**

Manual preemption is the default behavior.

**Command Modes**

Privileged EXEC

**Usage Guidelines**

When you enter the `rep preempt segment segment-id` command, a confirmation message appears before the command is executed because preemption can cause network disruption.

Enter this command on the switch on the segment that has the primary edge port.

If you do not configure VLAN load balancing, entering this command results in the default behavior—the primary edge port blocks all VLANs.

You configure VLAN load balancing by entering the `rep block port {id | port-id | neighbor-offset | preferred} vlan {vlan-list | all}` interface configuration command on the REP primary edge port before you manually start preemption.

There is not a `no` version of this command.

**Examples**

This example shows how to manually trigger REP preemption on segment 100 with the confirmation message:

```
Switch)#
rep preempt segment 100

The command will cause a momentary traffic disruption.

Do you still want to continue? [confirm]
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>rep block port</code></td>
</tr>
<tr>
<td>Configures VLAN load balancing.</td>
</tr>
<tr>
<td><code>show interfaces rep [detail]</code></td>
</tr>
<tr>
<td>(IOS command)</td>
</tr>
<tr>
<td>Displays REP configuration and status for all interfaces or the specified interface.</td>
</tr>
</tbody>
</table>
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 rep segment` form of this command to disable REP on the interface.

### Syntax Description

- **segment-id**
  - Assign a segment ID to the interface. The range is from 1 to 1024.

- **edge**
  - (Optional) Identify the interface as one of the two REP edge ports. Entering the `edge` keyword without the `primary` keyword configures the port as the secondary edge port.

- **no-neighbor**
  - (Optional) Configure a segment edge with no external REP neighbor.

- **primary**
  - (Optional) On 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.

### Defaults
- REP is disabled on the interface.
- When REP is enabled on an interface, the default is for the port to be a regular segment port.

### Command Modes
- Interface configuration

### Usage Guidelines
- REP ports must be Layer 2 trunk ports. A non-ES REP port can be either an IEEE 802.1Q trunk port or an ISL trunk port.
- REP ports should not be configured 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

This example shows how to enable REP on a regular (nonedge) segment port:

```
Switch (config)#
interface gigabitethernet 1/0/1
Switch (config-if)#
rep segment 100
```

This example shows how to enable REP on a port and identify the port as the REP primary edge port:

```
Switch (config)#
interface gigabitethernet 1/1
Switch (config-if)#
rep segment 100 edge primary
```

This example shows how to configure the same configuration when the interface has no external REP neighbor:

```
Switch#
configure terminal
Switch (config)#
interface gigabitethernet 1/1
Switch (config-if)#
rep segment 100 edge no-neighbor primary
```

This example shows how to enable REP on a port and identify the port as the REP secondary edge port:

```
Switch (config)#
interface GigabitEthernet 1/1
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.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rep segment</td>
<td>Displays REP configuration and status for all interfaces or the specified interface.</td>
</tr>
<tr>
<td>show interfaces rep [detail]</td>
<td>Displays information about all ports in the segment, including which one was configured and selected as the primary edge port.</td>
</tr>
</tbody>
</table>
Use the `rep stcn` 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
```

**Defaults**

Transmission of STCNs to other interfaces, segments, or STP networks is disabled.

**Command Modes**

Interface configuration

**Usage Guidelines**

Enter this command on a segment edge port. You use this command to notify other portions of the Layer 2 network of topology changes that occur in the local REP segment. This removes obsolete entries in the Layer 2 forwarding table in other parts of the network, which allows faster network convergence.

**Examples**

This example shows how to configure a REP edge port to send STCNs to segments 25 to 50:

```
Switch (config)#
interface GigabitEthernet1/1
Switch (config-if)#
rep stcn segment 25-50
Switch (config-if)#
exit
```

You can verify your settings by entering the `show interfaces rep detail` privileged EXEC command.

**Related Commands**

`interface`

Identify a physical interface or port channel to receive STCNs.

`segment`

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.

`show interfaces rep [detail]`

Displays REP configuration and status for all interfaces or the specified interface.
Chapter 2      Cisco IOS Commands for  the Catalyst 4500 Series Switches

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.

Defaults

This command has no default settings.

Command Modes

VLAN configuration mode

Examples

This example shows how to reset the proposed new VLAN database to the current VLAN database:

Switch(vlan-config)# reset
RESET completed.
Switch(vlan-config)#
To set the MST configuration revision number, use the `revision` command. To return to the default settings, use the `no` form of this command.

**Syntax Description**

- **Defaults**: Revision version is set to 0.
- **Command Modes**: MST configuration mode

**Usage Guidelines**

If two Catalyst 4500 series switches have the same configuration but have different configuration revision numbers, they are considered to be part of two different regions.

**Caution**

Be careful when using the `revision` command to set the MST configuration revision number because a mistake can put the switch in a different region.

**Examples**

This example shows how to set the configuration revision number:

```
Switch(config-mst)# revision 5
Switch(config-mst)#
```

**Related Commands**

- `version` Configuration revision number; valid values are from 0 to 65535.
- `instance` Maps a VLAN or a set of VLANs to an MST instance.
- `name` Sets the MST region name.
- `show spanning-tree mst` Displays MST protocol information.
- `spanning-tree mst configuration` Enters the MST configuration submode.
service-policy (interface configuration)

To attach a policy map to an interface or to apply different QoS policies on VLANs that an interface belongs to, use the `service-policy` command. To remove a policy map from an interface, use the `no` form of this command.

```
service-policy {input | output} policy-map name
no service-policy {input | output} policy-map name
```

**Syntax Description**
- **input** Specifies the input policy maps.
- **output** Specifies the output policy maps.
- **policy-map name** Name of a previously configured policy map.

**Defaults**
A policy map is not attached to an interface or a VLAN.

**Command Modes**
Interface configuration mode

**Usage Guidelines**
Layer 2 interfaces can be part of multiple VLANs (for example, a typical trunk port). In conjunction with the `vlan-range` command, you can use the `service-policy` command to specify different QoS policies on different VLANs.

**Example**
This 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
```

This example shows how to apply policy map p1 for traffic in VLANs 20 and 400, and policy map p2 for traffic in VLANs 300 through 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
```
This example shows how to attach a policy map to a VLAN using a Supervisor Engine 6-E:
Chapter 2      Cisco IOS Commands for  the Catalyst 4500 Series Switches

service-policy (interface configuration)

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.
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` command. To disable the service policy within a policy map, use the `no` form of this command.

```
service-policy policy-map-name
no service-policy policy-map-name
```

**Syntax Description**

- `policy-map-name`: Name of the policy map.

**Defaults**

No service policies maps are defined.

**Command Modes**

- Policy-map class configuration mode

**Usage Guidelines**

- Use the `service-policy` command only in a hierarchical policy map attached to a physical port. This command is valid in policy maps at level two of the hierarchy.
- You can create a hierarchy by having the parent policy map specify marking and/or policing actions and having the child policy map specify the queueing actions.
- If you enter this command in policy-map class configuration mode, you return to policy-map configuration mode by using the `exit` command. To return to privileged EXEC mode, use the `end` command.

**Examples**

This example shows how to create a hierarchical service policy in the service policy called “parent”:

```
Switch# configure terminal
Switch(config)# policy-map child
Switch(config-pmap)# class voice
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# policy-map parent
Switch(config-pmap)# class class1
Switch(config-pmap-c)# police 32k
Switch(config-pmap-c)# service-policy child
Switch#
```

You can verify your settings by entering the `show policy-map` privileged EXEC command.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bandwidth</td>
<td>Creates a signaling class structure that can be referred to by its name.</td>
</tr>
<tr>
<td>class</td>
<td>Specifies the name of the class whose traffic policy you want to create or change.</td>
</tr>
<tr>
<td>dbl</td>
<td>Enables active queue management on a transmit queue used by a class of traffic.</td>
</tr>
<tr>
<td>policy-map</td>
<td>Creates a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.</td>
</tr>
<tr>
<td>priority</td>
<td>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.</td>
</tr>
<tr>
<td>random-detect</td>
<td>Enables Weighted Random Early Detection (WRED) or distributed WRED.</td>
</tr>
<tr>
<td>shape (class-based queueing)</td>
<td>Enables traffic shaping a class of traffic in a policy map attached to a physical port.</td>
</tr>
<tr>
<td>show policy-map</td>
<td>Displays information about the policy map.</td>
</tr>
</tbody>
</table>
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

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**

- **Defaults**: No service policy is specified.
- **Command Modes**: Control-plane configuration mode

**Usage Guidelines**

In this release, the only policy-map accepted on the control-plane is `system-cpp-policy`. It is already attached to the control-plane at start up. If not (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**

This example shows how to configure trusted hosts with source addresses 10.1.1.1 and 10.1.1.2 to forward Telnet packets to the control plane without constraint, while allowing all remaining Telnet packets to be policed at the specified rate:

```
Switch(config)#
access-list 140 deny tcp host 10.1.1.1 any eq telnet

! 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
```
**Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>service-policy input</td>
<td>Enters control-plane configuration mode.</td>
</tr>
<tr>
<td>control-plane</td>
<td>Applies the control plane policing default template to the switch.</td>
</tr>
<tr>
<td>macro</td>
<td>Creates a policy map that can be attached to multiple ports to specify a</td>
</tr>
<tr>
<td></td>
<td>service policy and to enter policy-map configuration mode.</td>
</tr>
<tr>
<td>show policy-map control</td>
<td>Displays the configuration either of a class or of all classes for the</td>
</tr>
<tr>
<td></td>
<td>policy map of a control plane.</td>
</tr>
</tbody>
</table>
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.

**Syntax Description**

This command has no default settings.

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Usage Guidelines**

Catalyst 4500 series switches can be configured with two supervisor engines to provide redundancy. When the switch is powered, one of the supervisor engines becomes active and remains active until a switchover occurs. The other supervisor engine remains in standby mode.

Each supervisor engine has its own console port. Access to the standby supervisor engine is possible only through the console port of the standby supervisor engine. Therefore, you must connect to the standby console to access, monitor or debug the standby supervisor.

The virtual console for the standby supervisor engine enables you to access the standby console from the active supervisor engine 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` and the `remote login module` 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
```
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
}
```

**Syntax Description**

- `cos new-cos`: New CoS value assigned to the classified traffic. The range is 0 to 7.
- `ip dscp new-dscp`: New DSCP value assigned to the classified traffic. The range is 0 to 63. You can also enter a mnemonic name for a commonly used value. The specified value sets the type of service (ToS) traffic class in the IPv4/IPv6 packet header.
- `ip precedence new-precedence`: New IP-precedence value assigned to the classified traffic. The range is 0 to 7. You can also enter a mnemonic name for a commonly used value. The specified value sets the precedence bit in the IP header.
- `qos group value`: Internal QoS group assigned to a classified packet on ingress to an interface.

**Defaults**

- No marking is enabled on packets.

**Command Modes**

- Policy-map class configuration mode

**Usage Guidelines**

- You can use the `set` command only in class-level classes.
- The `set dscp new-dscp` and the `set precedence new-precedence` commands are the same as the `set ip dscp new-dscp` and the `set ip precedence new-precedence` commands.
- For the `set dscp new-dscp` or the `set precedence new-precedence` command, you can enter a mnemonic name for a commonly used value. For example, you can enter the `set dscp af11` command, which is the same as entering the `set dscp 10` command. You can also enter the `set precedence critical` command, which is the same as entering the `set precedence 5` command. For a list of supported mnemonics, enter the `set dscp ?` or the `set precedence ?` command to see the command-line help strings.
- You can configure the `set cos new-cos`, `set dscp new-dscp`, or `set precedence new-precedence` command in an ingress and an egress policy map attached to an interface or VLAN.
- To return to policy-map configuration mode, use the `exit` command. To return to privileged EXEC mode, use the `end` command.

**Examples**

This example shows how to create a policy map called p1 with CoS values assigned to different traffic types. Class maps for voice and video-data have already been created.

```
Switch# configure terminal
```
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

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

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>class</td>
<td>Specifies the name of the class whose traffic policy you want to create or change.</td>
</tr>
<tr>
<td>policy-map</td>
<td>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.</td>
</tr>
<tr>
<td>show policy-map</td>
<td>Displays information about the policy map.</td>
</tr>
<tr>
<td>trust</td>
<td>Defines a trust state for traffic classified through the class policy-map configuration command.</td>
</tr>
</tbody>
</table>
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]}
```

**Syntax Description**

- **cos-value**: Specific IEEE 802.1Q CoS value from 0 to 7.
- **from-field**: 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:
  - precedence
  - dscp
  - cos
  - qos group
- **table**: (Optional) Indicates that the values set in a specified table map will be used to set the CoS value.
- **table-map-name**: (Optional) Name of the table map used to specify the CoS value. The table map name can be a maximum of 64 alphanumeric characters.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

Note
If you configure the `set cos dscp` command, only the first three bits (the class selector bits) of the DSCP field are used.

Note
If you configure the `set cos qos group` command, only the three least significant bits of the qos group field are used.

Examples
This example shows how to configure a policy map called cos-set and assign different CoS values for different types of traffic. This example assumes that the class maps called voice and video-data have already been created.

Switch#
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#

This example shows how to configure a policy map called policy-cos and to use the values defined in a table map called table-map1. The table map called table-map1 was created earlier with the `table-map (value mapping)` command. For more information about the `table-map (value mapping)` command, see the `table-map (value mapping)` command page.

This example shows how the setting of the CoS value is based on the precedence value defined in table-map1:

Switch#
configure terminal
Switch(config)#
policy-map policy-cos
Switch(config-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.
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.
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]}
```

**Syntax Description**

- **Command Default**: Disabled
- **Command Modes**: Policy-map class configuration mode

**Usage Guidelines**

Once the DSCP bit is set, other quality of service (QoS) features can then operate on the bit settings.

**DSCP and Precedence Values Are Mutually Exclusive**

The `set dscp` command cannot be used with the `set precedence` command to mark the same packet. The two values, DSCP and precedence, are mutually exclusive. A packet can have one value or the other, but not both.

You can use this command to specify the "from-field" packet-marking category to be used for mapping and setting the DSCP value. The "from-field" packet-marking categories are as follows:

- Class of service (CoS)
- QoS group
- DSCP
- Precedence

**ip** *(Optional)* Specifies that the match is for IPv4 packets only. If not used, the match is on both IPv4 and IPv6 packets.

**dscp-value** A number from 0 to 63 that sets the DSCP value. A mnemonic name for commonly used values can also be used.

**from-field** Specific packet-marking category to be used to set the DSCP value of the packet. If you are using a table map for mapping and converting packet-marking values, this establishes the "map from" packet-marking category. Packet-marking category keywords are as follows:

- CoS
- QoS group
- DSCP
- Precedence

**table** *(Optional)* Used in conjunction with the `from-field` argument. Indicates that the values set in a specified table map will be used to set the DSCP value.

**table-map-name** *(Optional)* Used in conjunction with the `table` keyword. Name of the table map used to specify the DSCP value. The name can be a maximum of 64 alphanumeric characters.
Chapter 2  
Cisco IOS Commands for the Catalyst 4500 Series Switches

set dscp

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.

This example shows how the DSCP value is set according to the CoS value defined in the table map called table-map1.

Switch#  
configure terminal  
Switch(config)#  
policy-map policy1  
Switch(config-pmap)#  
class class-default  
Switch(config-pmap-c)#  
set dscp cos table table-map1  
Switch(config-pmap-c)#  
end  
Switch#  


cisco ios commands for the catalyst 4500 series switches

set dscp

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.

This example shows how the DSCP value is set according to the CoS value defined in the table map called table-map1.

Switch#  
configure terminal  
Switch(config)#  
policy-map policy1  
Switch(config-pmap)#  
class class-default  
Switch(config-pmap-c)#  
set dscp cos table table-map1  
Switch(config-pmap-c)#  
end  
Switch#
## Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>set ds cp</code></td>
<td>Sets IP traffic by setting a class of service (CoS).</td>
</tr>
<tr>
<td><code>policy-map</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>service-policy (policy-map class)</code></td>
<td>Creates a service policy that is a quality of service (QoS) policy within a policy map.</td>
</tr>
<tr>
<td><code>set cos</code></td>
<td>Sets the precedence value in the packet header.</td>
</tr>
<tr>
<td><code>set precedence</code></td>
<td>Sets the precedence value in the packet header.</td>
</tr>
<tr>
<td><code>show policy-map</code></td>
<td>Displays information about the policy map.</td>
</tr>
<tr>
<td><code>show policy-map interface</code></td>
<td>Displays the statistics and configurations of the input and output policies that are attached to an interface.</td>
</tr>
<tr>
<td><code>table-map (value mapping)</code></td>
<td>Modifies metric and tag values when the IP routing table is updated with BGP learned routes.</td>
</tr>
</tbody>
</table>
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.

```plaintext
set precedence {
    precedence-value |
    from-field [table table-map-name ]
}
no set precedence {
    precedence-value |
    from-field [table table-map-name ]
}
```

**Syntax Description**

**Command Default**

Disabled

**Command Modes**

Policy-map class configuration mode

**Usage Guidelines Command Compatibility**

The `set precedence` command cannot be used with the `set dscp` command to mark the same packet. The two 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

**precedence-value**

A number from 0 to 7 that sets the precedence bit in the packet header.

**from-field**

Specific packet-marking category to be used to set the precedence value of the packet. If you are using a table map for mapping and converting packet-marking values, this argument value establishes the "map from" packet-marking category. Packet-marking category keywords are as follows:

- cos
- qos-group
- dscp
- precedence

**table**

(Optional) Indicates that the values set in a specified table map will be used to set the precedence value.

**table-map-name**

(Optional) Name of the table map used to specify a precedence value based on the class of service (CoS) value. The name can be a maximum of 64 alphanumeric characters.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

set 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.

This 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#
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

- set precedence
- 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.
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
```

**Syntax Description**

- **group-id**
  - Group ID number in the range from 0 to 63.

**Command Modes**

- Policy-map class configuration mode

**Usage Guidelines**

The `set qos-group` command allows you to associate a group ID with a packet. This association is made through a service-policy attached to an interface or VLAN in the input direction. The group ID can be later used in the output direction to apply QoS service policies to the packet.

**Examples**

This example shows how to set the qos-group 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**

- `group-id`
- `match (class-map configuration)`
- `policy-map`
- `service-policy (policy-map class)`
- `show policy-map`
- `show policy-map interface`
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

shape (class-based queueing)

To enable traffic shaping a class of traffic in a policy map attached to a physical port, use the `shape` command. Traffic shaping limits the data transmission rate. To return to the default setting, use the `no` form of this command.

```
shape average {
  rate } [kbps | mbps | gbps]

shape average percent {
  percent_value}

no shape average
```

**Syntax Description**

- `shape average` specifies an average rate for traffic shaping; the range is 16000 to 10000000000.
- `rate` specifies a rate in bits per seconds.
- `kbps` specifies a rate in kilobytes per seconds.
- `mbps` specifies a rate in megabits per seconds.
- `gbps` specifies a rate in gigabits per seconds.
- `percent` specifies a percentage of bandwidth for traffic shaping.
- `percent_value` specifies a percentage of the bandwidth used for traffic shaping; valid values are from 1 to 100 percent.

**Defaults**

Average-rate traffic shaping is disabled.

**Command Modes**

Policy-map class configuration mode

**Usage Guidelines**

Use the `shape` command only in a policy map attached to a physical port. This command is valid in policy maps at any level of the hierarchy.

Shaping is the process of delaying out-of-profile packets in queues so that they conform to a specified profile. Shaping is distinct from policing. Policing drops packets that exceed a configured threshold, but shaping buffers packets so that traffic remains within the threshold. Shaping offers greater smoothness in handling traffic than policing.

You cannot use the `bandwidth`, `dbl`, and the `shape` policy-map class configuration commands with the `priority` policy-map class configuration command in the same class within the same policy map. However, you can use these commands in the same policy map.

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

**Examples**

This example shows how to limit the specified traffic class to a data transmission rate of 256 kbps:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
```

This example shows how to limit the specified traffic class to a data transmission rate of 256 kbps:

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
  rate 256k

Switch(config-pmap)#
```
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

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

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bandwidth</td>
<td>Creates a signaling class structure that can be referred to by its name.</td>
</tr>
<tr>
<td>class</td>
<td>Specifies the name of the class whose traffic policy you want to create or</td>
</tr>
<tr>
<td></td>
<td>change.</td>
</tr>
<tr>
<td>dbl</td>
<td>Enables active queue management on a transmit queue used by a class of</td>
</tr>
<tr>
<td></td>
<td>traffic.</td>
</tr>
<tr>
<td>policy-map</td>
<td>Creates a policy map that can be attached to multiple ports to specify a</td>
</tr>
<tr>
<td></td>
<td>service policy and to enter policy-map configuration mode.</td>
</tr>
<tr>
<td>service-policy</td>
<td>Creates a service policy that is a quality of service (QoS) policy within</td>
</tr>
<tr>
<td></td>
<td>a policy map.</td>
</tr>
<tr>
<td>show policy-map</td>
<td>Displays information about the policy map.</td>
</tr>
</tbody>
</table>
To specify traffic shaping on an interface, use the `shape` command. To remove traffic shaping, use the `no` form of this command `shape`.

```
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.
```

**Defaults**
Default is no traffic shaping.

**Command Modes**
Interface transmit queue configuration mode

**Usage Guidelines**
Traffic shaping is available on all the ports, and it sets an upper limit on the bandwidth.

Some examples of ports that are connected directly to the backplane are as follows:

- Ports on the WS-X4306-GB module
- The two 1000BASE-X ports on the WS-X4232-GB-RJ module
- The first two ports on the WS-X4418-GB module
- The two 1000BASE-X ports on the WS-X4412-2GB-TX module

All ports on the 24-port modules and the 48-port modules are multiplexed through a Stub ASIC. Some examples of ports multiplexed through a Stub ASIC are as follows:

- 10/100 ports on the WS-X4148-RJ45 module
- 10/100/1000 ports on the WS-X4124-GB-RJ45 module
- 10/100/1000 ports on the WS-X4448-GB-RJ45 module

**Examples**
This example shows how to configure a maximum bandwidth (70 percent) for the interface fa3/1:

```
Switch(config)#
interface fastethernet3/1
Switch(config-if)#
tx-queue 3
Switch(config-if-tx-queue)#
shape 70m
Switch(config-if-tx-queue)#
```
Use the `shell trigger` global configuration command to create a user-defined trigger. Use the `no` form of this command to delete the trigger.

**Syntax Description**

**identifier**
- Specifies the event trigger identifier.
- The identifier should have no spaces or hyphens between words.

**description**
- Specifies the event trigger description text.

**Defaults**

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

**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**

This 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
```
## shell trigger

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>macro auto</td>
<td>Enables Auto Smartports on a switch.</td>
</tr>
<tr>
<td>macro auto processing</td>
<td>Enable Auto SmartPorts macros on a specific interface.</td>
</tr>
<tr>
<td>show shell</td>
<td>Displays information about event triggers and macros.</td>
</tr>
<tr>
<td>macro auto device</td>
<td>Simplifies changing the parameters for a built-in functions for a device type.</td>
</tr>
<tr>
<td>macro auto execute</td>
<td>Changes built-in function default values or to map user-defined triggers to built-in functions, and to pass the parameter values.</td>
</tr>
<tr>
<td>macro auto execute</td>
<td>Maps a trigger to a user-defined function.</td>
</tr>
<tr>
<td>macro auto execute</td>
<td>Maps a trigger to a remotely defined function.</td>
</tr>
<tr>
<td>macro auto processing</td>
<td>Enables Auto SmartPorts macros on a specific interface.</td>
</tr>
<tr>
<td>macro auto sticky</td>
<td>Specifies not to remove configurations applied by ASP across link flaps and device removal.</td>
</tr>
</tbody>
</table>
To display the ACL configuration on a Layer 2 interface, use the `show access-group mode interface` command.

**Syntax Description**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Usage Guidelines**

The valid values for the port number depend on the chassis used.

**Examples**

This example shows how to display the ACL configuration on the Fast Ethernet interface 6/1:

```
Switch# show access-group mode interface fa6/1
Interface FastEthernet6/1:
Access group mode is: merge
Switch#
```

**Related Commands**

`interface` (Optional) Interface type; valid values are `ethernet`, `fastethernet`, `gigabitethernet`, `tengigabitethernet`, and `port-channel`.

`interface-number` (Optional) Interface number.
show adjacency

To display information about the Layer 3 switching adjacency table, use the `show adjacency` command.

```
show adjacency

interface
interface-number
null
port-channel
number
vlan
vlan-id
detail
internal
summary

Syntax Description

Defaults
This command has no default settings.

Command Modes
EXEC

Usage Guidelines
The `interface-number` argument designates the module and port number. Valid values for `interface-number` depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-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.

```

interface
(Optional) Interface type; possible valid values are ethernet, fastethernet, gigabitethernet, tengigabitethernet, pos, ge-wan, and atm.

interface-number
(Optional) Module and port number; see the "Usage Guidelines" section for valid values.

null
interface-number
(Optional) Specifies the null interface; the valid value is 0.

port-channel
number
(Optional) Specifies the channel interface; valid values are a maximum of 64 values ranging from 1 to 256.

vlan
vlan-id
(Optional) Specifies the VLAN; valid values are from 1 to 4094.

detail
(Optional) Displays the information about the protocol detail and timer.

internal
(Optional) Displays the information about the internal data structure.

summary
(Optional) Displays a summary of CEF-adjacency information.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

show adjacency

Examples

This example shows how to display adjacency information:

Switch#
show adjacency

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Interface</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>FastEthernet2/3</td>
<td>172.20.52.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(3045)</td>
</tr>
<tr>
<td>IP</td>
<td>FastEthernet2/3</td>
<td>172.20.52.22</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(11)</td>
</tr>
</tbody>
</table>

Switch#

This example shows how to display a summary of adjacency information:

Switch#
show adjacency summary

Adjacency Table has 2 adjacencies

<table>
<thead>
<tr>
<th>Interface</th>
<th>Adjacency Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>FastEthernet2/3</td>
<td>2</td>
</tr>
</tbody>
</table>

Switch#

This example shows how to display protocol detail and timer information:

Switch#
show adjacency detail

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Interface</th>
<th>Address</th>
<th>Packets</th>
<th>Bytes</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>FastEthernet2/3</td>
<td>172.20.52.1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>ARP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>03:58:12</td>
</tr>
<tr>
<td>IP</td>
<td>FastEthernet2/3</td>
<td>172.20.52.22</td>
<td>0</td>
<td>0</td>
<td>03:58:06</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>ARP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>03:58:06</td>
</tr>
</tbody>
</table>

Switch#

This example shows how to display adjacency information for a specific interface:

Switch#
show adjacency fastethernet2/3

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Interface</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>FastEthernet2/3</td>
<td>172.20.52.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(3045)</td>
</tr>
<tr>
<td>IP</td>
<td>FastEthernet2/3</td>
<td>172.20.52.22</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(11)</td>
</tr>
</tbody>
</table>

Switch#

Related Commands

Command Description

display adjacency
  Displays information about the adjacency debugging.
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` (Optional) Specifies a multicast group address.
- `source` (Optional) Specifies a multicast source address.
- `interface` (Optional) Specifies a multicast flowing on a specific interface.

**Defaults**
Displays all the multicast streams activated with ANCP.

**Command Modes**
Privileged EXEC

**Examples**
This example shows how to display multicast streams activated by ANCP:

```
ANCP-Client# show ancp 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#
```
To display detailed information on an ARP access list, use the `show arp access-list` command.

Syntax Description
This command has no arguments or keywords.

Defaults
This command has no default settings.

Command Modes
EXEC

Examples
This example shows how to display the ARP ACL information for a switch:

```
Switch# show arp access-list
ARP access list 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.
To display the Auth Manager information, use the `show authentication` command in EXEC or Privileged EXEC mode.

```
show authentication

interface
registrations
sessions
    [session-id]
    [handle]
    [interface]
    [mac]
    [method]
    [interface]
    [details]
    [policy]
```

**Syntax Description**

- **Command Default**: This command has no default settings.
- **Command Modes**: EXEC
- **Usage Guidelines**: Table 2-10 describes the significant fields shown in the show authentication display.

**Note**: The possible values for the status of sessions are given below. For a session in terminal state, “Authz Success” or “Authz Failed” are displayed. “No methods” is displayed if no method has provided a result.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

show authentication

Table 2-11 lists the possible values for the state of methods. For a session in terminal state, “Authc Success,” “Authc Failed,” or “Failed over” are displayed (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.

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

Table 2-10 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 2-11 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.
### show authentication

Runnable methods list:

<table>
<thead>
<tr>
<th>Method</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1x</td>
<td>Failed over</td>
</tr>
</tbody>
</table>

### show authentication sessions

The following example shows how to display all Auth Manager sessions on the switch:

```text
Switch# show authentication sessions
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>MAC Address</th>
<th>Method</th>
<th>Domain</th>
<th>Status</th>
<th>Session ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi3/45</td>
<td>(unknown)</td>
<td>N/A</td>
<td>DATA</td>
<td>Authz Failed</td>
<td>0908140400000007003651EC</td>
</tr>
<tr>
<td>Gi3/46</td>
<td>(unknown)</td>
<td>N/A</td>
<td>DATA</td>
<td>Authz Success</td>
<td>09081404000000080057C274</td>
</tr>
</tbody>
</table>

The following example shows how to display all Auth Manager sessions on an interface:

```text
Switch# show authentication sessions int gi 3/46
```

<table>
<thead>
<tr>
<th>Interface: GigabitEthernet3/46</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address: Unknown</td>
</tr>
<tr>
<td>IP Address: Unknown</td>
</tr>
<tr>
<td>Status: Authz Success</td>
</tr>
<tr>
<td>Domain: DATA</td>
</tr>
<tr>
<td>Oper host mode: multi-host</td>
</tr>
<tr>
<td>Oper control dir: both</td>
</tr>
<tr>
<td>Authorized By: Guest Vlan</td>
</tr>
<tr>
<td>Vlan Policy: 4094</td>
</tr>
<tr>
<td>Session timeout: N/A</td>
</tr>
<tr>
<td>Idle timeout: N/A</td>
</tr>
<tr>
<td>Common Session ID: 09081404000000080057C274</td>
</tr>
<tr>
<td>Acct Session ID: 0x0000000A</td>
</tr>
<tr>
<td>Handle: 0xCC000008</td>
</tr>
</tbody>
</table>

### show authentication sessions mac

The following example shows how to display Auth Manager session for a specified MAC address:

```text
Switch# show authentication sessions mac 000e.84af.59bd
```

<table>
<thead>
<tr>
<th>Interface: GigabitEthernet1/23</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address: 000e.84af.59bd</td>
</tr>
<tr>
<td>Status: Authz Success</td>
</tr>
<tr>
<td>Domain: DATA</td>
</tr>
<tr>
<td>Oper host mode: single-host</td>
</tr>
<tr>
<td>Authorized By: Authentication Server</td>
</tr>
<tr>
<td>Vlan Policy: 10</td>
</tr>
<tr>
<td>Handle: 0xE0000000</td>
</tr>
</tbody>
</table>

Runnable methods list:

<table>
<thead>
<tr>
<th>Method</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1x</td>
<td>Authc Success</td>
</tr>
</tbody>
</table>

### show authentication sessions method

The following example shows how to display all clients authorized via a specified auth method:

```text
Switch# show authentication sessions method mab
```

No Auth Manager contexts match supplied criteria

```
Switch# show authentication sessions method dot1x
```

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>Domain</th>
<th>Status</th>
<th>Handle</th>
</tr>
</thead>
<tbody>
<tr>
<td>000e.84af.59bd</td>
<td>DATA</td>
<td>Authz Success</td>
<td>0xE0000000</td>
</tr>
</tbody>
</table>

### show authentication sessions interface

The following example displays the policies applied on interface e0/0:

```text
AUTH# show authentication sessions interface e0/0 policy
```

<table>
<thead>
<tr>
<th>Interface: Ethernet0/0</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address: aabb.cc01.ff00</td>
</tr>
</tbody>
</table>
# Chapter 2  Cisco IOS Commands for the Catalyst 4500 Series Switches

show authentication

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:

<table>
<thead>
<tr>
<th>Method</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1x</td>
<td>Authc Success</td>
</tr>
</tbody>
</table>

## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authentication</td>
<td></td>
</tr>
<tr>
<td>control-direction</td>
<td>Changes the port control to unidirectional or bidirectional.</td>
</tr>
<tr>
<td>authentication critical</td>
<td>Configures the 802.1X critical authentication parameters.</td>
</tr>
<tr>
<td>authentication event</td>
<td>Configures the actions for authentication events.</td>
</tr>
<tr>
<td>authentication fallback</td>
<td>Enables the Webauth fallback and specifies the fallback profile to use when failing over to Webauth.</td>
</tr>
<tr>
<td>authentication host-mode</td>
<td>Defines the classification of a session that will be used to apply the access-policies using the host-mode configuration.</td>
</tr>
<tr>
<td>authentication open</td>
<td>Enables open access on this port.</td>
</tr>
<tr>
<td>authentication order</td>
<td>Specifies the order in which authentication methods should be attempted for a client on an interface.</td>
</tr>
</tbody>
</table>
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

show authentication

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.
To display the status of an automatic installation, use the `show auto install status` command.

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Examples**

This example shows how to display the IP address of the TFTP server and to display whether or not the switch is currently acquiring the configuration file on the TFTP server:

```
Switch# show auto install status
Status              : Downloading config file
DHCP Server         : 20.0.0.1
TFTP Server         : 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.
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**

- **Command Modes**: Privileged EXEC mode
- **Usage Guidelines**:
  - The `show auto qos interface interface-id` command displays the auto-QoS configuration; it does not display any user changes to the configuration that might be in effect.
  - To display information about the QoS configuration that might be affected by auto-QoS, use one of these commands:
    - `show qos`
    - `show qos map`
    - `show qos interface interface-id`
    - `show running-config`
  - Expressions are case sensitive. For example, if you enter `exclude output`, the lines that contain `output` do not appear, but the lines that contain `Output` appear.

**Examples**

This example shows output from the `show auto qos` command when auto-QoS is enabled:

```
Switch# show auto qos
GigabitEthernet1/2
auto qos voip cisco-phone
Switch#
```

**Related Commands**

- `interface interface-id` (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.
- `expression` (Optional) Expression in the output to use as a reference point.
To display information about the bootflash: file system, use the `show bootflash:` command.

Syntax Description

This command has no default settings.

Command Modes

EXEC

Examples

This example shows how to display file system status information:

```
Switch> show bootflash: filesys
-------- F I L E   S Y S T E M   S T A T U S --------
Device Number = 0
DEVICE INFO 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>
```

This example shows how to display system image information:

```
Switch> show bootflash:
---#--- ---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>
```

all

(Optional) Displays all possible Flash information.

chips

(Optional) Displays Flash chip information.

filesys

(Optional) Displays file system information.
Chapter 2      Cisco IOS Commands for  the Catalyst 4500 Series Switches

show bootflash:

This 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>
```
To display BOOT environment variable information, use the `show bootvar` command.

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Examples**

This example shows how to display BOOT environment variable information:

```
Switch# show bootvar
BOOT variable = sup:1;
CONFIG_FILE variable does not exist
BOOTLDR variable does not exist
Configuration register is 0x0
Switch#
```
To display the test results for the TDR cable diagnostics, use the `show cable-diagnostics tdr` command.

```plaintext
show cable-diagnostics tdr
```

**Syntax Description**

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Usage Guidelines**

The TDR test is supported for the following line cards only:

- WS-X4548-GB-RJ45
- WS-X4548-GB-RJ45V
- WS-X4524-GB-RJ45V
- WS-X4013+TS
- WS-C4948
- WS-C4948-10GE

The distance to the fault is displayed in meters (m).

**Examples**

This example shows how to display information about the TDR test:

```
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 2-12 describes the fields in the `show cable-diagnostics tdr` command output.

**interface**

Interface type; valid values are `fastethernet` and `gigabitethernet`.

**interface-number**

Module and port number.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

show cable-diagnostics tdr

Related Commands

Table 2-12 show cable-diagnostics tdr Command Output Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Interface tested.</td>
</tr>
<tr>
<td>Speed</td>
<td>Current line speed.</td>
</tr>
<tr>
<td>Pair</td>
<td>Local pair name.</td>
</tr>
<tr>
<td>Cable Length</td>
<td>Distance to the fault in meters (m).</td>
</tr>
<tr>
<td>Channel</td>
<td>Pair designation (A, B, C, or D).</td>
</tr>
<tr>
<td>Status</td>
<td>Pair status displayed is one of the following:</td>
</tr>
<tr>
<td></td>
<td>Terminated—The link is up.</td>
</tr>
<tr>
<td></td>
<td>Fault—Cable fault (open or short)</td>
</tr>
</tbody>
</table>

Command Description

test cable-diagnostics tdr
Tests the condition of copper cables on 48-port 10/100/1000 BASE-T modules.
To display the configured CallHome information, use the `show call-home` command in privileged EXEC mode.

```
show call-home
```

**Syntax Description**

This command has no default settings.

**Command Modes**

Privileged EXEC (privileged EXEC)

**Examples**

The following example displays the configured CallHome settings:

```
Switch# show call-home
Current call home settings:
call home feature : disable
call home 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
```

- **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.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

show call-home
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
show call-home

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
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

show call-home

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

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
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

show call-home

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 Rate
-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.
Chapter 2     Cisco IOS Commands for the Catalyst 4500 Series Switches

**show cdp neighbors**

To display detailed information about the neighboring devices that are discovered through CDP, use the `show cdp neighbors` command.

**Syntax Description**

- **Syntax:**
  ```
  show cdp neighbors
  [type number] [detail]
  ```

- **Defaults:**
  This command has no default settings.

- **Command Modes:**
  Privileged EXEC mode

- **Usage Guidelines:**
  The `vlan` keyword is supported in Catalyst 4500 series switches that are configured with a Supervisor Engine 2.
  The `port-channel` values are from 0 to 282; values from 257 to 282 are supported on the CSM and the FWSM only.

- **Examples**
  This example shows how to display the information about the CDP neighbors:
  ```
  Switch#
  show cdp neighbors
  Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
  Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
  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-telco Fas 0/0
  008024 2758E0    Eth 0              132          T        CAT3000   1/2
  Switch#
  ```

- **type** (Optional) Interface type that is connected to the neighbors about which you want information; possible valid values are `ethernet`, `fastethernet`, `gigabitethernet`, `tengigabitethernet`, `port-channel`, and `vlan`.
- **number** (Optional) Interface number that is connected to the neighbors about which you want information.
- **detail** (Optional) Displays detailed information about a neighbor (or neighbors) including network address, enabled protocols, hold time, and software version.
Table 2-13 describes the fields that are shown in the example.

This example shows how to display detailed information about your CDP neighbors:

Switch# show cdp neighbors detail

<table>
<thead>
<tr>
<th>Device ID</th>
<th>Configured ID (name), MAC address, or serial number of the neighbor</th>
</tr>
</thead>
<tbody>
<tr>
<td>lab-7206</td>
<td></td>
</tr>
<tr>
<td>Entry address(es): IP address: 172.19.169.83</td>
<td></td>
</tr>
<tr>
<td>Platform: cisco 7206VXR, Capabilities: Router</td>
<td></td>
</tr>
<tr>
<td>Interface: Ethernet0, Port ID (outgoing port): FastEthernet0/0/0</td>
<td></td>
</tr>
<tr>
<td>Holdtime: 123 sec</td>
<td></td>
</tr>
<tr>
<td>Version: Cisco Internetwork Operating System Software</td>
<td></td>
</tr>
<tr>
<td>IOS (tm) 5800 Software (C5800-P4-M), Version 12.1(2)</td>
<td></td>
</tr>
<tr>
<td>Copyright (c) 1986-2002 by Cisco Systems, Inc.</td>
<td></td>
</tr>
<tr>
<td>advertisement version: 2</td>
<td></td>
</tr>
<tr>
<td>Duplex: half</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Device ID</th>
<th>Configured ID (name), MAC address, or serial number of the neighbor</th>
</tr>
</thead>
<tbody>
<tr>
<td>lab-as5300-1</td>
<td></td>
</tr>
<tr>
<td>Entry address(es): IP address: 172.19.169.87</td>
<td></td>
</tr>
</tbody>
</table>

Table 2-13 show cdp neighbors Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device ID</td>
<td>Configured ID (name), MAC address, or serial number of the neighbor</td>
</tr>
<tr>
<td>Local Interface</td>
<td>The protocol that is used by the connectivity media.</td>
</tr>
<tr>
<td>Holdtime</td>
<td>Remaining amount of time, in seconds, that the current device holds the</td>
</tr>
<tr>
<td></td>
<td>CDP advertisement from a transmitting router before discarding it.</td>
</tr>
<tr>
<td>Capability</td>
<td>Capability code that is discovered on the device. Possible values are as</td>
</tr>
<tr>
<td></td>
<td>follows: R—Router, T—Transparent bridge, B—Source-routing bridge, S—</td>
</tr>
<tr>
<td></td>
<td>Switch, H—Host, I—IGMP device, r—Repeater, P—Phone</td>
</tr>
<tr>
<td>Platform</td>
<td>Product number of the device.</td>
</tr>
<tr>
<td>Port ID</td>
<td>Protocol and port number of the device.</td>
</tr>
</tbody>
</table>
Table 2-14 describes the fields that are shown in the example.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show cdp</td>
<td>Displays global CDP information, including timer and hold-time information.</td>
</tr>
<tr>
<td>show cdp entry</td>
<td>Displays information about a specific neighboring device discovered using CDP.</td>
</tr>
<tr>
<td>show cdp interface</td>
<td>Displays information about the interfaces on which CDP is enabled.</td>
</tr>
<tr>
<td>show cdp traffic</td>
<td>Displays traffic information from the CDP table.</td>
</tr>
</tbody>
</table>
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

show class-map

To display class map information, use the show class-map command.

```
show class-map class_name
```

**Syntax Description**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Examples**

This example shows how to display class map information for all class maps:

```
Switch# show class-map
Class Map match-any class-default (id 0)
Class Map match-any class-simple (id 2)
Class Map match-all ipp5 (id 1)
Switch#
```

This example shows how to display class map information for a specific class map:

```
Switch# show class-map ipp5
Class Map match-all ipp5 (id 1)
Switch#
```

Assume there are two active flows as shown below on Fast Ethernet interface 6/1:

<table>
<thead>
<tr>
<th>SrcIp</th>
<th>DstIp</th>
<th>IpProt</th>
<th>SrcL4Port</th>
<th>DstL4Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.10.10</td>
<td>192.168.20.20</td>
<td>20</td>
<td>6789</td>
<td>81</td>
</tr>
<tr>
<td>192.168.10.10</td>
<td>192.168.20.20</td>
<td>20</td>
<td>6789</td>
<td>21</td>
</tr>
</tbody>
</table>

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 l4 source-port l4 destination-port
Switch(config-cmap)# exit
Switch(config)# policy-map p1
Switch(config-pmap)# class c1
```

```
[290x375]OL_2 87 38 -01
[318x374]Catalyst 4500 Series Switch Cisco IOS Command Reference—Release IOS XE 3.3.0XO(15.1(1)XO)
[291x417]Chapter 2      Cisco IOS Commands for  the Catalyst 4500 Series Switches
[290x414]show class-map
[290x411]show class-map
[295x410]To display class map information, use the
[306x410]show class-map
[306x407]command.
[297x410]show class-map
[297x408]class_name
[290x405]Syntax Description
[290x403]This command has no default settings.
[290x401]Command Modes
[290x401]Privileged EXEC mode
[290x398]Examples
[290x397]This example shows how to display class map information for all class maps:
[295x396]Switch#
[298x396]show class-map
[295x394]Class Map match-any class-default (id 0)
[295x396]Match any
[295x395]Class Map match-any class-simple (id 2)
[295x393]Match any
[295x392]Class Map match-all ipp5 (id 1)
[295x391]Switch#
[295x390]This example shows how to display class map information for a specific class map:
[295x388]Switch#
[298x388]show class-map ipp5
[295x386]Class Map match-all ipp5 (id 1)
[295x385]Match ip precedence 5
[295x384]Switch#
[295x383]Assume there are two active flows as shown below on Fast Ethernet interface 6/1:
[295x382]SrcIp          DstIp          IpProt SrcL4Port DstL4Port
[295x381]--------------------------------------------------------
[295x381]192.168.10.10  192.168.20.20  20     6789       81
[295x380]192.168.10.10  192.168.20.20  20     6789       21
[295x379]With following configuration, each flow will be policed to a 1000000 bps with an allowed 9000-byte burst value.
[293x377]Note
[0x0]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.
[295x376]Switch#
[298x375]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 l4 source-port l4 destination-port
Switch(config-cmap)# exit
Switch(config)# policy-map p1
Switch(config-pmap)# class c1
```
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

show class-map
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 l4 source-port l4 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 l4 source-port l4 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.
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
```

**Syntax Description**

This command has no default settings.

**Command Modes**

EXEC

**Examples**

This 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

all
Displays all the modules on the chassis.
num
Module number.
## Chapter 2: Cisco IOS Commands for the Catalyst 4500 Series Switches

### `show diagnostic content`

<table>
<thead>
<tr>
<th>ID</th>
<th>Test Name</th>
<th>Attributes</th>
<th>(day hh:mm:ss.ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1)</td>
<td>linecard-online-diag</td>
<td><strong>D</strong> not configured</td>
<td></td>
</tr>
</tbody>
</table>

Switch#  

- **Related Commands**
  - `show diagnostic result module`
    - Displays the module-based diagnostic test results.
  - `test 2`
    - Displays the results of the bootup packet memory test.
  - `test 3`
    - Displays the results from the ongoing packet memory test.
To display the module-based diagnostic test results, use the `show diagnostic result module` command.

```
show diagnostic result module
```

**Syntax Description**

- `slot-num` (Optional) Specifies the slot on which diagnostics are displayed.
- `all` (Optional) Displays the diagnostics for all slots.
- `test` (Optional) Displays selected tests on the specified module.
- `test-id` (Optional) Specifies a single test ID.
- `test-id-range` (Optional) Specifies a range of test IDs.
- `all` (Optional) Displays the diagnostics for all tests.
- `detail` (Optional) Displays the complete test results.

**Defaults**

A summary of the test results for all modules in the chassis is displayed.

**Command Modes**

Privileged EXEC mode

**Examples**

This example shows how to display the summary results for all modules in the chassis:

```
Switch# show diagnostic result module
Current bootup diagnostic level: minimal
module 1:
Overall diagnostic result: PASS
Diagnostic level at card bootup: bypass
Test results: (. = Pass, F = Fail, U = Untested)
  1) supervisor-bootup -----------------------> U
  2) packet-memory-bootup --------------------> U
  3) packet-memory-ongoing -------------------> U

module 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
```
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

show diagnostic result module

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 --------------------> .
This example shows how to display the online diagnostics for module 1:

Switch#
show diagnostic result module 1 detail

Current bootup diagnostic level: minimal
module 1:
Overall diagnostic result: PASS
Diagnostic level at card bootup: minimal

Error code --------------------------> 0 (DIAG_SUCCESS)
Total run count --------------------> 0
Last test execution time ------------> n/a
First 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: .
Port Traffic: L2 Asic Loopback ...
0: .  1: .  2: .  3: .  4: .  5: .  6: .  7: .  8: .  9: . 10: . 11: .
Port Traffic: L3 Asic Loopback ...
0: .  1: .  2: .  3: .  4: .  5: .  6: .  7: .  8: .  9: . 10: . 11: .
Chapter 2      Cisco IOS Commands for  the Catalyst 4500 Series Switches

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
show diagnostic result module

Per hour in the last day:

Per day in the last 30 days:

Direct memory test failures per minute in the last hour:

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:
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.

**Syntax Description**

- `show diagnostic result module [N | all] [test test-id] detail`

**Defaults**

Non-detailed results.

**Command Modes**

EXEC mode

**Usage Guidelines**

The `detail` keyword is intended for use by Cisco support personnel when analyzing failures.

**Examples**

This example shows how to display the results of the bootup packet memory tests:

```
Switch# show diagnostic result module 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
```

This option is recommended.
### Chapter 2: Cisco IOS Commands for the Catalyst 4500 Series Switches

#### show diagnostic result module test

<table>
<thead>
<tr>
<th>Slot</th>
<th>Ports</th>
<th>Card Type</th>
<th>Diag Status</th>
<th>Diag Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>48</td>
<td>10/100/1000BaseT (RJ45)V, Cisco/IEEE</td>
<td>Passed</td>
<td>None</td>
</tr>
</tbody>
</table>

**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 | 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 |
|-------|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| .    |   |   | . |   | . |   |   | . |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |   |
| Ports | 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| . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . |
| .    |   |   | . |   | . |   |   | . |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |   |
| Ports | 33| 34| 35| 36| 37| 38| 39| 40| 41| 42| 43| 44| 45| 46| 47| 48| . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . |

---

2) online-diag-tdr:

| Ports | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 |
|-------|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|-------|
| .    |   |   | . |   | . |   |   | . |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |   |
| Ports | 25| 26| 27| 28| 29| 30| 31| 32| 33| 34| 35| 36| 37| 38| 39| 40| 41| 42| 43| 44| 45| 46| 47| 48| . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . |
| .    |   |   | . |   | . |   |   | . |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |   |
| Ports | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . | . |

---

**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

---

### Related Commands

- **diagnostic start**
  - Runs the specified diagnostic test.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

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.

**Syntax Description**

- `detail` (Optional) Specifies the display of detailed information for analysis.

**Defaults**

Non-detailed results.

**Command Modes**

EXEC mode

**Usage Guidelines**

The `detail` keyword is intended for use by Cisco support personnel when analyzing failures.

**Examples**

This example shows how to display the results of the bootup packet memory tests:

```
Switch# show diagnostic result module 1 test 2
Test results: (. = Pass, F = Fail, U = Untested)
2) packet-memory-bootup ------------> .
```

This example shows how to display detailed results from the bootup packet memory tests:

```
Switch# show diagnostic result module 2 test 2 detail
Test results: (. = Pass, F = Fail, U = Untested)
___________________________________________________________________________
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
```
show diagnostic result module test 2
bad buffers: 0 (0.0%)
good buffers: 65536 (100.0%)
Bootup test results:
No errors.

Related Commands
- diagnostic monitor action
directs the action of the switch when it detects a packet memory failure.
- show diagnostic result module
displays the results from the ongoing packet memory test.
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.

**Syntax Description**

- Module number.
- `detail` (Optional) Specifies the display of detailed information for analysis.

**Defaults**

- Non-detailed results.

**Command Modes**

- EXEC mode

**Usage Guidelines**

The `detail` keyword is intended for use by Cisco support personnel when analyzing failures.

**Examples**

This example shows how to display the results from the ongoing packet memory tests:

```
Switch# show diagnostic result module 1 test 3
Test results: (. = Pass, F = Fail, U = Untested)
3) packet-memory-ongoing -----------> .
```

This example shows how to display the detailed results from the ongoing packet memory tests:

```
Switch# show diagnostic result module 1 test 3 detail
Test results: (. = Pass, F = Fail, U = Untested)
___________________________________________________________________________
3) packet-memory-ongoing -----------> .
Error code ------------------> 0 (DIAG_SUCCESS)
Total 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
```

This example shows how to display the results from the ongoing packet memory tests with detailed information:

```
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
```

**Module number.**

- Module number.

**detail** (Optional) Specifies the display of detailed information for analysis.
show diagnostic result module test 3

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
0 0 0 0 0 0 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
0 0 0 0 0 0 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
First 1000 Packet Memory errors:
Related Commands
Command Description
di agnostic 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.
To display the 802.1X statistics and operational status for the entire switch or for a specified interface, use the `show dot1x` command.

```
show dot1x [interface interface-id] | [statistics [interface interface-id]] | [all]
```

**Syntax Description**
- `interface interface-id` (Optional) Displays the 802.1X status for the specified port.
- `statistics` (Optional) Displays 802.1X statistics for the switch or the specified interface.
- `all` (Optional) Displays per-interface 802.1X configuration information for all interfaces with a nondefault 802.1X configuration.

**Defaults**
This command has no default settings.

**Command Modes**
Privileged EXEC mode

**Command History**
- **12.1(12c)EW** Support for this command was introduced on the Catalyst 4500 series switch.
- **12.1(19)EW** Display enhanced to show the guest-VLAN value.
- **12.2(25)EW** Support for the 10-Gigabit Ethernet interface was introduced on the Catalyst 4500 series switch.
- **12.2(25)EWA** Support for currently assigned reauthentication timer (if the timer is configured 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.
Chapter 2 Cisco IOS Commands for the Catalyst 4500 Series Switches

show dot1x

Examples

This 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#

This 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             = 30
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 2-15 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.
This is an example of output from the `show dot1x` command.

Table 2-16 describes the fields in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PortStatus</td>
<td>Status of the port (authorized or unauthorized). The status of a port is displayed as authorized if the <code>dot1x port-control</code> command is set to <code>auto</code> and has successfully completed authentication.</td>
</tr>
<tr>
<td>Port Control</td>
<td>Setting of the <code>dot1x port-control</code> interface configuration command.</td>
</tr>
<tr>
<td>MultiHosts</td>
<td>Setting of the <code>dot1x multiple-hosts</code> interface configuration command (allowed or disallowed).</td>
</tr>
</tbody>
</table>

Table 2-16 show dot1x statistics Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TxReq/TxReqId</td>
<td>Number of EAP-request/identity frames that have been sent.</td>
</tr>
<tr>
<td>TxTotal</td>
<td>Number of EAPOL frames of any type that have been sent.</td>
</tr>
<tr>
<td>RxStart</td>
<td>Number of valid EAPOL-start frames that have been received.</td>
</tr>
<tr>
<td>RxLogoff</td>
<td>Number of EAPOL-logoff frames that have been received.</td>
</tr>
<tr>
<td>RxRespId</td>
<td>Number of EAP-response/identity frames that have been received.</td>
</tr>
<tr>
<td>RxResp</td>
<td>Number of valid EAP-response frames (other than response/identity frames) that have been received.</td>
</tr>
<tr>
<td>RxInvalid</td>
<td>Number of EAPOL frames that have been received and have an unrecognized frame type.</td>
</tr>
<tr>
<td>RxLenError</td>
<td>Number of EAPOL frames that have been received in which the packet body length field is invalid.</td>
</tr>
<tr>
<td>RxTotal</td>
<td>Number of valid EAPOL frames of any type that have been received.</td>
</tr>
<tr>
<td>RxVersion</td>
<td>Protocol version number carried in the most recently received EAPOL frame.</td>
</tr>
<tr>
<td>LastRxSrcMac</td>
<td>Source MAC address carried in the most recently received EAPOL frame.</td>
</tr>
</tbody>
</table>
## Chapter 2  Cisco IOS Commands for the Catalyst 4500 Series Switches

### show dot1x

<table>
<thead>
<tr>
<th>Command Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dot1x critical</code></td>
</tr>
<tr>
<td><code>dot1x critical eapol</code></td>
</tr>
<tr>
<td><code>dot1x critical vlan</code></td>
</tr>
<tr>
<td><code>dot1x max-reauth-req</code></td>
</tr>
<tr>
<td><code>dot1x port-control</code></td>
</tr>
<tr>
<td><code>mac-address-table notification</code></td>
</tr>
</tbody>
</table>
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

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

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

Examples

This example shows how to display information about the environment alarms, operational status, and current temperature readings for the chassis:

```
Switch# show environment
no temperature alarms
Module Sensor                     Temperature          Status
------  --------------------------+--------------------+------------
1       Air inlet                  38C (56C,68C,71C)              ok
1       Air inlet remote           32C (46C,59C,62C)              ok
1       Air outlet                 44C (66C,76C,79C)              ok
1       Air outlet remote          37C (60C,71C,74C)              ok
3       XPP                        60C (85C,90C,95C)              ok
3       IFE                        38C (85C,90C,95C)              ok
3       CONAN                      48C (85C,90C,95C)              ok
3       CPU                        50C (85C,90C,95C)              ok
4       XPP                        76C (85C,90C,95C)              ok
4       IFE                        44C (85C,90C,95C)              ok
4       CONAN                      53C (85C,90C,95C)              ok
4       CPU                        53C (85C,90C,95C)              ok
7       Air inlet                  32C (45C,60C,70C)              ok
7       Air outlet                 37C (61C,76C,86C)              ok
```

Power supplies needed by system    : 1

```
Power                                             Fan      Inline
------  ----------------  ---------  -----------  -------  -------
PS1     PWR-C45-1300ACV   AC 1300W   good         good     good
PS2     none              -- --      --           --       --
```

Power supplies needed by system    : 1
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

show environment

Power supplies currently available : 1
Chassis Type : WS-C4507R+E
Power consumed by backplane : 40 Watts
Switch Bandwidth Utilization : 0%
Supervisor Led Color : Green
Module  1 Status Led Color  : Green           PoE Led Color : Green
Module  3 Status Led Color  : Orange
Module  4 Status Led Color  : Green
Module  7 Status Led Color  : Green           PoE Led Color : Green
Beacon Led Status : off
Fantray : Good
Fantray removal timeout : 30
Power consumed by Fantray : 135 Watts

This example shows how to display information about the environment alarms:
Switch#
show environment alarm
no alarm
Switch#

This example shows how to display information about the power supplies, chassis type, and fan trays:
Switch#
show environment status

Power                                            Fan
Supply  Model No         Type       Status       Sensor
------  ---------------  ---------  -----------  ------
PS1     PWR-C45-1400AC   AC 1400W   good         good
PS2     none             --         --           --

Power Supply    Max     Min     Max     Min     Absolute
---------------  ------  ------  ------  ------  --------
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#

This example shows how to display information about the chassis:
Switch#
show environment status chassis

Chassis Type : WS-C4507R
Switch#

This example shows how to display information about the fan tray:
Switch#
show environment status fantray
### Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

**show environment**

Fantray: good  
Power consumed by Fantray: 50 Watts  

This example shows how to display information about the power supply:

```
Switch# show environment status powersupply

Power                                      Fan
Supply  Model No  Type       Status   Sensor
------  ---------------  ---------  -------  -----
PS1     WS-X4008     AC 400W    good     good
PS2     WS-X4008     AC 400W    good     good
PS3     none         --         --       --
```

This example shows how to display information about the supervisor engine:

```
Switch# show environment status supervisor

Supervisor Led Color: Green
```

This example shows how to display information about the temperature of the chassis:

```
Switch# show environment temperature

Module Sensor                     Temperature          Status
------+--------------------------+--------------------+------------
1      Air inlet                  38C (56C,68C,71C)              ok
1      Air inlet remote           32C (46C,59C,62C)              ok
1      Air outlet                 44C (66C,76C,79C)              ok
1      Air outlet remote          37C (60C,71C,74C)              ok
3      XPP                        60C (85C,90C,95C)              ok
3      IFE                        38C (85C,90C,95C)              ok
3      CONAN                      48C (85C,90C,95C)              ok
3      CPU                        50C (85C,90C,95C)              ok
4      XPP                        76C (85C,90C,95C)              ok
4      IFE                        44C (85C,90C,95C)              ok
4      CONAN                      53C (85C,90C,95C)              ok
4      CPU                        53C (85C,90C,95C)              ok
7      Air inlet                  32C (45C,60C,70C)              ok
7      Air outlet                 37C (61C,76C,86C)              ok
```

Switch#
To display the error disable detection status, use the `show errdisable detect` command.

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Examples**

This example shows how to display the error disable detection status:

```
Switch# show errdisable detect
ErrDisable Reason    Detection status
-----------------    ----------------
udld                 Enabled
bpduguard            Enabled
security-violation   Enabled
channel-misconfig    Disabled
psecure-violation    Enabled
vmps                 Enabled
pagp-flap            Enabled
dtp-flap             Enabled
link-flap            Enabled
l2ptguard            Enabled
gbic-invalid         Enabled
dhcp-rate-limit      Enabled
unicast-flood        Enabled
storm-control        Enabled
ilpower              Enabled
arp-inspection       Enabled
Switch#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>errdisable detect</code></td>
<td>Enables error-disable detection.</td>
</tr>
<tr>
<td><code>errdisable recovery</code></td>
<td>Configures the recovery mechanism variables.</td>
</tr>
<tr>
<td><code>show interfaces status</code></td>
<td>Displays the interface status or a list of interfaces in error-disabled state.</td>
</tr>
</tbody>
</table>
show errdisable recovery

To display error disable recovery timer information, use the show errdisable recovery command.

Syntax Description
This command has no arguments or keywords.

Defaults
This command has no default settings.

Command Modes
Privileged EXEC mode

Examples
This example shows how to display recovery timer information for error disable:

Switch# show errdisable recovery

ErrDisable Reason    Timer Status
-----------------    --------------
udld                 Disabled
bpduguard            Disabled
security-violation   Disabled
channel-misconfig    Disabled
vmps                 Disabled
pagp-flap            Disabled
dtp-flap             Disabled
link-flap            Disabled
l2ptguard            Disabled
psecure-violation    Disabled
gbic-invalid         Disabled
dhcp-rate-limit       Disabled
unicast-flood        Disabled
storm-control        Disabled
arp-inspection       Disabled

Timer interval: 30 seconds

Interfaces that will be enabled at the next timeout:

Interface    Errdisable reason    Time left(sec)
---------    -----------------    -------------
Fa7/32       arp-inspect           13

Related Commands

Command Description
errdisable detect
Enables error-disable detection.
errdisable recovery
Configures the recovery mechanism variables.
show interfaces status
Displays the interface status or a list of interfaces in error-disabled state.
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**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Usage Guidelines**

If you do not specify a channel group, all channel groups are displayed.

In the output below, the Passive port list field is displayed for Layer 3 port channels only. This field means that the physical interface, which is still not up, is configured to be in the channel group (and indirectly is in the only port channel in the channel group).

**Examples**

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

```
Switch# show etherchannel 1 port-channel
Port-channels in the group:
----------------------
Port-channel: Po1
----------------------
Age of the Port-channel   = 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
-------------------
```

This example shows how to display load-balancing information:

```
Switch# show etherchannel load-balance
```

- **channel-group** (Optional) Number of the channel group; valid values are from 1 to 64.
- **port-channel** Displays port-channel information.
- **brief** Displays a summary of EtherChannel information.
- **detail** Displays detailed EtherChannel information.
- **summary** Displays a one-line summary per channel group.
- **port** Displays EtherChannel port information.
- **load-balance** Displays load-balance information.
- **protocol** Displays the enabled protocol.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

show etherchannel

Source XOR Destination mac address

Switch#

This example shows how to display a summary of information for a specific group:

Switch#

show etherchannel 1 brief

Group state = L3
Ports: 2   Maxports = 8
port-channels: 1 Max port-channels = 1

Switch#

This 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:
Hello    Partner  PAgP     Learning  Group
Port      Flags State   Timers  Interval Count   Priority   Method  Ifindex
Fa5/4     d     U1/S1           1s       0        128        Any      0
Age of the port in the current state: 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:
Hello    Partner  PAgP     Learning  Group
Port      Flags State   Timers  Interval Count   Priority   Method  Ifindex
Fa5/5     d     U1/S1           1s       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
### show etherchannel

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

<table>
<thead>
<tr>
<th>Ports in the Port-channel:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
</tr>
<tr>
<td>-------</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

This example shows how to display a one-line summary per channel group:

```
Switch# show etherchannel summary
```

Flags:  D - down         P - bundled in  port-channel
I -  stand-alone s - suspended
H - Hot-standby (LACP only)
R  - Layer3      S -  Layer2
U - in use       f - failed to allocate  aggregator
M - not in  use, minimum links not  met
u - unsuitable for  bundling
w - waiting to be  aggregated
d - default  port

Number of channel-groups in use: 2

<table>
<thead>
<tr>
<th>Group</th>
<th>Port-channel</th>
<th>Protocol</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Po1(SD)</td>
<td>LACP</td>
<td>Gi1/23(H)   Gi1/24(H)</td>
</tr>
</tbody>
</table>

This example shows how to display EtherChannel port information for all ports and all groups:

```
Switch# show etherchannel port
```

Channel-group listing:

<table>
<thead>
<tr>
<th>Group: 1</th>
</tr>
</thead>
</table>

Ports in the group:

<table>
<thead>
<tr>
<th>Port: Fa5/4</th>
</tr>
</thead>
</table>

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:

<table>
<thead>
<tr>
<th>Hello</th>
<th>Partner</th>
<th>PAgP</th>
<th>Learning</th>
<th>Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Flags</td>
<td>State</td>
<td>Timers</td>
<td>Interval</td>
</tr>
<tr>
<td>Fa5/4</td>
<td>d</td>
<td>U1/S1</td>
<td>1s</td>
<td>0</td>
</tr>
</tbody>
</table>

Age of the port in the current state: 02h:40m:35s

Port: Fa5/5

------------
show etherchannel

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.

This example shows how to display the protocol enabled:

Switch#
show etherchannel protocol
Channel-group listing:
-----------------------
Group: 12
----------
Protocol:  PAgP
Group: 24
----------
Protocol:   -  (Mode ON)

Switch#

Related Commands
Command Description
channel-group  Assigns and configures an EtherChannel interface to an
EtherChannel group.
interface port-channel Accesses or creates a port-channel interface.
To display the per-interface status and statistics related to flow control, use the `show flowcontrol` command.

**Syntax Description**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Usage Guidelines**

Table 2-17 describes the fields in the `show flowcontrol` command output.

**Examples**

This example shows how to display the flow control status on all the Gigabit Ethernet interfaces:

```
Switch# show flowcontrol
Port       Send FlowControl  Receive FlowControl  RxPause  TxPause
admin    oper     admin    oper
---------  -------- -------- -------- --------    ------- -------
Te1/1      off      off      on       off         0       0
Te1/2      off      off      on       off         0       0
Gi1/3      off      off      desired  on          0       0
```

- **module** (Optional) Limits the display to interfaces on a specific module.
- **interface** (Optional) Displays the status on a specific interface.
This example shows how to display the flow control status on module 1:

```
Switch#
show flowcontrol module 1
```

<table>
<thead>
<tr>
<th>Port</th>
<th>Send FlowControl</th>
<th>Receive FlowControl</th>
<th>RxPause</th>
<th>TxPause</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/1</td>
<td>desired</td>
<td>off</td>
<td>off</td>
<td>off</td>
</tr>
<tr>
<td>Gi1/2</td>
<td>on</td>
<td>disagree</td>
<td>on</td>
<td>on</td>
</tr>
</tbody>
</table>

This example shows how to display the flow control status on Gigabit Ethernet interface 3/4:

```
Switch#
show flowcontrol interface gigabitethernet3/4
```

<table>
<thead>
<tr>
<th>Port</th>
<th>Send FlowControl</th>
<th>Receive FlowControl</th>
<th>RxPause</th>
<th>TxPause</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi3/4</td>
<td>off</td>
<td>off</td>
<td>on</td>
<td>on</td>
</tr>
</tbody>
</table>

This example shows how to display the flow control status on 10-Gigabit Ethernet interface 1/1:

```
Switch#
show flowcontrol interface tengigabitethernet1/1
```

<table>
<thead>
<tr>
<th>Port</th>
<th>Send FlowControl</th>
<th>Receive FlowControl</th>
<th>RxPause</th>
<th>TxPause</th>
</tr>
</thead>
<tbody>
<tr>
<td>Te1/1</td>
<td>off</td>
<td>off</td>
<td>on</td>
<td>off</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>channel-group</td>
<td>Configures a Gigabit Ethernet interface to send or receive pause frames.</td>
</tr>
<tr>
<td>show interfaces status</td>
<td>Displays the interface status or a list of interfaces in error-disabled state.</td>
</tr>
</tbody>
</table>
Chapter 2 Cisco IOS Commands for the Catalyst 4500 Series Switches

**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.
- **mod**: (Optional) Specifies the module name.
- **interface**: Displays information for the GBIC or SFP IDPROMs.
- **int_name**: Specifies the interface name.
- **supervisor**: Displays information for the supervisor engine IDPROMs.
- **power-supply number**: Displays information for the power supply IDPROMs.
- **fan-tray**: Displays information for the fan tray IDPROMs.

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Usage Guidelines**

When you enter the `show idprom interface int_name` command, the output lines for Calibration type and Rx (receive) power measurement may not be displayed for all GBICs.

**Examples**

This example shows how to display IDPROM information for module 4:

```
Switch# show idprom module 4
```

```
Module 4 Idprom:
Common Block Signature = 0xABAB
Common Block Version = 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 = <tbd>
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
```
This 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 measuremnt: 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
- 20944D40 1A 80 ED 00 00 00 00 00 00 00 00 00 38 23 3C 1B

SEEPROM contents (hex) size 128:

```
0x0000 01 00 01 00 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
```
Switch# This 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:
This 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 = 0.0.0.0.0.0.0.0
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

This 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 = 0.0.0.0.0.0.0.0
This 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 = 0x00000000FFFFFFFF
Current @ 110V = -1
Current @ 220V = -1
StackMIB OID = 65535
```

This example shows how to display IDPROM information for the fan tray:

```
Switch# show idprom fan-tray
Fan Tray Idprom:
Common Block Signature = 0xABAB
Common Block Version = 1
Common Block Length = 144
Common Block Checksum = 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
```
show idprom

Snmp OID = 65535.65535.65535.65535.65535.65535.65535.65535

Power Consumption = -1

RMA Failure Code = 255 255 255 255

Switch#
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**

(Optional) Specifies the Fast Ethernet module and interface.

**gigabitethernet**

(Optional) Specifies the Gigabit Ethernet module and interface.

**tengigabitethernet**

(Optional) Specifies the 10-Gigabit Ethernet module and interface.

**null**

(Optional) Specifies the null interface; the valid value is 0.

**vlan**

(Optional) Specifies the VLAN; valid values are from 1 to 4094.

**status**

(Optional) Displays status information.

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Usage Guidelines**

The statistics are collected per VLAN for Layer 2 switched packets and Layer 3 switched packets. The statistics are available for both unicast and multicast. The Layer 3 switched packet counts are available for both 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**

This 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
```
This example shows how to display traffic for 10-Gigabit Ethernet interface 1/1:

```
Switch#
```

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.
This example shows how to display status information for Gigabit Ethernet interface 1/2:

```
Switch# show interfaces gigabitethernet1/2 status
Port      Name         Status       Vlan       Duplex  Speed Type
Gi1/2                  notconnect   1            auto   1000 1000-XWDM-RXONLY
Switch#
```

This example shows how to display status information for the interfaces on the supervisor engine:

```
Switch# show interfaces status
Port      Name               Status       Vlan       Duplex  Speed Type
Te1/1                        connected    1            full    10G 10GBase-LR
Te1/2                        connected    1            full    10G 10GBase-LR
Switch#
```
show interfaces capabilities

To display the interface capabilities for an interface or for all the interfaces on a switch, use the `show interfaces capabilities` command.

```
show interfaces capabilities
[{{module|mod}}]
show interfaces [interface|interface-number] capabilities
```

**Syntax Description**
- **module** (Optional) Displays information for the specified module only.
- **interface** (Optional) Interface type; valid values are `fastethernet`, `gigabitethernet`, `tengigabitethernet`, and `port-channel`.
- **interface-number** (Optional) Port number.

**Defaults**
This command has no default settings.

**Command Modes**
Privileged EXEC mode

**Usage Guidelines**
The `interface-number` argument designates the module and port number. Valid values for `interface-number` depend on the chassis and module used. For example, if you have a 48-port 10/100-Mbps Fast Ethernet RJ-21 (telco connector) switching module installed in a Catalyst 4507 chassis, valid values for the slot number are from 2 to 13 and valid values for the port number are 1 to 48.

Line cards that support auto-MDIX configuration on their copper media ports include: WS-X4124-RJ45, WS-X4148-RJ with hardware revision 3.0 or higher, and WS-X4232-GB-RJ with hardware revision 3.0 or higher.

**Examples**
This example shows how to display the interface capabilities for a module:

```
Switch# show interfaces capabilities module 1
GigabitEthernet1/1
Model:                WS-X4516-Gbic
Type:                 Unsupported GBIC
Speed:                1000
Duplex:               full
Trunk encap. type:    802.1Q,ISL
Trunk mode:           on,off,desirable,nonegotiate
Channel:              yes
Broadcast suppression:percentage(0-100), hw
Flowcontrol:          rx-(off,on,desired),tx-(off,on,desired)
VLAN Membership:      static, dynamic
Fast Start:           yes
Queuing:              rx-(N/A), tx-(4q1t, Sharing/Shaping)
CoS rewrite:          yes
ToS rewrite:          yes
Inline power:         no
SPAN:                 source/destination
UDLD                   yes
Link Debounce:        no
```
This example shows how to display the interface capabilities for the 10-Gigabit Ethernet interface 1/1:

```
Switch# show interfaces tengigabitethernet1/1 capabilities
TenGigabitEthernet1/1
Model:                 WS-X4517-X2
Type:                  10GBase-LR
Speed:                 10000
Duplex:                full
Trunk encap. type:     802.1Q,ISL
Trunk mode:            on,off,desirable,nonegotiate
Channel:               yes
Broadcast suppression: percentage(0-100), hw
Flowcontrol:           rx-(off,on),tx-(off,on)
VLAN Membership:       static, dynamic
Fast Start:            yes
Queuing:               rx-(N/A), tx-(1p3q1t, Sharing/Shaping)
CoS rewrite:           yes
ToS rewrite:           yes
Inline power:          no
SPAN:                  source/destination
UDLD:                  yes
Link Debounce:         no
Link Debounce Time:    no
Port Security:         yes
Dot1x:                 yes
Maximum MTU:           9198 bytes (Jumbo Frames)
Multiple Media Types:  no
Diagnostic Monitoring: N/A
```

This example shows how to display the interface capabilities for Gigabit Ethernet interface 1/1:

```
Switch# show interfaces gigabitethernet1/1 capabilities
GigabitEthernet1/1
Model:                WS-X4014-Gbic
Type:                 No Gbic
Speed:                1000
```
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

show interfaces capabilities

Duplex:               full
Trunk encap. type:    802.1Q,ISL
Trunk mode:           on,off,desirable,nonegotiate
Channel:              yes
Broadcast suppression: percentage(0-100), hw
Flowcontrol:          rx-(off,on,desired),tx-(off,on,desired)
VLAN Membership:      static, dynamic
Fast Start:           yes
Queuing:              rx-(N/A), tx-(4q1t, Sharing/Shaping)
CoS rewrite:          yes
ToS rewrite:          yes
Inline power:         no
SPAN:                 source/destination
UDLD:                 yes
Link Debounce:        no
Link Debounce Time:   no
Port Security:        yes
Dot1x:                yes
MTU Supported:        jumbo frames, baby giants

Switch#
This example shows how to display the interface capabilities for Fast Ethernet interface 3/1:

Switch#
show interfaces fastethernet3/1 capabilities

FastEthernet3/1
Model:                WS-X4148-RJ-RJ-45
Type:                 10/100BaseTX
Speed:                10,100,auto
Duplex:               half,full,auto
Trunk encap. type:    802.1Q,ISL
Trunk mode:           on,off,desirable,nonegotiate
Channel:              yes
Broadcast suppression: percentage(0-100), sw
Flowcontrol:          rx-(none),tx-(none)
VLAN Membership:      static, dynamic
Fast Start:           yes
Queuing:              rx-(N/A), tx-(4q1t, Shaping)
CoS rewrite:          yes
ToS rewrite:          yes
Inline power:         no
SPAN:                 source/destination
UDLD:                 yes
Link Debounce:        no
Link Debounce Time:   no
Port Security:        yes
Dot1x:                yes
MTU Supported:        no jumbo frames, baby giants

Switch#
This example shows how to verify that the auto-MDIX configuration is supported on a port:

Switch#
show interfaces fastethernet6/3 capabilities

FastEthernet6/3
Model:                 WS-X4232-GB-RJ-RJ-45
Type:                  10/100BaseTX
Speed:                 10,100,auto
Duplex:                half,full,auto
Auto-MDIX              yes
Trunk encap. type:     802.1Q,ISL
Trunk mode:            on,off,desirable,nonegotiate
Channel:               yes
Broadcast suppression: percentage(0-100), hw
Flowcontrol:           rx-(none),tx-(none)
VLAN Membership:       static, dynamic
show interfaces capabilities

Fast Start: yes
Queuing: rx-(N/A), tx-(1p3q1t, Sharing/Shaping)
CoS rewrite: yes
ToS rewrite: yes
Inline power: no
SPAN: source/destination
UDLD: yes
Link Debounce: no
Link Debounce Time: no
Port Security: yes
Dot1x: yes
Maximum MTU: 1552 bytes (Baby Giants)
Multiple Media Types: no
Diagnostic Monitoring: N/A

Switch#

Related Commands
Command Description
show interfaces counters Displays the traffic on the physical interface.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

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]
```

**Syntax Description**

- **Defaults**: This command has no default settings.
- **Command Modes**: Privileged EXEC mode
- **Usage Guidelines**: If you do not enter any keywords, all the counters for all modules are displayed.
  
  The display for the `storm-control` keyword includes the suppressed multicast bytes.

**Examples**

This example shows how to display the error counters for a specific module:

```
Switch#
show interfaces counters errors module 1
```

```
Port        Align-Err    FCS-Err   Xmit-Err    Rcv-Err UnderSize
Gi1/1               0          0          0          0         0
Gi1/2               0          0          0          0         0
```

This example shows how to display the traffic that is seen by a specific module:

```
Switch#
show interfaces counters module 1
```

```
Port            InOctets   InUcastPkts   InMcastPkts   InBcastPkts
Gi1/1                0             0             0             0
Gi1/2                0             0             0             0
```

This example shows how to display the trunk counters for a specific module:

```
Switch#
show interfaces counters module 1
```

```
Storm-Ctl
```

(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 (Optional) Limits the display to interfaces on a specific module.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

show interfaces counters

Switch#
show interfaces counters trunk module 1

Port        TrunkFramesTx  TrunkFramesRx  WrongEncap
Gi1/1                   0              0           0
Gi1/2                   0              0           0

Switch#

This example shows how to display the number of packets that are discarded due to suppression:

Switch#
show interfaces counters storm-control

Multicast Suppression : Enabled

Port        BcastSuppLevel  TotalSuppressionDiscards
Fa5/35              10.00%               6278550

Switch#

Related Commands Command Description
show interfaces capabilities
Displays the interface capabilities for an interface or for all
the interfaces on a switch.
To display a description and status of an interface, use the `show interfaces description` command.

```
show interfaces [interface] description
```

**Syntax Description**

This command has no default settings.

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Examples**

This example shows how to display information for all interfaces:

```
Switch#
show interfaces description

Interface Status         Protocol Description
PO0/0     admin down     down     First interface
PO0/1     admin down     down
Gi1/1     up             up       GigE to server farm
Switch#
```

**Related Commands**

- `interface` (Optional) Type of interface.
- `description` (refer to Cisco IOS documentation)

Includes a specific description about the digital signal processor (DSP) interface.
To display how long a cable has been disconnected from an interface, use the `show interfaces link` command:

```
show interfaces link
```

**Syntax Description**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Usage Guidelines**

If the interface state is up, the command displays 0:00. If the interface state is down, the time (in hours, minutes, and seconds) is displayed.

**Examples**

This example shows how to display active link-level information:

```
Switch# show interfaces link
Port    Name               Down Time     
Gi1/1                       00:00:00     
Gi1/2                       00:00:00     
Gi3/1              00:00:00     
Gi3/2              00:00:00     
Fa4/1                       00:00:00     
Fa4/2                       00:00:00     
Fa4/3                       00:00:00     
Fa4/4                       00:00:00     
```

This example shows how to display inactive link-level information:

```
Switch# show interfaces link
Port    Name               Down Time     
Gi3/4                      1 minute 28 secs 
Gi3/5                      1 minute 28 secs 
Gi3/6                      1 minute 28 secs 
Gi4/1                      1 minute 28 secs 
```

In this example, the cable has been disconnected from the port for 1 minute and 28 seconds.
To display the maximum transmission unit (MTU) size of all the physical interfaces and SVIs on the switch, use the `show interfaces mtu` command.

Syntax Description

This command has no default settings.

Command Modes

EXEC

Examples

This example shows how to display the MTU size for all interfaces on module 1:

```
Switch> show interfaces mtu module 1

Port    Name               MTU
Gi1/1                      1500
Gi1/2                      1500

Switch>
```

Related Commands

- `module mod` (Optional) Limits the display to interfaces on a specific module.
- `mtu` Enables jumbo frames on an interface by adjusting the maximum size of a packet or maximum transmission unit (MTU).
To display PVLAN mapping information for VLAN SVIs, use the `show interfaces private-vlan mapping` command.

**Syntax Description**

This command has no default settings.

**Defaults**

This command displays SVI information only.

**Command Modes**

Privileged EXEC mode

**Usage Guidelines**

This command displays SVI information only.

**Examples**

This example shows how to display PVLAN mapping information:

```
Switch# show interfaces private-vlan mapping
Interface Secondary VLAN Type
--------- -------------- -----------------
vlan2     301            isolated
vlan2     302            isolated
Switch#
```

**Related Commands**

- `active` (Optional) Displays active interfaces only.
- `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.
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]
```

**Syntax Description**

This command has no default settings.

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Command History**

Release   Modification
12.1(8a)EW Support for this command was introduced on the Catalyst 4500 series switch.
12.2(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**

This example shows how to display the status of all interfaces:

```
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
```

This example shows how to display the status of interfaces in an error-disabled state:

```
Switch#
show interfaces status err-disabled
Port    Name               Status       Reason
Fa9/4                      notconnect  link-flap  
Fa9/5                      err-disabled psecure_violation 3-5
Fa9/6                      connected  psecure_violation 10,15
```

`err-disabled` (Optional) Displays interfaces in error-disabled state.

`inactive` (Optional) Displays interfaces in inactive state.

`module` (Optional) Displays interfaces on a specific module.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

show interfaces status

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

Switch#
show interfaces status module 1

<table>
<thead>
<tr>
<th>Port Name</th>
<th>Status</th>
<th>Vlan</th>
<th>Duplex</th>
<th>Speed</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Te1/1</td>
<td>inactive</td>
<td>1</td>
<td>full</td>
<td>10G</td>
<td>No X2</td>
</tr>
<tr>
<td>Te1/2</td>
<td>inactive</td>
<td>1</td>
<td>full</td>
<td>10G</td>
<td>No X2</td>
</tr>
<tr>
<td>Te1/3</td>
<td>inactive</td>
<td>1</td>
<td>full</td>
<td>10G</td>
<td>No X2</td>
</tr>
<tr>
<td>Te1/4</td>
<td>notconnect</td>
<td>1</td>
<td>full</td>
<td>10G</td>
<td>No X2</td>
</tr>
<tr>
<td>Te1/5</td>
<td>notconnect</td>
<td>1</td>
<td>full</td>
<td>10G</td>
<td>No X2</td>
</tr>
<tr>
<td>Te1/6</td>
<td>notconnect</td>
<td>1</td>
<td>full</td>
<td>10G</td>
<td>No X2</td>
</tr>
<tr>
<td>Gi1/7</td>
<td>notconnect</td>
<td>1</td>
<td>full</td>
<td>1000</td>
<td>No Gbic</td>
</tr>
<tr>
<td>Gi1/8</td>
<td>notconnect</td>
<td>1</td>
<td>full</td>
<td>1000</td>
<td>No Gbic</td>
</tr>
<tr>
<td>Gi1/9</td>
<td>notconnect</td>
<td>1</td>
<td>full</td>
<td>1000</td>
<td>No Gbic</td>
</tr>
<tr>
<td>Gi1/10</td>
<td>notconnect</td>
<td>1</td>
<td>full</td>
<td>1000</td>
<td>No Gbic</td>
</tr>
<tr>
<td>Gi1/11</td>
<td>notconnect</td>
<td>1</td>
<td>full</td>
<td>1000</td>
<td>No Gbic</td>
</tr>
<tr>
<td>Gi1/12</td>
<td>notconnect</td>
<td>1</td>
<td>full</td>
<td>1000</td>
<td>No Gbic</td>
</tr>
<tr>
<td>Gi1/13</td>
<td>inactive</td>
<td>1</td>
<td>full</td>
<td>1000</td>
<td>No Gbic</td>
</tr>
<tr>
<td>Gi1/14</td>
<td>inactive</td>
<td>1</td>
<td>full</td>
<td>1000</td>
<td>No Gbic</td>
</tr>
<tr>
<td>Gi1/15</td>
<td>inactive</td>
<td>1</td>
<td>full</td>
<td>1000</td>
<td>No Gbic</td>
</tr>
<tr>
<td>Gi1/16</td>
<td>inactive</td>
<td>1</td>
<td>full</td>
<td>1000</td>
<td>No Gbic</td>
</tr>
<tr>
<td>Gi1/17</td>
<td>inactive</td>
<td>1</td>
<td>full</td>
<td>1000</td>
<td>No Gbic</td>
</tr>
<tr>
<td>Gi1/18</td>
<td>inactive</td>
<td>1</td>
<td>full</td>
<td>1000</td>
<td>No Gbic</td>
</tr>
</tbody>
</table>

Switch#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>errdisable detect</td>
<td>Enables error-disable detection.</td>
</tr>
<tr>
<td>show errdisable recovery</td>
<td>Displays error-disable recovery timer information.</td>
</tr>
</tbody>
</table>
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

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`

**Syntax Description**

- **interface-id** (Optional) Interface ID for the physical port.
- **module** (Optional) Limits the display to interfaces on the specified module; valid values are from 1 to 6.

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Examples**

This example shows how to display switch-port information using the `begin` 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#
```

This 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
```

Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

show interfaces switchport

Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Switch#

This example shows how to display the status of native VLAN tagging on the port:
Switch#

show interfaces 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 capabilities
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.
To display diagnostic-monitoring data for all interfaces that have transceivers installed, use the `show interfaces transceiver` command.

```
show interfaces transceiver
```

**Syntax Description**

- **Defaults**
  - The noninterface-specific versions of the `show interfaces transceiver` command are enabled by default.
  - The interface-specific versions of these commands are enabled by default if the specified interface has a transceiver (GBIC or SFP) that is configured for diagnostic monitoring, and the transceiver is in a module that supports diagnostic monitoring.

**Command Modes**

- Privileged EXEC mode

**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**

This example shows how to display diagnostic monitoring data for all interfaces with transceivers installed on the switch:

```
Switch# show interfaces transceiver
```

If device is externally calibrated, only calibrated values are printed.

<table>
<thead>
<tr>
<th>Port</th>
<th>Optical Temperature (Celsius)</th>
<th>Voltage (Volts)</th>
<th>Current (mA)</th>
<th>Tx Power (dBm)</th>
<th>Rx Power (dBm)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/1</td>
<td>48.1</td>
<td>3.30</td>
<td>0.0</td>
<td>8.1 ++</td>
<td>N/A</td>
</tr>
<tr>
<td>Gi1/2</td>
<td>33.0</td>
<td>3.30</td>
<td>1.8</td>
<td>-10.0</td>
<td>-36.9</td>
</tr>
<tr>
<td>Gi2/1</td>
<td>43.7</td>
<td>5.03</td>
<td>50.6 +</td>
<td>-16.7 --</td>
<td>N/A</td>
</tr>
<tr>
<td>Gi2/2</td>
<td>39.2</td>
<td>5.02</td>
<td>25.7</td>
<td>0.8</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Switch#
**Chapter 2: Cisco IOS Commands for the Catalyst 4500 Series Switches**

**show interfaces transceiver**

---

### 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 * 0.477 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).

This 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.

<table>
<thead>
<tr>
<th>Port</th>
<th>Temperature (Celsius)</th>
<th>High Alarm</th>
<th>High Warn</th>
<th>Low Warn</th>
<th>Low Alarm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/1</td>
<td>48.1</td>
<td>100.0</td>
<td>100.0</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>Gi1/2</td>
<td>34.9</td>
<td>100.0</td>
<td>100.0</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>Gi2/1</td>
<td>43.5</td>
<td>70.0</td>
<td>60.0</td>
<td>5.0</td>
<td>0.0</td>
</tr>
<tr>
<td>Gi2/2</td>
<td>39.1</td>
<td>70.0</td>
<td>60.0</td>
<td>5.0</td>
<td>0.0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Voltage (Volts)</th>
<th>High Alarm</th>
<th>High Warn</th>
<th>Low Warn</th>
<th>Low Alarm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/1</td>
<td>3.30</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi1/2</td>
<td>3.30</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi2/1</td>
<td>5.03</td>
<td>6.50</td>
<td>6.50</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi2/2</td>
<td>5.02</td>
<td>6.50</td>
<td>6.50</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Current (mA)</th>
<th>High Alarm</th>
<th>High Warn</th>
<th>Low Warn</th>
<th>Low Alarm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/1</td>
<td>0.0</td>
<td>130.0</td>
<td>130.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi1/2</td>
<td>1.7</td>
<td>130.0</td>
<td>130.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi2/1</td>
<td>50.6</td>
<td></td>
<td>+</td>
<td>60.0</td>
<td>40.0</td>
</tr>
<tr>
<td>Gi2/2</td>
<td>25.8</td>
<td></td>
<td></td>
<td>60.0</td>
<td>40.0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Optical Transmit Power (dBm)</th>
<th>High Alarm</th>
<th>High Warn</th>
<th>Low Warn</th>
<th>Low Alarm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/1</td>
<td>8.1 (8.1)</td>
<td>++</td>
<td>8.1</td>
<td>8.1</td>
<td>N/A</td>
</tr>
<tr>
<td>Gi1/2</td>
<td>-9.8 (-13.0)</td>
<td></td>
<td>8.1</td>
<td>8.1</td>
<td>N/A</td>
</tr>
<tr>
<td>Gi2/1</td>
<td>3.4 (-22.7) (-15.0)</td>
<td>--</td>
<td>3.4</td>
<td>3.2</td>
<td>-0.3</td>
</tr>
<tr>
<td>Gi2/2</td>
<td>3.2 ( 5.1)</td>
<td></td>
<td>3.4</td>
<td>3.2</td>
<td>-0.3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Optical Receive Power (dBm)</th>
<th>High Alarm</th>
<th>High Warn</th>
<th>Low Warn</th>
<th>Low Alarm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/1</td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi1/2</td>
<td>-30.9</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi2/1</td>
<td>-28.5 (-30.9)</td>
<td></td>
<td>5.9</td>
<td>-6.7</td>
<td>-28.5</td>
</tr>
<tr>
<td>Gi2/2</td>
<td>-28.5 (-30.9)</td>
<td></td>
<td>5.9</td>
<td>-6.7</td>
<td>-28.5</td>
</tr>
</tbody>
</table>

Switch#
This 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).

<table>
<thead>
<tr>
<th>Port</th>
<th>Optical Temperature</th>
<th>Optical Voltage</th>
<th>Optical Current</th>
<th>Optical Tx Power</th>
<th>Optical Rx Power</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi2/1</td>
<td>43.7</td>
<td>5.03</td>
<td>50.6 +</td>
<td>-16.7 --</td>
<td>N/A</td>
</tr>
<tr>
<td>Gi2/2</td>
<td>39.2</td>
<td>5.02</td>
<td>25.7</td>
<td>0.8</td>
<td>N/A</td>
</tr>
</tbody>
</table>

This example shows how to display the detailed monitoring data for the interfaces that have transceivers installed on module 2:

```
Switch#
show interfaces transceiver detail module 2
```

mA: milliamperes, dBm: decibels (milliwatts), 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.

<table>
<thead>
<tr>
<th>Port</th>
<th>High Alarm</th>
<th>High Warn</th>
<th>Low Warn</th>
<th>Low Alarm</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Temperature</td>
<td>Voltage</td>
<td>Current</td>
<td>Transmit Power</td>
</tr>
<tr>
<td>-------</td>
<td>------------</td>
<td>-----------</td>
<td>----------</td>
<td>----------------</td>
</tr>
<tr>
<td>Gi2/1</td>
<td>43.5</td>
<td>5.03</td>
<td>50.6</td>
<td>-16.7 (-13.0) --</td>
</tr>
<tr>
<td>Gi2/2</td>
<td>39.1</td>
<td>5.02</td>
<td>25.7</td>
<td>0.8</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>High Alarm</th>
<th>High Warn</th>
<th>Low Warn</th>
<th>Low Alarm</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Voltage</td>
<td>Current</td>
<td>Optical Transmit Power</td>
<td>Optical Receive Power</td>
</tr>
<tr>
<td>-------</td>
<td>------------</td>
<td>-----------</td>
<td>------------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>Gi2/1</td>
<td>5.03</td>
<td>50.6</td>
<td>+</td>
<td>-16.7 (-13.0) --</td>
</tr>
<tr>
<td>Gi2/2</td>
<td>5.02</td>
<td>25.7</td>
<td>+</td>
<td>0.8 (  5.1)</td>
</tr>
</tbody>
</table>

```

Switch#
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

show interfaces transceiver

This 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.
NA or N/A: not applicable, Tx: transmit, Rx: receive.
mA: milliamperes, dBm: decibels (milliwatts).

<table>
<thead>
<tr>
<th>Optical</th>
<th>Optical</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temperature</td>
<td>Voltage</td>
</tr>
<tr>
<td>Port</td>
<td>(Celsius)</td>
</tr>
<tr>
<td>-------</td>
<td>----------</td>
</tr>
<tr>
<td>Gi2/1</td>
<td>43.7</td>
</tr>
</tbody>
</table>

Switch#

This 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.
A2D readouts (if they differ), are reported in parentheses.
The threshold values are calibrated.

<table>
<thead>
<tr>
<th>High Alarm</th>
<th>High Warn</th>
<th>Low Warn</th>
<th>Low Alarm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temperature</td>
<td>Threshold</td>
<td>Threshold</td>
<td>Threshold</td>
</tr>
<tr>
<td>Port</td>
<td>(Celsius)</td>
<td>(Celsius)</td>
<td>(Celsius)</td>
</tr>
<tr>
<td>-------</td>
<td>----------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>Gi2/1</td>
<td>43.5</td>
<td>70.0</td>
<td>60.0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>High Alarm</th>
<th>High Warn</th>
<th>Low Warn</th>
<th>Low Alarm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voltage</td>
<td>Threshold</td>
<td>Threshold</td>
<td>Threshold</td>
</tr>
<tr>
<td>Port</td>
<td>(Volts)</td>
<td>(Volts)</td>
<td>(Volts)</td>
</tr>
<tr>
<td>-------</td>
<td>------------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>Gi2/1</td>
<td>5.03</td>
<td>5.50</td>
<td>5.25</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>High Alarm</th>
<th>High Warn</th>
<th>Low Warn</th>
<th>Low Alarm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current</td>
<td>Threshold</td>
<td>Threshold</td>
<td>Threshold</td>
</tr>
<tr>
<td>Port</td>
<td>(milliamperes)</td>
<td>(mA)</td>
<td>(mA)</td>
</tr>
<tr>
<td>-------</td>
<td>-----------------</td>
<td>--------</td>
<td>--------</td>
</tr>
<tr>
<td>Gi2/1</td>
<td>50.6</td>
<td>+</td>
<td>60.0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Optical</th>
<th>Optical</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transmit Power</td>
<td>Receive Power</td>
</tr>
<tr>
<td>Port</td>
<td>(dBm)</td>
</tr>
<tr>
<td>-------</td>
<td>-------</td>
</tr>
<tr>
<td>Gi2/1</td>
<td>-16.7</td>
</tr>
</tbody>
</table>

Switch#
## Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show interfaces transceiver</code></td>
<td>Displays information about the transceivers on the interfaces.</td>
</tr>
<tr>
<td><code>show idprom</code></td>
<td>Displays the IDPROMs for the chassis.</td>
</tr>
<tr>
<td><code>show interfaces status</code></td>
<td>Displays the interface status or a list of interfaces in error-disabled state.</td>
</tr>
</tbody>
</table>
To display port and module interface-trunk information, use the `show interfaces trunk` command.

**Syntax Description**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Usage Guidelines**

If you do not specify a keyword, only information for trunking ports is displayed.

**Examples**

This example shows how to display interface-trunk information for module 5:

```
Switch# show interfaces trunk module 5
```

<table>
<thead>
<tr>
<th>Port</th>
<th>Mode</th>
<th>Encapsulation</th>
<th>Status</th>
<th>Native vlan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa5/1</td>
<td>routed</td>
<td>negotiate</td>
<td>routed</td>
<td>1</td>
</tr>
<tr>
<td>Fa5/2</td>
<td>routed</td>
<td>negotiate</td>
<td>routed</td>
<td>1</td>
</tr>
<tr>
<td>Fa5/3</td>
<td>routed</td>
<td>negotiate</td>
<td>routed</td>
<td>1</td>
</tr>
<tr>
<td>Fa5/4</td>
<td>routed</td>
<td>negotiate</td>
<td>routed</td>
<td>1</td>
</tr>
<tr>
<td>Fa5/5</td>
<td>routed</td>
<td>negotiate</td>
<td>routed</td>
<td>1</td>
</tr>
<tr>
<td>Fa5/6</td>
<td>off</td>
<td>negotiate</td>
<td>not-trunking</td>
<td>10</td>
</tr>
<tr>
<td>Fa5/7</td>
<td>off</td>
<td>negotiate</td>
<td>not-trunking</td>
<td>10</td>
</tr>
<tr>
<td>Fa5/8</td>
<td>off</td>
<td>negotiate</td>
<td>not-trunking</td>
<td>1</td>
</tr>
<tr>
<td>Fa5/9</td>
<td>desirable</td>
<td>n-isl</td>
<td>trunking</td>
<td>1</td>
</tr>
<tr>
<td>Fa5/10</td>
<td>desirable</td>
<td>negotiate</td>
<td>not-trunking</td>
<td>1</td>
</tr>
<tr>
<td>Fa5/11</td>
<td>routed</td>
<td>negotiate</td>
<td>routed</td>
<td>1</td>
</tr>
<tr>
<td>Fa5/12</td>
<td>routed</td>
<td>negotiate</td>
<td>routed</td>
<td>1</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fa5/48</td>
<td>routed</td>
<td>negotiate</td>
<td>routed</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Vlans allowed on trunk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa5/1</td>
<td>none</td>
</tr>
<tr>
<td>Fa5/2</td>
<td>none</td>
</tr>
<tr>
<td>Fa5/3</td>
<td>none</td>
</tr>
<tr>
<td>Fa5/4</td>
<td>none</td>
</tr>
<tr>
<td>Fa5/5</td>
<td>none</td>
</tr>
<tr>
<td>Fa5/6</td>
<td>none</td>
</tr>
<tr>
<td>Fa5/7</td>
<td>none</td>
</tr>
<tr>
<td>Fa5/8</td>
<td>200</td>
</tr>
<tr>
<td>Fa5/9</td>
<td>1-1005</td>
</tr>
<tr>
<td>Fa5/10</td>
<td>none</td>
</tr>
<tr>
<td>Fa5/11</td>
<td>none</td>
</tr>
<tr>
<td>Fa5/12</td>
<td>none</td>
</tr>
<tr>
<td>Fa5/48</td>
<td>none</td>
</tr>
</tbody>
</table>
### Chapter 2: Cisco IOS Commands for the Catalyst 4500 Series Switches

#### show interfaces trunk

<table>
<thead>
<tr>
<th>Port</th>
<th>Vlans allowed and active in management domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa5/1</td>
<td>none</td>
</tr>
<tr>
<td>Fa5/2</td>
<td>none</td>
</tr>
<tr>
<td>Fa5/3</td>
<td>none</td>
</tr>
<tr>
<td>Fa5/4</td>
<td>none</td>
</tr>
<tr>
<td>Fa5/5</td>
<td>none</td>
</tr>
<tr>
<td>Fa5/6</td>
<td>none</td>
</tr>
<tr>
<td>Fa5/7</td>
<td>none</td>
</tr>
<tr>
<td>Fa5/8</td>
<td>200</td>
</tr>
<tr>
<td>Fa5/9</td>
<td>1-6,10,20,50,100,152,200,300,303-305,349-351,400,500,521,524,570,801-802,850,917,999,1002-1005</td>
</tr>
<tr>
<td>Fa5/10</td>
<td>none</td>
</tr>
<tr>
<td>Fa5/11</td>
<td>none</td>
</tr>
<tr>
<td>Fa5/12</td>
<td>none</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Vlans in spanning tree forwarding state and not pruned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa5/1</td>
<td>none</td>
</tr>
<tr>
<td>Fa5/2</td>
<td>none</td>
</tr>
<tr>
<td>Fa5/3</td>
<td>none</td>
</tr>
<tr>
<td>Fa5/4</td>
<td>none</td>
</tr>
<tr>
<td>Fa5/5</td>
<td>none</td>
</tr>
<tr>
<td>Fa5/6</td>
<td>none</td>
</tr>
<tr>
<td>Fa5/7</td>
<td>none</td>
</tr>
<tr>
<td>Fa5/8</td>
<td>200</td>
</tr>
<tr>
<td>Fa5/9</td>
<td>1-6,10,20,50,100,152,200,300,303-305,349-351,400,500,521,524,570,801-802,850,917,999,1002-1005</td>
</tr>
<tr>
<td>Fa5/10</td>
<td>none</td>
</tr>
<tr>
<td>Fa5/11</td>
<td>none</td>
</tr>
<tr>
<td>Fa5/48</td>
<td>none</td>
</tr>
</tbody>
</table>

---

Switch#  

This example shows how to display trunking information for active trunking ports:

```
Switch#
```

<table>
<thead>
<tr>
<th>Port</th>
<th>Mode</th>
<th>Encapsulation</th>
<th>Status</th>
<th>Native vlan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa5/9</td>
<td>desirable</td>
<td>n-isl</td>
<td>trunking</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Vlans allowed on trunk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa5/9</td>
<td>1-1005</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Vlans allowed and active in management domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa5/9</td>
<td>1-6,10,20,50,100,152,200,300,303-305,349-351,400,500,521,524,570,801-802,850,917,999,1002-1005</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Vlans in spanning tree forwarding state and not pruned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa5/9</td>
<td>1-6,10,20,50,100,152,200,300,303-305,349-351,400,500,521,524,570,801-802,850,917,999,1002-1005</td>
</tr>
</tbody>
</table>

Switch#
Cisco IOS Commands for the Catalyst 4500 Series Switches

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 DAI: forwarded, dropped, MAC validation failure, and IP validation failure.
- **vlan vlan-range** (Optional) When used with the `statistics` keyword, displays the statistics for the selected range of VLANs. Without the `statistics` keyword, displays the configuration and operating state of DAI for the selected range of VLANs.
- **interfaces interface-name** (Optional) Displays the trust state and the rate limit of ARP packets for the provided interface. When the interface name is not specified, the command displays the trust state and rate limit for all applicable interfaces in the system.

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Examples**

This example shows how to display the statistics of packets that have been processed by DAI for 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#
```

This example shows how to display the statistics of packets that have been processed by DAI for all active VLANs:

```
Switch# show ip arp inspection statistics
Vlan      Forwarded        Dropped     DHCP Drops     ACL Drops
----      ---------        -------     ----------     ----------
1              0              0              0              0
2              0              0              0              0
3          68322         220356         220356              0
statistics
```

```
```
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

show ip arp inspection

<table>
<thead>
<tr>
<th>Vlan</th>
<th>DHCP Permits</th>
<th>ACL Permits</th>
<th>Source MAC Failures</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>68322</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>100</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>101</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1006</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1007</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Dest MAC Failures</th>
<th>IP Validation Failures</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>100</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>101</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1006</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1007</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Switch#

This example shows how to display the configuration and operating state of DAI for VLAN 1:
Switch#

```
show ip arp inspection vlan 1
```

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Configuration</th>
<th>Operation</th>
<th>ACL Match</th>
<th>Static ACL</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enabled</td>
<td>Active</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Switch#

This example shows how to display the trust state of Fast Ethernet interface 6/1:
Switch#

```
show ip arp inspection interfaces fastEthernet 6/1
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>Trust State</th>
<th>Rate (pps)</th>
<th>Burst Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa6/1</td>
<td>Untrusted</td>
<td></td>
<td>20</td>
</tr>
</tbody>
</table>

Switch#

This example shows how to display the trust state of the interfaces on the switch:
Switch#

```
show ip arp inspection interfaces
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>Trust State</th>
<th>Rate (pps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/1</td>
<td>Untrusted</td>
<td>15</td>
</tr>
<tr>
<td>Gi1/2</td>
<td>Untrusted</td>
<td>15</td>
</tr>
<tr>
<td>Gi3/1</td>
<td>Untrusted</td>
<td>15</td>
</tr>
<tr>
<td>Gi3/2</td>
<td>Untrusted</td>
<td>15</td>
</tr>
<tr>
<td>Fa3/3</td>
<td>Trusted</td>
<td>None</td>
</tr>
<tr>
<td>Fa3/4</td>
<td>Untrusted</td>
<td>15</td>
</tr>
<tr>
<td>Fa3/5</td>
<td>Untrusted</td>
<td>15</td>
</tr>
</tbody>
</table>
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

show ip arp inspection

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.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

show ip arp inspection log

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

show ip arp inspection log

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Examples

This example shows how to display the current contents of the log buffer before and after the buffers are cleared:

Switch# show ip arp inspection log
Total Log Buffer Size : 10
Syslog rate : 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#

This example shows how to clear the buffer with the clear ip arp inspection log command:

Switch# clear ip arp inspection log
Switch# show ip arp inspection log
Total Log Buffer Size : 10
Syslog rate : 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.
Chapter 2 Cisco IOS Commands for the Catalyst 4500 Series Switches

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**

- **Defaults**: This command has no default settings.

**Command Modes**: Privileged EXEC mode

**Examples**

This example shows how to display the prefixes for a specific VLAN:

```
Switch# show ip cef vlan 1003
Prefix              Next Hop             Interface
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#
```

This 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#
```
To display the DHCP snooping configuration, use the `show ip dhcp snooping` command.

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Examples**

This example shows how to display the DHCP snooping configuration:

```
Switch# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
500, 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
  FastEthernet2/1 no unlimited
  Custom circuit-ids:
  VLAN 555: customer-555
  VLAN 500: customer-500
Switch#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip dhcp snooping</td>
<td>Globally enables DHCP snooping.</td>
</tr>
<tr>
<td>ip dhcp snooping information option</td>
<td>Enables DHCP option 82 data insertion.</td>
</tr>
<tr>
<td>ip dhcp snooping limit rate</td>
<td>Configures the number of the DHCP messages that an interface can receive per second.</td>
</tr>
<tr>
<td>ip dhcp snooping trust</td>
<td>Enables DHCP snooping on a trusted VLAN.</td>
</tr>
<tr>
<td>ip dhcp snooping vlan</td>
<td>Enables DHCP snooping on a VLAN or a group of VLANs.</td>
</tr>
</tbody>
</table>
To display the DHCP snooping binding entries, use the `show ip dhcp snooping binding` command.

```
show ip dhcp snooping binding [ip-address] [mac-address] [vlan vlan_num] [interface interface_num]
```

**Syntax Description**

- `ip-address` (Optional) IP address for the binding entries.
- `mac-address` (Optional) MAC address for the binding entries.
- `vlan` `vlan_num` (Optional) Specifies a VLAN.
- `interface` `interface_num` (Optional) Specifies an interface.

**Defaults**

If no argument is specified, the switch will display the entire DHCP snooping binding table.

**Command Modes**

Privileged EXEC mode

**Usage Guidelines**

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

To configure a range of VLANs, use the optional `last_vlan` argument to specify the end of the VLAN range.

**Examples**

This example shows how to display the DHCP snooping binding entries for a switch:

```
Switch#
show ip dhcp snooping binding
```

<table>
<thead>
<tr>
<th>MacAddress</th>
<th>IP Address</th>
<th>Lease (seconds)</th>
<th>Type</th>
<th>VLAN</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000.0100.0201</td>
<td>10.0.0.1</td>
<td>1600</td>
<td>dhcp-snooping</td>
<td>100</td>
<td>FastEthernet3/1</td>
</tr>
</tbody>
</table>

Switch#

This example shows how to display an IP address for DHCP snooping binding entries:

```
Switch#
show ip dhcp snooping binding 172.100.101.102
```

<table>
<thead>
<tr>
<th>MacAddress</th>
<th>IP Address</th>
<th>Lease (seconds)</th>
<th>Type</th>
<th>VLAN</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000.0100.0201</td>
<td>172.100.101.102</td>
<td>1600</td>
<td>dhcp-snooping</td>
<td>100</td>
<td>FastEthernet3/1</td>
</tr>
</tbody>
</table>

Switch#

This 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
```

<table>
<thead>
<tr>
<th>MacAddress</th>
<th>IpAddress</th>
<th>Lease (sec)</th>
<th>Type</th>
<th>VLAN</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:02:B3:3F:3D:5F</td>
<td>55.5.5.2</td>
<td>492</td>
<td>dhcp-snooping</td>
<td>99</td>
<td>FastEthernet6/36</td>
</tr>
</tbody>
</table>

Switch#
This example shows how to display the DHCP snooping binding entries' MAC address for a specific VLAN:

```
Switch# show ip dhcp snooping binding 55.5.5.2 0002.b33f.3d5f vlan 99
```

<table>
<thead>
<tr>
<th>MacAddress</th>
<th>IpAddress</th>
<th>Lease (sec)</th>
<th>Type</th>
<th>VLAN</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:02:B3:3F:3D:5F</td>
<td>55.5.5.2</td>
<td>479</td>
<td>dhcp-snooping</td>
<td>99</td>
<td>FastEthernet6/36</td>
</tr>
</tbody>
</table>

This example shows how to display the dynamic DHCP snooping binding entries:

```
Switch# show ip dhcp snooping binding dynamic
```

<table>
<thead>
<tr>
<th>MacAddress</th>
<th>IP Address</th>
<th>Lease (seconds)</th>
<th>Type</th>
<th>VLAN</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000.0100.0201</td>
<td>10.0.0.1</td>
<td>1600</td>
<td>dhcp-snooping</td>
<td>100</td>
<td>FastEthernet3/1</td>
</tr>
</tbody>
</table>

This example shows how to display the DHCP snooping binding entries on VLAN 100:

```
Switch# show ip dhcp snooping binding vlan 100
```

<table>
<thead>
<tr>
<th>MacAddress</th>
<th>IP Address</th>
<th>Lease (seconds)</th>
<th>Type</th>
<th>VLAN</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000.0100.0201</td>
<td>10.0.0.1</td>
<td>1600</td>
<td>dhcp-snooping</td>
<td>100</td>
<td>FastEthernet3/1</td>
</tr>
</tbody>
</table>

This example shows how to display the DHCP snooping binding entries on Ethernet interface 0/1:

```
Switch# show ip dhcp snooping binding interface fastethernet3/1
```

<table>
<thead>
<tr>
<th>MacAddress</th>
<th>IP Address</th>
<th>Lease (seconds)</th>
<th>Type</th>
<th>VLAN</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000.0100.0201</td>
<td>10.0.0.1</td>
<td>1600</td>
<td>dhcp-snooping</td>
<td>100</td>
<td>FastEthernet3/1</td>
</tr>
</tbody>
</table>

Table 2-18 describes the fields in the show ip dhcp snooping command output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mac Address</td>
<td>Client hardware MAC address.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Client IP address assigned from the DHCP server.</td>
</tr>
<tr>
<td>Lease (seconds)</td>
<td>IP address lease time.</td>
</tr>
<tr>
<td>Type</td>
<td>Binding type; statically configured from CLI or dynamically learned.</td>
</tr>
<tr>
<td>VLAN</td>
<td>VLAN number of the client interface.</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface that connects to the DHCP client host.</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip dhcp snooping information option</td>
<td>Enables DHCP option 82 data insertion.</td>
</tr>
<tr>
<td>ip dhcp snooping limit rate</td>
<td>Configures the number of the DHCP messages that an interface can receive per second.</td>
</tr>
<tr>
<td>ip dhcp snooping trust</td>
<td>Enables DHCP snooping on a trusted VLAN.</td>
</tr>
<tr>
<td>ip dhcp snooping vlan</td>
<td>Enables DHCP snooping on a VLAN or a group of VLANs.</td>
</tr>
</tbody>
</table>
Chapter 2 Cisco IOS Commands for the Catalyst 4500 Series Switches

show ip dhcp snoop ing binding

ip igmp snooping
Enables IGMP snooping.

ip igmp snooping vlan
Enables IGMP snooping for a VLAN.
To display the status of the DHCP snooping database agent, use the `show ip dhcp snooping database` command.

```
show ip dhcp snooping database

Syntax Description
This command has no default settings.

Command Modes
Privileged EXEC mode

Examples
This example shows how to display the DHCP snooping database:

Switch# show ip dhcp snooping database
Agent URL : 
Write delay Timer : 300 seconds
Abort Timer : 300 seconds
Agent Running : No
Delay Timer Expiry : Not Running
Abort Timer Expiry : Not Running
Last Succeded Time : None
Last Failed Time : None
Last Failed Reason : No failure recorded.
Total Attempts       :        0   Startup Failures :        0
Successful Transfers :        0   Failed Transfers :        0
Successful Reads     :        0   Failed Reads     :        0
Successful Writes    :        0   Failed Writes    :        0
Media Failures       :        0
Switch#

This example shows how to view additional operating statistics:

Switch# show ip dhcp snooping database detail
Agent URL : tftp://10.1.1.1/directory/file
Write delay Timer : 300 seconds
Abort Timer : 300 seconds
Agent Running : No
Delay Timer Expiry : 7 (00:00:07)
Abort Timer Expiry : Not Running
Last Succeded Time : None
Last Failed Time : 17:14:25 UTC Sat Jul 7 2001
Last Failed Reason : Unable to access URL.
Total Attempts       :       21   Startup Failures :        0
Successful Transfers :        0   Failed Transfers :       21
Successful Reads     :        0   Failed Reads     :        0
Successful Writes    :        0   Failed Writes    :        0
Media Failures       :        0

(detail) (Optional) Provides additional operating state and statistics information.
show ip dhcp snooping database

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

<table>
<thead>
<tr>
<th>Command Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip dhcp snooping</td>
</tr>
<tr>
<td>Globally enables DHCP snooping.</td>
</tr>
<tr>
<td>ip dhcp snooping database</td>
</tr>
<tr>
<td>Stores the bindings that are generated by DHCP snooping.</td>
</tr>
<tr>
<td>ip dhcp snooping information option</td>
</tr>
<tr>
<td>Enables DHCP option 82 data insertion.</td>
</tr>
<tr>
<td>ip dhcp snooping limit rate</td>
</tr>
<tr>
<td>Configures the number of DHCP messages that an interface can receive per second.</td>
</tr>
<tr>
<td>ip dhcp snooping trust</td>
</tr>
<tr>
<td>Enables DHCP snooping on a trusted VLAN.</td>
</tr>
<tr>
<td>ip dhcp snooping vlan</td>
</tr>
<tr>
<td>Enables DHCP snooping on a VLAN or a group of VLANs.</td>
</tr>
</tbody>
</table>
show ip igmp interface

To view IP IGMP interface status and configuration information, use the show ip igmp interface command.

**Syntax Description**

- **fastethernet** slot/port
- **gigabitethernet** slot/port
- **tengigabitethernet** slot/port
- **null** interface-number
- **vlan** vlan_id

**Defaults**

If you do not specify a VLAN, information for VLAN 1 is shown.

**Command Modes**

Privileged EXEC mode

**Usage Guidelines**

If you omit the optional arguments, the show ip igmp interface command displays information about all interfaces.

**Examples**

This example shows how to view IGMP information for VLAN 200:

```
Switch# show ip igmp interface vlan 200
IGMP snooping is globally enabled
IGMP snooping is 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**

- **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.
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**

This command has no default settings.

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Usage Guidelines**

If no profile number is entered, all IGMP profiles are displayed.

**Examples**

This example shows how to display IGMP profile 40:

```
Switch# show ip igmp profile 40
IGMP Profile 40
permit
range 233.1.1.1 233.255.255.255
Switch#
```

This example shows how to display all IGMP profiles:

```
Switch# show ip igmp profile
IGMP Profile 3
range 230.9.9.0 230.9.9.0
IGMP Profile 4
permit
range 229.9.9.0 229.255.255.255
Switch#
```

**Related Commands**

```
profile number
```

(Optional) IGMP profile number to be displayed; valid ranges are from 1 to 4294967295.

**Command Description**

```
ip igmp profile
```

Creates an IGMP profile.
Chapter 2 Cisco IOS Commands for the Catalyst 4500 Series Switches

show ip igmp snooping

To display information on dynamically learned and manually configured VLAN switch interfaces, use the 
show ip igmp snooping command.

Syntax Description

- querier
- groups
- mrouter
- vlan vlan_id
- a.b.c.d
- summary
- sources
- hosts
- count

Defaults

This command has no default settings.

Command Modes

EXEC

Usage Guidelines

You can also use the show mac-address-table multicast command to display the entries in the MAC
address table for a VLAN that has IGMP snooping enabled.

You can display IGMP snooping information for VLAN interfaces by entering the show ip igmp snooping command.

Examples

This example shows how to display the global snooping information on the switch:

Switch# show ip igmp snooping
Global IGMP Snooping configuration:
-----------------------------------
IGMP snooping             : Enabled
IGMPv3 snooping           : Enabled
Report suppression        : Enabled
TCN solicit query         : Disabled
TCN flood query count     : 2
Vlan 1:
--------
IGMP snooping                  : Enabled
IGMPv2 immediate leave         : Disabled

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.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

show ip igmp snooping

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>

This example shows how to display the snooping information on VLAN 2:

Switch#

show ip igmp snooping vlan 2

Global IGMP Snooping configuration:
-----------------------------------
IGMP snooping             : Enabled
IGMPv3 snooping           : Enabled
Report suppression        : Enabled
TCN solicit query         : Disabled
TCN flood query count     : 2

Vlan 2:
--------
IGMP snooping                  : Enabled
IGMPv2 immediate leave         : Disabled
Explicit host tracking         : Enabled
Multicast router learning mode : pim-dvmrp
CGMP interoperability mode     : IGMP_ONLY

Switch>

This example shows how to display IGMP querier information for all VLANs on a switch:

Switch#

show ip igmp snooping querier

<table>
<thead>
<tr>
<th>Vlan</th>
<th>IP Address</th>
<th>IGMP Version</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>10.10.10.1</td>
<td>v2</td>
<td>Router</td>
</tr>
<tr>
<td>3</td>
<td>172.20.50.22</td>
<td>v3</td>
<td>Fa3/15</td>
</tr>
</tbody>
</table>

Switch>

This example shows how to display IGMP querier information for VLAN 5 when running IGMPv2:

Switch#

show ip igmp snooping querier vlan 5

<table>
<thead>
<tr>
<th>IP address</th>
<th>IGMP version</th>
<th>Port</th>
<th>Max response time</th>
<th>Query interval</th>
<th>Robustness variable</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5.5.10</td>
<td>v2</td>
<td>Fa3/1</td>
<td>10s</td>
<td>60s</td>
<td>2</td>
</tr>
</tbody>
</table>

Switch>

This example shows how to display IGMP querier information for VLAN 5 when running IGMPv3:

Switch#

show ip igmp snooping querier vlan 5

<table>
<thead>
<tr>
<th>IP address</th>
<th>IGMP version</th>
<th>Port</th>
<th>Max response time</th>
<th>Query interval</th>
<th>Robustness variable</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5.5.10</td>
<td>v3</td>
<td>Fa3/1</td>
<td>10s</td>
<td>60s</td>
<td>2</td>
</tr>
</tbody>
</table>

Switch>
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

show ip igmp snooping

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Group</th>
<th>Version</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>224.0.1.40</td>
<td>v3</td>
<td>Router</td>
</tr>
<tr>
<td>2</td>
<td>224.2.2.2</td>
<td>v3</td>
<td>Fa6/2</td>
</tr>
</tbody>
</table>

Switch>

This example shows how to display the group's host types and ports in VLAN 1:

Switch#
show ip igmp snooping group vlan 1

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Group</th>
<th>Host Type</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>229.2.3.4</td>
<td>v3</td>
<td>fa2/1</td>
</tr>
<tr>
<td>1</td>
<td>224.2.2.2</td>
<td>v3</td>
<td>Fa6/2</td>
</tr>
</tbody>
</table>

Switch>

This example shows how to display the group's host types and ports in VLAN 1:

Switch#
show ip igmp snooping group vlan 10 226.6.6.7

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Group</th>
<th>Version</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>226.6.6.7</td>
<td>v3</td>
<td>Fa7/13, Fa7/14</td>
</tr>
</tbody>
</table>

Switch>

This example shows how to display the current state of a group with respect to a source IP address:

Switch#
show ip igmp snooping group vlan 10 226.6.6.7 sources

Source information for group 226.6.6.7:

Timers: Expired sources are deleted on next IGMP General Query

<table>
<thead>
<tr>
<th>SourceIP</th>
<th>Expires</th>
<th>Uptime</th>
<th>Inc Hosts</th>
<th>Exc Hosts</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.0.0.1</td>
<td>00:03:04</td>
<td>00:03:48</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>2.0.0.2</td>
<td>00:03:04</td>
<td>00:02:07</td>
<td>2</td>
<td>0</td>
</tr>
</tbody>
</table>

Switch>

This example shows how to display the current state of a group with respect to a host MAC address:

Switch#
show ip igmp snooping group vlan 10 226.6.6.7 hosts

IGMPv3 host information for group 226.6.6.7

Timers: Expired hosts are deleted on next IGMP General Query

<table>
<thead>
<tr>
<th>Host (MAC/IP)</th>
<th>Filter mode</th>
<th>Expires</th>
<th>Uptime</th>
<th># Sources</th>
</tr>
</thead>
<tbody>
<tr>
<td>175.1.0.29</td>
<td>INCLUDE</td>
<td>stopped</td>
<td>00:00:51</td>
<td>2</td>
</tr>
<tr>
<td>175.2.0.30</td>
<td>INCLUDE</td>
<td>stopped</td>
<td>00:04:14</td>
<td>2</td>
</tr>
</tbody>
</table>

Switch>

This 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>

This example shows how to display multicast router information for VLAN 1:

Switch#
show ip igmp snooping mrouter vlan 1

<table>
<thead>
<tr>
<th>vlan</th>
<th>ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>-----</td>
<td>-------</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
This example shows how to display the total number of group addresses learned by the system globally:

```
Switch# show ip igmp snooping group count
Total number of groups:   54
Switch>
```

This example shows how to display the total number of group addresses learned on VLAN 5:

```
Switch# show ip igmp snooping group vlan 5 count
Total number of groups:   30
Switch>
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip igmp snooping</td>
<td>Enable IGMP snooping.</td>
</tr>
<tr>
<td>ip igmp snooping vlan immediate-leave</td>
<td>Enable IGMP immediate-leave processing.</td>
</tr>
<tr>
<td>ip igmp snooping vlan mrouter</td>
<td>Configures a Layer 2 interface as a multicast router.</td>
</tr>
<tr>
<td>ip igmp snooping vlan static</td>
<td>Configures a Layer 2 interface as a member of a group.</td>
</tr>
<tr>
<td>show ip igmp interface</td>
<td>Displays the information about the IGMP-interface status</td>
</tr>
<tr>
<td>show ip igmp snooping mrouter</td>
<td>Displays information on the dynamically learned and manually configured multicast switch interfaces.</td>
</tr>
<tr>
<td>show mac-address-table multicast</td>
<td>Displays information about the multicast MAC address table.</td>
</tr>
</tbody>
</table>

Chapter 2  
Cisco IOS Commands for the Catalyst 4500 Series Switches

show ip igmp snooping membership

To display host membership information, use the `show ip igmp snooping membership` command.

```
[interface]
[interface_num]
[vlan]
[vlan_i d]
[reporter]
[a.b.c.d]
[source]
[a.b.c.d]
[group]
[a.b.c.d]
```

**Syntax Description**

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Usage Guidelines**

This command is valid only if explicit host tracking is enabled on the switch.

**Examples**

This example shows how to display host membership for the Gigabit Ethernet interface 4/1:

```
Switch#
show ip igmp snooping membership interface gigabitethernet4/1
#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#
```

This example shows how to display host membership for VLAN 20 and group 224.10.10:

```
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#
```

This example shows how to display host membership information for VLAN 20 and to delete the explicit host tracking:

```
Switch#
show ip igmp snooping membership vlan 20
Snooping Membership Summary for Vlan 20
------------------------------------------
Total number of channels:5
Total number of hosts   :4
```

### show ip igmp snooping membership

<table>
<thead>
<tr>
<th>Source/Group</th>
<th>Interface</th>
<th>Reporter</th>
<th>Uptime</th>
<th>Last-Join/Leave</th>
</tr>
</thead>
<tbody>
<tr>
<td>40.0.0.1/224.1.1</td>
<td>Fa7/37</td>
<td>0002.4ba0.a4f6</td>
<td>00:00:04</td>
<td>00:00:04</td>
</tr>
<tr>
<td>40.0.0.2/224.1.1</td>
<td>Fa7/37</td>
<td>0002.fd80.f770</td>
<td>00:00:17</td>
<td>00:00:17</td>
</tr>
<tr>
<td>40.0.0.3/224.1.1</td>
<td>Fa7/36</td>
<td>20.20.20.20</td>
<td>00:00:04</td>
<td>00:00:04</td>
</tr>
<tr>
<td>40.0.0.4/224.1.1</td>
<td>Fa7/35</td>
<td>20.20.20.210</td>
<td>00:00:17</td>
<td>00:00:17</td>
</tr>
<tr>
<td>40.0.0.5/224.1.1</td>
<td>Fa7/37</td>
<td>0002.fd80.f770</td>
<td>00:00:17</td>
<td>00:00:17</td>
</tr>
</tbody>
</table>

Switch#

### clear ip igmp snooping membership vlan 20

Switch#

#### Related Commands

- **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.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

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
```

**Syntax Description**

- **Syntax:** `show ip igmp snooping mrouter
```

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Usage Guidelines**

You can also use the `show mac-address-table multicast` command to display entries in the MAC address table for a VLAN that has IGMP snooping enabled.

You can display IGMP snooping information for the VLAN interfaces by entering the `show ip igmp interface` command.

**Examples**

This example shows how to display snooping information for a specific VLAN:

```
Switch# show ip igmp snooping mrouter vlan 1
vlan            ports
-----+----------------------------------------
1          Gi1/1,Gi2/1,Fa3/48,Switch
Switch#
```

**Related Commands**

- `vlan vlan-id` *(Optional)* Specifies a VLAN; valid values are from 1 to 1001 and from 1006 to 4094.
- **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**: This command has no default settings.
- **Defaults**: None.
- **Command Modes**: Privileged EXEC mode.
- **Usage Guidelines**: You can also use the `show mac-address-table multicast` command to display the entries in the MAC address table for a VLAN that has IGMP snooping enabled.

**Examples**

This example shows how to display snooping information for a specific VLAN:

```
Switch# show ip igmp snooping vlan 2
vlan 2
----------
IGMP snooping is globally enabled
IGMP snooping TCN solicit query is globally enabled
IGMP snooping global TCN flood query count is 2
IGMP snooping is enabled on this Vlan
IGMP snooping immediate-leave is disabled on this Vlan
IGMP snooping mrouter learn mode is pim-dvmrp on this Vlan
IGMP snooping is running in IGMP_ONLY mode on this Vlan
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip igmp snooping</code></td>
</tr>
<tr>
<td><code>ip igmp snooping vlan immediate-leave</code></td>
</tr>
<tr>
<td><code>ip igmp snooping vlan mrouter</code></td>
</tr>
<tr>
<td><code>ip igmp snooping vlan static</code></td>
</tr>
<tr>
<td><code>show ip igmp interface</code></td>
</tr>
<tr>
<td><code>show ip igmp snooping mrouter</code></td>
</tr>
<tr>
<td><code>show mac-address-table multicast</code></td>
</tr>
</tbody>
</table>
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**
- `type` (Optional) Interface type.
- `number` (Optional) Interface number.

**Defaults**
This command has no default settings.

**Command Modes**
EXEC

**Usage Guidelines**
The Cisco IOS software automatically enters a directly connected route in the routing table if the interface is usable. A usable interface is one through which the software can send and receive packets.

If the software determines that an interface is not usable, it removes the directly connected routing entry from the routing table. Removing the entry allows the software to use dynamic routing protocols to determine backup routes to the network, if any.

If the interface can provide two-way communication, the line protocol is marked "up." If the interface hardware is usable, the interface is marked "up."

If you specify an optional interface type, you see information only on that specific interface. If you specify no optional arguments, you see information on all the interfaces.

When an asynchronous interface is encapsulated with PPP or Serial Line Internet Protocol (SLIP), IP fast switching is enabled. The `show ip interface` command on an asynchronous interface that is encapsulated with PPP or SLIP displays a message indicating that IP fast switching is enabled.

**Examples**
This example shows how to display the 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 unreachables are always sent
ICMP mask replies are never sent
```
Table 2-19 describes the fields that are shown in the example.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet0</td>
<td>is up If the interface hardware is usable, the interface is marked “up.”</td>
</tr>
<tr>
<td>line protocol</td>
<td>is up If the interface can provide two-way communication, the line protocol</td>
</tr>
<tr>
<td></td>
<td>is marked “up.” For an interface to be usable, both the interface hardware</td>
</tr>
<tr>
<td></td>
<td>and line protocol must be up.</td>
</tr>
<tr>
<td>Internet address</td>
<td>and subnet mask IP address and subnet mask of the interface.</td>
</tr>
<tr>
<td>Broadcast address</td>
<td>Broadcast address.</td>
</tr>
<tr>
<td>Address determined</td>
<td>by... Status of how the IP address of the interface was determined.</td>
</tr>
<tr>
<td>MTU</td>
<td>MTU value that is set on the interface.</td>
</tr>
<tr>
<td>Helper address</td>
<td>Helper address, if one has been set.</td>
</tr>
<tr>
<td>Secondary address</td>
<td>Secondary address, if one has been set.</td>
</tr>
<tr>
<td>Directed broadcast</td>
<td>forwarding Status of directed broadcast forwarding.</td>
</tr>
<tr>
<td>Multicast groups</td>
<td>joined Multicast groups to which this interface belongs.</td>
</tr>
<tr>
<td>Outgoing access</td>
<td>list Status of whether the interface has an outgoing access list set.</td>
</tr>
<tr>
<td>Inbound access</td>
<td>list Status of whether the interface has an incoming access list set.</td>
</tr>
<tr>
<td>Proxy ARP</td>
<td>Status of whether Proxy Address Resolution Protocol (ARP) is enabled for the</td>
</tr>
<tr>
<td></td>
<td>interface.</td>
</tr>
<tr>
<td>Security level</td>
<td>IP Security Option (IPSO) security level set for this interface.</td>
</tr>
<tr>
<td>Split horizon</td>
<td>Status of split horizon.</td>
</tr>
</tbody>
</table>
show ip interface

ICMP redirects Status of the redirect messages on this interface.

ICMP unreachables Status of the unreachable messages on this interface.

ICMP mask replies Status of the mask replies on this interface.

IP fast switching Status of whether fast switching has been enabled for this interface. Fast switching is typically enabled on serial interfaces, such as this one.

IP SSE switching Status of the IP silicon switching engine (SSE).

Router Discovery Status of the discovery process for this interface. It is typically disabled on serial interfaces.

IP output packet accounting Status of IP accounting for this interface and the threshold (maximum number of entries).

TCP/IP header compression Status of compression.

Probe proxy name Status of whether the HP Probe proxy name replies are generated.

WCCP Redirect outbound is enabled Status of whether packets that are received on an interface are redirected to a cache engine.

WCCP Redirect exclude is disabled Status of whether packets that are targeted for an interface are excluded from being redirected to a cache engine.

Netflow Data Export (hardware) is enabled NDE hardware flow status on the interface.

Table 2-19 show ip interface Field Descriptions (continued)
Chapter 2  Cisco IOS Commands for the Catalyst 4500 Series Switches

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.

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Usage Guidelines**

The MFIB table contains a set of IP multicast routes; each route in the MFIB table contains several flags that associate to the route.

The route flags indicate how a packet that matches a route is forwarded. For example, the IC flag on 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.
show ip mfib

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

This 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip mfib counters</td>
<td>Clears the global MFIB counters and the counters for all active MFIB routes.</td>
</tr>
</tbody>
</table>
To display all currently active fast-drop entries and to show whether fast drop is enabled, use the `show ip mfib fastdrop` command.

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

**Defaults**: This command has no default settings.

**Command Modes**: Privileged EXEC mode

**Examples**: This example shows how to display 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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip mfib fastdrop</td>
<td>Clears all the MFIB fast-drop entries.</td>
</tr>
</tbody>
</table>
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**

- **Interface type** (Optional) Interface type and number of the slot and port; valid values for interface type are `fastethernet`, `gigabitethernet`, `tengigabitethernet`, null, and `vlan`.
- **Host Name** (Optional) Name or IP address as defined in the DNS hosts table.
- **Host Address** (Optional) IP address or name of a multicast source.
- **Active** (Optional) Displays the rate that active sources are sending to multicast groups.
- **Kbps** (Optional) Minimum rate at which active sources are sending to multicast groups; active sources sending at this rate or greater will be displayed. Valid values are from 1 to 4294967295 kbps.
- **Count** (Optional) Displays the route and packet count information.
- **Pruned** (Optional) Displays the pruned routes.
- **Static** (Optional) Displays the static multicast routes.
- **Summary** (Optional) Displays a one-line, abbreviated summary of each entry in the IP multicast routing table.

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Usage Guidelines**

If you 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)).
This example shows how to display the rate that the active sources are sending to the multicast groups and to display only the active sources that are sending at greater than the default rate:

Switch# show ip 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#

This example shows how to display route and packet count information:

Switch# show ip mroute count

IP Multicast Statistics
56 routes using 28552 bytes of memory
13 groups, 3.30 average sources per group
Forwarding Counts:Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other 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#
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

show ip mroute

This 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

Outgoing interface flags: H - Hardware switched

Timers: Uptime/Expires

Interface state: Interface, Next-Hop or VCD, State/Mode

Switch#

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flags</td>
<td>Information about the entry.</td>
</tr>
<tr>
<td>D</td>
<td>Dense Entry is operating in dense mode.</td>
</tr>
<tr>
<td>S</td>
<td>Sparse Entry is operating in sparse mode.</td>
</tr>
<tr>
<td>s</td>
<td>SSM Group Entry is a member of an SSM group.</td>
</tr>
<tr>
<td>C</td>
<td>Connected Member of the multicast group is present on the directly connected interface.</td>
</tr>
<tr>
<td>L</td>
<td>Local Switch is a member of the multicast group.</td>
</tr>
<tr>
<td>P</td>
<td>Pruned Route has been pruned. This information is retained in case a downstream member wants to join the source.</td>
</tr>
<tr>
<td>R</td>
<td>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.</td>
</tr>
<tr>
<td>F</td>
<td>Register flag Status of the software; indicates if the software is registered for a multicast source.</td>
</tr>
<tr>
<td>T</td>
<td>SPT-bit set Status of the packets; indicates if the packets been received on the shortest path source tree.</td>
</tr>
</tbody>
</table>
show ip mroute

J - Join SPT 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.

For (S, G) entries, indicates that the entry was created because the SPT-Threshold for the group was exceeded. When the J-Join SPT flag is set for (S,G) entries, the switch monitors the traffic rate on the source tree and attempts to switch back to the shared tree for this source if the traffic rate on the source tree falls below the group's SPT-Threshold for more than one minute.

The switch measures the traffic rate on the shared tree and compares 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.

If the default SPT-Threshold value of 0 Kbps is used for the group, the J-Join SPT flag is always set on (*, G) entries and is never cleared. When the default SPT-Threshold value is used, the switch immediately switches to the shortest-path tree when traffic from a new source is received.

Outgoing interface flag: Information about the outgoing entry.

H - Hardware switched Entry is 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)

Entry in the IP multicast routing table. The entry consists of the IP address of the source switch followed by the IP address of the multicast group. An asterisk (*) in place of the source switch indicates all sources.

Entries in the first format are referred to as (*,G) or "star comma G" entries. Entries in the second format are referred to as (S,G) or "S comma G" entries. (*,G) entries are used to build (S,G) entries.

uptime How long (in hours, minutes, and seconds) the entry has been in the IP multicast routing table.

expires How long (in hours, minutes, and seconds) until the entry is removed from the IP multicast routing table on the outgoing interface.
**show ip mroute**

**Related Commands**

- **RP Address**: 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**: 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**: Status of the packets; indicates if they are 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**: 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.

**Table 2-20 show ip mroute Field Descriptions (continued)**

**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.
To display IP source bindings that are configured on the system, use the `show ip source binding` EXEC command.

```
show ip source binding [ip-address] [mac-address] [dhcp-snooping | static] [vlan vlan-id] [interface interface-name]
```

**Syntax Description**
- `ip-address`: Binding IP address.
- `mac-address`: Binding MAC address.
- `dhcp-snooping`: DHCP-snooping type binding.
- `static`: Statically configured binding.
- `vlan vlan-id`: VLAN number.
- `interface interface-name`: Binding interface.

**Defaults**
Displays both static and DHCP snooping bindings.

**Command Modes**
Privileged EXEC mode

**Usage Guidelines**
The optional parameters filter the display output result.

**Examples**
This example shows how to display the IP source bindings:
```
Switch# show ip source binding
```
```
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:00:00:0A:00:0B   11.0.0.1         infinite    static         10    FastEthernet6/10
```
```
Switch#
```
This example shows how to display the static IP binding entry of IP address 11.0.0.1:
```
Switch# 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**
- `ip-address`: (Optional) Binding IP address.
- `mac-address`: (Optional) Binding MAC address.
- `dhcp-snooping`: (Optional) DHCP-snooping type binding.
- `static`: (Optional) Statically configured binding.
- `vlan vlan-id`: (Optional) VLAN number.
- `interface interface-name`: (Optional) Binding interface.

**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

This command has no default settings.

Command Modes

Privileged EXEC mode

Examples

These examples show how to display the IP source guard configuration and filters on a particular interface with the `show ip verify source interface` command:

1. 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:

<table>
<thead>
<tr>
<th>Interface</th>
<th>Filter-type</th>
<th>Filter-mode</th>
<th>IP-address</th>
<th>Mac-address</th>
<th>Vlan</th>
</tr>
</thead>
<tbody>
<tr>
<td>fa6/1</td>
<td>ip</td>
<td>active</td>
<td>10.0.0.1</td>
<td></td>
<td>10</td>
</tr>
<tr>
<td>fa6/1</td>
<td>ip</td>
<td>active</td>
<td>deny-all</td>
<td></td>
<td>11-20</td>
</tr>
</tbody>
</table>

   Note: The second entry shows that a default PV ACL (deny all IP traffic) is installed on the port for those snooping-enabled VLANs that do not have a valid IP source binding.

2. 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:

<table>
<thead>
<tr>
<th>Interface</th>
<th>Filter-type</th>
<th>Filter-mode</th>
<th>IP-address</th>
<th>Mac-address</th>
<th>Vlan</th>
</tr>
</thead>
<tbody>
<tr>
<td>fa6/2</td>
<td>ip</td>
<td>inactive-trust-port</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3. 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:

<table>
<thead>
<tr>
<th>Interface</th>
<th>Filter-type</th>
<th>Filter-mode</th>
<th>IP-address</th>
<th>Mac-address</th>
<th>Vlan</th>
</tr>
</thead>
<tbody>
<tr>
<td>fa6/3</td>
<td>ip</td>
<td>inactive-no-snooping-vlan</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4. 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:

<table>
<thead>
<tr>
<th>Interface</th>
<th>Filter-type</th>
<th>Filter-mode</th>
<th>IP-address</th>
<th>Mac-address</th>
<th>Vlan</th>
</tr>
</thead>
<tbody>
<tr>
<td>fa6/4</td>
<td>ip-mac</td>
<td>active</td>
<td>10.0.0.2</td>
<td>aaaa.bbbb.cccc</td>
<td>10</td>
</tr>
</tbody>
</table>

```
interface
interface_num
```
Chapter 2
Cisco IOS Commands for the Catalyst 4500 Series Switches

show ip verify source

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.ccce on VLAN 10, but port security is not enabled on fa6/5:

<table>
<thead>
<tr>
<th>Interface</th>
<th>Filter-type</th>
<th>Filter-mode</th>
<th>IP-address</th>
<th>Mac-address</th>
<th>Vlan</th>
</tr>
</thead>
<tbody>
<tr>
<td>fa6/5</td>
<td>ip-mac</td>
<td>active</td>
<td>10.0.0.3</td>
<td>permit-all</td>
<td>10</td>
</tr>
<tr>
<td>fa6/5</td>
<td>ip-mac</td>
<td>active</td>
<td>deny-all</td>
<td>permit-all</td>
<td>11-20</td>
</tr>
</tbody>
</table>

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.

This example shows how to display all the interfaces on the switch that have DHCP snooping security and IP Port Security tracking enabled with the `show ip verify source` command.

The output is an accumulation of per-interface `show` CLIs:

<table>
<thead>
<tr>
<th>Interface</th>
<th>Filter-type</th>
<th>Filter-mode</th>
<th>IP-address</th>
<th>Mac-address</th>
</tr>
</thead>
<tbody>
<tr>
<td>fa6/1</td>
<td>ip</td>
<td>active</td>
<td>10.0.0.1</td>
<td></td>
</tr>
<tr>
<td>fa6/1</td>
<td>ip</td>
<td>active</td>
<td>deny-all</td>
<td></td>
</tr>
<tr>
<td>fa6/2</td>
<td>ip trk</td>
<td>inactive-trust-port</td>
<td></td>
<td></td>
</tr>
<tr>
<td>fa6/3</td>
<td>ip trk</td>
<td>active</td>
<td>40.1.1.24</td>
<td></td>
</tr>
<tr>
<td>fa6/3</td>
<td>ip trk</td>
<td>active</td>
<td>40.1.1.20</td>
<td></td>
</tr>
<tr>
<td>fa6/3</td>
<td>ip trk</td>
<td>active</td>
<td>40.1.1.21</td>
<td></td>
</tr>
<tr>
<td>fa6/4</td>
<td>ip-mac</td>
<td>active</td>
<td>10.0.0.2</td>
<td>aaaa.bbbb.cccc</td>
</tr>
<tr>
<td>fa6/4</td>
<td>ip-mac</td>
<td>active</td>
<td>11.0.0.1</td>
<td>aaaa.bbbb.cccd</td>
</tr>
<tr>
<td>fa6/4</td>
<td>ip-mac</td>
<td>active</td>
<td>deny-all</td>
<td>deny-all</td>
</tr>
<tr>
<td>fa6/5</td>
<td>ip-mac</td>
<td>active</td>
<td>10.0.0.3</td>
<td>permit-all</td>
</tr>
<tr>
<td>fa6/5</td>
<td>ip-mac</td>
<td>active</td>
<td>deny-all</td>
<td>permit-all</td>
</tr>
</tbody>
</table>

Related Commands

- `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 (#)

**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.

**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

The following is sample output from the `show ip wccp` 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 21 describes the significant fields shown in the display:

<table>
<thead>
<tr>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router information A list of routers detected by the current router.</td>
</tr>
<tr>
<td>Protocol Version The version of WCCP being used by the router in the service group.</td>
</tr>
<tr>
<td>Service Identifier Indicates which service is detailed.</td>
</tr>
<tr>
<td>Number of Service Group Clients: The number of clients that are visible to the router and other clients in the service group.</td>
</tr>
<tr>
<td>Number of Service Group Routers The number of routers in the service group.</td>
</tr>
<tr>
<td>Total Packets s/w Redirected Total number of packets s/w redirected by the router.</td>
</tr>
<tr>
<td>Redirect Access-list The name or number of the access list that determines which packets will be redirected.</td>
</tr>
<tr>
<td>Total Packets Denied Redirect Total number of packets that were not redirected because they did not match the access list.</td>
</tr>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>
Chapter 2      Cisco IOS Commands for  the Catalyst 4500 Series Switches

**show ip wccp**

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 22 describes the significant fields shown in the display.

**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
Group Access-list Indicates which cache engine is allowed to connect to the router.
Total Messages Denied to Group Indicates the number of packets denied by the group-list access list.
Total Authentication failures The number of instances where a password did not match.
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.
```

Table 21 show ip wccp service-number Field Descriptions (continued)

<table>
<thead>
<tr>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCCP Router Informed of A list of routers detected by the current router.</td>
</tr>
<tr>
<td>WCCP Clients Visible A list of clients that are visible to the router and other clients in the service group.</td>
</tr>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>
show ip wccp

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 |

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 23 describes the significant fields shown in the display:

<table>
<thead>
<tr>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output services</td>
</tr>
<tr>
<td>Input services</td>
</tr>
<tr>
<td>Mcast services</td>
</tr>
<tr>
<td>Exclude In</td>
</tr>
</tbody>
</table>

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

Table 23 show ip wccp interfaces Field Descriptions

<table>
<thead>
<tr>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output services</td>
</tr>
<tr>
<td>Input services</td>
</tr>
<tr>
<td>Mcast services</td>
</tr>
<tr>
<td>Exclude In</td>
</tr>
</tbody>
</table>
show ip wccp

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 24 describes the significant fields shown in the display.

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

<table>
<thead>
<tr>
<th>Value</th>
<th>SrcAddr</th>
<th>DstAddr</th>
<th>SrcPort</th>
<th>DstPort</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000:</td>
<td>0x00000000</td>
<td>0x00000001</td>
<td>0x0000</td>
<td>0x0000</td>
</tr>
</tbody>
</table>

Table 24 show ip wccp web-cache Field Descriptions

<table>
<thead>
<tr>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol Version</td>
</tr>
<tr>
<td>Service Identifier</td>
</tr>
<tr>
<td>Number of Service Group Clients</td>
</tr>
<tr>
<td>Number of Service Group Routers</td>
</tr>
<tr>
<td>Total Packets s/w Redirected</td>
</tr>
<tr>
<td>Redirect access-list</td>
</tr>
<tr>
<td>Total Packets Denied Redirect</td>
</tr>
<tr>
<td>Total Packets Unassigned</td>
</tr>
<tr>
<td>Group access-list</td>
</tr>
<tr>
<td>Total Messages Denied to Group</td>
</tr>
<tr>
<td>Total Authentication failures</td>
</tr>
</tbody>
</table>
show ip wccp

Table 25 describes the significant fields shown in the display.

```
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
  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
```

Table 25 show ip wccp web-cache detail Field Descriptions

<table>
<thead>
<tr>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCCP Client Information</td>
</tr>
<tr>
<td>WCCP Client ID</td>
</tr>
<tr>
<td>Protocol Version</td>
</tr>
<tr>
<td>State</td>
</tr>
<tr>
<td>Packets Redirected</td>
</tr>
<tr>
<td>Connect Time</td>
</tr>
</tbody>
</table>
show ip wccp

Total Bypassed Packets Received:     0

Related Commands

- 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.
To display IPC information, use the `show ipc` command.

```
show ipc {nodes | ports | queue | status}
```

**Syntax Description**

- **nodes**: Displays the participating nodes.
- **ports**: Displays the local IPC ports.
- **queue**: Displays the contents of the IPC retransmission queue.
- **status**: Displays the status of the local IPC server.

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Examples**

This example shows how to display the participating nodes:

```
Switch# show ipc nodes
There are 3 nodes in this IPC realm.
ID     Type                 Name                       Last  Last
Sent  Heard
10000 Local      IPC Master                               0      0
2010000 Local      GALIOS IPC:Card 1                        0      0
2020000 Ethernet   GALIOS IPC:Card 2                        12     26
Switch#
```

This example shows how to display the local IPC ports:

```
Switch# show ipc ports
There are 11 ports defined.
Port ID        Type       Name                 (current/peak/total)
10000.1     unicast    IPC Master: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#
```
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.

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 snooping counters

To display the number of packets dropped per port due to RA Guard, use the `show ipv6 snooping counters` command.

**Syntax Description**

**Defaults**

None

**Command Modes**

Interface mode

**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**

- **interface**
  - Specifies the interface.
  - Command Description
  - epm access control
    Configures access control.
To display IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping configuration of the switch or the VLAN, use the `show ipv6 mld snooping` command.

```
show ipv6 mld snooping [vlan vlan-id]
```

**Syntax Description**

- `vlan vlan-id` (Optional) Specifies a VLAN; the range is 1 to 1001 and 1006 to 4094.

**Command Modes**

- User EXEC mode

**Usage Guidelines**

Use this command to display MLD snooping configuration for the switch or for a specific VLAN. VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in MLD snooping.

**Examples**

This is an example of output from the `show ipv6 mld snooping vlan` command. It shows snooping characteristics for a specific VLAN.

```
Switch> show ipv6 mld snooping vlan 100
Global MLD Snooping configuration:  
-------------------------------------------
MLD snooping                  : Enabled
MLDv2 snooping (minimal)      : Enabled
Listener message suppression  : Enabled
TCN solicit query             : Disabled
TCN flood query count         : 2
Robustness variable           : 3
Last listener query count     : 2
Last listener query interval  : 1000
Vlan 100:  
--------
MLD snooping                        : Disabled
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
```
show ipv6 mld snooping

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
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
ip v6 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.

**Syntax Description**

**Command Modes**

User EXEC mode

**Usage Guidelines**

Use this command to display MLD snooping switch ports for the switch or for a specific VLAN.

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

**Examples**

This is an example of output from the `show ipv6 mld snooping mrouter` command. It displays snooping characteristics for all VLANs on the switch that are participating in MLD snooping.

```
Switch> show ipv6 mld snooping mrouter
Vlan    ports
----    -----  
2    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**

`vlan vlan-id` (Optional) Specifies a VLAN; the range is 1 to 1001 and 1006 to 4094.

`ipv6 mld snooping` Command Description

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.
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**
- **Command Modes**: User EXEC mode

**Usage Guidelines**
- Use the `show ipv6 mld snooping querier` command to display the MLD version and IPv6 address of a detected device that sends MLD query messages, which is also called a querier. A subnet can have multiple multicast switches but has only one MLD querier. The querier can be a Layer 3 switch.
- The `show ipv6 mld snooping querier` command output also shows the VLAN and interface on which the querier was detected. If the querier is the switch, the output shows the Port field as Router. If the querier is a router, the output shows the port number on which the querier is learned in the Port field.
- The output of the `show ipv6 mld snooping querier vlan` command displays the information received in response to a query message from an external or internal querier. It does not display 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
```
show ipv6 mld snooping querier

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) MLD snooping 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).
Chapter 2  Cisco IOS Commands for the Catalyst 4500 Series Switches

show issu capability

To display the ISSU capability for a client, use the `show issu capability` command.

```
show issu capability {entries | groups | types} [client_id]
```

**Syntax Description**

- **entries**: Displays a list of Capability Types and Dependent Capability Types that are included in a single Capability Entry. Types within an entry can also be independent.
- **groups**: Displays a list of Capability Entries in priority order (the order that they will be negotiated on a session).
- **types**: Displays an ID that identifies a particular capability.
- **client_id** (Optional): Identifies the client registered to the ISSU infrastructure. To obtain a list of client IDs, use the `show issu clients` command.

**Defaults**

This command has no default settings.

**Command Modes**

User EXEC mode

**Usage Guidelines**

Capability is a functionality that an ISSU client can support and is required to interoperate with peers. When an ISSU-aware client establishes its session with the peer, an ISSU negotiation takes place. The ISSU infrastructure uses the 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 :
```

## Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

### Command Description

<table>
<thead>
<tr>
<th>Related Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show issu clients</td>
<td>Displays the ISSU clients.</td>
</tr>
</tbody>
</table>
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

*show issu clients*

To display the ISSU clients, use the `show issu clients` command.

```plaintext
[peer_uid]
```

**Syntax Description**

**Defaults**

Displays a list of clients registered to the ISSU infrastructure at the supervisor engine where the command is entered.

**Command Modes**

User EXEC mode

**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
```
### show issu clients

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

### Related Commands

- **show issu capability**
  Displays the ISSU capability for a client.
- **show issu entities**
  Displays the ISSU entity information.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

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**

This command has no default settings.

**Defaults**

This command has no default settings.

**Command Modes**

User EXEC mode

**Usage Guidelines**

Before attempting an ISSU, you should know the compatibility level between the old and the new Cisco IOS software versions on the active and the standby supervisor engines. ISSU will not work if the two versions are incompatible.

The compatibility matrix is available on Cisco.com so that you can also view in advance whether an upgrade 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:

1. **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.
2. **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.
3. **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.

**negotiated**

Displays negotiated compatibility matrix information.

**stored**

Displays stored compatibility matrix information.

**xml**

Displays negotiated compatibility matrix information in XML format.
show issu comp-matrix

Examples

This example displays negotiated compatibility matrix information:

Switch# show issu comp-matrix negotiated

<table>
<thead>
<tr>
<th>Cid</th>
<th>Eid</th>
<th>Sid</th>
<th>pSid</th>
<th>pUid</th>
<th>Compatibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1</td>
<td>262151</td>
<td>3</td>
<td>1</td>
<td>COMPATIBLE</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>262160</td>
<td>5</td>
<td>1</td>
<td>COMPATIBLE</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>262163</td>
<td>9</td>
<td>1</td>
<td>COMPATIBLE</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>262186</td>
<td>25</td>
<td>1</td>
<td>COMPATIBLE</td>
</tr>
<tr>
<td>7</td>
<td>1</td>
<td>262156</td>
<td>10</td>
<td>1</td>
<td>COMPATIBLE</td>
</tr>
<tr>
<td>8</td>
<td>1</td>
<td>262148</td>
<td>7</td>
<td>1</td>
<td>COMPATIBLE</td>
</tr>
<tr>
<td>9</td>
<td>1</td>
<td>262155</td>
<td>1</td>
<td>1</td>
<td>COMPATIBLE</td>
</tr>
<tr>
<td>10</td>
<td>1</td>
<td>262158</td>
<td>2</td>
<td>1</td>
<td>COMPATIBLE</td>
</tr>
<tr>
<td>11</td>
<td>1</td>
<td>262172</td>
<td>6</td>
<td>1</td>
<td>COMPATIBLE</td>
</tr>
<tr>
<td>100</td>
<td>1</td>
<td>262166</td>
<td>13</td>
<td>1</td>
<td>COMPATIBLE</td>
</tr>
<tr>
<td>110</td>
<td>113</td>
<td>262159</td>
<td>14</td>
<td>1</td>
<td>COMPATIBLE</td>
</tr>
<tr>
<td>200</td>
<td>1</td>
<td>262167</td>
<td>24</td>
<td>1</td>
<td>COMPATIBLE</td>
</tr>
<tr>
<td>2002</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>UNAVAILABLE</td>
</tr>
<tr>
<td>2003</td>
<td>1</td>
<td>262185</td>
<td>23</td>
<td>1</td>
<td>COMPATIBLE</td>
</tr>
<tr>
<td>2004</td>
<td>1</td>
<td>262175</td>
<td>16</td>
<td>1</td>
<td>COMPATIBLE</td>
</tr>
<tr>
<td>2008</td>
<td>1</td>
<td>262147</td>
<td>26</td>
<td>1</td>
<td>COMPATIBLE</td>
</tr>
<tr>
<td>2008</td>
<td>1</td>
<td>262168</td>
<td>27</td>
<td>1</td>
<td>COMPATIBLE</td>
</tr>
<tr>
<td>2010</td>
<td>1</td>
<td>262171</td>
<td>32</td>
<td>1</td>
<td>COMPATIBLE</td>
</tr>
<tr>
<td>2012</td>
<td>1</td>
<td>262180</td>
<td>31</td>
<td>1</td>
<td>COMPATIBLE</td>
</tr>
<tr>
<td>2021</td>
<td>1</td>
<td>262170</td>
<td>41</td>
<td>1</td>
<td>COMPATIBLE</td>
</tr>
<tr>
<td>2022</td>
<td>1</td>
<td>262152</td>
<td>42</td>
<td>1</td>
<td>COMPATIBLE</td>
</tr>
<tr>
<td>2023</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>UNAVAILABLE</td>
</tr>
<tr>
<td>2024</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>UNAVAILABLE</td>
</tr>
<tr>
<td>2025</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>UNAVAILABLE</td>
</tr>
<tr>
<td>2026</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>UNAVAILABLE</td>
</tr>
<tr>
<td>2027</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>UNAVAILABLE</td>
</tr>
<tr>
<td>2028</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>UNAVAILABLE</td>
</tr>
<tr>
<td>2054</td>
<td>1</td>
<td>262169</td>
<td>8</td>
<td>1</td>
<td>COMPATIBLE</td>
</tr>
<tr>
<td>2058</td>
<td>1</td>
<td>262154</td>
<td>29</td>
<td>1</td>
<td>COMPATIBLE</td>
</tr>
<tr>
<td>2059</td>
<td>1</td>
<td>262179</td>
<td>30</td>
<td>1</td>
<td>COMPATIBLE</td>
</tr>
<tr>
<td>2067</td>
<td>1</td>
<td>262153</td>
<td>12</td>
<td>1</td>
<td>COMPATIBLE</td>
</tr>
<tr>
<td>2068</td>
<td>1</td>
<td>196638</td>
<td>40</td>
<td>1</td>
<td>COMPATIBLE</td>
</tr>
<tr>
<td>2070</td>
<td>1</td>
<td>262145</td>
<td>21</td>
<td>1</td>
<td>COMPATIBLE</td>
</tr>
<tr>
<td>2071</td>
<td>1</td>
<td>262178</td>
<td>11</td>
<td>1</td>
<td>COMPATIBLE</td>
</tr>
<tr>
<td>2072</td>
<td>1</td>
<td>262162</td>
<td>28</td>
<td>1</td>
<td>COMPATIBLE</td>
</tr>
<tr>
<td>2073</td>
<td>1</td>
<td>262177</td>
<td>33</td>
<td>1</td>
<td>COMPATIBLE</td>
</tr>
<tr>
<td>2077</td>
<td>1</td>
<td>262165</td>
<td>35</td>
<td>1</td>
<td>COMPATIBLE</td>
</tr>
<tr>
<td>2078</td>
<td>1</td>
<td>196637</td>
<td>34</td>
<td>1</td>
<td>COMPATIBLE</td>
</tr>
<tr>
<td>2079</td>
<td>1</td>
<td>262176</td>
<td>36</td>
<td>1</td>
<td>COMPATIBLE</td>
</tr>
<tr>
<td>2081</td>
<td>1</td>
<td>262150</td>
<td>37</td>
<td>1</td>
<td>COMPATIBLE</td>
</tr>
<tr>
<td>2082</td>
<td>1</td>
<td>262161</td>
<td>39</td>
<td>1</td>
<td>COMPATIBLE</td>
</tr>
<tr>
<td>2083</td>
<td>1</td>
<td>262184</td>
<td>20</td>
<td>1</td>
<td>COMPATIBLE</td>
</tr>
<tr>
<td>2084</td>
<td>1</td>
<td>262183</td>
<td>38</td>
<td>1</td>
<td>COMPATIBLE</td>
</tr>
<tr>
<td>4001</td>
<td>101</td>
<td>262181</td>
<td>17</td>
<td>1</td>
<td>COMPATIBLE</td>
</tr>
<tr>
<td>4002</td>
<td>201</td>
<td>262164</td>
<td>18</td>
<td>1</td>
<td>COMPATIBLE</td>
</tr>
<tr>
<td>4003</td>
<td>301</td>
<td>262182</td>
<td>19</td>
<td>1</td>
<td>COMPATIBLE</td>
</tr>
<tr>
<td>4004</td>
<td>401</td>
<td>262146</td>
<td>22</td>
<td>1</td>
<td>COMPATIBLE</td>
</tr>
<tr>
<td>4005</td>
<td>1</td>
<td>262149</td>
<td>4</td>
<td>1</td>
<td>COMPATIBLE</td>
</tr>
</tbody>
</table>

Message group summary:

<table>
<thead>
<tr>
<th>Cid</th>
<th>Eid</th>
<th>GrpId</th>
<th>Sid</th>
<th>pSid</th>
<th>pUid</th>
<th>Nego Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1</td>
<td>1</td>
<td>262151</td>
<td>3</td>
<td>1</td>
<td>Y</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>1</td>
<td>262160</td>
<td>5</td>
<td>1</td>
<td>Y</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>1</td>
<td>262163</td>
<td>9</td>
<td>1</td>
<td>Y</td>
</tr>
</tbody>
</table>
# List of Clients

<table>
<thead>
<tr>
<th>Cid</th>
<th>Client Name</th>
<th>Base/Non-Base</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>ISSU Proto client</td>
<td>Base</td>
</tr>
<tr>
<td>3</td>
<td>ISSU RF</td>
<td>Base</td>
</tr>
<tr>
<td>4</td>
<td>ISSU CF client</td>
<td>Base</td>
</tr>
<tr>
<td>5</td>
<td>ISSU Network RF client</td>
<td>Base</td>
</tr>
<tr>
<td>7</td>
<td>ISSU CONFIG SYNC</td>
<td>Base</td>
</tr>
<tr>
<td>8</td>
<td>ISSU ifIndex sync</td>
<td>Base</td>
</tr>
<tr>
<td>9</td>
<td>ISSU IPC client</td>
<td>Base</td>
</tr>
<tr>
<td>10</td>
<td>ISSU IPC Server client</td>
<td>Base</td>
</tr>
<tr>
<td>11</td>
<td>ISSU Red Mode Client</td>
<td>Base</td>
</tr>
<tr>
<td>100</td>
<td>ISSU rfs client</td>
<td>Base</td>
</tr>
<tr>
<td>110</td>
<td>ISSU ifs client</td>
<td>Base</td>
</tr>
<tr>
<td>200</td>
<td>ISSU Event Manager client</td>
<td>Base</td>
</tr>
<tr>
<td>2002</td>
<td>CEF Push ISSU client</td>
<td>Base</td>
</tr>
<tr>
<td>2003</td>
<td>ISSU XDR client</td>
<td>Base</td>
</tr>
<tr>
<td>2004</td>
<td>ISSU SNMP client</td>
<td>Non-Base</td>
</tr>
<tr>
<td>4001</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4002</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4003</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4004</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4005</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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.
To display the ISSU endpoint information, use the `show issu endpoints` command.

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

**Defaults**
This command has no default settings.

**Command Modes**
User EXEC mode

**Usage Guidelines**
Endpoint is an execution unit within a redundancy domain. There are only 2 endpoints on the Catalyst 4500 series switch redundant chassis: 1 and 2. The endpoints correspond to the slot numbers for the supervisor engine. The ISSU infrastructure communicates between these two endpoints to establish 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**
- `show issu clients` Displays the ISSU clients.
To display the ISSU entity information, use the `show issu entities` command.

```
show issu entities [client_id]
```

**Syntax Description**

- `client_id` (Optional) ISSU client ID.

**Defaults**

This command has no default settings.

**Command Modes**

Use in EXEC mode.

**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**

- `show issu clients` Displays the ISSU clients.
To display the ISSU finite state machine (FSM) information corresponding to an ISSU session, use the `show issu fsm` command.

`show issu fsm [session_id]`

**Syntax Description**

- **session_id** (Optional): Provides detailed information about the FSM for the specified session.

**Defaults**

This command has no default settings.

**Command Modes**

User EXEC mode

**Examples**

The following example displays and verifies the ISSU state after LOADVERSION:

```
Switch# show issu fsm 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**

- `show issu clients`: Displays the ISSU clients.
- `show issu sessions`: Displays ISSU session information for a specified client.
To display checkpoint messages for a specified ISSU client, use the `show issu message` command.

```
show issu message [groups | types] [client_id]
```

**Syntax Description**

- **Defaults**: If client ID is not specified, displays message groups or message types information for all clients registered to the ISSU infrastructure.

**Command Modes**: Use r EXEC mode

**Usage Guidelines**

Messages are sync-data (also known as checkpoint data) sent between two endpoints. When an ISSU-aware client establishes its session with a peer, an ISSU negotiation takes place. The ISSU infrastructure uses the registered information to negotiate the capabilities and the message version to be used during the session.

**Examples**

The following example shows how to display the message 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#
```

**Related Commands**

- `show issu clients`: Displays the ISSU clients.
To display the negotiated capability and message version information of the ISSU clients, use the `show issu negotiated` command.

```
show issu negotiated
```

**Syntax Description**

- `capability` (Optional) Displays negotiated capability information.
- `version` (Optional) Displays negotiated version information.
- `session_id` (Optional) Specifies the ISSU session ID for which the capability or version information is displayed.

**Defaults**

Displays negotiated capability or version information for all ISSU sessions.

**Command Modes**

User EXEC mode

**Examples**

The following example shows how to display the message types for a specific group:

```
Switch# show issu negotiated capability 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**

- `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 Description**

- `show issu sessions` Displays ISSU session information for a specified client.
To display ISSU rollback-timer status, use the `show issu rollback-timer` command.

Syntax Description
This command has no arguments or keywords.

Defaults
This command has no default settings.

Command Modes
Privledged EXEC mode

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
- `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.
To display ISSU session information for a specified client, use the `show issu sessions` command.

```
show issu sessions [client_id]
```

**Syntax Description**

- `client_id` (Optional) Specifies the ISSU client ID.

**Defaults**

Displays session information for all clients registered to the ISSU infrastructure.

**Command Modes**

User EXEC mode

**Usage Guidelines**

Session is bidirectional and a reliable connection is established between two endpoints. Sync-data and negotiation messages are sent to the peer 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**

- `show issu clients` Displays the ISSU clients.
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**

- **Defaults**: The command displays the ISSU state and current booted image name of both the active and standby supervisor engines.

- **Command Modes**: Privileged EXEC mode

**Usage Guidelines**

It might take several seconds after the `issu loadversion` command is entered for Cisco IOS software to load onto the standby supervisor engine and the standby supervisor engine to 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#
```
### Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>issu abortversion</td>
<td>Cancels the ISSU upgrade or the downgrade process and restores the switch</td>
</tr>
<tr>
<td></td>
<td>to its state before the start of the process.</td>
</tr>
<tr>
<td>issu acceptversion</td>
<td>Halts the rollback timer and ensures that the new Cisco IOS software image</td>
</tr>
<tr>
<td></td>
<td>is not automatically stopped during the ISSU process.</td>
</tr>
<tr>
<td>issu commitversion</td>
<td>Loads the new Cisco IOS software image into the new standby supervisor</td>
</tr>
<tr>
<td></td>
<td>engine.</td>
</tr>
<tr>
<td>issu loadversion</td>
<td>Starts the ISSU process.</td>
</tr>
<tr>
<td>issu runversion</td>
<td>Forces a change from the active supervisor engine to the standby supervisor</td>
</tr>
<tr>
<td></td>
<td>engine and causes the newly active supervisor engine to run the new image</td>
</tr>
<tr>
<td></td>
<td>specified.</td>
</tr>
</tbody>
</table>
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
```

**Syntax Description**

**Command Modes**

Use in EXEC mode

**Usage Guidelines**

After enabling Layer 2 protocol tunneling on an access or 802.1Q tunnel port with the `l2protocol-tunnel` command, you can configure some or all of these parameters:

- Protocol type to be tunneled
- Shut down threshold
- Drop threshold

If you enter the `show l2protocol-tunnel` 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
```

**interface**

(Optional) Specifies the interface for which protocol tunneling information appears. Valid interfaces are physical ports and port channels; the port channel range is 1 to 64.

**summary**

(Optional) Displays only Layer 2 protocol summary information.

**begin**

(Optional) Displays information beginning with the line that matches the expression.

**exclude**

(Optional) Displays information that excludes lines that match the expression.

**include**

(Optional) Displays the lines that match the specified expression.

**expression**

(Optional) Expression in the output to use as a reference point.
This is an example of output from the `show l2protocol-tunnel summary` command:

```
Switch> show l2protocol-tunnel summary
COS for Encapsulated Packets: 5

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Shutdown</th>
<th>Drop</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Threshold</td>
<td>Threshold</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(cdp/stp/vtp)</td>
<td>(cdp/stp/vtp)</td>
<td>(pagp/lacp/udld)</td>
<td>(pagp/lacp/udld)</td>
</tr>
<tr>
<td>Fa0/10</td>
<td>---</td>
<td>stp</td>
<td>vtp</td>
<td>up</td>
</tr>
<tr>
<td></td>
<td></td>
<td>---/----/----</td>
<td>---/----/----</td>
<td>--/----/----</td>
</tr>
<tr>
<td>Fa0/11</td>
<td>cdp</td>
<td>stp</td>
<td>vtp</td>
<td>up</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1100/1100/1100</td>
<td>----/----/----</td>
<td>900/ 900/ 900</td>
</tr>
<tr>
<td>Fa0/12</td>
<td>cdp</td>
<td>stp</td>
<td>vtp</td>
<td>up</td>
</tr>
<tr>
<td></td>
<td></td>
<td>----/----/----</td>
<td>----/----/----</td>
<td>----/----/----</td>
</tr>
<tr>
<td>Fa0/13</td>
<td>cdp</td>
<td>stp</td>
<td>vtp</td>
<td>up</td>
</tr>
<tr>
<td></td>
<td></td>
<td>----/----/----</td>
<td>----/----/----</td>
<td>----/----/----</td>
</tr>
<tr>
<td>Fa0/14</td>
<td>cdp</td>
<td>stp</td>
<td>vtp</td>
<td>down</td>
</tr>
<tr>
<td></td>
<td></td>
<td>----/----/----</td>
<td>----/----/----</td>
<td>----/----/----</td>
</tr>
<tr>
<td>Fa0/15</td>
<td>cdp</td>
<td>stp</td>
<td>vtp</td>
<td>down</td>
</tr>
<tr>
<td></td>
<td></td>
<td>----/----/----</td>
<td>----/----/----</td>
<td>----/----/----</td>
</tr>
<tr>
<td>Fa0/16</td>
<td>cdp</td>
<td>stp</td>
<td>vtp</td>
<td>down</td>
</tr>
<tr>
<td></td>
<td></td>
<td>----/----/----</td>
<td>----/----/----</td>
<td>----/----/----</td>
</tr>
<tr>
<td>Fa0/17</td>
<td>cdp</td>
<td>stp</td>
<td>vtp</td>
<td>down</td>
</tr>
<tr>
<td></td>
<td></td>
<td>----/----/----</td>
<td>----/----/----</td>
<td>----/----/----</td>
</tr>
</tbody>
</table>

Switch#```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>l2protocol-tunnel</td>
<td>Enables protocol tunneling on an interface.</td>
</tr>
<tr>
<td>l2protocol-tunnel cos</td>
<td>Configures the class of service (CoS) value for all tunneled Layer 2 protocol packets.</td>
</tr>
</tbody>
</table>
To display LACP information, use the `show lacp` command.

```
show lacp [channel-group] {counters | internal | neighbors | sys-id}
```

**Syntax Description**

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

This example shows how to display LACP statistical information for a specific channel group:

```
Switch# show lacp 1 counters
```

```
LACPDUs Marker LACPDUs  
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 0  
Fa4/4 13 18 0 0 0 0  
```

The output displays the following information:

- The LACPUs Sent and Recv columns display the LACPUs sent and received on each specific interface.
- The LACPUs Pkts and Err columns display the marker protocol packets.

This example shows how to display internal information for the interfaces belonging to a specific channel:

```
Switch# show lacp 1 internal
```

```
Flags:  S - Device 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  
LACPDUs LACP Port Admin Oper Port Port  
channel-group (Optional) Number of the channel group; valid values are from 1 to 64.
```
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

show lacp

<table>
<thead>
<tr>
<th>Port</th>
<th>Flags</th>
<th>State</th>
<th>Interval</th>
<th>Priority</th>
<th>Key</th>
<th>Key</th>
<th>Number</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa4/1</td>
<td>saC</td>
<td>bndl</td>
<td>30s</td>
<td>32768</td>
<td>100</td>
<td>100</td>
<td>0xc1</td>
<td>0x75</td>
</tr>
<tr>
<td>Fa4/2</td>
<td>saC</td>
<td>bndl</td>
<td>30s</td>
<td>32768</td>
<td>100</td>
<td>100</td>
<td>0xc2</td>
<td>0x75</td>
</tr>
<tr>
<td>Fa4/3</td>
<td>saC</td>
<td>bndl</td>
<td>30s</td>
<td>32768</td>
<td>100</td>
<td>100</td>
<td>0xc3</td>
<td>0x75</td>
</tr>
<tr>
<td>Fa4/4</td>
<td>saC</td>
<td>bndl</td>
<td>30s</td>
<td>32768</td>
<td>100</td>
<td>100</td>
<td>0xc4</td>
<td>0x75</td>
</tr>
</tbody>
</table>

Switch#

Table 2-26  lists the output field definitions.

This 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

Table 2-26 show lacp internal Command Output Fields

<table>
<thead>
<tr>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
</tr>
<tr>
<td>Port</td>
</tr>
<tr>
<td>LACPDUs Interval</td>
</tr>
<tr>
<td>LACP Port Priority</td>
</tr>
<tr>
<td>Admin Key</td>
</tr>
<tr>
<td>Oper Key</td>
</tr>
<tr>
<td>Port Number</td>
</tr>
</tbody>
</table>

State State of the specific port at the current moment is displayed; allowed values are as follows:

- **bndl** — Port is attached to an aggregator and bundled with other ports.
- **susp** — Port is in a suspended state; it is not attached to any aggregator.
- **indep** — Port is in an independent state (not bundled but able to switch data traffic. In this case, LACP is not running on the partner port).
- **hot-sby** — Port is in a hot-standby state.
- **down** — Port is down.

LACPDUs Interval Interval setting.

LACP Port Priority Port priority setting.

Admin Key Administrative key.

Oper Key Operator key.

Port Number Port number.

Port State State variables for the port encoded as individual bits within a single octet with the following meaning [1]:

- **bit0**: LACP_Activity
- **bit1**: LACP_Timeout
- **bit2**: Aggregation
- **bit3**: Synchronization
- **bit4**: Collecting
- **bit5**: Distributing
- **bit6**: Defaulted
- **bit7**: Expired
show lacp

<table>
<thead>
<tr>
<th>Port</th>
<th>System ID</th>
<th>Port Number</th>
<th>Age</th>
<th>Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa4/1</td>
<td>8000,00b0.c23e.d84e</td>
<td>0x81</td>
<td>29s</td>
<td>P</td>
</tr>
<tr>
<td>Fa4/2</td>
<td>8000,00b0.c23e.d84e</td>
<td>0x82</td>
<td>0s</td>
<td>P</td>
</tr>
<tr>
<td>Fa4/3</td>
<td>8000,00b0.c23e.d84e</td>
<td>0x83</td>
<td>0s</td>
<td>P</td>
</tr>
<tr>
<td>Fa4/4</td>
<td>8000,00b0.c23e.d84e</td>
<td>0x84</td>
<td>0s</td>
<td>P</td>
</tr>
</tbody>
</table>

In the case where no PDUs have been received, the default administrative information is displayed in braces.

This 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**

- `lacp port-priority`: Sets the LACP priority for the physical interfaces.
- `lacp system-priority`: Sets the priority of the system for LACP.
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**

- **Command Default**: None.
- **Command Modes**: Privileged EXEC mode.
- **Usage Guidelines**: Table 2-27 lists the fields in the `show mab` command. Table 2-28 lists the possible values for the state of the MAB state machine.

**Interface**

- Interface type; possible valid value is `gigabitethernet`.

**interface-number**

- Module and port number.

**all**

- Displays MAB information for all interfaces.

**detail**

- (Optional) Displays detailed MAB information.

**Table 2-27 show mab Command Output**

<table>
<thead>
<tr>
<th>Field Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mac-Auth-Bypass</td>
<td>MAB state</td>
</tr>
<tr>
<td>Inactivity Timeout</td>
<td>Inactivity timeout</td>
</tr>
<tr>
<td>Client MAC</td>
<td>Client MAC address</td>
</tr>
<tr>
<td>MAB SM state</td>
<td>MAB state machine state</td>
</tr>
<tr>
<td>Auth Status</td>
<td>Authorization status</td>
</tr>
</tbody>
</table>

**Table 2-28 MAB State Machine Values**

<table>
<thead>
<tr>
<th>State</th>
<th>State Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initialize</td>
<td>Intermediate</td>
<td>The state of the session when it initializes</td>
</tr>
<tr>
<td>Acquiring</td>
<td>Intermediate</td>
<td>The state of the session when it is obtaining the client MAC address</td>
</tr>
<tr>
<td>Authorizing</td>
<td>Intermediate</td>
<td>The state of the session during MAC-based authorization</td>
</tr>
<tr>
<td>Terminate</td>
<td>Terminal</td>
<td>The state of the session once a result has been obtained. For a session in terminal state, &quot;TERMINATE&quot; displays.</td>
</tr>
</tbody>
</table>
Table 2-29  lists the possible displayed values for the MAB authorization status.

**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
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mab</td>
<td>Enables and configures MAC authorization bypass (MAB) on a port.</td>
</tr>
</tbody>
</table>
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

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

- **Defaults:** This command has no default settings.
- **Command Modes:** Privileged EXEC mode
- **Usage Guidelines:** The valid values for the port number depend on the chassis used.
- **Examples:** This example shows how to display the ACL configuration on interface fast 6/1:

```
Switch# show mac access-group interface fast 6/1
Interface FastEthernet6/1:
Inbound access-list is simple-mac-acl
Outbound access-list is not set
```

**Related Commands**

- `interface` (Optional) Specifies the interface type; valid values are `ethernet`, `fastethernet`, `gigabitethernet`, `tengigabitethernet`, `pos`, `atm`, `port-channel`, and `ge-wan`.
- `interface-number` (Optional) Specifies the port number.
- **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).
To display MAC address table information for a specific MAC address, use the `show mac-address-table address` command.

```
syntax
  show mac-address-table address mac_addr [interface type slot/port | protocol protocol | vlan vlan_id]
  
  mac_addr  48-bit MAC address; the valid format is H.H.H.
  interface  type  slot/port  (Optional) Displays information for a specific interface; valid values for type are fastethernet, gigabitethernet, and tengigabitethernet.
  protocol  protocol  (Optional) Specifies a protocol. See the "Usage Guidelines" section for more information.
  vlan  vlan_id  (Optional) Displays entries for the specific VLAN only; valid values are from 1 to 4094.

defaults
  This command has no default settings.

command modes
  Privileged EXEC mode

usage guidelines
  For the MAC address table entries that are used by the routed ports, the routed port name is displayed in the "vlan" column not the 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
  This example shows how to display MAC address table information for a specific MAC address:

  Switch# show mac-address-table address 0030.94fc.0dff
  
  Unicast Entries
  vlan   mac address     type        protocols               port
  -------+---------------+--------+---------------------+-------------------
  1    0030.94fc.0dff    static ip,ipx,assigned,other  Switch
  Fa6/1   0030.94fc.0dff    static ip,ipx,assigned,other  Switch
  Fa6/2   0030.94fc.0dff    static ip,ipx,assigned,other  Switch

  Switch#
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

show mac-address-table address

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.
Chapter 2      Cisco IOS Commands for  the Catalyst 4500 Series Switches

show mac-address-table aging-time

To display the MAC address aging time, use the show mac-address-table aging-time command.

**Syntax Description**

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Examples**

This example shows how to display the currently configured aging time for all VLANs:

```
Switch# show mac-address-table aging-time
Vlan    Aging Time
----    ----------
100     300
200     1000
Switch#
```

This example shows how to display the currently configured aging time for a specific VLAN:

```
Switch# show mac-address-table aging-time vlan 100
Vlan    Aging Time
----    ----------
100    300
Switch#
```

**Related Commands**

`vlan vlan_id` (Optional) Specifies a VLAN; valid values are from 1 to 4094.

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.
- `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.
To display the number of entries currently in the MAC address table, use the `show mac-address-table count` command.

**Syntax Description**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Examples**

This example shows how to display the entry count for a specific VLAN:

```
Switch# show mac-address-table count vlan 1
MAC Entries for Vlan 1:
  Dynamic Unicast Address Count:                 0
  Static Unicast Address (User-defined) Count:   0
  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
```

**Related Commands**

- `vlan vlan_id`: (Optional) Specifies a VLAN; valid values are from 1 to 4094.
- `show mac-address-table address`: Displays the information about the MAC-address table.
- `show mac-address-table aging-time`: Displays MAC address table aging information.
- `show mac-address-table dynamic`: Displays the dynamic MAC address table entries only.
- `show mac-address-table interface`: Displays the MAC address table information for a specific interface.
- `show mac-address-table multicast`: Displays information about the multicast MAC address table.
- `show mac-address-table protocol`: Displays the MAC address table information that is based on the protocol.
- `show mac-address-table static`: Displays the static MAC address table entries only.
- `show mac-address-table vlan`: Displays information about the MAC address table for a specific VLAN.
To display the dynamic MAC address table entries only, use the `show mac-address-table dynamic` command.

<table>
<thead>
<tr>
<th>Address</th>
<th>MAC Addr</th>
<th>Interface Type</th>
<th>Slot/Port</th>
<th>Protocol</th>
<th>VLAN ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unicast</td>
<td>0000.0000.0201</td>
<td>dynamic ip</td>
<td>FastEthernet6/15</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Unicast</td>
<td>0000.0000.0202</td>
<td>dynamic ip</td>
<td>FastEthernet6/15</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Unicast</td>
<td>0000.0000.0203</td>
<td>dynamic ip,assigned</td>
<td>FastEthernet6/15</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Unicast</td>
<td>0000.0000.0204</td>
<td>dynamic ip,assigned</td>
<td>FastEthernet6/15</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Unicast</td>
<td>0000.0000.0205</td>
<td>dynamic ip,assigned</td>
<td>FastEthernet6/15</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Unicast</td>
<td>0000.0000.0101</td>
<td>dynamic ip</td>
<td>FastEthernet6/16</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>Unicast</td>
<td>0000.0000.0102</td>
<td>dynamic ip</td>
<td>FastEthernet6/16</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>Unicast</td>
<td>0000.0000.0103</td>
<td>dynamic ip,assigned</td>
<td>FastEthernet6/16</td>
<td></td>
<td>2</td>
</tr>
</tbody>
</table>

**Syntax Description**

- **address**
  - (Optional) Specifies a 48-bit MAC address; the valid format is H.H.H.
- **interface**
  - (Optional) Specifies an interface to match; valid values for `type` are `fastethernet`, `gigabitethernet`, and `tengigabitethernet`.
- **protocol**
  - (Optional) Specifies a protocol. See the "Usage Guidelines" section for more information.
- **vlan**
  - (Optional) Displays entries for a specific VLAN; valid values are from 1 to 4094.
This example shows how to display the dynamic MAC address entries with a specific protocol type (in this case, assigned):

```
Switch# show mac-address-table dynamic protocol assigned

Unicast Entries

<table>
<thead>
<tr>
<th>vlan</th>
<th>mac address</th>
<th>type</th>
<th>protocols</th>
<th>port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0000.0000.0203</td>
<td>dynamic ip</td>
<td>assigned</td>
<td>FastEthernet6/15</td>
</tr>
<tr>
<td>1</td>
<td>0000.0000.0204</td>
<td>dynamic ip</td>
<td>assigned</td>
<td>FastEthernet6/15</td>
</tr>
<tr>
<td>1</td>
<td>0000.0000.0205</td>
<td>dynamic ip</td>
<td>assigned</td>
<td>FastEthernet6/15</td>
</tr>
<tr>
<td>2</td>
<td>0000.0000.0103</td>
<td>dynamic ip</td>
<td>assigned</td>
<td>FastEthernet6/16</td>
</tr>
<tr>
<td>2</td>
<td>0000.0000.0104</td>
<td>dynamic ip</td>
<td>assigned</td>
<td>FastEthernet6/16</td>
</tr>
<tr>
<td>2</td>
<td>0000.0000.0105</td>
<td>dynamic ip</td>
<td>assigned</td>
<td>FastEthernet6/16</td>
</tr>
</tbody>
</table>
```

Related Commands:
- `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.
To display the MAC address table information for a specific interface, use the `show mac-address-table interface` command.

**Syntax Description**

```
show mac-address-table interface [type slot/port]
```

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Usage Guidelines**

For the MAC address table entries that are used by the routed ports, the routed port name is displayed in the "vlan" column not the internal VLAN number.

**Examples**

This example shows how to display MAC address table information for a specific interface:

```
Switch# show mac-address-table interface fastethernet6/16
```

<table>
<thead>
<tr>
<th>VLAN</th>
<th>MAC Address</th>
<th>Type</th>
<th>Protocols</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>0000.0000.0101</td>
<td>dynamic</td>
<td>other</td>
<td>FastEthernet6/16</td>
</tr>
<tr>
<td>2</td>
<td>0000.0000.0102</td>
<td>dynamic</td>
<td>other</td>
<td>FastEthernet6/16</td>
</tr>
<tr>
<td>2</td>
<td>0000.0000.0103</td>
<td>dynamic</td>
<td>other</td>
<td>FastEthernet6/16</td>
</tr>
<tr>
<td>2</td>
<td>0000.0000.0104</td>
<td>dynamic</td>
<td>other</td>
<td>FastEthernet6/16</td>
</tr>
<tr>
<td>2</td>
<td>0000.0000.0105</td>
<td>dynamic</td>
<td>other</td>
<td>FastEthernet6/16</td>
</tr>
<tr>
<td>2</td>
<td>0000.0000.0106</td>
<td>dynamic</td>
<td>other</td>
<td>FastEthernet6/16</td>
</tr>
</tbody>
</table>

**Multicast Entries**

<table>
<thead>
<tr>
<th>VLAN</th>
<th>MAC Address</th>
<th>Type</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>ffff.ffff.ffff</td>
<td>system</td>
<td>Fa6/16</td>
</tr>
</tbody>
</table>

**Related Commands**

- `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 multicast`

**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.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

```
show mac-address-table interface
show mac-address-table protocol
Displays the MAC address table information that is based
on the protocol.
show mac-address-table static
Displays the static MAC address table entries only .
show mac-address-table vlan
Displays information about the MAC address table for a
specific VLAN.
```

Command Description
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] expr expression
```

**Syntax Description**

- **Defaults**
  - MAC address learning is enabled on all VLANs.

- **Command Modes**
  - User EXEC

- **Usage Guidelines**
  - To display configured VLANs, and whether MAC address learning is enabled or disabled, use the `show mac address-table learning` command without keywords.
  - To display the learning status on an individual VLAN, use the command with a specific VLAN ID.
  - Expressions are case sensitive. For example, if you enter `| exclude output` the lines that contain output do not appear, but the lines that contain Output appear.

**Examples**

This example shows that MAC address learning is disabled on VLAN 200:

```
Switch> show mac address-table learning
VLAN    Learning Status
----    ---------------
1             yes
100           yes
200           no
```

**Related Commands**

- `vlan vlan-id` (Optional) Displays information for a specific VLAN. The range is 1 to 4094.
- `| begin` (Optional) Displays the line that matches the expression.
- `| exclude` (Optional) Displays excluded lines that match the expression.
- `| include` (Optional) Displays included lines that match the specified expression.
- `expression` (Optional) Specifies the expression in the output as a reference point.

**Command Description**

- `mac address-table learning vlan` Enables or disables MAC address learning on a VLAN.
To display information about the multicast MAC address table, use the `show mac-address-table multicast` command.

```plaintext
Syntax Description

- `count` (Optional) Displays the number of multicast entries.
- `igmp-snooping` (Optional) Displays only the addresses learned by IGMP snooping.
- `user` (Optional) Displays only the user-entered static addresses.
- `vlan vlan_num` (Optional) Displays information for a specific VLAN only; valid values are from 1 to 4094.

Command Modes

Privileged EXEC mode

Usage Guidelines

For the MAC address table entries that are used by the routed ports, the routed port name is displayed in the "vlan" column not in the internal VLAN number.

Examples

This example shows how to display multicast MAC address table information for a specific VLAN:

```
Switch# show mac-address-table multicast vlan 1
Multicast Entries
vlan    mac address     type    ports
-------+---------------+-------+-------------------------------------------
1    ffff.ffff.ffff   system Switch,Fa6/15
Switch#
```

This example shows how to display the number of multicast MAC entries for all VLANs:

```
Switch# show mac-address-table multicast count
MAC Entries for all vlans:
Multicast MAC Address Count:                   141
Total Multicast MAC Addresses Available:       16384
Switch#
```

Related Commands

- `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.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

show mac-address-table multicast
Displays the MAC address table information for a specific interface.

show mac-address-table interface
Displays information about the MAC address table for a specific interface.

show mac-address-table protocol
Displays the MAC address table information that is based on the protocol.

show mac-address-table static
Displays the static MAC address table entries only.

show mac-address-table vlan
Displays information about the MAC address table for a specific VLAN.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

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` (Optional) Displays the MAC address change notification status.
`interface` (Optional) Displays MAC change information for an interfaces.
`interface-id` (Optional) Displays the information for a specific interface. Valid interfaces include physical ports and port channels.
`mac-move` (Optional) Displays MAC move notification status.
`threshold` (Optional) Displays the MAC threshold notification status.
`learn-fail` (Optional) Displays general information of hardware MAC learning failure notifications.
This example shows how to display the MAC address change status on the FastEthernet interface 7/1:

Switch# show mac-address-table notification change interface FastEthernet 7/1
MAC Notification Feature is Enabled on the switch

<table>
<thead>
<tr>
<th>Interface</th>
<th>MAC Added Trap</th>
<th>MAC Removed Trap</th>
</tr>
</thead>
<tbody>
<tr>
<td>FastEthernet7/1</td>
<td>Enabled</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

This example shows how to display the MAC address move status:

Switch# show mac-address-table notification mac-move
MAC Move Notification: Enabled

This example shows how to display the MAC address table utilization status:

Switch# show mac-address-table notification threshold
Status       limit        Interval
-------------+-----------+-------------
enabled        50           120

This example shows how to display general information of MAC learning failure notifications:

Switch# show mac-address-table notification learn-fail
Status       limit        Interval
-------------+-----------+-------------
disabled        2000           120

Related Commands
- 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.
To display the MAC address table information that is based on the protocol, use the `show mac-address-table protocol` command.

```markdown
## Syntax Description

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Usage Guidelines**

For the MAC address table entries that are used by the routed ports, the routed port name is displayed in the "vlan" column not the the internal VLAN number.

**Examples**

This example shows how to display the MAC address table entries that have a specific protocol type (in this case, assigned):

```
Switch# show mac-address-table protocol assigned
```

<table>
<thead>
<tr>
<th>vlan</th>
<th>mac address</th>
<th>type</th>
<th>protocol</th>
<th>qos</th>
<th>ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>0050.3e8d.6400</td>
<td>static</td>
<td>assigned</td>
<td>--</td>
<td>Switch</td>
</tr>
<tr>
<td>100</td>
<td>0050.3e8d.6400</td>
<td>static</td>
<td>assigned</td>
<td>--</td>
<td>Switch</td>
</tr>
<tr>
<td>5</td>
<td>0050.3e8d.6400</td>
<td>static</td>
<td>assigned</td>
<td>--</td>
<td>Switch</td>
</tr>
<tr>
<td>4092</td>
<td>0000.0000.0000</td>
<td>dynamic</td>
<td>assigned</td>
<td>--</td>
<td>Switch</td>
</tr>
<tr>
<td>1</td>
<td>0050.3e8d.6400</td>
<td>static</td>
<td>assigned</td>
<td>--</td>
<td>Switch</td>
</tr>
<tr>
<td>4</td>
<td>0050.3e8d.6400</td>
<td>static</td>
<td>assigned</td>
<td>--</td>
<td>Switch</td>
</tr>
<tr>
<td>4092</td>
<td>0050.f0ac.3058</td>
<td>static</td>
<td>assigned</td>
<td>--</td>
<td>Switch</td>
</tr>
<tr>
<td>4092</td>
<td>0050.f0ac.3059</td>
<td>dynamic</td>
<td>assigned</td>
<td>--</td>
<td>Switch</td>
</tr>
<tr>
<td>1</td>
<td>0010.7b3b.0978</td>
<td>dynamic</td>
<td>assigned</td>
<td>--</td>
<td>Fa5/9</td>
</tr>
</tbody>
</table>

Switch#
```

This example shows the other output for the previous example:

```
Switch# show mac-address-table protocol other
```

<table>
<thead>
<tr>
<th>Unicast Entries</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan</td>
</tr>
<tr>
<td>------</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>2</td>
</tr>
</tbody>
</table>
```
### Multicast Entries

<table>
<thead>
<tr>
<th>VLAN</th>
<th>MAC Address</th>
<th>Type</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ffff.ffff.ffff</td>
<td>system</td>
<td>Switch, Fa6/15</td>
</tr>
<tr>
<td>2</td>
<td>ffff.ffff.ffff</td>
<td>system</td>
<td>Fa6/16</td>
</tr>
<tr>
<td>1002</td>
<td>ffff.ffff.ffff</td>
<td>system</td>
<td></td>
</tr>
<tr>
<td>1003</td>
<td>ffff.ffff.ffff</td>
<td>system</td>
<td></td>
</tr>
<tr>
<td>1004</td>
<td>ffff.ffff.ffff</td>
<td>system</td>
<td></td>
</tr>
<tr>
<td>1005</td>
<td>ffff.ffff.ffff</td>
<td>system</td>
<td></td>
</tr>
<tr>
<td>Fa6/1</td>
<td>ffff.ffff.ffff</td>
<td>system</td>
<td>Switch, Fa6/1</td>
</tr>
<tr>
<td>Fa6/2</td>
<td>ffff.ffff.ffff</td>
<td>system</td>
<td>Switch, Fa6/2</td>
</tr>
</tbody>
</table>

**Switch#**

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show mac-address-table address</code></td>
<td>Displays the information about the MAC-address table.</td>
</tr>
<tr>
<td><code>show mac-address-table aging-time</code></td>
<td>Displays MAC address table aging information.</td>
</tr>
<tr>
<td><code>show mac-address-table count</code></td>
<td>Displays the number of entries currently in the MAC address table.</td>
</tr>
<tr>
<td><code>show mac-address-table dynamic</code></td>
<td>Displays the dynamic MAC address table entries only.</td>
</tr>
<tr>
<td><code>show mac-address-table interface</code></td>
<td>Displays the MAC address table information for a specific interface.</td>
</tr>
<tr>
<td><code>show mac-address-table multicast</code></td>
<td>Displays information about the multicast MAC address table.</td>
</tr>
<tr>
<td><code>show mac-address-table static</code></td>
<td>Displays the static MAC address table entries only.</td>
</tr>
<tr>
<td><code>show mac-address-table vlan</code></td>
<td>Displays information about the MAC address table for a specific VLAN.</td>
</tr>
</tbody>
</table>
To display the static MAC address table entries only, use the `show mac-address-table static` command.

<table>
<thead>
<tr>
<th>address</th>
<th>mac_addr</th>
<th>interface</th>
<th>type</th>
<th>protocols</th>
<th>port</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Syntax Description**

- **address**: (Optional) Specifies a 48-bit MAC address to match; the valid format is H. H. H.
- **interface type number**: (Optional) Specifies an interface to match; valid values for **type** are `fastethernet`, `gigabitethernet`, and `tengigabitethernet`.
- **protocol** (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.

**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**

This example shows how to display all the static MAC address entries:

```
Switch# show mac-address-table static
```

**Unicast Entries**

```
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**

```
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
```
This example shows how to display the static MAC address entries with a specific protocol type (in this case, assigned):

```
Switch# show mac-address-table static protocol assigned
```

### Unicast Entries

<table>
<thead>
<tr>
<th>VLAN</th>
<th>MAC Address</th>
<th>Type</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0030.94fc.0dff</td>
<td>static ip, ipx, assigned, other</td>
<td>Switch, Fa6/1</td>
</tr>
<tr>
<td></td>
<td>0030.94fc.0dff</td>
<td>static ip, ipx, assigned, other</td>
<td>Switch, Fa6/2</td>
</tr>
</tbody>
</table>

### Multicast Entries

<table>
<thead>
<tr>
<th>VLAN</th>
<th>MAC Address</th>
<th>Type</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ffff.ffff.ffff</td>
<td>system</td>
<td>Switch, Fa6/15</td>
</tr>
<tr>
<td>2</td>
<td>ffff.ffff.ffff</td>
<td>system</td>
<td>Fa6/16</td>
</tr>
</tbody>
</table>

Switch#
To display information about the MAC address table for a specific VLAN, use the `show mac-address-table vlan` command.

```plaintext
Syntax Description

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

For the MAC address table entries used by the routed ports, the routed port name is displayed in the "vlan" column not the the internal VLAN number.

The keyword definitions for the `protocol` variable are as follows:

- `assigned` specifies the assigned protocol entries.
- `ip` specifies the IP protocol.
- `ipx` specifies the IPX protocols.
- `other` specifies the other protocol entries.

Examples

This example shows how to display information about the MAC address table for a specific VLAN:

```
Switch# show mac-address-table vlan 1
Unicast Entries
  vlan   mac address     type        protocols               port
  -------+---------------+--------+---------------------+---------------------
  1    0000.0000.0201   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#
```

This example shows how to display MAC address table information for a specific protocol type:

```
Switch# show mac-address-table vlan 100 protocol other
Unicast Entries
  vlan   mac address     type        protocols               port
  -------+---------------+--------+---------------------+---------------------
  1    0000.0000.0201   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
```
## show mac-address-table vlan

<table>
<thead>
<tr>
<th>VLAN</th>
<th>MAC Address</th>
<th>Type</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0000.0000.0203</td>
<td>dynamic other</td>
<td>FastEthernet6/15</td>
</tr>
<tr>
<td>1</td>
<td>0000.0000.0204</td>
<td>dynamic other</td>
<td>FastEthernet6/15</td>
</tr>
<tr>
<td>1</td>
<td>0030.94fc.0dff</td>
<td>static ip,ipx,assigned,other</td>
<td>Switch</td>
</tr>
</tbody>
</table>

### Multicast Entries

**VLAN** | **MAC Address** | **Type** | **Ports** |
---|----------------|----------|-----------|
1 | ffff.ffff.ffff | system | Switch,Fa6/15 |

### Related Commands

- **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.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

show macro auto mac-address-group

Use the `show macro auto mac-address-group` command to display the configuration of MAC address group.

**Syntax Description**

**Examples**

This example shows how to display the configuration of the MAC address group:

Switch# show macro auto address-group

MAC Address Group Configuration:

<table>
<thead>
<tr>
<th>Group Name</th>
<th>OUI</th>
<th>MAC ADDRESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>testGroup</td>
<td></td>
<td>2222.2222.2222</td>
</tr>
<tr>
<td></td>
<td>1111.1111.1111</td>
<td></td>
</tr>
</tbody>
</table>

No keywords
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

show macro auto device

Use the show macro auto device global configuration command to display the default information for a device, including built-in function name and the parameters that can be provided for the commands when executing the built-in function.

**Syntax Description**

None

**Command Modes**

Global configuration

**Usage Guidelines**

This command displays the default values as well as the currently used values if configured.

**Examples**

This example shows how to display the default information for the device access-point:

```
Switch# show macro auto device access-point
Device: access-point
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**

- **device_id**: Specifies the device ID.

**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.
Use the `show macro auto interface` command to display Auto SmartPorts status and the functions applied on an interface.

```
show macro auto interface

Syntax Description

Defaults
None

Command Modes
Global configuration

Examples
This example shows how to display Auto SmartPorts status and the applied macros:

Switch# show macro auto int 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

- `interface_id`: Specifies an interface ID.

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.
To display the clients using the device classifier facility on the switch, use the `show macro auto monitor clients` user EXEC command.

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Use r EXEC

**Privileged EXEC**

**Usage Guidelines**

Device classifier (DC) is enabled by default when you enable a client application (for example, Auto Smartports) that uses its functionality. Use the `show macro auto monitor clients` command to display the clients that are using the DC feature on the switch.

As long as any clients are using the DC, you cannot disable it by using the `no macro auto monitor` command. If you attempt to disable the DC while a client is using it, an error message appears.

**Examples**

This example shows how to use the `show macro auto monitor clients` privileged EXEC command to view the clients using the DC on the switch:

```
Switch#
show macro auto monitor clients
```

Client Name

---

Auto Smart Ports

This example shows the error message that appears when you attempt to disable DC while a client is using it:

```
Switch(config)#
no macro auto monitor
These subsystems should be disabled before disabling Device classifier
Auto Smart Ports
% Error - device classifier is not disabled
```

**Related Commands**

- `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 type`
  - Displays all the device types recognized by the device classifier.
- `show shell triggers`
  - Displays information about event triggers and macros.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

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.

**Syntax Description**

- **Command Modes**: User EXEC, Privileged EXEC

**Usage Guidelines**

Use this command to display the devices connected to a switch. Use the `show macro auto device` privileged EXEC command to display the configurable parameters for a device.

**Examples**

This example shows how to use the `show macro auto monitor device` privileged EXEC command with 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
```

This 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
```

This example shows how to use the `show macro auto monitor device` privileged EXEC command with the optional `mac-address` and `detail` keywords to view detailed information about the connected device with the specified MAC address:

```
Switch# show macro auto monitor device mac-address 001f.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
```
This example shows how to use the `show macro auto monitor device` privileged EXEC command with the optional `interface` keyword to view summary information about the device connected to the specified interface:

```
Switch# show macro auto monitor device interface gi 1/0/2
MAC_Address           Port_Id          Profile Name
==============    =======     ============================
000a.b8c6.1e07    Gi1/0/2    Cisco-Device
```

This example shows how to use the `show macro auto monitor device` privileged EXEC command with the optional `interface` and `detail` keywords to view detailed information about the device connected to the specified interface:

```
Switch# show macro auto monitor device interface gi 1/0/2 detail
MAC_Address       Port_Id     Certainty Parent    ProfileType  Profile Name
Device_Name
==============    =======     ========= ======    ===========  =============
000a.b8c6.1e07    Gi1/0/2      10       0        Default       Cisco-Device        cisco
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>macro auto device</code></td>
<td>Configures macro default parameter values.</td>
</tr>
<tr>
<td><code>macro auto execute</code></td>
<td>Configures mapping from an event trigger to a built-in macro.</td>
</tr>
<tr>
<td><code>macro auto global processing</code></td>
<td>Enables Auto Smartports on a switch.</td>
</tr>
<tr>
<td><code>macro auto mac-address-group</code></td>
<td>Configures MAC address groups.</td>
</tr>
<tr>
<td><code>macro auto sticky</code></td>
<td>Configures macro persistence.</td>
</tr>
<tr>
<td><code>shell trigger</code></td>
<td>Creates event triggers.</td>
</tr>
<tr>
<td><code>show macro auto monitor clients</code></td>
<td>Displays all the device types recognized by the device classifier.</td>
</tr>
<tr>
<td><code>show macro auto monitor type</code></td>
<td>Displays all the device types recognized by the device classifier.</td>
</tr>
<tr>
<td><code>show shell triggers</code></td>
<td>Displays information about event triggers and macros.</td>
</tr>
</tbody>
</table>
To display all the device types recognized by the device classifier, use the `show macro auto monitor type` user EXEC command.

```
Syntax Description

Table: Displays device classification in a table.
built-in: Displays device classification information from the built-in device table.
default: Displays device classification information from the default device table.
filter: Displays information for devices that match the filter.
```

```
Usage Guidelines

This command displays all the device types recognized by the device classification engine. The number of available device types is the number of profiles stored on the switch. Because the number of profiles can be very large, you can use the `filter` keyword to limit the command output.

Examples

This example shows how to use the `show macro auto monitor type` privileged EXEC command with no optional keywords to view the devices recognized by the device classifier:

```
Switch# show macro auto monitor type table
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
```
<table>
<thead>
<tr>
<th>Vendor</th>
<th>Type</th>
<th>Valid</th>
<th>Built-in</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco</td>
<td>Catalyst 4500 Series</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch</td>
<td>Valid</td>
<td>Built-in</td>
</tr>
<tr>
<td></td>
<td>Cisco-WLC-2100-Series</td>
<td>40</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>Cisco-DMP-4400G</td>
<td>70</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>Cisco-DMP-4310G</td>
<td>70</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>Cisco-DMP-4305G</td>
<td>70</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>Cisco-DMP</td>
<td>10</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td>IP-Phone</td>
<td>20</td>
<td>15</td>
</tr>
<tr>
<td></td>
<td>Cisco-IP-Phone</td>
<td>20</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td>Cisco-Switch</td>
<td>10</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>Cisco-Source-Bridge</td>
<td>10</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>Transparent-Bridge</td>
<td>8</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>Cisco-Transparent-Bridge</td>
<td>8</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>Cisco-IP-Camera-4xxx</td>
<td>50</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>Cisco-IP-Camera-2530</td>
<td>50</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>Cisco-IP-Camera-2520</td>
<td>50</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>Cisco-IP-Camera-2500</td>
<td>50</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>Cisco-IP-Camera-2421</td>
<td>50</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>Cisco-IP-Camera</td>
<td>30</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>Cisco-IP-Camera</td>
<td>10</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Router</td>
<td>10</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Cisco-Router</td>
<td>10</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Cisco-Device</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>ISE-Appliance</td>
<td>10</td>
<td>66</td>
</tr>
<tr>
<td></td>
<td>VMWare-Device</td>
<td>10</td>
<td>65</td>
</tr>
<tr>
<td></td>
<td>MotorolaMobile-Device</td>
<td>10</td>
<td>64</td>
</tr>
<tr>
<td></td>
<td>HTC-Device</td>
<td>10</td>
<td>63</td>
</tr>
<tr>
<td></td>
<td>LinksysWAP54G-Device</td>
<td>30</td>
<td>62</td>
</tr>
<tr>
<td></td>
<td>Linksys-Device</td>
<td>20</td>
<td>61</td>
</tr>
<tr>
<td></td>
<td>Sun-Workstation</td>
<td>10</td>
<td>60</td>
</tr>
<tr>
<td></td>
<td>Cisco-AIR-AP-1250</td>
<td>50</td>
<td>59</td>
</tr>
<tr>
<td></td>
<td>Cisco-AIR-AP-1240</td>
<td>50</td>
<td>58</td>
</tr>
<tr>
<td></td>
<td>Cisco-AIR-AP-1130</td>
<td>30</td>
<td>57</td>
</tr>
<tr>
<td></td>
<td>Cisco-AIR-AP-1250</td>
<td>25</td>
<td>56</td>
</tr>
<tr>
<td></td>
<td>Cisco-AIR-LAP-1250</td>
<td>50</td>
<td>55</td>
</tr>
<tr>
<td></td>
<td>Cisco-AIR-LAP-1240</td>
<td>50</td>
<td>54</td>
</tr>
<tr>
<td></td>
<td>Cisco-AIR-LAP-1130</td>
<td>30</td>
<td>53</td>
</tr>
<tr>
<td></td>
<td>Cisco-AIR-LAP-1250</td>
<td>25</td>
<td>52</td>
</tr>
<tr>
<td></td>
<td>Cisco-AP-Aironet-1250</td>
<td>30</td>
<td>51</td>
</tr>
<tr>
<td></td>
<td>Cisco-AP-Aironet-1240</td>
<td>30</td>
<td>50</td>
</tr>
<tr>
<td></td>
<td>Cisco-AP-Aironet-1130</td>
<td>30</td>
<td>49</td>
</tr>
<tr>
<td></td>
<td>DLink-DAP-1522</td>
<td>20</td>
<td>48</td>
</tr>
<tr>
<td></td>
<td>Cisco-IP-Conference-Station-7937</td>
<td>70</td>
<td>47</td>
</tr>
<tr>
<td></td>
<td>Cisco-IP-Conference-Station-7936</td>
<td>70</td>
<td>46</td>
</tr>
<tr>
<td></td>
<td>Cisco-IP-Conference-Station-7935</td>
<td>70</td>
<td>45</td>
</tr>
<tr>
<td></td>
<td>Cisco-Access-Point</td>
<td>10</td>
<td>44</td>
</tr>
<tr>
<td></td>
<td>Aruba-AP</td>
<td>20</td>
<td>43</td>
</tr>
<tr>
<td></td>
<td>Xerox-Printer-Phaser3250</td>
<td>30</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td>Xerox-Device</td>
<td>10</td>
<td>41</td>
</tr>
<tr>
<td></td>
<td>XBOX360</td>
<td>20</td>
<td>40</td>
</tr>
<tr>
<td></td>
<td>SonyPS3</td>
<td>10</td>
<td>39</td>
</tr>
<tr>
<td></td>
<td>Nortel-IP-Phone-2000-Series</td>
<td>20</td>
<td>38</td>
</tr>
<tr>
<td></td>
<td>Nortel-Device</td>
<td>10</td>
<td>37</td>
</tr>
<tr>
<td></td>
<td>NintendoWII</td>
<td>10</td>
<td>36</td>
</tr>
<tr>
<td></td>
<td>Netgear-Device</td>
<td>10</td>
<td>35</td>
</tr>
<tr>
<td></td>
<td>Microsoft-Device</td>
<td>10</td>
<td>34</td>
</tr>
<tr>
<td></td>
<td>Lexmark-Printer-E260dn</td>
<td>30</td>
<td>33</td>
</tr>
<tr>
<td></td>
<td>Lexmark-Device</td>
<td>10</td>
<td>32</td>
</tr>
<tr>
<td></td>
<td>HP-JetDirect-Printer</td>
<td>30</td>
<td>31</td>
</tr>
<tr>
<td></td>
<td>HP-Device</td>
<td>10</td>
<td>30</td>
</tr>
<tr>
<td></td>
<td>Enterasys-Device</td>
<td>10</td>
<td>29</td>
</tr>
<tr>
<td></td>
<td>DLink-Device</td>
<td>10</td>
<td>28</td>
</tr>
<tr>
<td></td>
<td>Cisco-WLC-2100-Series</td>
<td>40</td>
<td>27</td>
</tr>
<tr>
<td></td>
<td>Cisco-IP-Phone-9971</td>
<td>70</td>
<td>26</td>
</tr>
<tr>
<td></td>
<td>Cisco-IP-Phone-7985</td>
<td>70</td>
<td>25</td>
</tr>
</tbody>
</table>

Chapter 2: Cisco IOS Commands for the Catalyst 4500 Series Switches
Chapter 2  Cisco IOS Commands for the Catalyst 4500 Series Switches

**Command Reference**

**show macro auto monitor type**

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**
  - **show macro auto device**
    - Configures macro default parameter values.
  - **show macro auto execute (built-in function)**
    - Configures mapping from an event trigger to a built-in macro.
  - **show macro auto global processing**
    - Enables Auto Smartports on a switch.
  - **show macro auto mac-address-group**
    - Configures MAC address groups.
  - **show 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.
To display information about the module, use the `show module` command.

### show module

**Syntax Description**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Usage Guidelines**

In the Mod Sub-Module fields in the command output, the `show module` command displays the supervisor engine number but appends the uplink daughter card's module type and information.

If the PoE consumed by the module is more than 50 W above the administratively allocated PoE, the “Status” displays as “PwrOver.” If the PoE consumed by the module is more than 50 W above the PoE module limit, the “Status” displays as “PwrFault.”

**Examples**

This example shows how to display information for all the modules.

```
Switch# show module all
```

<table>
<thead>
<tr>
<th>Mod</th>
<th>Ports</th>
<th>Card Type</th>
<th>Model</th>
<th>Serial No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>1000BaseX (GBIC) Supervisor</td>
<td>WS-X4014</td>
<td>JAB054109GH</td>
</tr>
<tr>
<td>2</td>
<td>6</td>
<td>1000BaseX (GBIC)</td>
<td>WS-X4306</td>
<td>00000110</td>
</tr>
<tr>
<td>3</td>
<td>18</td>
<td>1000BaseX (GBIC)</td>
<td>WS-X4418</td>
<td>JAB025104WK</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>Not enough power for module</td>
<td>WS-X4148-FX-MT</td>
<td>00000000000</td>
</tr>
<tr>
<td>6</td>
<td>48</td>
<td>10/100BaseTX (RJ45)</td>
<td>WS-X4148</td>
<td>JAB023402RP</td>
</tr>
</tbody>
</table>

**MAC addresses**

<table>
<thead>
<tr>
<th>MAC addresses</th>
<th>Hw</th>
<th>Fw</th>
<th>Sw</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>005c.9d1a.f9d0 to 005c.9d1a.f9df</td>
<td>0.5</td>
<td>12.1(11br)EW</td>
<td>12.1(20020313:00</td>
<td>Ok</td>
</tr>
<tr>
<td>0010.7bab.9920 to 0010.7bab.9925</td>
<td>0.2</td>
<td></td>
<td></td>
<td>Ok</td>
</tr>
<tr>
<td>0050.7356.2b36 to 0050.7356.2b47</td>
<td>1.0</td>
<td></td>
<td></td>
<td>Ok</td>
</tr>
<tr>
<td>0001.64fe.a930 to 0001.64fe.a95f</td>
<td>0.0</td>
<td>PwrDeny</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0050.0f10.28b0 to 0050.0f10.28df</td>
<td>1.0</td>
<td></td>
<td></td>
<td>Ok</td>
</tr>
</tbody>
</table>

This example shows how to display information for a specific module:

```
Switch# show module mod2
```

<table>
<thead>
<tr>
<th>Mod</th>
<th>Ports</th>
<th>Card Type</th>
<th>Model</th>
<th>Serial No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2</td>
<td>Catalyst 4000 supervisor 2</td>
<td>WS-X6K-SUP2-2GE</td>
<td>SAD04450LF1</td>
</tr>
</tbody>
</table>

```
Switch#
```

| mod (Optional) Number of the module; valid values vary from chassis to chassis. |
| all (Optional) Displays information for all modules. |
This 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

Mod 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#```
To display information about the SPAN session, use the `show monitor` command.

```
syntax
show monitor [session | range | session-range | local | remote | all | session-number] [detail]
```

**Syntax Description**
- `session` (Optional) Displays the SPAN information for a session.
- `range` (Optional) Displays information for a range of sessions.
- `session-range` (Optional) Specifies a range of sessions.
- `local` (Optional) Displays all local SPAN sessions.
- `remote` (Optional) Displays the RSPAN source and destination sessions.
- `all` (Optional) Displays the SPAN and RSPAN sessions.
- `session-number` (Optional) Session number; valid values are from 1 to 6.
- `detail` (Optional) Displays the detailed SPAN information for a session.

**Defaults**
- The `detail` keyword only displays lines with a nondefault configuration.

**Command Modes**
- Privileged EXEC mode

**Examples**
This example shows how to display whether ACLs are applied to a given SPAN session on a Catalyst 4500 series switch:

```
Switch# show monitor
Session 1
---------
Type              : Local Session
Source Ports      :
Both          : Fa6/1
Destination Ports : Fa6/2
Encapsulation : Native
Ingress : Disabled
Learning : Disabled
Filter VLANs      : 1
IP Access-group   : 10
```

This example shows how to display SPAN information for session 2:

```
Switch# show monitor session 2
Session 2
------------
Type : Remote Source Session
Source Ports:
RX Only:       Fa1/1-3
Dest RSPAN VLAN:  901
Ingress : Enabled, default VLAN=2
Learning : Disabled
```

Switch#
This example shows how to display the detailed SPAN information for session 1:

Switch# show monitor session 1 detail

Session 1
---------
Type              : Local Session
Source Ports      :
RX Only       : None
TX Only       : None
Both          : Gi1/1, CPU
Source VLANs      :
RX Only       : None
TX Only       : None
Both          : None
Source RSPAN VLAN : 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

This example shows how to display SPAN information for session 1 beginning with the line that starts with Destination:

Switch# show monitor session 1 | begin Destination

Destination Ports: None
Filter VLANs:      None

Switch#
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

- **Defaults**
  - If the capture point name is not provided, the command displays all the capture point details.
  - If the display mode is not specified, the command defaults to brief mode.

### Command Modes

- **Privileged EXEC mode**

### Usage Guidelines

- When the command is issued with no parameters, it displays the details of all the capture points.
- When specified with a capture point name and no other parameters, it displays the details of the specific capture point name.
- With the `parameter` keyword, the command 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 examples 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
```
Chapter 2 Cisco IOS Commands for the Catalyst 4500 Series Switches

```
show monitor capture
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]
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)
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)
.... .... .... .... .... .... = 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 
0010  00 ee 00 00 00 00 40 11 59 25 0a 01 01 d7 14 01 
0020  01 02 4e 21 4n 22 00 da 6d e0 00 01 02 03 04 05 
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 
0060  36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45 
0070  46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 
0080  56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 
0090  66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 
00a0  76 77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85 
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
To decode and display packets from a previously captured .pcap file, use the `show monitor capture file` command.

```plaintext
show monitor capture file
```

**Syntax Description**

- `name`: Specifies the filename.
- `display-filter`: Specifies the display filter string according to Wireshark's display-filter syntax.
- `brief`, `detailed`, `dump`: Determines the display mode.
  - `brief`: Displays a one line summary of the packet with key fields.
  - `detailed`: Displays all the fields in the packet for the protocols supported and displays the payload in hexadecimal form.
  - `dump`: Displays a one line summary of the packet with key fields and also displays the packet in hexadecimal form.

**Examples**

This example shows how to display packets from a .pcap file with a display filter:

```
Switch# show monitor capture file bootflash:test.pcap display-filter
```

This example displays a brief output from a .pcap file:

```
Switch# show monitor capture file bootflash: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
```
<table>
<thead>
<tr>
<th></th>
<th>Time</th>
<th>Source Address</th>
<th>Destination Address</th>
<th>Source Port</th>
<th>Destination Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>7.000000</td>
<td>10.1.1.147</td>
<td>20.1.1.2</td>
<td>20001</td>
<td>20002</td>
</tr>
<tr>
<td>2</td>
<td>8.000000</td>
<td>10.1.1.148</td>
<td>20.1.1.2</td>
<td>20001</td>
<td>20002</td>
</tr>
<tr>
<td>3</td>
<td>9.000000</td>
<td>10.1.1.149</td>
<td>20.1.1.2</td>
<td>20001</td>
<td>20002</td>
</tr>
<tr>
<td>4</td>
<td>10.000000</td>
<td>10.1.1.150</td>
<td>20.1.1.2</td>
<td>20001</td>
<td>20002</td>
</tr>
<tr>
<td>5</td>
<td>11.000000</td>
<td>10.1.1.151</td>
<td>20.1.1.2</td>
<td>20001</td>
<td>20002</td>
</tr>
<tr>
<td>6</td>
<td>12.000000</td>
<td>10.1.1.152</td>
<td>20.1.1.2</td>
<td>20001</td>
<td>20002</td>
</tr>
<tr>
<td>7</td>
<td>13.000000</td>
<td>10.1.1.153</td>
<td>20.1.1.2</td>
<td>20001</td>
<td>20002</td>
</tr>
<tr>
<td>8</td>
<td>14.000000</td>
<td>10.1.1.154</td>
<td>20.1.1.2</td>
<td>20001</td>
<td>20002</td>
</tr>
<tr>
<td>9</td>
<td>15.000000</td>
<td>10.1.1.155</td>
<td>20.1.1.2</td>
<td>20001</td>
<td>20002</td>
</tr>
<tr>
<td>10</td>
<td>16.000000</td>
<td>10.1.1.156</td>
<td>20.1.1.2</td>
<td>20001</td>
<td>20002</td>
</tr>
<tr>
<td>11</td>
<td>17.000000</td>
<td>10.1.1.157</td>
<td>20.1.1.2</td>
<td>20001</td>
<td>20002</td>
</tr>
<tr>
<td>12</td>
<td>18.000000</td>
<td>10.1.1.158</td>
<td>20.1.1.2</td>
<td>20001</td>
<td>20002</td>
</tr>
<tr>
<td>13</td>
<td>19.000000</td>
<td>10.1.1.159</td>
<td>20.1.1.2</td>
<td>20001</td>
<td>20002</td>
</tr>
<tr>
<td>14</td>
<td>20.000000</td>
<td>10.1.1.160</td>
<td>20.1.1.2</td>
<td>20001</td>
<td>20002</td>
</tr>
<tr>
<td>15</td>
<td>21.000000</td>
<td>10.1.1.161</td>
<td>20.1.1.2</td>
<td>20001</td>
<td>20002</td>
</tr>
<tr>
<td>16</td>
<td>22.000000</td>
<td>10.1.1.162</td>
<td>20.1.1.2</td>
<td>20001</td>
<td>20002</td>
</tr>
<tr>
<td>17</td>
<td>23.000000</td>
<td>10.1.1.163</td>
<td>20.1.1.2</td>
<td>20001</td>
<td>20002</td>
</tr>
<tr>
<td>18</td>
<td>24.000000</td>
<td>10.1.1.164</td>
<td>20.1.1.2</td>
<td>20001</td>
<td>20002</td>
</tr>
<tr>
<td>19</td>
<td>25.000000</td>
<td>10.1.1.165</td>
<td>20.1.1.2</td>
<td>20001</td>
<td>20002</td>
</tr>
<tr>
<td>20</td>
<td>26.000000</td>
<td>10.1.1.166</td>
<td>20.1.1.2</td>
<td>20001</td>
<td>20002</td>
</tr>
<tr>
<td>21</td>
<td>27.000000</td>
<td>10.1.1.167</td>
<td>20.1.1.2</td>
<td>20001</td>
<td>20002</td>
</tr>
<tr>
<td>22</td>
<td>28.000000</td>
<td>10.1.1.168</td>
<td>20.1.1.2</td>
<td>20001</td>
<td>20002</td>
</tr>
<tr>
<td>23</td>
<td>29.000000</td>
<td>10.1.1.169</td>
<td>20.1.1.2</td>
<td>20001</td>
<td>20002</td>
</tr>
<tr>
<td>24</td>
<td>30.000000</td>
<td>10.1.1.170</td>
<td>20.1.1.2</td>
<td>20001</td>
<td>20002</td>
</tr>
<tr>
<td>25</td>
<td>31.000000</td>
<td>10.1.1.171</td>
<td>20.1.1.2</td>
<td>20001</td>
<td>20002</td>
</tr>
<tr>
<td>26</td>
<td>32.000000</td>
<td>10.1.1.172</td>
<td>20.1.1.2</td>
<td>20001</td>
<td>20002</td>
</tr>
<tr>
<td>27</td>
<td>33.000000</td>
<td>10.1.1.173</td>
<td>20.1.1.2</td>
<td>20001</td>
<td>20002</td>
</tr>
<tr>
<td>28</td>
<td>34.000000</td>
<td>10.1.1.174</td>
<td>20.1.1.2</td>
<td>20001</td>
<td>20002</td>
</tr>
<tr>
<td>29</td>
<td>35.000000</td>
<td>10.1.1.175</td>
<td>20.1.1.2</td>
<td>20001</td>
<td>20002</td>
</tr>
<tr>
<td>30</td>
<td>36.000000</td>
<td>10.1.1.176</td>
<td>20.1.1.2</td>
<td>20001</td>
<td>20002</td>
</tr>
<tr>
<td>31</td>
<td>37.000000</td>
<td>10.1.1.177</td>
<td>20.1.1.2</td>
<td>20001</td>
<td>20002</td>
</tr>
<tr>
<td>32</td>
<td>38.000000</td>
<td>10.1.1.178</td>
<td>20.1.1.2</td>
<td>20001</td>
<td>20002</td>
</tr>
</tbody>
</table>
This 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]
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)
Frame 2: 256 bytes on wire (2048 bits), 256 bytes captured (2048 bits)
Arrival Time: Mar 21, 2012 14:35:10.111993000 PDT
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.

**Syntax Description**

- `attachment suppress interface`  
- `capability`  
- `notification interval`  
- `status`  
- `subscription`  
- `statistics {connection | summary}`

**Command Modes**

Privileged EXEC mode

**Examples**

This is an example of output from the `show nmsp attachment suppress interface` command:

```
Switch# show nmsp attachment suppress interface
NMSP Attachment Suppression Interfaces
--------------------------------------
GigabitEthernet1/1
GigabitEthernet1/2
Switch#
```

This is an example of output from the `show nmsp capability` command:

```
Switch# show nmsp capability
NMSP Switch Capability
------------------------
Service          Subservice
-----------       --------------
Attachment       Wired Station Location
Subscription
Switch#
```

This is an example of output from the `show nmsp notification interval` command:

```
Switch# show nmsp notification interval
NMSP Notification Intervals
----------------------------------
attachment suppress
interface
```

- `attachment suppress` 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` Displays the message counters on each connection.  
  - `summary` Displays the global counters.
- `status` Displays information about the NMSP connections.
- `subscription`  
  - `detail` Displays all services and subservices subscribed on each connection.
  - `summary` Displays all services subscribed on each connection.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

This is an example of output from the `show nmsp statistics connection` and `show nmsp statistics summary` commands:

```
Switch# show nmsp statistics connection
NMSP Connection Counters
----------------------------------
Connection 1:
Connection status: UP
Freed connection: 0
Tx message count
-----------------------     -----------------------
Subscr Resp: 1             Subscr Req: 1
Capa Notif: 1             Capa Notif: 1
Atta Resp: 1              Atta Req: 1
Loc Resp: 1               Loc Notif: 0
Unsupported msg: 0
Switch#
```

```
Switch# show nmsp statistics summary
NMSP Global Counters
------------------------
Send too big msg: 0     Failed socket write: 0
Partial socket write: 0
Socket write would block: 0
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 show subscription detail
Mobility Services Subscribed by 172.19.35.109:
Services
-------
Attachment:
---------
Wired Station
Location:
Subscription
Switch# show nmsp show subscription summary
```
<table>
<thead>
<tr>
<th>MSE IP Address</th>
<th>Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.19.35.109</td>
<td>Attachment, Location</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear nmsp</td>
<td>Clears the NMSP statistic counters.</td>
</tr>
<tr>
<td>nm sp</td>
<td>Configures Network Mobility Services Protocol (NMSP) on the switch.</td>
</tr>
</tbody>
</table>
To display information about the port channel, use the `show pagp` command.

```
show pagp [group-number]  
  [counters | dual-active | internal | neighbor]
```

**Syntax Description**

- This command has no default settings.
- **Command Modes**: Privileged EXEC mode

**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**

This example shows how to display information about the PAgP counter:

```
Switch# show pagp counters
Information        Flush
Port       Sent   Recv     Sent   Recv
--------------------------------------
Channel group: 1
Fa5/4    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
```

This 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 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 Partner
Port Detect Capable Name Port Version
Gi1/43 Yes VS3 Gi1/1/43 1.1
```

- **group-number**: (Optional) Channel-group number; valid values are from 1 to 64.
- **counters**: Specifies the traffic counter information.
- **dual-active**: Specifies the dual-active information.
- **internal**: Specifies the PAgP internal information.
- **neighbor**: Specifies the PAgP neighbor information.
This example shows how to display internal PAgP information:

```
Switch# show pagp 1 internal
Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
        A - Device is in Auto mode.
        Timers: H - Hello timer is running.        Q - Quit timer is running.
        S - Switching timer is running.    I - Interface timer is running.
Channel group 1
Hello    Partner  PAgP     Learning
Port      Flags State   Timers  Interval Count   Priority  Method
IfIndx
Fa5/4     SC    U6/S7           30s      1        128      Any
129
Fa5/5     SC    U6/S7           30s      1        128      Any
129
Switch#
```

This example shows how to display PAgP neighbor information for all neighbors:

```
Switch# show pagp neighbor
Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
        A - Device is in Auto mode.        P - Device learns on physical port.
Channel group 1 neighbors
Partner              Partner          Partner         Partner Group
Port      Name                 Device ID        Port       Age  Flags   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
Partner              Partner          Partner         Partner Group
Port      Name                 Device ID        Port       Age  Flags   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
- `pagp learn-method` Learns the input interface of the incoming packets.
- `pagp port-priority` Selects a port in hot standby mode.
To display information about the policy map, use the `show policy-map` command.

```
show policy-map [policy_map_name]
```

**Syntax Description**

- **policy_map_name**: (Optional) Name of the policy map.

**Defaults**

This command has no default settings.

**Command Modes**

- Privileged EXEC mode

**Examples**

This example shows how to display information for all the policy maps:

```
Switch# show policy-map
Policy Map ipp5-policy
  class ipp5
  set ip precedence 6
Switch#
```

This example shows how to display information for a specific policy map:

```
Switch# show policy-map ipp5-policy
Policy Map ipp5-policy
  class ipp5
  set ip precedence 6
Switch#
```

**Related Commands**

- `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.
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
```

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.

**Syntax Description**

- `input` (Optional) Displays statistics for the attached input policy.
- `class class-name` (Optional) Displays the name of the class.

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Usage Guidelines**

**Examples**

This example shows that the policy map TEST is associated with the control plane. This policy map polices traffic that matches the class-map TEST, while allowing all other traffic (that matches the class-map class-default) to go through as is. Table 2-30 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
```
show policy-map control-plane

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 2-30 show policy-map control-plane Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fields Associated with Classes or Service Polices</td>
<td>Name of the input service policy that is applied to the control plane. (If configured, this field will also show the output service policy.)</td>
</tr>
</tbody>
</table>
show policy-map control-plane

Related Commands

Class-map Class of traffic being displayed. Traffic is displayed for each configured class. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.

Match Match criteria for the specified class of traffic.

Note For more information about the variety of match criteria options available, refer to the chapter “Configuring the Modular Quality of Service Command-Line Interface” in the Cisco IOS Quality of Service Solutions Configuration Guide.

Fields Associated with Traffic Policing

The 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.

Table 2-30 show policy-map control-plane Field Descriptions (continued)

Field Description

Command Description

class-map
Enters class-map configuration mode. The class-name or number of the class to be configured.

service-policy input (control-plane)
Attaches a policy map to a control plane for aggregate control plane services.
Chapter 2 Cisco IOS Commands for the Catalyst 4500 Series Switches

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.

```
[[fastethernet] interface-number] | [[gigabitethernet] interface-number] | [port-channel number] | [vlan vlan_id]] [input | output]
```

**Syntax Description**

- `fastethernet` (Optional) Specifies the Fast Ethernet 802.3 interface.
- `gigabitethernet` (Optional) Specifies the Gigabit Ethernet 802.3z interface.
- `port-channel number` (Optional) Specifies the port channel.
- `vlan vlan_id` (Optional) Specifies the VLAN ID; valid values are from 1 to 4094.
- `input` (Optional) Specifies input policies only.
- `output` (Optional) Specifies output policies only.

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Examples**

This example shows how to display the statistics and configurations of all input and output policies attached to an interface:

```
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)
```

fastethernet

interface-number

(Optional) Specifies the Fast Ethernet 802.3 interface.

gigabitethernet

interface-number

(Optional) Specifies the Gigabit Ethernet 802.3z interface.

port-channel

number

(Optional) Specifies the port channel.

vlan

vlan_id

(Optional) Specifies the VLAN ID; valid values are from 1 to 4094.

input

(Optional) Specifies input policies only.

output

(Optional) Specifies output policies only.
This example shows how to display the input policy statistics and configurations for a specific interface:

Switch# show policy-map interface fastethernet 5/36 input

service-policy input: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

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 l4 source-port l4 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 l4 source-port l4 destination-port

Switch# show policy-map p1
Policy Map p1
  Class c1
  police 1000000 bps 9000 byte conform-action transmit exceed-action drop
show policy-map interface

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 l4 source-port l4 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.
To show the QoS policy-map information applied to a specific VLAN on an interface, use the `show policy-map interface vlan` command.

**Syntax Description**

- `show policy-map interface vlan`

**Command Modes**

- Privileged EXEC mode

**Examples**

The following example shows a typical 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
```

This example shows how to display policy-map statistics on VLAN 20 on the Gigabit Ethernet 6/1 interface:

```
Switch# show policy-map interface gigabitEthernet 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
```

The following example shows a configuration on a non-Supervisor Engine 6-E:

```
interface fastethernet6/1
vlan-range 100
service-policy in p1
```

This example shows how to display policy-map statistics on VLAN 100 on the FastEthernet interface:

```
Switch# show policy-map interface fastEthernet 6/1 vlan 100
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
```
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

show policy-map interface vlan

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

This example shows how to display policy-map statistics on VLAN 100 on the FastEthernet interface:

Switch#

show policy-map interface gigabitethernet 3/1 vlan 100

GigabitEthernet3/1 vlan 100

Service-policy input: p1

Class-map: 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.
Chapter 2  Cisco IOS Commands for the Catalyst 4500 Series Switches

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

**Usage Guidelines**

- If you enter the command without keywords, the output includes the administrative and operational status of all secure ports on the switch.
- If you enter the `interface-id` value or `port-channel-interface` value, the `show port-security` command displays port security settings for the interface.
- If you enter the `address` keyword, the `show port-security address` command displays the secure MAC addresses for all interfaces and the aging information for each secure address.
- If you enter the `interface-id` value and the `address` keyword, the `show port-security address interface` command displays all the MAC addresses for the interface with aging information for each secure address. You can also use this command to display all the MAC addresses for an interface even if you have not enabled port security on it.
- Sticky MAC addresses are addresses that persist across switch reboots and link flaps.

**Examples**

This example shows how to display port security settings for the entire switch:

```
Switch# show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
(Count)       (Count)          (Count)          (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
```
<table>
<thead>
<tr>
<th>Interface</th>
<th>Port Status</th>
<th>Security Violation Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa3/14</td>
<td>Secure-up</td>
<td>0</td>
</tr>
<tr>
<td>Fa3/15</td>
<td>Secure-up</td>
<td>0</td>
</tr>
<tr>
<td>Fa3/16</td>
<td>Secure-up</td>
<td>0</td>
</tr>
<tr>
<td>Po2</td>
<td>Secure-up</td>
<td>0</td>
</tr>
</tbody>
</table>

This example shows how to display port security settings for interface Fast Ethernet port 1:

Switch# show port-security interface fastethernet 5/1

Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address        : 0000.0001.001a
Security Violation Count   : 0
Switch#
show port-security

This example shows how to display all secure MAC addresses configured on all switch interfaces:

Switch#

show port-security address

Secure Mac Address Table

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Mac Address</th>
<th>Type</th>
<th>Ports</th>
<th>Remaining Age (mins)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0000.0001.0000</td>
<td>SecureConfigured</td>
<td>Fa3/1</td>
<td>15 (I)</td>
</tr>
<tr>
<td>1</td>
<td>0000.0001.0001</td>
<td>SecureConfigured</td>
<td>Fa3/1</td>
<td>14 (I)</td>
</tr>
<tr>
<td>1</td>
<td>0000.0001.0100</td>
<td>SecureConfigured</td>
<td>Fa3/2</td>
<td>-</td>
</tr>
<tr>
<td>1</td>
<td>0000.0001.0101</td>
<td>SecureConfigured</td>
<td>Fa3/2</td>
<td>-</td>
</tr>
<tr>
<td>1</td>
<td>0000.0001.0200</td>
<td>SecureConfigured</td>
<td>Fa3/3</td>
<td>-</td>
</tr>
<tr>
<td>1</td>
<td>0000.0001.0201</td>
<td>SecureConfigured</td>
<td>Fa3/3</td>
<td>-</td>
</tr>
<tr>
<td>1</td>
<td>0000.0001.0300</td>
<td>SecureConfigured</td>
<td>Fa3/4</td>
<td>-</td>
</tr>
<tr>
<td>1</td>
<td>0000.0001.0301</td>
<td>SecureConfigured</td>
<td>Fa3/4</td>
<td>-</td>
</tr>
<tr>
<td>1</td>
<td>0000.0001.1000</td>
<td>SecureDynamic</td>
<td>Fa3/5</td>
<td>-</td>
</tr>
<tr>
<td>1</td>
<td>0000.0001.1001</td>
<td>SecureDynamic</td>
<td>Fa3/5</td>
<td>-</td>
</tr>
<tr>
<td>1</td>
<td>0000.0001.1100</td>
<td>SecureDynamic</td>
<td>Fa3/6</td>
<td>-</td>
</tr>
<tr>
<td>1</td>
<td>0000.0001.1101</td>
<td>SecureDynamic</td>
<td>Fa3/6</td>
<td>-</td>
</tr>
<tr>
<td>1</td>
<td>0000.0001.1200</td>
<td>SecureSticky</td>
<td>Fa3/7</td>
<td>-</td>
</tr>
<tr>
<td>1</td>
<td>0000.0001.1201</td>
<td>SecureSticky</td>
<td>Fa3/7</td>
<td>-</td>
</tr>
<tr>
<td>1</td>
<td>0000.0001.1300</td>
<td>SecureSticky</td>
<td>Fa3/8</td>
<td>-</td>
</tr>
<tr>
<td>1</td>
<td>0000.0001.1301</td>
<td>SecureSticky</td>
<td>Fa3/8</td>
<td>-</td>
</tr>
<tr>
<td>1</td>
<td>0000.0001.2000</td>
<td>SecureSticky</td>
<td>Po2</td>
<td>-</td>
</tr>
</tbody>
</table>

Total Addresses in System (excluding one mac per port) : 8
Max Addresses limit in System (excluding one mac per port) : 3072

This example shows how to display the maximum allowed number of secure MAC addresses and the current number of secure MAC addresses on interface Gigabitethernet1/1:

Switch#

show port-security interface gigabitethernet1/1 vlan

Default maximum: 22

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Maximum</th>
<th>Current</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>22</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>22</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>22</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>22</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>22</td>
<td>2</td>
</tr>
</tbody>
</table>

This example shows how to display the port security settings on interface Gigabitethernet1/1 for VLANs 2 and 3:

Switch#

show port-security interface gigabitethernet1/1 vlan 2-3

Default maximum: 22

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Maximum</th>
<th>Current</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>22</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>22</td>
<td>3</td>
</tr>
</tbody>
</table>

This example shows how to display all secure MAC addresses configured on interface Gigabitethernet1/1 with aging information for each address.

Switch#

show port-security interface gigabitethernet1/1 address

Secure Mac Address Table

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Mac Address</th>
<th>Type</th>
<th>Ports</th>
<th>Remaining Age (mins)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>0001.0001.0001</td>
<td>SecureConfigured</td>
<td>Gi1/1</td>
<td>-</td>
</tr>
<tr>
<td>2</td>
<td>0001.0001.0002</td>
<td>SecureSticky</td>
<td>Gi1/1</td>
<td>-</td>
</tr>
<tr>
<td>3</td>
<td>0001.0001.0001</td>
<td>SecureConfigured</td>
<td>Gi1/1</td>
<td>-</td>
</tr>
<tr>
<td>3</td>
<td>0001.0001.0002</td>
<td>SecureSticky</td>
<td>Gi1/1</td>
<td>-</td>
</tr>
<tr>
<td>3</td>
<td>0001.0001.0003</td>
<td>SecureSticky</td>
<td>Gi1/1</td>
<td>-</td>
</tr>
</tbody>
</table>
This example shows how to display all secure MAC addresses configured on VLANs 2 and 3 on interface Gigabitethernet1/1 with aging information for each address:

```
Switch#
    show port-security interface gigabitethernet1/1 address vlan 2-3
```

Secure Mac Address Table

```
<table>
<thead>
<tr>
<th>Vlan</th>
<th>Mac Address</th>
<th>Type</th>
<th>Ports</th>
<th>Remaining Age(mins)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>0001.0001.0001</td>
<td>SecureConfigured</td>
<td>Gi1/1</td>
<td>-</td>
</tr>
<tr>
<td>2</td>
<td>0001.0001.0002</td>
<td>SecureSticky</td>
<td>Gi1/1</td>
<td>-</td>
</tr>
<tr>
<td>2</td>
<td>0001.0001.0003</td>
<td>SecureSticky</td>
<td>Gi1/1</td>
<td>-</td>
</tr>
<tr>
<td>3</td>
<td>0001.0001.0001</td>
<td>SecureConfigured</td>
<td>Gi1/1</td>
<td>-</td>
</tr>
<tr>
<td>3</td>
<td>0001.0001.0002</td>
<td>SecureSticky</td>
<td>Gi1/1</td>
<td>-</td>
</tr>
<tr>
<td>3</td>
<td>0001.0001.0003</td>
<td>SecureSticky</td>
<td>Gi1/1</td>
<td>-</td>
</tr>
</tbody>
</table>
```

Total Addresses: 12

Switch#

This example shows how to display the maximum allowed number of secure MAC addresses and the current number of secure MAC addresses on Fast Ethernet port 1:

```
Switch#
    show port-security interface fastethernet5/1 vlan
```

Default maximum: 22

```
VLAN  Maximum    Current
------    -------    -------
2         22          3
3         22          3
5         22          1
6         22          2
```

Switch#

This example shows how to display the port security settings on Fast Ethernet port 1 for VLANs 2 and 3:

```
Switch#
    show port-security interface fastethernet5/1 vlan 2-3
```

Default maximum: 22

```
VLAN  Maximum    Current
------    -------    -------
2         22          3
3         22          3
```

Switch#

This example shows how to display all secure MAC addresses configured on Fast Ethernet port 1 with aging information for each address.

```
Switch#
    show port-security interface fastethernet5/1 address
```

Secure Mac Address Table

```
<table>
<thead>
<tr>
<th>Vlan</th>
<th>Mac Address</th>
<th>Type</th>
<th>Ports</th>
<th>Remaining Age(mins)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>0001.0001.0001</td>
<td>SecureConfigured</td>
<td>Gi1/1</td>
<td>-</td>
</tr>
<tr>
<td>2</td>
<td>0001.0001.0002</td>
<td>SecureSticky</td>
<td>Gi1/1</td>
<td>-</td>
</tr>
<tr>
<td>2</td>
<td>0001.0001.0003</td>
<td>SecureSticky</td>
<td>Gi1/1</td>
<td>-</td>
</tr>
<tr>
<td>3</td>
<td>0001.0001.0001</td>
<td>SecureConfigured</td>
<td>Gi1/1</td>
<td>-</td>
</tr>
<tr>
<td>3</td>
<td>0001.0001.0002</td>
<td>SecureSticky</td>
<td>Gi1/1</td>
<td>-</td>
</tr>
</tbody>
</table>
```

Total Addresses: 12

Switch#
This example shows how to display all secure MAC addresses configured on VLANs 2 and 3 on Fast Ethernet port 1 with aging information for each address:

Switch# show port-security interface fastethernet5/1 address vlan 2-3

Secure Mac Address Table

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Mac Address</th>
<th>Type</th>
<th>Ports</th>
<th>Remaining Age(mins)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>0001.0001.0001</td>
<td>SecureConfigured</td>
<td>Gi1/1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>0001.0001.0002</td>
<td>SecureSticky</td>
<td>Gi1/1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>0001.0001.0003</td>
<td>SecureSticky</td>
<td>Gi1/1</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>0001.0001.0001</td>
<td>SecureConfigured</td>
<td>Gi1/1</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>0001.0001.0002</td>
<td>SecureSticky</td>
<td>Gi1/1</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>0001.0001.0003</td>
<td>SecureSticky</td>
<td>Gi1/1</td>
<td></td>
</tr>
</tbody>
</table>

Total Addresses: 12

This example shows how to display all secure MAC addresses configured on all switch interfaces:

Switch# show port-security address

Secure Mac Address Table

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Mac Address</th>
<th>Type</th>
<th>Ports</th>
<th>Remaining Age</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0000.0001.0000</td>
<td>SecureConfigured</td>
<td>Fa3/1</td>
<td>15 (I)</td>
</tr>
<tr>
<td>1</td>
<td>0000.0001.0001</td>
<td>SecureConfigured</td>
<td>Fa3/1</td>
<td>14 (I)</td>
</tr>
<tr>
<td>1</td>
<td>0000.0001.0100</td>
<td>SecureConfigured</td>
<td>Fa3/2</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0000.0001.0101</td>
<td>SecureConfigured</td>
<td>Fa3/2</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0000.0001.0200</td>
<td>SecureConfigured</td>
<td>Fa3/3</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0000.0001.0201</td>
<td>SecureConfigured</td>
<td>Fa3/3</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0000.0001.0300</td>
<td>SecureConfigured</td>
<td>Fa3/4</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0000.0001.0301</td>
<td>SecureConfigured</td>
<td>Fa3/4</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0000.0001.1000</td>
<td>SecureDynamic</td>
<td>Fa3/5</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0000.0001.1001</td>
<td>SecureDynamic</td>
<td>Fa3/5</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0000.0001.1100</td>
<td>SecureDynamic</td>
<td>Fa3/6</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0000.0001.1101</td>
<td>SecureDynamic</td>
<td>Fa3/6</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0000.0001.1200</td>
<td>SecureSticky</td>
<td>Fa3/7</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0000.0001.1201</td>
<td>SecureSticky</td>
<td>Fa3/7</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0000.0001.1300</td>
<td>SecureSticky</td>
<td>Fa3/8</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0000.0001.1301</td>
<td>SecureSticky</td>
<td>Fa3/8</td>
<td></td>
</tr>
</tbody>
</table>

Total Addresses in System (excluding one mac per port) :8
Max Addresses limit in System (excluding one mac per port) :3072

This example shows how to display the maximum allowed number of secure MAC addresses and the current number of secure MAC addresses on interface Gigabitethernet1/1:

Switch# show port-security interface gigabitethernet1/1 vlan

Default maximum: 22

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Maximum</th>
<th>Current</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>22</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>22</td>
<td>3</td>
</tr>
</tbody>
</table>
This example shows how to display the port security settings on interface Gigabitethernet1/1 for VLANs 2 and 3:

Switch# show port-security interface gigabitethernet1/1 vlan 2-3

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Maximum</th>
<th>Current</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>22</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>22</td>
<td>3</td>
</tr>
</tbody>
</table>

Switch# show port-security interface gigabitethernet1/1 address

Secure Mac Address Table

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Mac Address</th>
<th>Type</th>
<th>Ports</th>
<th>Remaining Age(mins)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>0001.0001.0001</td>
<td>SecureConfigured</td>
<td>Gi1/1</td>
<td>-</td>
</tr>
<tr>
<td>2</td>
<td>0001.0001.0002</td>
<td>SecureSticky</td>
<td>Gi1/1</td>
<td>-</td>
</tr>
<tr>
<td>3</td>
<td>0001.0001.0001</td>
<td>SecureConfigured</td>
<td>Gi1/1</td>
<td>-</td>
</tr>
<tr>
<td>3</td>
<td>0001.0001.0002</td>
<td>SecureSticky</td>
<td>Gi1/1</td>
<td>-</td>
</tr>
<tr>
<td>3</td>
<td>0001.0001.0003</td>
<td>SecureSticky</td>
<td>Gi1/1</td>
<td>-</td>
</tr>
<tr>
<td>4</td>
<td>0001.0001.0001</td>
<td>SecureConfigured</td>
<td>Gi1/1</td>
<td>-</td>
</tr>
<tr>
<td>4</td>
<td>0001.0001.0003</td>
<td>SecureSticky</td>
<td>Gi1/1</td>
<td>-</td>
</tr>
<tr>
<td>6</td>
<td>0001.0001.0001</td>
<td>SecureConfigured</td>
<td>Gi1/1</td>
<td>-</td>
</tr>
<tr>
<td>6</td>
<td>0001.0001.0002</td>
<td>SecureConfigured</td>
<td>Gi1/1</td>
<td>-</td>
</tr>
</tbody>
</table>

Total Addresses: 12

Switch# show port-security interface gigabitethernet1/1 address vlan 2-3

Secure Mac Address Table

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Mac Address</th>
<th>Type</th>
<th>Ports</th>
<th>Remaining Age(mins)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>0001.0001.0001</td>
<td>SecureConfigured</td>
<td>Gi1/1</td>
<td>-</td>
</tr>
<tr>
<td>2</td>
<td>0001.0001.0002</td>
<td>SecureSticky</td>
<td>Gi1/1</td>
<td>-</td>
</tr>
<tr>
<td>2</td>
<td>0001.0001.0003</td>
<td>SecureSticky</td>
<td>Gi1/1</td>
<td>-</td>
</tr>
<tr>
<td>3</td>
<td>0001.0001.0001</td>
<td>SecureConfigured</td>
<td>Gi1/1</td>
<td>-</td>
</tr>
<tr>
<td>3</td>
<td>0001.0001.0002</td>
<td>SecureSticky</td>
<td>Gi1/1</td>
<td>-</td>
</tr>
<tr>
<td>3</td>
<td>0001.0001.0003</td>
<td>SecureSticky</td>
<td>Gi1/1</td>
<td>-</td>
</tr>
</tbody>
</table>

Total Addresses: 12

Switch#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>switchport port-security</td>
<td>Enables port security on an interface.</td>
</tr>
</tbody>
</table>
To display information about the power status, use the `show power` command.

```
Syntax Description
```

This command has no default settings.

```
Command Modes
```

Privileged EXEC mode

```
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
```

This example shows how to display information about the general power supply:

```
Switch# show power
Power                                             Fan     Inline
Supply  Model No          Type       Status       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***
```

```
available
```
(Optional) Displays the available system power.

```
capabilities
```
(Optional) Displays the individual power supply capabilities.

```
detail
```
(Optional) Displays detailed information on power resources.

```
inline
```
(Optional) Displays the PoE status.

```
interface
detail
```
(Optional) Detailed information on the PoE status for the interface

```
consumption default
```
(Optional) Displays the PoE consumption.

```
module
```
```
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.
show power

Power supplies needed by system : 1
Power supplies currently available : 1

Power Summary

<table>
<thead>
<tr>
<th></th>
<th>Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Power (12V)</td>
<td>328</td>
</tr>
<tr>
<td>Inline Power (50V)</td>
<td>0</td>
</tr>
<tr>
<td>Backplane Power (3.3V)</td>
<td>10</td>
</tr>
</tbody>
</table>

Total Used: 338 (not to exceed Total Maximum Available = 750)

Switch#

Example shows how to display the amount of available system power:

Switch#
show power available

Power Summary

<table>
<thead>
<tr>
<th></th>
<th>Available</th>
<th>Used</th>
<th>Remaining</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Power</td>
<td>1360</td>
<td>280</td>
<td>1080</td>
</tr>
<tr>
<td>Inline Power</td>
<td>1400</td>
<td>0</td>
<td>1400</td>
</tr>
<tr>
<td>Maximum Power</td>
<td>2800</td>
<td>280</td>
<td>2520</td>
</tr>
</tbody>
</table>

Switch#

Example shows how to display the power status information:

Switch#
show power status

Power                                             Fan     Inline
Supply  Model No          Type       Status       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
---------------  ------  ------  ------  ------  --------
PS1             1400    1400    1360    1360    2800
PS2             1400    1400    1360    1360    2800

Switch#

Example shows how to verify the PoE consumption for the switch:

Switch#
show power inline consumption default

Default PD consumption : 5000 mW

Switch#

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

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.
Chapter 2      Cisco IOS Commands for  the Catalyst 4500 Series Switches

show power

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#

This example shows how to display the number of power supplies needed by the system:

Switch#

show power supplies

Power supplies needed by system = 2

Switch#

This example shows how to display the PoE status for Fast Ethernet interface 3/1:

Switch#

show power inline fastethernet3/1

Available:677(w)  Used: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       (Watts)           (Watts)
From PS    To Device
--------- --------------- --------------------
Fa3/1                 15.4                 10.0

Switch#

The output of the commands show power 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                                             Fan      Inline
Supply  Model No          Type       Status       Sensor   Status
------  ----------------  ---------  -----------  -------  -------  
PS1     PWR-C45-1400DC    DCSP1400W  good         good     n.a.
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
### Chapter 2: Cisco IOS Commands for the Catalyst 4500 Series Switches

#### show power

**Power Summary**

<table>
<thead>
<tr>
<th></th>
<th>Maximum</th>
<th>Used</th>
<th>Available</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Power (12V)</td>
<td>360</td>
<td>360</td>
<td></td>
</tr>
<tr>
<td>Inline Power (-50V)</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Backplane Power (3.3V)</td>
<td>0</td>
<td>40</td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>360</td>
<td>400</td>
<td></td>
</tr>
</tbody>
</table>

#### Module Inline Power Summary (Watts) (12V -> -48V on board conversion)

<table>
<thead>
<tr>
<th>Mod</th>
<th>Used</th>
<th>Available</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>5</td>
<td>25</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Watts Used of System Power (12V)

<table>
<thead>
<tr>
<th>Mod</th>
<th>Model</th>
<th>currently</th>
<th>out of reset</th>
<th>in reset</th>
<th>Efficiency</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>WS-X4013+TS</td>
<td>180</td>
<td>180</td>
<td>180</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>WS-X4506-GB-T</td>
<td>60</td>
<td>60</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>WS-X4424-GB-RJ45</td>
<td>90</td>
<td>90</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td>--</td>
<td>Fan Tray</td>
<td>30</td>
<td>--</td>
<td>--</td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td>360</td>
<td>330</td>
<td>250</td>
<td></td>
</tr>
</tbody>
</table>

#### Watts used of Chassis Inline Power (-50V)

<table>
<thead>
<tr>
<th>Mod</th>
<th>Model</th>
<th>PS</th>
<th>Device</th>
<th>PS</th>
<th>Device</th>
<th>Efficiency</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>WS-X4506-GB-T</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>89</td>
</tr>
<tr>
<td>3</td>
<td>WS-X4424-GB-RJ45</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-</td>
</tr>
</tbody>
</table>

#### Watts used of Module Inline Power (12V -> -50V)

<table>
<thead>
<tr>
<th>Mod</th>
<th>Model</th>
<th>PS</th>
<th>Device</th>
<th>PS</th>
<th>Device</th>
<th>Efficiency</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>WS-X4013+TS</td>
<td>6</td>
<td>5</td>
<td>3</td>
<td>3</td>
<td>90</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td>6</td>
<td>5</td>
<td>3</td>
<td>3</td>
<td>-</td>
</tr>
</tbody>
</table>
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

show power

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#

This 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#

This example shows how to display the PoE status for all all ports of the module:

Switch#
show module

Chassis Type : WS-C4503-E
Power consumed by backplane : 0 Watts

Mod Ports Card Type                              Model              Serial No.
---+-----+--------------------------------------+------------------+----
1     6  Sup 6-E 10GE (X2), 1000BaseX (SFP)     WS-X45-SUP6-E      JAE1132SXRP
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
show power

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
show power

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
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

show power

Power drawn from the source: 0.0
Power available to the device: 0.0

Related Commands

- **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.
To display PoE policing and monitoring status, use the `show power inline police` command.

```
show power inline police [interfacename] [module n]
```

**Syntax Description**

- `interfacename` (optional): Displays PoE policing and monitoring status for a particular interface.
- `module n` (optional): Display PoE policing and monitoring status for all interfaces on this module.

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Usage Guidelines**

- The `Oper Power` field displays the true power consumption of the connected device.
- If this command is executed at the global level, the last line of the output under the `Oper Power` field displays the total true inline power consumption of all devices connected to the switch.

**Examples**

This example shows how to display PoE policing status for a interface GigabitEthernet 2/1:

```
Switch# show power inline police gigabitEthernet 2/1
Available:421(w)  Used:44(w)  Remaining:377(w)
Interface Admin  Oper       Admin  Oper       Cutoff  Oper
              State  State      Police Power  Power
--------- ------ ---------- ---------- ---------- ------ -----
Gi2/1     auto   on         errdisable ok         22.6   9.6
```

**Related Commands**

- `power inline police`: Configures PoE policing on a particular interface.
To display PPPoE Intermediate Agent configuration and statistics (packet counters), use the
`show pppoe intermediate-agent interface` command.

```
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
```

This example shows how to display PPPoE Intermediate Agent statistics on an interface:

```
Switch# show pppoe intermediate-agent statistics interface g3/7
Interface : GigabitEthernet3/7
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
```

Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

show pppoe intermediate-agent interface

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.
To display QoS information, use the `show qos` command.

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Examples**

This example shows the output that might be displayed if you do not enter any keywords:

```
Switch# show qos
QoS is enabled globally
Switch#
```

**Related Commands**

- `qos account layer-all encapsulation`
  
  Globally enables QoS functionality on the switch.
To display QoS aggregate policer information, use the `show qos aggregate policer` command.

```
show qos aggregate policer
```

Syntax Description

- `aggregate_name` (Optional) Named aggregate policer.

Defaults

This command has no default settings.

Command Modes

- Privileged EXEC mode

Usage Guidelines

The aggregate policer name is case sensitive.

Examples

This example shows the output if you do not enter any keywords:

```
Switch# show qos aggregate policer
Policer 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

- `aggregate_name`
- `qos t rust`
  Defines a named aggregate policer.
To display global Dynamic Buffer Limiting (DBL) information, use the `show qos dbl` command.

**Syntax**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Examples**

This example shows how to display global DBL information:

```
Switch# show qos dbl
DBL is enabled globally
DBL flow includes vlan
DBL flow includes l4-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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>qos account layer-all encapsulation</td>
<td>Globally enables QoS functionality on the switch.</td>
</tr>
</tbody>
</table>
show qos interface

To display queueing information, use the `show qos interface` command.

```
show qos interface
{fastethernet interface-number | gigabitethernet interface-number} |
[vlan vlan_id | port-channel number]
```

**Syntax Description**

- **fastethernet** `interface-number`: Specifies the Fast Ethernet 802.3 interface.
- **gigabitethernet** `interface-number`: Specifies the Gigabit Ethernet 802.3z interface.
- **vlan** `vlan_id`: (Optional) Specifies the VLAN ID; valid values are from 1 to 4094.
- **port-channel** `number`: (Optional) Specifies the port channel; valid ranges are from 1 to 64.

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Examples**

This example shows how to display queueing information:

```
Switch# show qos interface fastethernet 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)                (packets)
1        31250000    disabled    N/A        240
2        31250000    disabled    normal     240
3        31250000    disabled    N/A        240

Switch#
```

**Related Commands**

- `fastethernet interface-number`: Specifies the Fast Ethernet 802.3 interface.
- `gigabitethernet interface-number`: Specifies the Gigabit Ethernet 802.3z interface.
- `vlan vlan_id`: (Optional) Specifies the VLAN ID; valid values are from 1 to 4094.
- `port-channel number`: (Optional) Specifies the port channel; valid ranges are from 1 to 64.
To display QoS map information, use the `show qos maps` command.

### Syntax Description
- `cos` (Optional) Displays CoS map information.
- `dscp` (Optional) Displays DSCP map information.
- `policed` (Optional) Displays policed map information.
- `tx-queue` (Optional) Displays tx-queue map information.

### Defaults
This command has no default settings.

### Command Modes
- Privileged EXEC mode

### Examples
This example shows how to display QoS map settings:

```bash
Switch# show qos maps
DSCP-TxQueue Mapping Table (dscp = d1d2)
<table>
<thead>
<tr>
<th>d1 :d2</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 :</td>
<td>01</td>
<td>01</td>
<td>01</td>
<td>01</td>
<td>01</td>
<td>01</td>
<td>01</td>
<td>01</td>
<td>01</td>
<td>01</td>
</tr>
<tr>
<td>1 :</td>
<td>01</td>
<td>01</td>
<td>01</td>
<td>01</td>
<td>01</td>
<td>01</td>
<td>02</td>
<td>02</td>
<td>02</td>
<td>02</td>
</tr>
<tr>
<td>2 :</td>
<td>02</td>
<td>02</td>
<td>02</td>
<td>02</td>
<td>02</td>
<td>02</td>
<td>02</td>
<td>02</td>
<td>02</td>
<td>02</td>
</tr>
<tr>
<td>3 :</td>
<td>02</td>
<td>02</td>
<td>03</td>
<td>03</td>
<td>03</td>
<td>03</td>
<td>03</td>
<td>03</td>
<td>03</td>
<td>03</td>
</tr>
<tr>
<td>4 :</td>
<td>03</td>
<td>03</td>
<td>03</td>
<td>03</td>
<td>03</td>
<td>03</td>
<td>03</td>
<td>04</td>
<td>04</td>
<td>04</td>
</tr>
<tr>
<td>5 :</td>
<td>04</td>
<td>04</td>
<td>04</td>
<td>04</td>
<td>04</td>
<td>04</td>
<td>04</td>
<td>04</td>
<td>04</td>
<td>04</td>
</tr>
<tr>
<td>6 :</td>
<td>04</td>
<td>04</td>
<td>04</td>
<td>04</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Policed DSCP Mapping Table (dscp = d1d2)
<table>
<thead>
<tr>
<th>d1 :d2</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 :</td>
<td>00</td>
<td>01</td>
<td>02</td>
<td>03</td>
<td>04</td>
<td>05</td>
<td>06</td>
<td>07</td>
<td>08</td>
<td>09</td>
</tr>
<tr>
<td>1 :</td>
<td>10</td>
<td>11</td>
<td>12</td>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>17</td>
<td>18</td>
<td>19</td>
</tr>
<tr>
<td>2 :</td>
<td>20</td>
<td>21</td>
<td>22</td>
<td>23</td>
<td>24</td>
<td>25</td>
<td>26</td>
<td>27</td>
<td>28</td>
<td>29</td>
</tr>
<tr>
<td>3 :</td>
<td>30</td>
<td>31</td>
<td>32</td>
<td>33</td>
<td>34</td>
<td>35</td>
<td>36</td>
<td>37</td>
<td>38</td>
<td>39</td>
</tr>
<tr>
<td>4 :</td>
<td>40</td>
<td>41</td>
<td>42</td>
<td>43</td>
<td>44</td>
<td>45</td>
<td>46</td>
<td>47</td>
<td>48</td>
<td>49</td>
</tr>
<tr>
<td>5 :</td>
<td>50</td>
<td>51</td>
<td>52</td>
<td>53</td>
<td>54</td>
<td>55</td>
<td>56</td>
<td>57</td>
<td>58</td>
<td>59</td>
</tr>
<tr>
<td>6 :</td>
<td>60</td>
<td>61</td>
<td>62</td>
<td>63</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

DSCP-CoS Mapping Table (dscp = d1d2)
<table>
<thead>
<tr>
<th>d1 :d2</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 :</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>01</td>
<td>01</td>
</tr>
<tr>
<td>1 :</td>
<td>01</td>
<td>01</td>
<td>01</td>
<td>01</td>
<td>01</td>
<td>01</td>
<td>02</td>
<td>02</td>
<td>02</td>
<td>02</td>
</tr>
<tr>
<td>2 :</td>
<td>02</td>
<td>02</td>
<td>02</td>
<td>02</td>
<td>03</td>
<td>03</td>
<td>03</td>
<td>03</td>
<td>03</td>
<td>03</td>
</tr>
<tr>
<td>3 :</td>
<td>03</td>
<td>03</td>
<td>04</td>
<td>04</td>
<td>04</td>
<td>04</td>
<td>04</td>
<td>04</td>
<td>04</td>
<td>04</td>
</tr>
<tr>
<td>4 :</td>
<td>05</td>
<td>05</td>
<td>05</td>
<td>05</td>
<td>05</td>
<td>05</td>
<td>05</td>
<td>05</td>
<td>06</td>
<td>06</td>
</tr>
<tr>
<td>5 :</td>
<td>06</td>
<td>06</td>
<td>06</td>
<td>06</td>
<td>06</td>
<td>06</td>
<td>07</td>
<td>07</td>
<td>07</td>
<td>07</td>
</tr>
<tr>
<td>6 :</td>
<td>07</td>
<td>07</td>
<td>07</td>
<td>07</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

CoS-DSCP Mapping Table
<table>
<thead>
<tr>
<th>d1 :d2</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 :</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>01</td>
<td>01</td>
</tr>
<tr>
<td>1 :</td>
<td>01</td>
<td>01</td>
<td>01</td>
<td>01</td>
<td>01</td>
<td>01</td>
<td>02</td>
<td>02</td>
<td>02</td>
<td>02</td>
</tr>
<tr>
<td>2 :</td>
<td>02</td>
<td>02</td>
<td>02</td>
<td>02</td>
<td>03</td>
<td>03</td>
<td>03</td>
<td>03</td>
<td>03</td>
<td>03</td>
</tr>
<tr>
<td>3 :</td>
<td>03</td>
<td>03</td>
<td>04</td>
<td>04</td>
<td>04</td>
<td>04</td>
<td>04</td>
<td>04</td>
<td>04</td>
<td>04</td>
</tr>
<tr>
<td>4 :</td>
<td>05</td>
<td>05</td>
<td>05</td>
<td>05</td>
<td>05</td>
<td>05</td>
<td>05</td>
<td>05</td>
<td>06</td>
<td>06</td>
</tr>
<tr>
<td>5 :</td>
<td>06</td>
<td>06</td>
<td>06</td>
<td>06</td>
<td>06</td>
<td>06</td>
<td>07</td>
<td>07</td>
<td>07</td>
<td>07</td>
</tr>
<tr>
<td>6 :</td>
<td>07</td>
<td>07</td>
<td>07</td>
<td>07</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

CoS-DSCP Mapping Table
<table>
<thead>
<tr>
<th>d1 :d2</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 :</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>01</td>
<td>01</td>
</tr>
<tr>
<td>1 :</td>
<td>01</td>
<td>01</td>
<td>01</td>
<td>01</td>
<td>01</td>
<td>01</td>
<td>02</td>
<td>02</td>
<td>02</td>
<td>02</td>
</tr>
<tr>
<td>2 :</td>
<td>02</td>
<td>02</td>
<td>02</td>
<td>02</td>
<td>03</td>
<td>03</td>
<td>03</td>
<td>03</td>
<td>03</td>
<td>03</td>
</tr>
<tr>
<td>3 :</td>
<td>03</td>
<td>03</td>
<td>04</td>
<td>04</td>
<td>04</td>
<td>04</td>
<td>04</td>
<td>04</td>
<td>04</td>
<td>04</td>
</tr>
<tr>
<td>4 :</td>
<td>05</td>
<td>05</td>
<td>05</td>
<td>05</td>
<td>05</td>
<td>05</td>
<td>05</td>
<td>05</td>
<td>06</td>
<td>06</td>
</tr>
<tr>
<td>5 :</td>
<td>06</td>
<td>06</td>
<td>06</td>
<td>06</td>
<td>06</td>
<td>06</td>
<td>07</td>
<td>07</td>
<td>07</td>
<td>07</td>
</tr>
<tr>
<td>6 :</td>
<td>07</td>
<td>07</td>
<td>07</td>
<td>07</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

show qos maps

CoS:  0  1  2  3  4  5  6  7

--------------------------------

DSCP:  0  8 16 24 32 40 48 56

Switch#

Related Commands

qos account layer-all encapsulation
Globally enables QoS functionality on the switch.
To display redundancy facility information, use the `show redundancy` command.

```
show redundancy {
  clients |
  counters |
  history |
  states  }
```

**Syntax Description**

- **clients** (Optional) Displays information about the redundancy facility client.
- **counters** (Optional) Displays information about the redundancy facility counter.
- **history** (Optional) Displays a log of past status and related information for the redundancy facility.
- **states** (Optional) Displays information about the redundancy facility state, such as disabled, initialization, standby, active.

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Examples**

This example shows how to display information about the redundancy facility:

```
Switch# show redundancy
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
```
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

This 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
```

The output displays the following information:

- `clientID` displays the client's ID number.
- `clientSeq` displays the client's notification sequence number.
- `Current redundancy facility state`.

This example shows how to display the redundancy facility counter information:

```
Switch# show redundancy counters

Redundancy Facility OMs
comm link up = 1
comm link down down = 0
invalid client tx = 0
null tx by client = 0
tax failures = 0
tax 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
```

This example shows how to display redundancy facility history information:

```
Switch# show redundancy history

00:00:01 client added: RF_INTERNAL_MSG(0) seq=0
00:00:01 client added: RF_LAST_CLIENT(65000) seq=65000
00:00:01 client added: 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
```
This 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>redundancy</td>
<td>Enters the redundancy configuration mode.</td>
</tr>
<tr>
<td>redundancy force-switchover</td>
<td>Forces a switchover from the active to the standby supervisor engine.</td>
</tr>
</tbody>
</table>
Chapter 2  Cisco IOS Commands for the Catalyst 4500 Series Switches

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}
```

**Syntax Description**

**Defaults**
This command has no default settings.

**Command Modes**
Use r EXEC mode

**Usage Guidelines**
When two versions of Cisco IOS images are involved, the command sets supported by two images might differ. If any of those mismatched commands are executed on the active supervisor engine, the standby supervisor engine might not recognize those commands. This causes a 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.

**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.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

show redundancy config-sync

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.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

show running-config

To display the module status and configuration, use the show running-config command.

show running-config [module slot]

Syntax Description

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

In some cases, you might see a difference in the duplex mode displayed when you enter the show interfaces command and the show running-config command. If you do see a difference, the duplex mode displayed in the show interfaces command is the actual duplex mode that the interface is running.

The 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

This example shows how to display the module and status configuration for all modules:

Switch# show running-config
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

(module slot) (Optional) Specifies the module slot number; valid values are from 1 to 6.
This 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#
```
Use the `show shell functions` command to display configurations for all built-in shell functions.

**Syntax**

```
show shell functions
```

**Description**

None

**Command Modes**

Privileged EXEC

**Usage Guidelines**

This command only displays the contents of built-in 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**

<table>
<thead>
<tr>
<th>Command Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>shell trigger</code></td>
</tr>
<tr>
<td><code>show shell triggers</code></td>
</tr>
</tbody>
</table>
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

show shell triggers

Use the `show shell triggers` command to display detail for all supported builtin and user created triggers.

**Syntax Description**

- **Defaults**: None

- **Command Modes**: Privileged EXEC

**Usage Guidelines**

This command displays builtin triggers and user defined triggers (with their mapped functions).

**Examples**

This example illustrates how to display detail for all supported triggers:

```
Switch#
show shell triggers
```

**Related Commands**

- `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:
```

### Syntax Description

This command has no default settings.

### Command Modes

Privileged EXEC mode

### Examples

This example shows how to display file system status information:

```
Switch# show slavebootflash: filesys
-------- F I L E   S Y S T E M   S T A T U S --------
Device Number = 0
DEVICE INFO BLOCK: bootflash
Magic Number          = 6887635   File System Vers = 10000    (1.0)
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>
```

This 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>
```

- `all` (Optional) Displays all possible Flash information.
- `chips` (Optional) Displays Flash chip information.
- `filesys` (Optional) Displays file system information.
This 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)
```

--- FILE SYSTEM STATUS ---

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:

STATS 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>
To display information about the file system on the standby supervisor engine, use the `show slaveslot0: filesys` command.

```
Switch# show slaveslot0: filesys
-# - 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)
```

This 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:
```

`all` (Optional) Displays all flash information including the output from the `show slot0:` and `show slot0: filesys` commands.
`chips` (Optional) Displays flash chip register information.
`filesys` (Optional) Displays file system status information.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

show slaveslot0:

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

This example shows how to display file system information:
Switch# show slaveslot0: filesys

-------- F I L E   S Y S T E M   S T A T U S --------
Device Number = 0

DEVICE INFO BLOCK: slot0
Magic Number          = 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#
To display information about the slot0: file system, use the `show slot0:` command.

```
show slot0: all | chips | filesys
```

**Syntax Description**

- **all** (Optional) Displays all flash information including the output from the `show slot0: chips` and `show slot0: filesys` commands.
- **chips** (Optional) Displays flash chip register information.
- **filesys** (Optional) Displays file system status information.

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Examples**

This example shows how to display a summary of the file system:

```
Switch# show slot0:
-# - 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>
```

This 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
```
This example shows how to display file system information:

Switch# show slot0: filesys

-------- FILE SYSTEM STATUS --------
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

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**
- `bridge_group` (Optional) Specifies the bridge group number; valid values are from 1 to 255.
- `active` (Optional) Displays the spanning-tree information on active interfaces only.
- `backbonefast` (Optional) Displays the spanning-tree BackboneFast status.
- `bridge` (Optional) Displays the bridge status and configuration information.
- `id` (Optional) Name of the bridge.
- `inconsistentports` (Optional) Displays the root inconsistency state.
- `interface type` (Optional) Specifies the interface type and number; valid values are `fastethernet`, `gigabitethernet`, `tengigabitethernet`, `port-channel` (1 to 64), and `vlan` (1 to 4094).
- `root` (Optional) Displays the root bridge status and configuration.
- `summary` (Optional) Specifies a summary of port states.
- `total` (Optional) Displays the total lines of the spanning-tree state section.
- `uplinkfast` (Optional) Displays the spanning-tree UplinkFast status.
- `vlan vlan_id` (Optional) Specifies the VLAN ID; valid values are from 1 to 4094.
- `pathcost method` (Optional) Displays the default path cost calculation method used.
- `detail` (Optional) Displays a summary of interface information.

**Defaults**
- Interface information summary is displayed.

**Command Modes**
- Privileged EXEC mode

**Examples**
This 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
```
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

show spanning-tree

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#

This 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#

This example shows how to display spanning-tree information for the bridge:
Switch#

show spanning-tree bridge

VLAN1
Bridge ID  Priority    32768
Address     0050.3e8d.6401
Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
VLAN2
Bridge ID  Priority    32768
Address     0050.3e8d.6402
Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
VLAN3
Bridge ID  Priority    32768
Address     0050.3e8d.6403
Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Switch#

This example shows how to display a summary of interface information:
Switch#

show spanning-tree

VLAN1
Spanning tree enabled protocol ieee
Root ID    Priority    32768
Address     0030.94fc.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                                       Designated
Name                   Port ID Prio  Cost Sts   Cost Bridge ID            Port ID
-------------------    ------- --- ------ ---   ---- -------------------- -------
FastEthernet6/15       129.79  128     19 FWD      0 32768 0030.94fc.0a00 129.79
VLAN2
Spanning tree enabled protocol ieee
Chapter 2      Cisco IOS Commands for  the Catalyst 4500 Series Switches

show spanning-tree

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                                       Designated
Name                   Port ID Prio  Cost Sts   Cost Bridge ID            Port ID
-------------------    ------- --- ------ ---   ---- -------------------- -------
FastEthernet6/16       129.80  128     19 FWD      0 32768 0030.94fc.0a01 129.80
Switch#

This example shows how to display spanning-tree information for Fast Ethernet interface 5/9:
Switch#
show spanning-tree interface fastethernet5/9
Interface 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#

This example shows how to display spanning-tree information for a specific VLAN:
Switch#
show spanning-tree vlan 1
VLAN1 is executing the ieee compatible Spanning Tree protocol
Bridge Identifier has priority 32768, address 0030.94fc.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#

This 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#

This example shows how to display a summary of port states:
Switch#
show spanning-tree summary
Root bridge for:VLAN1, VLAN2.
show spanning-tree

- PortFast BPDU Guard is disabled
- EtherChannel misconfiguration guard is enabled
- UplinkFast is disabled
- BackboneFast is disabled
- Default pathcost method used is short

<table>
<thead>
<tr>
<th>Name</th>
<th>Blocking</th>
<th>Listening</th>
<th>Learning</th>
<th>Forwarding</th>
<th>STP Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>VLAN2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>VLANs</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

Switch#

This example shows how to display the total lines of the spanning-tree state section:

Switch# show spanning-tree summary totals

Root bridge for: VLAN1, VLAN2.

PortFast BPDU Guard is disabled
EtherChannel misconfiguration guard is enabled
UplinkFast is disabled
BackboneFast is disabled
Default pathcost method used is short

<table>
<thead>
<tr>
<th>Name</th>
<th>Blocking</th>
<th>Listening</th>
<th>Learning</th>
<th>Forwarding</th>
<th>STP Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>VLAN2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

Switch#

This example shows how to determine whether any ports are in root inconsistent state:

Switch# show spanning-tree inconsistentports

<table>
<thead>
<tr>
<th>Name</th>
<th>Interface</th>
<th>Inconsistency</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN1</td>
<td>FastEthernet3/1</td>
<td>Root Inconsistent</td>
</tr>
</tbody>
</table>

Number of inconsistent ports (segments) in the system: 1

Switch#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>spanning-tree backbonefast</td>
<td>Enables BackboneFast on a spanning-tree VLAN.</td>
</tr>
<tr>
<td>spanning-tree cost</td>
<td>Calculates the path cost of STP on an interface.</td>
</tr>
<tr>
<td>spanning-tree guard</td>
<td>Enables root guard.</td>
</tr>
<tr>
<td>spanning-tree pathcost method</td>
<td>Sets the path cost calculation method.</td>
</tr>
<tr>
<td>spanning-tree portfast default</td>
<td>Enables PortFast by default on all access ports.</td>
</tr>
<tr>
<td>spanning-tree portfast</td>
<td>Enables PortFast mode.</td>
</tr>
<tr>
<td>spanning-tree port-priority</td>
<td>Prioritizes an interface when two bridges compete for position as the root bridge.</td>
</tr>
<tr>
<td>spanning-tree uplinkfast</td>
<td>Enables the UplinkFast feature.</td>
</tr>
<tr>
<td>spanning-tree vlan</td>
<td>Configures STP on a per-VLAN basis.</td>
</tr>
</tbody>
</table>
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

show spanning-tree mst

To display MST protocol information, use the `show spanning-tree mst` command.

Syntax Description

Defaults

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

In the output display of the `show spanning-tree mst` 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

This 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

-------------------------------------------------------------------------------
```

This 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
```

Configuration

(Optional) Displays region configuration information.

instance-id

(Optional) Instance identification number; valid values are from 0 to 15.

detail

(Optional) Displays detailed MST protocol information.

interface

(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.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

show spanning-tree mst

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 sent 3, received 252
Switch#

This example shows how to display MST information for a specific interface:
Switch#
show spanning-tree mst 0 interface fastethernet4/1 detail

Edge port: no (trunk) port guard : none (default)
Link type: point-to-point (point-to-point) bpdu filter: disable (default)
Boundary : internal bpdu guard : disable (default)
FastEthernet4/1 of MST00 is designated forwarding
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
spanning-tree mst  Sets the path cost and port-priority parameters for any MST instance.
spanning-tree mst forward-time  Sets the forward delay timer for all the instances.
spanning-tree mst hello-time  Sets the hello-time delay timer for all the instances.
spanning-tree mst max-hops  Specifies the number of possible hops in the region before a BPDU is discarded.
spanning-tree mst root  Designates the primary root.
show storm-control

To display the broadcast storm control settings on the switch or on the specified interface, use the `show storm-control` command.

`show storm-control [interface-id | broadcast | multicast]`

**Syntax Description**

- **interface-id** (Optional) Specifies the interface ID for the physical port.
- **broadcast** (Optional) Displays the broadcast storm threshold setting.
- **multicast** (Optional) Displays the multicast storm threshold setting.

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**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 //Supervisor Engine 6-E` command:

```
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 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#
```
Chapter 2  
Cisco IOS Commands for the Catalyst 4500 Series Switches

show storm-control

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:

Switch#

show storm-control interface fastethernet6/1

Interface  Filter State   Broadcast Multicast Level
---------  -------------  -------  -------
Fa6/1     Blocking        Enabled    Disabled     81%
Switch#

Table 2-31 describes the fields in the show storm-control display.

<table>
<thead>
<tr>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
</tr>
<tr>
<td>Filter State</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Level</td>
</tr>
<tr>
<td>Current</td>
</tr>
</tbody>
</table>

Note: N/A is displayed for interfaces that do not perform storm control in the hardware.

**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.
To display the global MTU setting, use the `show system mtu` command.

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Examples**

This example shows how to display the global MTU setting:

```
Switch# show system mtu
Global Ethernet MTU is 1550 bytes.
Switch#
```

**Related Commands**

- `system mtu` — Sets the maximum Layer 2 or Layer 3 payload size.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

show tech-support

To display troubleshooting information for TAC, use the show tech-support command.

Syntax Description

Defaults

The defaults are as follows:

- Outputs are displayed without page breaks.
- Passwords and other security information are removed from the output.

Command Modes

Privileged EXEC mode

Usage Guidelines

Output from the show tech-support command may be terminated in 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

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.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

*show tech-support*

If you enter the `ip multicast` 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.
To display the administrative and operational UDLD status, use the `show udld` privileged EXEC command.

```
show udld interface-id | neighbors | fast-hello {
    interface id
}
```

**Syntax Description**

- `interface-id`: Specifies the administrative and operational UDLD status for a specific interface.
- `neighbors`: Specifies the UDLD neighbor summary.
- `fast-hello`: Specifies Fast UDLD neighbor summary and interface specific status.
- `interface-id`: Specifies the name of the interface.

**Defaults**

- None

**Command Modes**

- Privileged EXEC

**Usage Guidelines**

If you do not enter an `interface-id` value, the administrative and operational UDLD status for all interfaces is displayed.

**Examples**

To verify status for a particular link as reported by UDLD, enter the following command:

```
Switch# show udld 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
To verify link status as reported by UDLD, enter the following command:
```
Switch# show udld neighbors
```

<table>
<thead>
<tr>
<th>Port</th>
<th>Device Name</th>
<th>Device ID</th>
<th>Port ID</th>
<th>Neighbor State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/33</td>
<td>FOX10430380</td>
<td>1</td>
<td>Gi1/33</td>
<td>Bidirectional</td>
</tr>
<tr>
<td>Gi1/34</td>
<td>FOX10430380</td>
<td>1</td>
<td>Gi1/34</td>
<td>Bidirectional</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Port-ID</th>
<th>Hello Neighbor</th>
<th>Neighbor-Port</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/45</td>
<td>200</td>
<td>FOX104303NL</td>
<td>Gi1/45</td>
</tr>
<tr>
<td>Gi1/46</td>
<td>200</td>
<td>FOX104303NL</td>
<td>Gi1/46</td>
</tr>
<tr>
<td>Gi1/47</td>
<td>200</td>
<td>FOX104303NL</td>
<td>Gi1/47</td>
</tr>
</tbody>
</table>

To verify status for a particular link as reported by Fast UDLD, enter the following command:
```
Switch# show udld fast-hello gi1/33
```

```
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
```
## show udld

### 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.
To display VLAN information, use the `show vlan` command.

```
show vlan

[ brief | id vlan_id | name name ]
```

**Syntax Description**

- This command has no default settings.
- **Command Modes**: Privileged EXEC mode

**Examples**

This example shows how to display the VLAN parameters for all VLANs within the administrative domain:

```
Switch# show vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa5/9
2    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
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
This example shows how to display the VLAN name, status, and associated ports only:

```
Switch# show vlan brief
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa5/9
2    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
```

This example shows how to display the VLAN parameters for VLAN 3 only:

```
Switch# show vlan id 3
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
3    VLAN0003                         active    Fa5/9
VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
3    enet  100003     1500  -      -      -        -    -        303    0
```

Table 2-32 describes the fields in the `show vlan` command output.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

show 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

<table>
<thead>
<tr>
<th>Primary</th>
<th>Secondary</th>
<th>Type</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>100</td>
<td>community</td>
<td>Fa3/1, Fa3/2</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Primary</th>
<th>Secondary</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>primary</td>
<td></td>
</tr>
<tr>
<td>100</td>
<td>community</td>
<td></td>
</tr>
</tbody>
</table>

This example show how to verify PVLAN configuration on the interface:

Switch#
show interface f3/2 status

<table>
<thead>
<tr>
<th>Port</th>
<th>Name</th>
<th>Status</th>
<th>Vlan</th>
<th>Duplex</th>
<th>Speed</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa3/2</td>
<td></td>
<td>connected</td>
<td>pvlan</td>
<td>a-full</td>
<td>a-100</td>
<td>10/100BaseTX</td>
</tr>
</tbody>
</table>

Switch#
show interface f3/1 status

<table>
<thead>
<tr>
<th>Port</th>
<th>Name</th>
<th>Status</th>
<th>Vlan</th>
<th>Duplex</th>
<th>Speed</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa3/1</td>
<td></td>
<td>connected</td>
<td>pvlan</td>
<td>a-full</td>
<td>a-100</td>
<td>10/100BaseTX</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Table 2-32 show vlan Command Output Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field Description</td>
</tr>
<tr>
<td>VLAN VLAN number.</td>
</tr>
<tr>
<td>Name Name, if configured, of the VLAN.</td>
</tr>
<tr>
<td>Status Status of the VLAN (active or suspend).</td>
</tr>
<tr>
<td>Ports Ports that belong to the VLAN.</td>
</tr>
<tr>
<td>Type Media type of the VLAN.</td>
</tr>
<tr>
<td>SAID Security Association Identifier value for the VLAN.</td>
</tr>
<tr>
<td>MTU Maximum transmission unit size for the VLAN.</td>
</tr>
<tr>
<td>Parent Parent VLAN, if one exists.</td>
</tr>
<tr>
<td>RingNo Ring number for the VLAN, if applicable.</td>
</tr>
<tr>
<td>BrdgNo Bridge number for the VLAN, if applicable.</td>
</tr>
<tr>
<td>Stp Spanning Tree Protocol type used on the VLAN.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan  (VLAN Database mode)</td>
</tr>
<tr>
<td>Configures a specific VLAN.</td>
</tr>
<tr>
<td>vlan database</td>
</tr>
<tr>
<td>Enters VLAN configuration mode.</td>
</tr>
<tr>
<td>vtp (global configuration mode)</td>
</tr>
<tr>
<td>Modifies the name of a VTP configuration storage file.</td>
</tr>
</tbody>
</table>
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

show vlan access-map

To display the contents of a VLAN access map, use the `show vlan access-map` command.

```
show vlan access-map [map-name]
```

**Syntax Description**

- **map-name** (Optional) Name of the VLAN access map.

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Examples**

This command shows how to display the contents of a VLAN access map:

```
Switch# show vlan access-map mordred
Vlan access-map "mordred"  1
  match: ip address 13
  action: forward capture
Switch#
```

**Related Commands**

- `vlan access-map` Enters VLAN access-map command mode to create a VLAN access map.
To display the software-cached counter values, use the `show vlan counters` command.

```
show vlan counters

Syntax Description
This command has no default settings.

Command Modes
Privileged EXEC mode

Usage Guidelines
If you enter the `show vlan counters` command without specifying the VLAN ID, the software-cached counter values for all VLANs are displayed.

Examples
This example shows how to display the software-cached counter values for a specific VLAN:

Switch# show vlan counters
* Multicast counters include broadcast packets
Vlan Id                                            : 1
L2 Unicast Packets                                 : 0
L2 Unicast Octets                                  : 0
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
id vlanid (Optional) Displays the software-cached counter values for a specific VLAN.

Command Description
clear vlan counters
Clears the software-cached counter values to start from zero again for a specified VLAN or all existing VLANs.
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.

### Syntax Description

This command has no arguments or keywords.

### Defaults

This command has no default settings.

### Command Modes

User EXEC mode

### Examples

This is an example of output from the `show vlan dot1q tag native` command:

```
Switch# show vlan dot1q tag native
dot1q native vlan tagging is disabled globally
Per Port Native Vlan Tagging State
----------------------------------
Port    Operational    Native VLAN  Mode       Tagging State
------------------------------------
  f3/2    trunk          enabled
  f3/16   PVLAN trunk    disabled
  f3/16   trunk          enabled
```

### Related Commands

- **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.
To display the VLANs mapped to VLAN groups, use the show vlan group privileged EXEC command.

show vlan group

Syntax Description

None

Command Modes

Privileged EXEC

Usage Guidelines

The show vlan group command displays the existing VLAN groups and lists the VLANs and VLAN ranges that are members of each VLAN group. If you use the group-name keyword, you display only the members of the VLAN group specified by the group-name argument.

Examples

This example shows how to display the members of a specified VLAN group:

Switch# show vlan group group-name ganymede

Group Name Vlans Mapped
---------------- -------------------
ganymede 7-9

Related Commands

group-name (Optional) Displays the VLANs mapped to the specified VLAN group.

Command Description

vlan group

Creates or modifies a VLAN group.
To display information about the internal VLAN allocation, use the `show vlan internal usage` command.

```
show vlan id [vlan-id] internal usage
```

**Syntax Description**

- `id vlan-id` (Optional) Displays internal VLAN allocation information for the specified VLAN; valid values are from 1 to 4094.

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Examples**

This example shows how to display information about the current internal VLAN allocation:

```
Switch# show vlan internal usage
VLAN Usage
---- --------------------
  1025 -
  1026 -
  1027 -
  1028 -
  1029 Port-channel6
  1030 GigabitEthernet1/2
  1032 FastEthernet3/20
  1033 FastEthernet3/21
  1129 -
```

This example shows how to display information about the internal VLAN allocation for a specific VLAN:

```
Switch# show vlan id 1030 internal usage
VLAN Usage
---- --------------------
  1030 GigabitEthernet1/2
```

**Related Commands**

- `vlan internal allocation policy` Configures the internal VLAN allocation scheme.
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**

None

**Command Modes**

Privileged EXEC

**Usage Guidelines**

Expressions are case sensitive. For example, if you enter \| exclude output, the lines that contain output are not displayed, but the lines that contain Output are displayed.

**Examples**

This is a sample output from the show vlan mapping command:

```
Switch# show vlan mapping
Interface 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**

- interface
- interface-id

(Optional) Displays VLAN mapping information for the specified interface.

- | begin

(Optional) Displays begins with the line that matches the expression.

- | exclude

(Optional) Displays excludes lines that match the expression.

- | include

(Optional) Displays includes lines that match the specified expression.

- expression

Specifies an expression in the output to use as a reference point.

**Command Description**

switchport vlan mapping

Configures VLAN mapping on an interface.
To display the minimum and maximum transmission unit (MTU) sizes of each VLAN, use the `show vlan mtu` command.

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

**Defaults**
This command has no default settings.

**Command Modes**
Privileged EXEC mode

**Usage Guidelines**
The MTU_Mismatch column in the command output indicates whether all the ports in the VLAN have the same MTU. When "yes" is displayed in the MTU_Mismatch column, it means that the VLAN has a port with different MTUs, and packets might be dropped that are switched from a port with a 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**
- `mtu` - Enables jumbo frames on an interface by adjusting the maximum size of a packet or maximum transmission unit (MTU).
To display private VLAN information, use the `show vlan private-vlan` command.

Syntax Description

This command has no default settings.

Command Modes

Privileged EXEC mode

Usage Guidelines

When the `show vlan private-vlan` command displays a VLAN type as normal, it indicates that a regular VLAN has been used in the private VLAN configuration. When normal is displayed, this indicates that two VLANs have been associated before the type was set, and the private VLAN is not operational. This information is useful for debugging purposes.

Examples

This example shows how to display information about all currently configured private VLANs:

```
Switch# show vlan private-vlan
Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
2       301       community         Fa5/3, Fa5/25
2       302       community
2       303       community         Fa5/3, Po63
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.

This 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
```

(Required) Displays the private VLAN type; valid types are isolated, primary, community, twoway-community, non-operational, and normal.
Chapter 2  Cisco IOS Commands for the Catalyst 4500 Series Switches

show vlan private-vlan

Table 2-33 describes the fields in the `show vlan private-vlan` command output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary</td>
<td>Number of the primary VLAN.</td>
</tr>
<tr>
<td>Secondary</td>
<td>Number of the secondary VLAN.</td>
</tr>
<tr>
<td>Secondary-Type</td>
<td>Secondary VLAN type is isolated or community.</td>
</tr>
<tr>
<td>Ports</td>
<td>Indicates the ports within a VLAN.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of VLAN; possible values are primary, isolated, community, nonoperational, or normal.</td>
</tr>
</tbody>
</table>

Related Commands

Table 2-33 `show vlan private-vlan` Command Output Fields

- `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.

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Examples**

This example shows how to display a list of RSPAN VLANs:

```
Router# show vlan remote-span
```

Remote SPAN VLANs
------------------------------------------------------------------
2,20

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>remote-span</td>
<td>Converts a VLAN into an RSPAN VLAN.</td>
</tr>
<tr>
<td>vlan (VLAN Database mode)</td>
<td>Configures a specific VLAN.</td>
</tr>
</tbody>
</table>
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.

```
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)

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
```

Related Commands:

- `vmps reconfirm` (privileged EXEC) sends VLAN Query Protocol (VQP) queries to reconfirm all the dynamic VLAN assignments with the VLAN Membership Policy Server (VMPS).
- `statistics` (Optional) Displays the client-side statistics.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

show vtp

To display VTP statistics and domain information, use the `show vtp` command.

show vtp {counters | status}

Syntax Description

This command has no default settings.

Command Modes

Privileged EXEC mode

Examples

This example shows how to display the VTP statistics:

```
Switch#
show vtp counters
VTP 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
non-pruning-capable device
---------------- ---------------- ---------------- ---------------------------
Fa5/9               1555             1564             0
Switch#
```

This example shows how to display the VTP domain status:

```
Switch#
show vtp status
VTP Version                     : 2
Configuration Revision          : 250
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 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 Vl1 (lowest numbered VLAN interface found)
Switch#
```
Chapter 2  
Cisco IOS Commands for the Catalyst 4500 Series Switches

show vtp

This example shows how to display only those lines in the show vtp output that contain the word Summary:

Switch# show vtp counters | include Summary
Summary advertisements received    : 1
Summary advertisements transmitted : 32

Table 2-34  describes the fields in the show vtp command output.

<table>
<thead>
<tr>
<th>Field Description</th>
<th>Command Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary advertisements received</td>
<td>vtp (global configuration mode)</td>
</tr>
<tr>
<td>Subset advertisements received</td>
<td>vtp client</td>
</tr>
<tr>
<td>Request advertisements received</td>
<td>vtp domain</td>
</tr>
<tr>
<td>Summary advertisements transmitted</td>
<td></td>
</tr>
<tr>
<td>Subset advertisements transmitted</td>
<td></td>
</tr>
<tr>
<td>Request advertisements transmitted</td>
<td></td>
</tr>
<tr>
<td>Number of config revision errors</td>
<td></td>
</tr>
<tr>
<td>Number of config digest errors</td>
<td></td>
</tr>
<tr>
<td>Number of V1 summary errors</td>
<td></td>
</tr>
<tr>
<td>Trunk</td>
<td></td>
</tr>
<tr>
<td>Join Transmitted</td>
<td></td>
</tr>
<tr>
<td>Join Received</td>
<td></td>
</tr>
<tr>
<td>Summary advts received from non-pruning-capable device</td>
<td></td>
</tr>
<tr>
<td>Number of existing VLANs</td>
<td></td>
</tr>
<tr>
<td>Configuration Revision</td>
<td></td>
</tr>
<tr>
<td>Maximum VLANs supported locally</td>
<td></td>
</tr>
<tr>
<td>Number of existing VLANs</td>
<td></td>
</tr>
<tr>
<td>VTP Operating Mode</td>
<td></td>
</tr>
<tr>
<td>VTP Domain Name</td>
<td></td>
</tr>
<tr>
<td>VTP Pruning Mode</td>
<td></td>
</tr>
<tr>
<td>VTP V2 Mode</td>
<td></td>
</tr>
<tr>
<td>VTP Traps Generation</td>
<td></td>
</tr>
<tr>
<td>MD5 digest</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

show vtp
Explains VTP status.

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 the device in VTP transparent mode.

vtp v2-mode
Enables version 2 mode.
To clear any previously configured `snmp ifindex` commands that were entered for a specific interface, use the `snmp ifindex clear` command.

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Interface configuration mode

**Usage Guidelines**

Interface index persistence occurs when ifIndex values in the interface MIB (IF-MIB) persist across reboots and allow for consistent identification of specific interfaces using SNMP. Use the `snmp ifindex clear` command on a specific interface when you want that interface to use the global configuration setting for ifIndex persistence. This command clears any ifIndex configuration commands previously entered for that specific interface.

**Examples**

This example shows how to enable ifIndex persistence for all interfaces:

```
Router(config)#
snmp-server ifindex persist
```

This example shows how to disable ifIndex persistence for FastEthernet 1/1 only:

```
Router(config)#
interface fastethernet 1/1
Router(config-if)#
no snmp ifindex persist
Router(config-if)#
exit
```

This example shows how to clear 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**

- `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.
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.

```
no snmp ifindex persist
```

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

### Defaults
Disabled.

### Command Modes
Interface configuration mode

### Usage Guidelines
Interface index persistence occurs when ifIndex values in the IF-MIB persist across reboots and allow for consistent identification of specific interfaces using SNMP.

The `snmp ifindex persist` interface configuration command enables and disables ifIndex persistence for individual entries (that correspond to individual interfaces) in the ifIndex table of the IF-MIB.

The `snmp-server ifindex persist` global configuration command enables and disables ifIndex persistence for all interfaces on the routing device. This action applies only to interfaces that have ifDescr and ifIndex entries in the ifIndex table of the IF-MIB.

### Examples
This example shows how to enable ifIndex persistence for interface FastEthernet 1/1 only:
```
Router(config)#
interface fastethernet 1/1
Router(config-if)#
snmp ifindex persist
Router(config-if)#
exit
```

This example shows how to enable ifIndex persistence for all interfaces, and then disable ifIndex persistence for interface FastEthernet 1/1 only:
```
Router(config)#
snmp-server ifindex persist
Router(config)#
interface fastethernet 1/1
Router(config-if)#
no snmp ifindex persist
Router(config-if)#
exit
```

### Related Commands
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>snmp ifindex clear</code></td>
<td>Clears any previously configured <code>snmp ifindex</code> commands that were entered for a specific interface.</td>
</tr>
<tr>
<td><code>snmp ifindex persist</code></td>
<td>Enables ifIndex values in the Interfaces MIB (IF-MIB) that persist across reboots (ifIndex persistence) on a specific interface.</td>
</tr>
</tbody>
</table>
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.

```
[flash | insertion | removal | fru-ctrl | port-security | mac-notification | change | move | threshold]
```

**Syntax Description**

**Defaults**
SNMP notifications are disabled.

**Command Modes**
Global configuration mode

**Usage Guidelines**
If you enter this command without an option, all notification types controlled by this command are enabled.

SNMP notifications can be sent as traps or inform requests. This command enables both traps and 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.

- **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** (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.
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**

This example shows how to send all traps to the host is specified by the name myhost.cisco.com using the community string defined as public:

```
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server host myhost.cisco.com public
```

This example shows how to enable the MAC address change MIB notification:

```
Switch(config)# snmp-server enable traps mac-notification change
```

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
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>clear mac-address-table dynamic</code></td>
<td>Clears the dynamic address entries from the Layer 2 MAC address table.</td>
</tr>
<tr>
<td><code>mac-address-table notification</code></td>
<td>Enables MAC address notification on a switch.</td>
</tr>
<tr>
<td><code>show mac-address-table notification</code></td>
<td>Displays the MAC address table notification status and history.</td>
</tr>
<tr>
<td><code>snmp-server enable traps</code></td>
<td>Enables SNMP notifications.</td>
</tr>
<tr>
<td><code>snmp-server enable traps mac-notification change</code></td>
<td>Enables SNMP MAC address notifications.</td>
</tr>
</tbody>
</table>
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.

This command has no arguments or keywords.

**Defaults**

Disabled.

**Command Modes**

Global configuration mode

**Usage Guidelines**

Interface index persistence occurs when ifIndex values in the IF-MIB persist across reboots and allow for consistent identification of specific interfaces using SNMP.

The `snmp-server ifindex persist` global configuration command does not override the interface-specific configuration. To override the interface-specific configuration of ifIndex persistence, enter the `no snmp ifindex persist` and `snmp ifindex clear` interface configuration commands.

Entering the `no snmp-server ifindex persist` global configuration command enables and disables ifIndex persistence for all interfaces on the routing device using ifDescr and ifIndex entries in the ifIndex table of the IF-MIB.

**Examples**

This example shows how to enable ifIndex persistence for all interfaces:

```
Router(config) #
snmp-server ifindex persist
```

**Related Commands**

- `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.
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.

```
Router(config)# snmp-server ifindex persist compress
```

```
Router(config)# no snmp-server ifindex persist compress
```

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

Disabled

**Command Modes**

Global configuration mode

**Usage Guidelines**

This command is hidden because the ifIndex table is always in a compressed format on the supervisor engine.

**Examples**

This example shows how to enable compression of the ifIndex table:

```
Router(config)# snmp-server ifindex persist compress
```

This example shows how to disable compression of the ifIndex table:

```
Router(config)# no snmp-server ifindex persist compress
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>snmp ifindex clear</code></td>
<td>Clears any previously configured <code>snmp ifindex</code> commands that were entered for a specific interface.</td>
</tr>
<tr>
<td><code>snmp ifindex persist</code></td>
<td>Enables ifIndex values in the Interfaces MIB (IF-MIB) that persist across reboots (ifIndex persistence) on a specific interface.</td>
</tr>
<tr>
<td><code>snmp-server ifindex persist</code></td>
<td>Enables ifIndex values that will remain constant across reboots for use by SNMP.</td>
</tr>
</tbody>
</table>
To enable SNMP MAC address notifications, use the `snmp trap mac-notification change` command. To return to the default setting, use the `no` form of this command.

```
no snmp trap mac-notification change {
  added |
  removed}
```

**Syntax Description**

- `added`: Specifies enabling the MAC address notification trap whenever a MAC address is added to an interface.
- `removed`: Specifies enabling the MAC address notification trap whenever a MAC address is removed from an interface.

**Defaults**

MAC address addition and removal are disabled.

**Command Modes**

Interface configuration mode

**Usage Guidelines**

Even though you enable the change notification trap for a specific interface by using the `snmp trap mac-notification change` command, the trap is generated only when you enable the `snmp-server enable traps mac-notification change` and `mac address-table notification change` global configuration commands.

**Examples**

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

```
Switch(config)#
interface gigabitethernet1/1
Switch(config-if)#
snmp trap mac-notification change added
```

You can verify your settings by entering the `show mac address-table notification change interface` privileged EXEC command.

**Related Commands**

- `clear mac-address-table`: Clears the address entries from the Layer 2 MAC address table.
- `mac-address-table notification`: Enables MAC address notification on a switch.
- `show mac-address-table notification`: Displays the MAC address table notification status and history.
- `snmp-server enable traps`: Enables SNMP notifications.
source-interface

To send out call home email messages with specific source interface, use the `source-interface` command.

**Syntax Description**

```
source-interface interface-name
```

**Defaults**

None

**Command Modes**

cfg-call-home

**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**

This example shows how to configure source interface for Call Home. Generally, the interface should already be configured with a valid IP address as usually configured for an interface.

```
Switch# config terminal
Switch(config)# call-home
Switch(cfg-call-home)# source-interface 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**

- `interface name` Source interface name for call home email messages
- `source-ip-address` Sends out Call Home email messages with specific source IP address.
To send out Call Home email messages with specific source IP address, use the `source-ip-address` command.

**Syntax Description**

- **Defaults**: None
- **Command Modes**: `cfg-call-home`

**Usage Guidelines**

It is best to configure `no shut` an interface with this valid IP address before specifying it as `source-ip-address` for Call Home. Doing this avoids a connection failure when sending Call Home email messages. You should only specify `source-ip-address` under Call Home if `source-interface` is not specified. You can only specify either source interface or `source-ip-address` in Call Home mode, not both simultaneously.

**Examples**

This example shows how to configure `source-ip-address` for Call Home:

```plaintext
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**

- `ip address`
  - Source IP address for Call Home messages.
- `source-interface`
  - Sends out call home email messages with specific source interface.
To enable BackboneFast on a spanning-tree VLAN, use the `spanning-tree backbonefast` command. To disable BackboneFast, use the `no spanning-tree backbonefast` command.

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

**Defaults**
BackboneFast is disabled.

**Command Modes**
global configuration mode

**Usage Guidelines**
BackboneFast should be enabled on all Catalyst 4506 series switches to allow the detection of indirect link failures. Enabling BackboneFast starts the spanning-tree reconfiguration more quickly.

**Examples**
This example shows how to enable BackboneFast on all VLANs:

```
Switch(config)#
spanning-tree backbonefast
Switch(config)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>spanning-tree cost</code></td>
<td>Calculates the path cost of STP on an interface.</td>
</tr>
<tr>
<td><code>spanning-tree portfast default</code></td>
<td>Enables PortFast by default on all access ports.</td>
</tr>
<tr>
<td><code>spanning-tree portfast (interface configuration)</code></td>
<td>Enables PortFast mode.</td>
</tr>
<tr>
<td><code>spanning-tree port-priority</code></td>
<td>Prioritizes an interface when two bridges compete for position as the root bridge.</td>
</tr>
<tr>
<td><code>spanning-tree uplinkfast</code></td>
<td>Enables the UplinkFast feature.</td>
</tr>
<tr>
<td><code>spanning-tree vlan</code></td>
<td>Configures STP on a per-VLAN basis.</td>
</tr>
<tr>
<td><code>show spanning-tree</code></td>
<td>Displays spanning-tree information.</td>
</tr>
</tbody>
</table>
To enable BPDU filtering on an interface, use the `spanning-tree bpdufilter` command. To return to the default settings, use the `no` form of this command.

```
spanning-tree bpdufilter {enable | disable}
```

**Syntax Description**

**Defaults**

Disabled

**Command Modes**

Interface configuration mode

**Usage Guidelines**

Caution

Use care when entering the `spanning-tree bpdufilter enable` command. Enabling BPDU filtering on an interface is approximately equivalent to disabling the spanning tree for this interface. It is possible to create bridging loops if this command is not 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 bpdufilter` command.

BPDU filtering allows you to prevent a port from sending and receiving BPDUs. The configuration is applicable to the whole interface, whether it is trunking or not. This command has three states:

- `spanning-tree bpdufilter enable` — This state unconditionally enables the BPDU filter feature on the interface.
- `spanning-tree bpdufilter disable` — This state unconditionally disables the BPDU filter feature on the interface.
- `no spanning-tree bpdufilter` — This state enables the BPDU filter feature on the interface if the interface is in operational PortFast state and if the `spanning-tree portfast bpdufilter default` command is configured.

**Examples**

This example shows how to enable the BPDU filter feature on this interface:

```
Switch(config-if)# spanning-tree bpdufilter enable
Switch(config-if)#
```

**Related Commands**

- `enable` — Enables BPDU filtering on this interface.
- `disable` — Disables BPDU filtering on this interface.
Chapter 2    Cisco IOS Commands for the Catalyst 4500 Series Switches

spanning-tree bpdufilter

Command Description

show spanning-tree

Displays spanning-tree information.

spanning-tree portfast bpdufilter default

Enables the BPDU filtering by default on all PortFast ports.
spanning-tree bpduguard

To enable BPDU guard on an interface, use the `spanning-tree bpduguard` command. To return to the default settings, use the `no` form of this command.

```
spanning-tree bpduguard {
  enable | disable
}
```

**Syntax Description**

**Defaults**

BPDU guard is disabled.

**Command Modes**

Interface configuration mode

**Command History**

Release Modification

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

**Usage Guidelines**

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 bpduguard default` command is configured.

**Examples**

This example shows how to enable BPDU guard on this interface:

```
Switch(config-if)# spanning-tree bpduguard enable
```

**Related Commands**

- `enable` — Enables BPDU guard on this interface.
- `disable` — Disables BPDU guard on this interface.

**Command Description**

- `show spanning-tree` — Displays spanning-tree information.
- `spanning-tree portfast bpdufilter default` — Enables the BPDU filtering by default on all PortFast ports.
To calculate the path cost of STP on an interface, use the `spanning-tree cost` command. To revert to the default, use the `no spanning-tree cost` command.

**Syntax Description**

- **Defaults**
  - The default settings are as follows:
    - FastEthernet—19
    - GigabitEthernet—1
  
- **Command Modes**
  - Interface configuration mode

**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**

This example shows how to access an interface and set a path cost value of 250 for the spanning-tree VLAN that is associated with that interface:

```
Switch(config)#
interface fastethernet 2/1
Switch(config-if)#
spanning-tree cost 250
Switch(config-if)#
```

**Related Commands**

- `cost` Path cost; valid values are from 1 to 200,000,000.
- `spanning-tree portfast default` Enables PortFast by default on all access ports.
- `spanning-tree portfast (interface configuration mode)` Enables PortFast mode.
- `spanning-tree port-priority` Prioritizes an interface when two bridges compete for position as the root bridge.
- `spanning-tree uplinkfast` Enables the UplinkFast feature.
- `spanning-tree vlan` Configures STP on a per-VLAN basis.
- `show spanning-tree` Displays spanning-tree information.
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
```

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

Spanning-tree EtherChannel guard is enabled.

**Command Modes**

Global configuration mode

**Usage Guidelines**

When an EtherChannel guard misconfiguration is detected, this message is displayed:

```
%SPANTREE-2-CHNL_MISCFG:Detected loop due to etherchannel misconfig of interface Port-Channel1
```

To determine which local ports are involved in the misconfiguration, enter the `show interfaces status err-disabled` command. To verify the EtherChannel configuration on the remote device, enter the `show etherchannel summary` command on the remote device.

After you correct the configuration, enter the `shutdown` and the `no shutdown` commands on the associated port-channel interface.

**Examples**

This example shows how to enable the EtherChannel guard misconfiguration feature:

```
Switch(config)# spanning-tree etherchannel guard misconfig
Switch(config)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show etherchannel</code></td>
<td>Displays EtherChannel information for a channel.</td>
</tr>
<tr>
<td><code>show interfaces status err-disabled</code></td>
<td>Displays the interface status or a list of interfaces in error-disabled state.</td>
</tr>
<tr>
<td><code>shutdown</code> (refer to Cisco IOS documentation)</td>
<td>Disables a port.</td>
</tr>
</tbody>
</table>
spanning-tree extend system-id

To enable the extended system ID feature on a chassis that supports 1024 MAC addresses, use the `spanning-tree extend system-id` command. To disable the feature, use the `no` form of this command.

```
spanning-tree extend system-id
no spanning-tree extend system-id
```

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

Enabled on systems that do not provide 1024 MAC addresses.

**Command Modes**

Global configuration mode

**Usage Guidelines**

Releases 12.1(13)E and later support chassis with 64 or 1024 MAC addresses. For chassis with 64 MAC addresses, STP uses the extended system ID plus a MAC address to make the bridge ID unique for each VLAN.

You cannot disable the extended system ID on chassis that support 64 MAC addresses.

Enabling or disabling the extended system ID updates the bridge IDs of all active STP instances, which might change the spanning-tree topology.

**Examples**

This example shows how to enable the extended system ID:

```
Switch(config)#
spanning-tree extend system-id
Switch(config)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show spanning-tree</td>
<td>Displays spanning-tree information.</td>
</tr>
</tbody>
</table>
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 }
```

Syntax Description

- `loop`: Enables the loop guard mode on the interface.
- `root`: Enables root guard mode on the interface.
- `none`: Sets the guard mode to none.

Defaults

Root guard is disabled.

Command Modes

Interface configuration mode

Examples

This example shows how to enable root guard:

```
Switch(config-if)# spanning-tree guard root
Switch(config-if)#
```

Related Commands

- `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 Description

- `show spanning-tree`: Displays spanning-tree information.
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}
```

**Syntax Description**

- **point-to-point**: Specifies that the interface is a point-to-point link.
- **shared**: Specifies that the interface is a shared medium.

**Defaults**

Link type is derived from the duplex mode.

**Command Modes**

Interface configuration mode

**Usage Guidelines**

RSTP+ fast transition works only on point-to-point links between two bridges. By default, the switch derives the link type of a port from the duplex mode. A full-duplex port is considered as a point-to-point link while a half-duplex configuration is assumed to be on a shared link. If you designate a port as a shared link, RSTP+ fast transition is forbidden, regardless of the duplex setting.

**Examples**

This example shows how to configure the port as a shared link:

```
Switch(config-if)# spanning-tree link-type shared
```

**Related Commands**

- `point-to-point`: Specifies that the interface is a point-to-point link.
- `shared`: Specifies that the interface is a shared medium.

**Command Description**

- `show spanning-tree`: Displays spanning-tree information.
To enable loop guard as the default on all ports of a specific bridge, use the `spanning-tree loopguard default` command. To disable loop guard, use the `no` form of this command.

```
spanning-tree loopguard default
no spanning-tree loopguard default
```

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

**Defaults**
Loop guard is disabled.

**Command Modes**
Global configuration mode

**Usage Guidelines**
Loop guard provides an additional security in the bridge network. Loop guard 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**
This example shows how to enable loop guard:
```
Switch(config)#
spanning-tree loopguard default
Switch(config)#
```

**Related Commands**
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>spanning-tree guard</code></td>
<td>Enables root guard.</td>
</tr>
<tr>
<td><code>show spanning-tree</code></td>
<td>Displays spanning-tree information.</td>
</tr>
</tbody>
</table>
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**

**Defaults**

PVST+ mode

**Command Modes**

Global configuration mode

**Usage Guidelines**

**Caution**

Be careful when using the `spanning-tree mode` command to switch between PVST+ and MST modes. When you enter the command, all spanning-tree instances are stopped for the previous mode and restarted in the new mode. Using this command may cause disruption of user traffic.

**Examples**

This example shows how to switch to MST mode:

```
Switch(config)# spanning-tree mode mst
Switch(config)#
```

This example shows how to return to the default mode (PVST):

```
Switch(config)# no spanning-tree mode
Switch(config)#
```

**Related Commands**

- `pvst`
  - Specifies PVST+ mode.
- `mst`
  - Specifies MST mode.
- `rapid-pvst`
  - Specifies Rapid PVST mode.

**Command Description**

- `show spanning-tree mst`
  - Displays MST protocol information.
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] | [port-priority]
no spanning-tree mst
instance-id {
cost |
port-priority}
```

**Syntax Description**

**Defaults**
- Port priority is 128.

**Command Modes**
- Interface configuration mode

**Usage Guidelines**
- The higher 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 values indicate smaller priorities.
- By default, the cost depends on the port speed; faster interface speeds indicate smaller costs. MST always uses long path costs.

**Examples**

This example shows how to set the interface path cost:

```
Switch(config-if)# spanning-tree mst 0 cost 17031970
Switch(config-if)#
```

This example shows how to set the interface priority:

```
Switch(config-if)# spanning-tree mst 0 port-priority 64
Switch(config-if)#
```

**Related Commands**

- `instance-id` - Instance ID number; valid values are from 0 to 15.
- `cost` - Specifies the path cost for an instance; valid values are from 1 to 200000000.
- `port-priority` - Specifies the port priority for an instance; valid values are from 0 to 240 in increments of 16.

**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.
To enter the MST configuration submode, use the `spanning-tree mst configuration` command. To return to the default MST configuration, use the `no spanning-tree mst configuration` command.

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

The default settings are as follows:

- No VLANs are mapped to any MST instance.
- All VLANs are mapped to the CIST instance.
- The region name is an empty string.
- The revision number is 0.

**Command Modes**

Global configuration mode

**Usage Guidelines**

The MST configuration consists of three main parameters:

- Instance VLAN mapping (see the `instance` command)
- Region name (see the `name` command)
- Configuration revision number (see the `revision` command)

By default, the value for the MST configuration is the default value for all its parameters.

The `abort` and `exit` commands allow you to exit the MST configuration submode. The difference between the two commands depends on whether you want to save your changes or not.

The `exit` command commits all the changes before leaving MST configuration submode. If you do not map the secondary VLANs to the same instance as the associated primary VLAN, when you exit the MST configuration submode, a message displays 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 the same time, this message is displayed:

```
Switch(config-mst)#
% MST CFG:Configuration change lost because of concurrent access
Switch(config-mst)#
```

**Examples**

This example shows how to enter the MST configuration submode:

```
Switch(config)#
spanning-tree mst configuration
Switch(config-mst)#
```

This example shows how to reset the MST configuration to the default settings:

```
Switch(config)#
no spanning-tree mst configuration
Switch(config)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>instance</td>
<td>Maps a VLAN or a set of VLANs to an MST instance.</td>
</tr>
<tr>
<td>name</td>
<td>Sets the MST region name.</td>
</tr>
<tr>
<td>revision</td>
<td>Sets the MST configuration revision number.</td>
</tr>
<tr>
<td>show spanning-tree mst</td>
<td>Displays MST protocol information.</td>
</tr>
</tbody>
</table>
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 spanning-tree mst forward-time` command.

**Syntax Description**

- `seconds`

  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 Modes**

- Global configuration mode

**Examples**

This example shows how to set the forward-delay timer:

```
Switch(config)# spanning-tree mst forward-time 20
Switch(config)#
```

**Related Commands**

- `show spanning-tree mst`
  
  Displays MST protocol information.
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
```

**Syntax Description**

- `seconds` Number of seconds to set the hello-time delay timer for all the instances on the Catalyst 4500 series switch; valid values are from 1 to 10 seconds.

**Defaults**

The hello-time delay timer is set for 2 seconds.

**Command Modes**

- Global configuration mode

**Usage Guidelines**

- If you do not specify the `hello-time` value, the value is calculated from the network diameter.

**Examples**

This example shows how to set the hello-time delay timer:

```
Switch(config)#
spanning-tree mst hello-time 3
Switch(config)#
```

**Related Commands**

- `show spanning-tree mst` Displays MST protocol information.
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 spanning-tree mst max-age` command.

**Syntax Description**
- `spanning-tree mst max-age` seconds
- `no spanning-tree mst max-age` seconds

**Defaults**
The max-age timer is set for 20 seconds.

**Command Modes**
Global configuration mode

**Examples**
This example shows how to set the max-age timer:

```
Switch(config)\# spanning-tree mst max-age 40
Switch(config)\#
```

**Related Commands**
- `show spanning-tree mst`: Displays MST protocol information.
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**

- **hopnumber**: Number of possible hops in the region before a BPDU is discarded; valid values are from 1 to 40 hops.

**Defaults**

Number of hops is 20.

**Command Modes**

Global configuration mode

**Examples**

This example shows how to set the number of possible hops in the region before a BPDU is discarded to 25:

```
Switch(config)#
spanning-tree mst max-hops 25
Switch(config)#
```

**Related Commands**

- `show spanning-tree mst`: Displays MST protocol information.
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]
```

**Syntax Description**

- **instance-id**: Instance identification number; valid values are from 1 to 15.
- **root**: Configures switch as the root switch.
- **primary**: Sets a high enough priority (low value) to make the bridge root of the spanning-tree instance.
- **secondary**: Designates this switch as a secondary root if the primary root fails.
- **priority**: Sets the bridge priority; see the "Usage Guidelines" section for valid values and additional information.
- **diameter**: (Optional) Sets the timer values for the bridge based on the network diameter; valid values are from 2 to 7.
- **hello-time**: (Optional) Specifies the duration between the generation of configuration messages by the root switch.

**Defaults**

- Bridge priority is 32768.

**Command Modes**

- Global configuration mode

**Usage Guidelines**

- The bridge priority can be set in increments of 4096 only. When you set the priority, valid values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440.
- You can set the priority to 0 to make the switch root.
- The `spanning-tree root secondary` bridge priority value is 16384.
- The `diameter` and `hello-time` options are available for instance 0 only.
- If you do not specify the `hello_time` value, the value is calculated from the network diameter.

**Examples**

This example shows how to set the priority and timer values for the bridge:

```
Switch(config)\# spanning-tree mst 0 root primary diameter 7 hello-time 2
Switch(config)\# spanning-tree mst 5 root primary
```

**Related Commands**

- `instance-id`: Instance identification number; valid values are from 1 to 15.
- `root`: Configures switch as the root switch.
- `primary`: Sets a high enough priority (low value) to make the bridge root of the spanning-tree instance.
- `secondary`: Designates this switch as a secondary root if the primary root fails.
- `priority`: Sets the bridge priority; see the "Usage Guidelines" section for valid values and additional information.
- `diameter`: (Optional) Sets the timer values for the bridge based on the network diameter; valid values are from 2 to 7.
- `hello-time`: (Optional) Specifies the duration between the generation of configuration messages by the root switch.

**Command Description**

- `show spanning-tree mst`: Displays MST protocol information.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

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}
```

### Syntax Description

- **long**: Specifies 32-bit-based values for port path costs.
- **short**: Specifies 16-bit-based values for port path costs.

### Defaults

Port path cost has 16-bit-based values.

### Command Modes

Global configuration mode

### Usage Guidelines

This command applies to all the spanning-tree instances on the switch.

- **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.
- **short** path cost calculation method (16 bits) yields values in the range of 1 through 65,535.

### Examples

This example shows how to set the path cost calculation method to long:

```
Switch(config)
spanning-tree pathcost method long
Switch(config)
```

This example shows how to set the path cost calculation method to short:

```
Switch(config)
spanning-tree pathcost method short
Switch(config)
```

### Related Commands

- `long`: Specifies 32-bit-based values for port path costs.
- `short`: Specifies 16-bit-based values for port path costs.
- `show spanning-tree`: Displays spanning-tree state information.
spanning-tree portfast (interface configuration mode)

To enable PortFast mode, where the interface is immediately put into the forwarding state upon linkup without waiting for the timer to expire, use the `spanning-tree portfast` command. To return to the default setting, use the `no` form of this command.

```
spanning-tree portfast {disable | trunk}
```

**Syntax Description**

- `disable`: Disables PortFast on the interface.
- `trunk`: Enables PortFast on the interface even while in the trunk mode.

**Defaults**

PortFast mode is disabled.

**Command Modes**

Interface configuration mode

**Usage Guidelines**

You should use this feature only with interfaces that connect to end stations; otherwise, an accidental topology loop could cause a data packet loop and disrupt the Catalyst 4500 series switch and network operation.

An interface with PortFast mode enabled is moved directly to the spanning-tree forwarding state when linkup occurs without waiting for the standard forward-time delay.

Be careful when using the `no spanning-tree portfast` command. This command does not disable PortFast if the `spanning-tree portfast default` command is enabled.

This command has four states:

- **`spanning-tree portfast`**: This command enables PortFast unconditionally on the given port.
- **`spanning-tree portfast disable`**: This command explicitly disables PortFast for the given port. The configuration line shows up in the running-configuration as it is not the default.
- **`spanning-tree portfast trunk`**: This command allows you to configure PortFast on trunk ports.
  
  **Note**: If you enter the `spanning-tree portfast trunk` command, the port is configured for PortFast even when in the access mode.
- **`no spanning-tree portfast`**: This command implicitly enables PortFast if the `spanning-tree portfast default` command is defined in global configuration and if the port is not a trunk port. If you do not configure PortFast globally, the `no spanning-tree portfast` command is equivalent to the `spanning-tree portfast disable` command.

**Examples**

This example shows how to enable PortFast mode:

```
Switch(config-if)#
spanning-tree portfast
Switch(config-if)
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>spanning-tree portfast</td>
<td>Enables PortFast by default on all access ports.</td>
</tr>
<tr>
<td>spanning-tree port-priority</td>
<td>Prioritizes an interface when two bridges compete for position as the root bridge.</td>
</tr>
<tr>
<td>spanning-tree uplinkfast</td>
<td>Enables the UplinkFast feature.</td>
</tr>
<tr>
<td>spanning-tree vlan</td>
<td>Configures STP on a per-VLAN basis.</td>
</tr>
<tr>
<td>show spanning-tree</td>
<td>Displays spanning-tree state information.</td>
</tr>
</tbody>
</table>
To enable the BPDU filtering by default on all PortFast ports, use the `spanning-tree portfast bpdufilter default` command. To return to the default settings, use the `no` form of this command.

```
spanning-tree portfast bpdufilter default
no spanning-tree portfast bpdufilter default
```

**Syntax Description**

This command has no keywords or arguments.

**Defaults**

BPDU filtering is disabled.

**Command Modes**

Global configuration mode

**Usage Guidelines**

The `spanning-tree portfast bpdufilter default` command enables BPDU filtering globally on the Catalyst 4500 series switch. BPDU filtering prevents a port from sending or receiving any BPDUs. You can override the effects of the `spanning-tree portfast bpdufilter default` command by configuring BPDU filtering at the interface level.

**Note**

Be careful when enabling BPDU filtering. Functionality is different when enabling on a per-port basis or globally. When enabled globally, BPDU filtering is applied only on ports that are in an operational PortFast state. Ports still send a few BPDUs at linkup before they effectively filter outbound BPDUs. If a BPDU is received on an edge port, it immediately loses its operational PortFast status and BPDU filtering is disabled.

When enabled locally on a port, BPDU filtering prevents the Catalyst 4500 series switch from receiving or sending BPDUs on this port.

**Caution**

Be careful when using this command. This command can cause bridging loops if not used correctly.

**Examples**

This example shows how to enable BPDU filtering by default:

```
Switch(config)＃
spanning-tree portfast bpdufilter default
Switch(config)＃
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show spanning-tree mst</code></td>
<td>Displays MST protocol information.</td>
</tr>
<tr>
<td><code>spanning-tree bpdufilter</code></td>
<td>Enables BPDU filtering on an interface.</td>
</tr>
</tbody>
</table>
Cisco IOS Commands for the Catalyst 4500 Series Switches

spanning-tree portfast bpduguard default

To enable BPDU guard by default on all the PortFast ports, use the `spanning-tree portfast bpduguard default` command. To return to the default settings, use the `no spanning-tree portfast bpduguard default` command.

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

**Defaults**
BPDU guard is disabled.

**Command Modes**
Global configuration mode

**Usage Guidelines**
*Caution*
Use this command only with the interfaces that connect to the end stations; otherwise, an accidental topology loop could cause a data packet loop and disrupt the Catalyst 4500 series switch and network operation.

BPDU guard disables a port if it receives a BPDU. BPDU guard is applied only on ports that are PortFast enabled and are in an operational PortFast state.

**Examples**
This example shows how to enable BPDU guard by default:

Switch(config)# spanning-tree portfast bpduguard default
Switch(config)#

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show spanning-tree mst</td>
<td>Displays MST protocol information.</td>
</tr>
<tr>
<td>spanning-tree bpduguard</td>
<td>Enables BPDU guard on an interface.</td>
</tr>
</tbody>
</table>
To globally enable PortFast by default on all access ports, use the `spanning-tree portfast default` command. To disable PortFast as default on all access ports, use the `no spanning-tree portfast default` command.

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

PortFast is disabled.

**Command Modes**

Global configuration mode

**Usage Guidelines**

*Caution*

Use this command only with the interfaces that connect to end stations; otherwise, an accidental topology loop could cause a data packet loop and disrupt the Catalyst 4500 series switch and network operation.

An interface with PortFast mode enabled is moved directly to the spanning-tree forwarding state when linkup occurs without waiting for the standard forward-time delay.

You can enable PortFast mode on individual interfaces using the `spanning-tree portfast (interface configuration mode)` command.

**Examples**

This example shows how to globally enable PortFast by default on all access ports:

```
Switch(config)# spanning-tree portfast default
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show spanning-tree</code></td>
<td>Displays spanning-tree state information.</td>
</tr>
<tr>
<td><code>spanning-tree portfast (interface configuration mode)</code></td>
<td>Enables PortFast mode.</td>
</tr>
</tbody>
</table>
To prioritize an interface when two bridges compete for position as the root bridge, use the `spanning-tree port-priority` command. The priority you set resolves the conflict. To revert to the default setting, use the `no` form of this command.

```
spanning-tree port-priority port_priority
no spanning-tree port-priority
```

**Syntax Description**
- `port_priority`: Port priority; valid values are from 0 to 240 in increments of 16.

**Defaults**
- Port priority value is set to 128.

**Command Modes**
- Interface configuration mode

**Examples**
This example shows how to increase the possibility that the spanning-tree instance 20 will be chosen as the root-bridge on interface FastEthernet 2/1:

```
Switch(config-if)# spanning-tree port-priority 0
Switch(config-if)#
```

**Related Commands**
- `port_priority` (Command Description)
- `spanning-tree cost` (Calculates the path cost of STP on an interface)
- `spanning-tree portfast default` (Enables PortFast by default on all access ports)
- `spanning-tree portfast (interface configuration mode)` (Enables PortFast mode)
- `spanning-tree uplinkfast` (Enables the UplinkFast feature)
- `spanning-tree vlan` (Configures STP on a per-VLAN basis)
- `show spanning-tree` (Displays spanning-tree state information)
spanning-tree uplinkfast

To enable the UplinkFast feature, use the `spanning-tree uplinkfast` command. To disable UplinkFast, use the `no` form of this command.

`spanning-tree uplinkfast [max-update-rate packets-per-second]`

**Syntax Description**

- `max-update-rate`: (Optional) Specifies the maximum rate (in packets per second) at which update packets are sent; valid values are from 0 to 65535.

**Defaults**

- Disabled.
- Maximum update rate is 150.

**Command Modes**

- Global configuration mode

**Usage Guidelines**

This command should be used only on access switches. When UplinkFast is configured, the bridge priority is changed to 49,152 so that this switch will not be selected as root. All interface path costs of all spanning-tree interfaces belonging to the specified spanning-tree instances are also increased by 3000.

When spanning tree detects that the root interface has failed, the UplinkFast feature causes an immediate switchover to 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**

This example shows how to enable UplinkFast and set the maximum rate to 200 packets per second:

```
Switch(config)#
spanning-tree uplinkfast
Switch(config)#
spanning-tree uplinkfast max-update-rate 200
```

**Related Commands**

- `max-update-rate packets_per_second`: (Optional) Specifies the maximum rate (in packets per second) at which update packets are sent; valid values are from 0 to 65535.
- `spanning-tree cost`: Calculates the path cost of STP on an interface.
- `spanning-tree port-priority`: Prioritizes an interface when two bridges compete for position as the root bridge.
- `spanning-tree portfast default`: Enables PortFast by default on all access ports.
spanning-tree uplinkfast

Enables PortFast mode.

spanning-tree portfast (interface configuration mode)

Configures STP on a per-VLAN basis.

Command Description
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]]
```

**Syntax Description**

**Defaults**

The default settings are as follows:

- **Forward-time**—15 seconds
- **Hello-time**—2 seconds
- **Max-age**—20 seconds
- **Priority**—32768 with STP enabled; 128 with MST enabled
- **Root**—No STP root

**Command Modes**

Global configuration mode

**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.

**vlan_id**

VLAN identification number; valid values are from 1 to 4094.

**forward-time** seconds (Optional) Sets the STP forward delay time; valid values are from 4 to 30 seconds.

**hello-time** seconds (Optional) Specifies, in seconds, the time between configuration messages generated by the root switch; valid values are from 1 to 10 seconds.

**max-age** seconds (Optional) Sets the maximum time, in seconds, that the information in a BPDU is valid; valid values are from 6 to 40 seconds.

**priority** priority (Optional) Sets the STP bridge priority; valid values are from 0 to 65535.

**protocol** protocol (Optional) Specifies the protocol.

**root primary** (Optional) Forces this switch to be the root bridge.

**root secondary** (Optional) Specifies this switch act as the root switch should the primary root fail.

**diameter** net-diameter (Optional) Specifies the maximum number of bridges between two end stations; valid values are from 2 to 7.
The `spanning-tree root secondary` command alters the switch bridge priority to 16384. If the root switch fails, this switch becomes the next root switch. Use the `spanning-tree root` commands on backbone switches only.

**Examples**

This example shows how to enable spanning tree on VLAN 200:

```
Switch(config)# spanning-tree vlan 200
```

This example shows how to configure the switch as the root switch for VLAN 10 with a network diameter of 4:

```
Switch(config)# spanning-tree vlan 10 root primary diameter 4
```

This example shows how to configure the switch as the secondary root switch for VLAN 10 with a network diameter of 4:

```
Switch(config)# spanning-tree vlan 10 root secondary diameter 4
```

**Related Commands**

- `spanning-tree cost`: Calculates the path cost of STP on an interface.
- `spanning-tree port-priority`: Prioritizes an interface when two bridges compete for position as the root bridge.
- `spanning-tree portfast default`: Enables PortFast by default on all access ports.
- `spanning-tree portfast (interface configuration mode)`: Enables PortFast mode.
- `spanning-tree vlan`: Configures STP on a per-VLAN basis.
- `show spanning-tree`: Displays spanning-tree state information.
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}
```

### 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.

### Defaults

The default values are shown in the following table:

<table>
<thead>
<tr>
<th>Interface Type Supported</th>
<th>Syntax</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/100-Mbps module</td>
<td>speed</td>
<td>auto [10</td>
</tr>
<tr>
<td>100-Mbps fiber modules</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Gigabit Ethernet Interface</td>
<td>speed nonegotiate</td>
<td>Nonegotiate</td>
</tr>
</tbody>
</table>

### Guidelines

- If the speed is set to 10 or 100 and you do not configure the duplex setting, the duplex is set to half.
- Gigabit Ethernet ports.

### Table 2-35 Supported speed Command Options

<table>
<thead>
<tr>
<th>Interface Type Supported</th>
<th>Syntax</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/100-Mbps module</td>
<td>speed</td>
<td>auto [10</td>
</tr>
<tr>
<td>100-Mbps fiber modules</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Gigabit Ethernet Interface</td>
<td>speed nonegotiate</td>
<td>Nonegotiate</td>
</tr>
</tbody>
</table>
Chapter 2  Cisco IOS Commands for the Catalyst 4500 Series Switches

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 reenable the interface during the reconfiguration.

Table 2-36 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.

### Examples
This example shows how to set the interface speed to 100 Mbps on the Fast Ethernet interface 5/4:

```
Switch(config)#
interface fastethernet 5/4
Switch(config-if)#
```

### Table 2-36 Supported speed Command Options (continued)

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Supported Syntax</th>
<th>Default Setting</th>
<th>Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>speed auto</td>
<td>Auto</td>
<td></td>
</tr>
<tr>
<td></td>
<td>speed 10</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td></td>
<td>speed 100</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td></td>
<td>speed 1000</td>
<td>1000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>speed auto 10</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>speed auto 100</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>speed auto 1000</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>speed auto half</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>speed full 10</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>speed full 100</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>speed full 1000</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Speed is always 1000. The duplex is half.
- Speed is always 1000. The duplex is full.
- Speed is always 1000. The duplex is full.

Table 2-36 System Action Using duplex and speed Commands

<table>
<thead>
<tr>
<th>duplex Command</th>
<th>speed Command</th>
<th>Resulting System Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>duplex auto</td>
<td>speed auto</td>
<td>Autonegotiates both speed and duplex modes</td>
</tr>
<tr>
<td>duplex half</td>
<td>speed 10</td>
<td>Forces 10 Mbps and half duplex</td>
</tr>
<tr>
<td>duplex full</td>
<td>speed 10</td>
<td>Forces 10 Mbps and full duplex</td>
</tr>
<tr>
<td>duplex half</td>
<td>speed 100</td>
<td>Forces 100 Mbps and half duplex</td>
</tr>
<tr>
<td>duplex full</td>
<td>speed 100</td>
<td>Forces 100 Mbps and full duplex</td>
</tr>
<tr>
<td>duplex full</td>
<td>speed 1000</td>
<td>Forces 1000 Mbps and full duplex</td>
</tr>
</tbody>
</table>
This 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.

This example shows how to limit the interface speed to 10 and 100 Mbps on the Gigabit Ethernet interface 1/1 in auto-negotiation mode:

Switch(config)#
interface gigabitethernet 1/1
Switch(config-if)#
speed auto 10 100

This example shows how to limit the speed negotiation to 100 Mbps on the Gigabit Ethernet interface 1/1:

Switch(config)#
interface gigabitethernet 1/1
Switch(config-if)#
speed auto 100

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>duplex</td>
<td>Configures the duplex operation on an interface.</td>
</tr>
<tr>
<td>interface</td>
<td>Configures an interface type and enter interface configuration mode.</td>
</tr>
<tr>
<td>show controllers</td>
<td>Displays controller information.</td>
</tr>
<tr>
<td>show interfaces</td>
<td>Displays traffic on a specific interface.</td>
</tr>
</tbody>
</table>
To enable broadcast storm control on a port and to specify what to do when a storm occurs on a port, use the `storm-control` interface configuration command. To disable storm control for the broadcast traffic and to disable a specified storm-control action, use the `no` form of this command.

```
storm-control {broadcast level high-level [lower-level]} | action {shutdown | trap} }
```

Syntax Description

- **broadcast**
  - Enables the broadcast storm control on the port.
- **level**
  - `high-level` and `lower-level` define the rising and falling suppression levels:
    - `high-level` — Rising suppression level as a percent of total bandwidth, up to two decimal places; valid values are from 0 to 100 percent. Blocks the flooding of storm packets when the value specified for `level` is reached.
    - `lower-level` — (Optional) Falling suppression level as a percent of total bandwidth, up to two decimal places; valid values are from 0 to 100. This value must be less than the rising suppression value.
- **action**
  - `shutdown` — Disables the port during a storm.
  - `trap` — Sends an SNMP trap when a storm occurs. This keyword is available but not supported in 12.1(19)EW.

Defaults

Broadcast storm control is disabled.

Command Modes

- Interface configuration mode

Usage Guidelines

Enter the `storm-control broadcast level high-level lower-level` command to enable traffic storm control on the interface, configure the traffic storm control level, and apply the traffic storm control level to the broadcast traffic on the interface.

The Catalyst 4500 series switch supports broadcast traffic storm control on all LAN ports.

The period is required when you enter the fractional suppression level.

The suppression level is entered as a percentage of the total bandwidth. A threshold value of 100 percent indicates that no limit is placed on traffic. A value of 0.0 means that all specified traffic on that port is blocked.

Enter the `show interfaces counters storm-control` command to display the discard count.

Enter the `show running-config` command to display the enabled suppression mode and level setting.

To turn off suppression for the specified traffic type, you can do one of the following:

- Set the `high-level` value to 100 percent for the specified traffic type.
storm-control

Use the no form of this command.
The lower level is ignored for the interfaces that perform storm control in the hardware.

Examples

This example shows how to enable broadcast storm control on a port with a 75.67 percent rising suppression level:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 3/1
Switch(config-if)# storm-control broadcast level 75.67
Switch(config-if)# end
```

This example shows how to disable the port during a storm:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 3/1
Switch(config-if)# storm-control action shutdown
Switch(config-if)# end
```

This example shows how to disable storm control on a port:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 3/1
Switch(config-if)# no storm-control broadcast level
Switch(config-if)# end
```

This example shows how to disable storm control by setting the high level to 100 percent:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 3/1
Switch(config-if)# storm-control broadcast level 100
Switch(config-if)# end
```

Related Commands

Command Description

- `show interfaces counters`
  Displays the traffic on the physical interface.
- `show running-config`
  Displays the running configuration of a switch.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

storm-control broadcast inclusion multicast

To enable multicast storm control on a port, use the storm-control broadcast inclusion multicast command. To disable multicast storm control, use the no form of this command.

storm-control broadcast inclusion multicast

Syntax Description
This command has no arguments or keywords.

Defaults
Multicast storm control is disabled.

Command Modes
Interface configuration mode

Usage Guidelines
This command prompts the hardware to filter multicast packets if it is already filtering broadcast packets.

The Catalyst 4500 series switch support per-interface multicast suppression. When you enable multicast suppression on an interface you subject incoming multicast and broadcast traffic on that interface to suppression.

Examples
This example shows how to enable multicast storm control globally:

Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# storm-control broadcast inclusion multicast
Switch(config)# end

This example shows how to enable per-port Multicast storm control:

Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet2/4
Switch(config-if)# storm-control broadcast inclusion multicast
Switch(config)# end

Related Commands
- storm-control
  Enables broadcast storm control on a port and specifies what to do when a storm occurs on a port.
To subscribe to all available alert groups, use the `subscribe-to-alert-group all` command.

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

**Defaults**
This command has no default settings.

**Command Modes**
cfg-call-home-profile

**Usage Guidelines**
To enter profile call-home configuration submode, use the `profile` command in call-home configuration mode.

**Examples**
This example 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**
- `destination address`: Configures the destination e-mail address or URL to which Call Home messages will be sent.
- `destination message-size-limit bytes`: Configures a maximum destination message size for the destination profile.
- `destination preferred-msg-format`: Configures a preferred message format.
- `destination transport-method`: Enables the message transport method.
- `profile`: Enters profile call-home configuration submode
- `subscribe-to-alert-group configuration`: Subscribes this destination profile to the Configuration alert group.
- `subscribe-to-alert-group diagnostic`: Subscribes this destination profile to the Diagnostic alert group.
- `subscribe-to-alert-group environment`: Subscribes this destination profile to the Environment alert group.
- `subscribe-to-alert-group inventory`: Subscribes this destination profile to the Inventory alert group.
- `subscribe-to-alert-group syslog`: Subscribes this destination profile to the Syslog alert group.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

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

- **Defaults**: This command has no default settings.
- **Command Modes**: `cfg-call-home-profile`
- **Usage Guidelines**: To enter profile call-home configuration submode, use the `profile` command in call-home configuration mode.

The Configuration alert group can be configured for periodic notification.

**Examples**

This example shows how to configure periodic "configuration" alert-group:

```
Switch(config)#
call-home
Switch(cfg-call-home)#
profile cisco
Switch(cfg-call-home-profile)#
subscribe-to-alert-group configuration periodic weekly Tuesday 21:16
```

**Related Commands**

- `periodic` (Optional) Specifies a periodic call-home message.
- `daily hh:mm` Sets a daily alert in hours and minutes.
- `monthly date hh:mm` Sets a monthly alert in day, hour, and minute.
- `weekly day hh:mm` Sets a weekly alert in day, hour, and minutes.

**Command Description**

- `destination address` Configures the destination e-mail address or URL to which Call Home messages will be sent.
- `destination message-size-limit bytes` Configures a maximum destination message size for the destination profile.
- `destination preferred-msg-format` Configures a preferred message format.
- `destination transport-method` Enables the message transport method.
- `profile` Enters profile call-home configuration submode
- `subscribe-to-alert-group all` Subscribes to all available alert groups.
- `subscribe-to-alert-group diagnostic` Subscribes this destination profile to the Diagnostic alert group.
- `subscribe-to-alert-group environment` Subscribes this destination profile to the Environment alert group.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

subscribe-to-alert-group configuration
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.
To subscribe a destination profile to the Diagnostic alert group, use the `subscribe-to-alert-group` command.

```
subscribe-to-alert-group diagnostic [severity catastrophic | disaster | fatal | critical | major | minor | warning | notification | normal | debugging]
```

**Syntax Description**

**Defaults**

- `normal`

**Command Modes**

- `cfg-call-home-profile`

**Usage Guidelines**

To enter profile call-home configuration submode, use the `profile` command in call-home configuration mode.

**Examples**

This example shows how to configure the "diagnostic" alert-group with "normal" severity:

```
Switch(config)#
call-home
Switch(cfg-call-home)#
profile cisco
Switch(cfg-call-home-profile)#
subscribe-to-alert-group diagnostic severity normal
```

**Related Commands**

- `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 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.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

subscribe-to-alert-group diagnostic
subscribe-to-alert-group all
subscribe-to-alert-group configuration
subscribe-to-alert-group environment
subscribe-to-alert-group inventory
subscribe-to-alert-group syslog

Command Description
To subscribe a destination profile to the Environment alert group, use the `subscribe-to-alert-group environment` command.

### Syntax Description

#### Defaults
- `normal`

#### Command Modes
- `cfg-call-home-profile`

#### Usage Guidelines
- To enter profile call-home configuration submode, use the `profile` command in call-home configuration mode.
- The Environment alert group can be configured to filter messages based on severity.

#### Examples

This example shows how to configure the “environmental” alert-group with “severity notification”:

```
Switch(config)#
 call-home
Switch(cfg-call-home)#
 profile cisco
Switch(cfg-call-home-profile)#
 subscribe-to-alert-group environment severity notification
```

#### Related Commands

- `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).

- `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.
subscribe-to-alert-group environment
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.
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**

- **Defaults**: This command has no default settings.
- **Command Modes**: `cfg-call-home-profile`
- **Usage Guidelines**: To enter profile call-home configuration submode, use the `profile` command in call-home configuration mode.
- **Examples**: This example 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**

- `periodic` (Optional) Specifies a periodic call-home message.
- `daily hh:mm` Sets a daily alert in hours and minutes.
- `monthly date hh:mm` Sets a monthly alert in day, hour, and minute.
- `weekly day hh:mm` Sets a weekly alert in day, hour, and minutes.

**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 inventory

Subscribes this destination profile to the Environment alert group.

subscribe-to-alert-group syslog

Subscribes this destination profile to the Syslog alert group.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

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

Defaults
normal

Command Modes
cfg-call-home-profile

Usage Guidelines
You can configure the Syslog alert group can be configured to filter messages based on severity by specifying a pattern to be matched in the syslog message. If the pattern contains spaces, you must enclose it in quotes (".

Examples
This example shows how to configure the syslog alert group with severity notification:

Switch(config)#
call-home
Switch(cfg-call-home)#
profile cisco
Switch(cfg-call-home-profile)#
subscribe-to-alert-group syslog severity notification
pattern "UPDOWN"

Related Commands

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 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.
subscribe-to-alert-group sysl og

Configures a preferred message format.

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.
To modify the switching characteristics of a Layer 2 switch interface, use the `switchport` command. To return the interface to the routed-interface status and cause all further Layer 2 configuration to be erased, use the `no` form of this command without parameters.

```
switchport [access vlan vlan_num] | [nonegotiate] | [voice vlan {vlan_id | dot1p | none | untagged}]
no switchport [access | nonegotiate | voice vlan]
```

### Syntax Description

- `access vlan vlan_num` (Optional) Sets the VLAN when the interface is in access mode; valid values are from 1 to 1005.
- `nonegotiate` (Optional) Specifies that the DISL/DTP negotiation packets will not be sent on the interface.
- `voice vlan vlan_id` (Optional) Specifies the number of the VLAN; valid values are from 1 to 1005.
- `dot1p` (Optional) Specifies that the PVID packets are tagged as priority.
- `none` (Optional) Specifies that the telephone and voice VLAN do not communicate.
- `untagged` (Optional) Specifies the untagged PVID packets.

### Defaults

- Switchport trunking mode is enabled.
- Dynamic negotiation parameter is set to auto.
- Access VLANs and trunk interface native VLANs are a default VLAN corresponding to the platform or interface hardware.
- All VLAN lists include all VLANs.
- No voice VLAN is enabled.

### Command Modes

Interface configuration mode

### Usage Guidelines

- The `no switchport` command shuts the port down and then reenables it, which may generate messages on the device to which the port is connected.
- The `no` form of the `switchport access` command resets the access mode VLAN to the appropriate default VLAN for the device. The `no` form of the `switchport nonegotiate` command removes the `nonegotiate` status.
- When you are using the `nonegotiate` keyword, DISL/DTP negotiation packets will not be sent on the interface. The device will trunk or not trunk according to the mode parameter given: access or trunk.
- This command will return an error if you attempt to execute it in dynamic (auto or desirable) mode.
- The voice VLAN is automatically set to VLAN 1 unless you use one of the optional keywords.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

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.

Examples

This example shows how to cause the port interface to stop operating as a Cisco-routed port and convert to a Layer 2-switched interface:

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

This example shows how to cause a port interface in access mode, which is configured as a switched interface, to operate in VLAN 2:

```
Switch(config-if)#
switchport access vlan 2
Switch(config-if)#
```

This example shows how to cause a port interface, which is configured as a switched interface, to refrain from negotiating in trunking mode and act as a trunk or access port (depending on the `mode` set):

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

This example shows how to set the voice VLAN for the interface to VLAN 2:

```
Switch(config-if)#
switchport voice vlan 2
```

---

Related Commands

Command Description

`show interfaces switchport` Displays the administrative and operational status of a switching (nonrouting) port.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

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}]
no switchport access vlan
```

**Syntax Description**

- **Defaults**
  The default settings are as follows:
  - The access VLAN and trunk interface native VLAN are default VLANs that correspond to the platform or the interface hardware.
  - All VLAN lists include all VLANs.

- **Command Modes**
  Interface configuration mode

- **Usage Guidelines**
  You must enter the `switchport` command without any keywords to configure the LAN interface as a Layer 2 interface before you can enter the `switchport access vlan` command. This action is required only if you have not already entered the `switchport` command for the interface.

  Entering the `no switchport` command shuts the port down and then reenables it, which could generate messages on the device to which the port is connected.

  The `no` form of the `switchport access vlan` command resets the access mode VLAN to the appropriate default VLAN for the device.

- **Valid values for vlan-id**
  valid values are from 1 to 4094.

**Examples**

This example shows how to cause the port interface to stop operating as a Cisco-routed port and convert to a Layer 2-switched interface:

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

Note

This command is not used on platforms that do not support Cisco-routed ports. All physical ports on such platforms are assumed to be Layer 2-switched interfaces.

This example shows how to cause a port interface that has already been configured as a switched interface to operate in VLAN 2 instead of the platform's default VLAN when in access mode:

```
Switch(config-if)#
switchport access vlan 2
```

**vlan-id** (Optional) Number of the VLAN on the interface in access mode; valid values are from 1 to 4094.

**dynamic** (Optional) Enables VMPS control of the VLAN.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

switchport access vlan

Related Commands

Command Description

show interfaces switchport
Displays the administrative and operational status of a switching (nonrouting) port.
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.

**Syntax Description**

This command has no keywords or arguments.

**Defaults**

All ports are included in the VLAN interface link-up calculation.

**Command Modes**

Interface configuration mode

**Usage Guidelines**

You must enter the `switchport` command without any keywords to configure the LAN interface as a Layer 2 interface before you can enter the `switchport autostate exclude` command. This action is required only if you have not entered the `switchport` command for the interface.

**Note**

The `switchport` command is not used on platforms that do not support Cisco-routed ports. All physical ports on such platforms are assumed to be Layer 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**

This example shows how to exclude a port from the VLAN interface link-up calculation:

```
Switch(config-if)#
switchport autostate exclude
Switch(config-if)#
```

This 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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show interfaces switchport</code></td>
<td>Displays the administrative and operational status of a switching (nonrouting) port.</td>
</tr>
</tbody>
</table>
To prevent the unknown multicast or unicast packets from being forwarded, use the \texttt{switchport block} interface configuration command. To allow the unknown multicast or unicast packets to be forwarded, use the \texttt{no} form of this command.

\[
\texttt{switchport block \{multicast | unicast\}} \\
\texttt{no switchport block \{multicast | unicast\}}
\]

\textbf{Syntax Description}

\textbf{Defaults}

Unknown multicast and unicast traffic are not blocked. All traffic with unknown MAC addresses is sent to all ports.

\textbf{Command Modes}

Interface configuration mode

\textbf{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.

\textbf{Examples}

This example shows how to block the unknown multicast traffic on an interface:

\begin{verbatim}
Switch(config-if)# switchport block multicast
\end{verbatim}

You can verify your setting by entering the \texttt{show interfaces interface-id switchport} privileged EXEC command.

\textbf{Related Commands}

\begin{itemize}
\item \texttt{multicast} - Specifies that the unknown multicast traffic should be blocked.
\item \texttt{unicast} - Specifies that the unknown unicast traffic should be blocked.
\end{itemize}

\textbf{Command Description}

\begin{itemize}
\item \texttt{show interfaces switchport} - Displays the administrative and operational status of a switching (nonrouting) port.
Chapter 2  
Cisco IOS Commands for the Catalyst 4500 Series Switches

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

Defaults

Link converts to a trunk link.
dot1q tunnel ports are disabled.

Command Modes

Interface configuration mode

Usage Guidelines

If you enter access mode, the interface goes into permanent nontrunking mode and negotiates to convert the link into a nontrunk link even if the neighboring interface does not approve the change.

If you enter trunk mode, the interface goes into permanent trunking mode and negotiates to convert the link into a trunk link even if the neighboring interface does not approve the change.

If you enter dynamic auto mode, the interface converts the link to a trunk link if the neighboring interface is set to trunk or desirable mode.

If you enter dynamic desirable mode, the interface becomes a trunk interface if the neighboring interface is set to trunk, desirable, or auto mode.

If you specify the dot1q-tunnel keyword, the port is set unconditionally as an 802.1Q tunnel port.

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.
switchport mode

The port becomes inactive if you configure it as a private VLAN trunk port and one of the following applies:

- The port does not have a valid PVLAN association.
- The port does not have valid allowed normal VLANs.

If a private port PVLAN association or mapping is deleted, or if a private port is configured as a SPAN destination, it becomes inactive.

Examples

This example shows how to set the interface to dynamic desirable mode:

Switch(config-if)#
switchport mode dynamic desirable
Switch(config-if)#

This example shows how to set a port to PVLAN host mode:

Switch(config-if)#
switchport mode private-vlan host
Switch(config-if)#

This example shows how to set a port to private VLAN trunk:

Switch(config-if)#
switchport mode private-vlan trunk
Switch(config-if)#

This example shows how to configure a port for an 802.1Q tunnel port:

Switch(config-if)#
switchport mode dot1q-tunnel
Switch(config-if)#

This example shows how to configure a promiscuous trunk port:

Switch(config-if)#
switchport mode private-vlan trunk promiscuous
Switch(config-if)#

This example shows how to configure an isolated trunk port:

Switch(config-if)#
switchport mode private-vlan trunk
OR
Switch(config-if)#
switchport mode private-vlan trunk secondary
Switch(config-if)#

You can verify your settings by entering the `show interfaces switchport` command and examining information in the Administrative Mode and Operational Mode rows.

This example shows how to configure interface FastEthernet 5/2 as a PVLAN promiscuous port, map it to a PVLAN, and verify the configuration:

Switch#
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
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

This 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
```

This example shows how to configure interface FastEthernet 5/2 as a secondary trunk port, and verify the configuration:

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/2
Switch(config-if)# switchport mode private-vlan trunk secondary
Switch(config-if)# switchport private-vlan trunk native vlan 10
Switch(config-if)# switchport private-vlan trunk allowed vlan 10. 3-4
Switch(config-if)# switchport private-vlan association trunk 3 301
Switch(config-if)# end

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)
```
This example shows how to configure interface FastEthernet 5/2 as a promiscuous trunk port and to verify the configuration:

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/2
Switch(config-if)# switchport mode private-vlan trunk promiscuous
Switch(config-if)# switchport private-vlan trunk native vlan 10
Switch(config-if)# switchport private-vlan trunk allowed vlan 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
```
### Chapter 2: Cisco IOS Commands for the Catalyst 4500 Series Switches

**switchport mode**

Switch(config-if)#

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show interfaces switchport</td>
<td>Displays the administrative and operational status of a switching (nonrouting) port.</td>
</tr>
<tr>
<td>switchport</td>
<td>Enables port security on an interface.</td>
</tr>
<tr>
<td>switchport private-vlan host-association</td>
<td>Defines a PVLAN association for an isolated or community port.</td>
</tr>
<tr>
<td>switchport private-vlan mapping</td>
<td>Defines private VLAN mapping for a promiscuous port.</td>
</tr>
</tbody>
</table>
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.

```
```

**Syntax Description**

- **aging** (Optional) Specifies aging for port security.
- **static** (Optional) Enables aging for statically configured secure addresses on this port.
- **time** (Optional) Specifies the aging time for this port. The valid values are from 0 to 1440 minutes. If the time is 0, aging is disabled for this port.
- **type absolute** (Optional) Sets the aging type as absolute aging. All the secure addresses on this port age out exactly after the time (minutes) specified and are removed from the secure address list.
- **type inactivity** (Optional) Sets the aging type as inactivity aging. The secure addresses on this port age out only if there is no data traffic from the secure source address for the specified time period.
- **limit rate** invalid-source-mac (Optional) Sets the rate limit for bad packets. This rate limit also applies to the port where DHCP snooping security mode is enabled as filtering the IP and MAC address.
- **N none** (Optional) Supplies a rate limit (N) or indicates none (none).
- **mac-address** mac-address (Optional) Specifies a secure MAC address for the interface; a 48-bit MAC address. You can add additional secure MAC addresses up to the maximum value that is configured.
- **sticky** (Optional) Configures the dynamic addresses as sticky on the interface.
- **vlan access** (Optional) Deletes the secure MAC addresses from access VLANs.
- **vlan voice** (Optional) Deletes the secure MAC addresses from voice VLANs.
- **maximum value** (Optional) Sets the maximum number of secure MAC addresses for the interface. Valid values are from 1 to 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.
Chapter 2  
Cisco IOS Commands for the Catalyst 4500 Series Switches

**switchport port-security**

**Defaults**
The default settings are as follows:
- Port security is disabled.
- When port security is enabled and no keywords are entered, the default maximum number of secure MAC addresses is 1.
- Aging is disabled.
- Aging time is 0 minutes.
- All secure addresses on this port age out immediately after they are removed from the secure address list.

**Command Modes**
Interface configuration mode

**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 shutdown` 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.

**shutdown** (Optional) Sets the security violation shut down 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.
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**

This example shows how to set the aging time to 2 hours (120 minutes) for the secure addresses on the Fast Ethernet port 12:

```
Switch(config)#
interface fastethernet 0/12
Switch(config-if)#
switchport port-security aging time 120
Switch(config-if)#
```

This example shows how to set the aging timer type to Inactivity for the secure addresses on the Fast Ethernet port 12:

```
Switch(config)#
interface fastethernet 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)#
```

You can verify the settings for all secure ports or the specified port by using the `show port-security` `privilege` `exec` command.

This example shows how to remove all sticky and static addresses that are configured on the interface:

```
Switch(config)#
interface fastethernet 2/12
Switch(config-if)#
no switchport port-security mac-address
Switch(config-if)
```

This example shows how to configure a secure MAC address on Fast Ethernet port 12:

```
Switch(config)#
interface fastethernet 0/12
Switch(config-if)#
switchport mode access
Switch(config-if)#
switchport port-security
```
Chapter 2  Cisco IOS Commands for the Catalyst 4500 Series Switches

switchport port-security

Switch(config-if)\#
switchport port-security mac-address 1000.2000.3000
Switch(config-if)

This example shows how to make all MAC addresses learned on Fast Ethernet port 12 sticky:
Switch(config)\#
interface fastethernet 2/12
Switch(config-if)\#
switchport port-security mac-address sticky
Switch(config-if)

This example shows how to make MAC address 1000.2000.3000 sticky on Fast Ethernet port 12:
Switch(config)\#
interface fastethernet 2/12
Switch(config-if)\#
switchport port-security mac-address sticky 1000.2000.3000
Switch(config-if)

This example shows how to disable the sticky feature on Fast Ethernet port 12:
Switch(config)\#
interface fastethernet 2/12
Switch(config-if)\#
no switchport port-security mac-address sticky
Switch(config-if)

Note
This command makes all sticky addresses on this interface normal learned entries. It does not delete the entries from the secure MAC address table.

Note
The following examples show how to configure sticky secure MAC addresses in access and voice VLANs on interfaces with voice VLAN configured. If you do not have voice VLAN configured the vlan [access | voice] keywords are not supported.

This example shows how to configure sticky MAC 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 0000.0000.0003 vlan voice
Switch(config-if)\#
switchport port-security mac-address sticky 0000.0000.0005 vlan access
Switch(config-if)\#
end

This example shows how to designate a maximum of one MAC address for a voice VLAN (for a Cisco IP Phone, let’s say) and one MAC address for the data VLAN (for a PC, let’s say) on Fast Ethernet interface 5/1 and to verify the configuration:
Switch# 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

This example shows how to configure a port to shut down only the VLAN if a violation occurs:
Switch(config)\#
interface gigabitethernet 5/1
Switch(config)\#
switchport port-security violation shutdown vlan
### switchport port-security

**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.

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show interfaces switchport</code></td>
<td>Displays the administrative and operational status of a switching (nonrouting) port.</td>
</tr>
<tr>
<td><code>show port-security</code></td>
<td>Displays the port security settings for an interface or for the switch.</td>
</tr>
<tr>
<td><code>switchport block</code></td>
<td>Prevents the unknown multicast or unicast packets from being forwarded.</td>
</tr>
</tbody>
</table>
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}
```

**Syntax Description**

- `primary-vlan-id`: Number of the primary VLAN of the private VLAN relationship.
- `secondary-vlan-id`: Number of the secondary VLAN of the private VLAN relationship.

**Defaults**

Private VLAN mapping is disabled.

**Command Modes**

Interface configuration mode

**Usage Guidelines**

Multiple private VLAN pairs can be specified so that a private VLAN trunk port can carry multiple secondary VLANs. If an association is specified for the existing primary VLAN, the existing association is replaced.

Only isolated secondary VLANs can be carried over a private VLAN trunk.

**Note**

Community secondary VLANs on a private VLAN trunk are not supported in this release.

If there is no trunk association, any packets received on the secondary VLANs are dropped.

**Examples**

This example shows how to configure a port with a primary VLAN (VLAN 18) and secondary VLAN (VLAN 20):

```
Switch(config-if)#
switchport private-vlan association trunk 18 20
Switch(config-if)#
```

This example shows how to remove the private VLAN association from the port:

```
Switch(config-if)#
no switchport private-vlan association trunk 18
Switch(config-if)#
```

This example shows how to configure interface FastEthernet 5/2 as a secondary trunk port, and verify the configuration:

```
Switch#
configure terminal
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
```
switchport privat e-vlan associati on t runk

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 private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: 10
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk 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 }
```

**Syntax Description**

- **primary-vlan-id**: Number of the primary VLAN of the PVLAN relationship; valid values are from 1 to 4094.
- **secondary-vlan-list**: Number of the secondary VLAN of the private VLAN relationship; valid values are from 1 to 4094.

**Defaults**

Private VLAN mapping is disabled.

**Command Modes**

Interface configuration mode

**Usage Guidelines**

There is no runtime effect on the port unless it is in PVLAN host mode. If the port is in PVLAN host mode but all VLANs do not exist, the command is allowed, but the port is made inactive.

The secondary VLAN may be an isolated or community VLAN.

**Examples**

This example shows how to configure a port with a primary VLAN (VLAN 18) and secondary VLAN (VLAN 20):

```
Switch(config-if)# switchport private-vlan host-association 18 20
```

This example shows how to remove the PVLAN association from the port:

```
Switch(config-if)# no switchport private-vlan host-association
```

This 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# 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
```
switchport privat e-vlan host -associ ation

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show interfaces</td>
<td>Displays the administrative and operational status of a switching (nonrouting) port.</td>
</tr>
<tr>
<td>switchport mode</td>
<td>Enables the interface type.</td>
</tr>
</tbody>
</table>
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
```

### Syntax Description

- **primary-vlan-id**: Number of the primary VLAN of the private VLAN relationship; valid values are from 2 to 4094 (excluding 1002 to 1005).
- **secondary-vlan-list**: Number of the secondary VLANs to map to the primary VLAN; valid values are from 2 to 4094.
- **add**: Maps the secondary VLANs to the primary VLAN.
- **remove**: Clears mapping between the secondary VLANs and the primary VLAN.
- **trunk**: Maps the trunks secondary VLANs to the primary VLAN.

### Defaults
Private VLAN mapping is disabled.

### Command Modes
Interface configuration mode

### Usage Guidelines
There is no run-time effect on the port unless it is in private VLAN promiscuous mode. If the port is in private VLAN promiscuous mode but the VLANs do not exist, the command is allowed, but the port is made inactive.

The secondary VLAN may be an isolated or community VLAN.

### Examples

This 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)#
```

This example shows how to add a VLAN to the mapping:

```
Switch(config-if)# switchport private-vlan mapping 18 add 21
Switch(config-if)#
```
This 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)#
```

This 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)#
```

This example shows how to configure interface FastEthernet 5/2 as a PVLAN promiscuous port, map it to a PVLAN, and verify the configuration:

```
Switch#
configure terminal
Switch(config)#
interface fastethernet 5/2
Switch(config-if)#
switchport mode private-vlan promiscuous
Switch(config-if)#
switchport private-vlan mapping 200 2
Switch(config-if)#
end
Switch#
show interfaces fastethernet 5/2 switchport
Name: Fa5/2
Switchport: Enabled
Administrative Mode: private-vlan promiscuous
Operational Mode: private-vlan promiscuous
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative Private VLAN Host Association: none
Administrative Private VLAN 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
```

This example shows how to configure interface FastEthernet 5/2 as a promiscuous trunk port and to verify the configuration:

```
Switch#
configure terminal
Switch(config)#
interface fastethernet 5/2
Switch(config-if)#
switchport mode private-vlan trunk promiscuous
Switch(config-if)#
switchport private-vlan trunk native vlan 10
Switch(config-if)#
switchport private-vlan trunk allowed vlan 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
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

switchport private-vlan mapping

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... ] }
```

Syntax Description

- **Defaults**: All allowed normal VLANs are removed from a private VLAN trunk port.
- **Command Modes**: Interface configuration mode
- **Usage Guidelines**: By default, no normal VLANs are allowed unless you explicitly configure the VLANs to be allowed.

Use this command only for normal VLANs on a private VLAN trunk port.

Use the `switchport private-vlan association trunk` command to configure a port that can carry private VLANs on a private VLAN trunk port.

**Examples**

This example shows how to configure the private VLAN trunk port that carries normal VLANs 1 to 10:

```
Switch(config-if)# switchport private-vlan trunk allowed vlan 1-10
```

This example shows how to remove all the allowed normal VLANs from a private VLAN trunk port:

```
Switch(config-if)# no switchport private-vlan trunk allowed vlan
```

**VLAN List**

- **Sets the list of allowed VLANs**: See the "Usage Guidelines" section for formatting guidelines for `vlan_list`.
- **all**: Specifies all VLANs from 1 to 4094. This keyword is not supported on commands that do not permit all VLANs in the list to be set at the same time.
- **none**: Indicates an empty list. This keyword is not supported on commands that require certain VLANs to be set or at least one VLAN to be set.
- **add** *(Optional)*: Adds the defined list of VLANs to those currently set instead of replacing the list.
- **remove** *(Optional)*: Removes the defined list of VLANs from those currently set instead of replacing the list.
- **except** *(Optional)*: Lists the VLANs that should be calculated by inverting the defined list of VLANs.
- **vlan_atom**: Either a single VLAN number from 1 to 4094 or a continuous range of VLANs described by two VLAN numbers, the lesser one first, separated by a hyphen.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

This example shows how to configure interface FastEthernet 5/2 as a secondary trunk port, and verify the configuration:

Switch#
configure terminal
Switch(config)#
interface fastethernet 5/2
Switch(config-if)#
switchport mode private-vlan trunk secondary
Switch(config-if)#
switchport private-vlan trunk native vlan 10
Switch(config-if)#
switchport private-vlan trunk allowed vlan 10, 3-4
Switch(config-if)#
switchport private-vlan association trunk 3 301
Switch(config-if)#
end
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
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)#

This example shows how to configure interface FastEthernet 5/2 as a promiscuous trunk port and to verify the configuration:

Switch#
configure terminal
Switch(config)#
interface fastethernet 5/2
Switch(config-if)#
switchport mode private-vlan trunk promiscuous
Switch(config-if)#
switchport private-vlan trunk native vlan 10
Switch(config-if)#
switchport private-vlan trunk allowed vlan 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
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

switchport privat e-vlan trunk al lowed vl an
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.
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.

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

### Defaults
The default setting is global; the settings on the port are determined by the global setting.

### Command Modes
Interface configuration mode

### Usage Guidelines
The configuration created with this command only applies to ports that are configured as private VLAN trunks.

### Examples
This example shows how to enable 802.1Q native VLAN tagging on a PVLAN trunk:

```plaintext
Switch(config-if)#
switchport private-vlan trunk native vlan tag
Switch(config-if)#
```

### Related Commands
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show interfaces switchport</code></td>
<td>Displays the administrative and operational status of a switching (nonrouting) port.</td>
</tr>
<tr>
<td><code>switchport mode</code></td>
<td>Enables the interface type.</td>
</tr>
</tbody>
</table>
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**

- `switchport trunk native vlan`  
  - `tag` or `vlan_id`  
- `no switchport trunk native vlan`  
  - `tag` or `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`

**Defaults**

The default settings are as follows:
- IOS-XE only supports dot1Q.
- The access VLANs and trunk interface native VLANs are a default VLAN that corresponds to the platform or the interface hardware.
- All VLAN lists include all VLANs.
- Native VLAN tagging is enabled on the port if enabled globally.

**Command Modes**

- Interface configuration mode

**Usage Guidelines**

The `vlan_list` format is `all | none | [add | remove | except] vlan_atom [vlan_atom...]`, where:
- `all` specifies all VLANs from 1 to 4094. This keyword is not supported on commands that do not permit all VLANs in the list to be set at the same time.
- `none` indicates an empty list. This keyword is 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.

**native vlan**

- `tag`  
- `vlan_id`
  
**allowed vlan**

- `vlan_list`

**pruning vlan**

- `vlan_list`
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

switchport trunk

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 reenable 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**

This example shows how to cause a port interface that is configured as a switched interface to encapsulate in 802.1Q trunking format regardless of its default trunking format in trunking mode:

```
Switch(config-if)#
switchport trunk encapsulation dot1q
Switch(config-if)#
```

This example shows how to enable 802.1Q tagging on a port:

```
Switch(config-if)#
switchport trunk native vlan tag
Switch(config-if)#
```

This example shows how to configure a secure MAC-address and a maximum limit of secure MAC addresses on Gigabit Ethernet port 1 for all VLANs:

```
Switch(config)#
interface gigabitethernet1/1
Switch(config-if)#
switchport trunk encapsulation dot1q
Switch(config-if)#
switchport mode trunk
Switch(config-if)#
switchport port-security
Switch(config-if)#
switchport port-security maximum 3
```

This example shows how to configure a secure MAC-address on Gigabit Ethernet port 1 in a specific VLAN 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)#
switchport port-security maximum 3
```

This example shows how to configure a secure MAC-address in a VLAN on Gigabit Ethernet port 1:

```
Switch(config)#
interface gigabitethernet1/1
Switch(config-if)#
switchport trunk encapsulation dot1q
Switch(config-if)#
switchport mode trunk
Switch(config-if)#
switchport port-security
Switch(config-if)#
switchport port-security mac-address sticky
Switch(config-if)#
switchport port-security mac-address 1.1.1
Switch(config-if)#
switchport port-security mac-address sticky 1.1.2
Switch(config-if)#
switchport 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**

- `show interfaces switchport`: Displays the administrative and operational status of a switching (nonrouting) port.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

switch port  vlan mapping
switchport vlan mapping
Use the switchport vlan mapping command to configure VLAN mapping on a trunk port. You can configure one-to-one VLAN mapping, traditional IEEE 802.1Q tunneling (QinQ) mapping, or selective QinQ mapping. Use the no form of the command to disable the configuration.

switchport vlan mapping vlan-id {translated-id | dot1q tunnel translated-id}
no switchport vlan mapping vlan-id {translated-id | dot1q tunnel translated-id}
no switchport vlan mapping all

Syntax Description

Defaults
No VLAN mapping is configured.

Command Modes
Interface configuration

Usage Guidelines
Before configuring VLAN mapping on an interface, enter the switchport mode trunk interface configuration command to configure the interface as a trunk port.

You can configure VLAN mapping on a physical interface or on a port channel of multiple interfaces with the same configuration.

To configure one-to-one VLAN mapping, use the switchport vlan mapping vlan-id translated-id command.

Note To avoid mixing customer traffic, when you configure traditional QinQ on a trunk port, you should 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 QinQ on the same interface.

vlun-id Specifies the original (customer) VLAN or VLANs (C-VLANs), also known as the VLAN on the wire, for one-to-one or selective QinQ mapping. You can enter multiple VLAN IDs separated by a comma or a series of VLAN IDs separated by a hyphen (for example 1,2,3-5). The range is from 1 to 4094.

translated-id Specifies the translated VLAN-ID: the S-VLAN to be used in the service provider network. The range is from 1 to 4094.

dot1q-tunnel translated-id Adds a translated VLAN-ID to specify a VLAN tunnel (add an outer S-VLAN tag). The range of the S-VLAN tag is 1 to 4094. Use these keywords for traditional QinQ mapping.

all In the no switchport vlan mapping command, specifies that all VLAN mapping configurations on the interface are deleted.
Chapter 2      Cisco IOS Commands for  the Catalyst 4500 Series Switches

switchport vlan mapping

The no form of the switchport vlan mapping commands 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 SP AN destination port if the source port is configured as a tunnel port or has a 1-to-2 mapping configured. Encapsulation replicate is supported with 1-to-1 VLAN mapping.

Examples

This example shows how to use one-to-one mapping to map VLAN IDs 1 and 2 in the customer network to VLANs 1001 and 1002 in the service-provider network and to drop traffic from any other VLAN IDs.

Switch(config)#
interface gigabitethernet0/1
Switch(config-if)#
switchport vlan mapping 1 1001
Switch(config-if)#
switchport vlan mapping 2 1002
Switch(config-if)#
exit

This example shows how to configure selective QinQ mapping on the port so that traffic with a C-VLAN ID of 5, 7, or 8 would enter the switch with an S-VLAN ID of 100. The traffic of any 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

Related Commands
Command          Description
show vlan mapping Displays VLAN mapping information.
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.

**Syntax Description**

```plaintext
system mtu datagram-size
no system mtu
```

**Defaults**

The default MTU setting is 1500 bytes.

**Command Modes**

Global configuration mode

**Usage Guidelines**

The `datagram-size` parameter specifies the Ethernet payload size, not the total Ethernet frame size, and the Layer 3 MTU is changed as a result of changing the `system mtu` command.

For ports from 3 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.

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.

**Examples**

This example shows how to set the MTU size to 1550 bytes:

```plaintext
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# system mtu 1550
Switch(config)# end
Switch#
```

This example shows how to revert to the default MTU setting:

```plaintext
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# no system mtu
Switch(config)# end
Switch#
```

**Related Commands**

- `datagram-size`: Layer 2 payload size; valid values from 1500 to 1552 bytes.
- `show interfaces`: Displays traffic on a specific interface.
- `show system mtu`: Displays the global MTU setting.
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-number
}
```

**Note**
This command will be deprecated in future Cisco IOS releases. Use the `diagnostic start` command instead.

**Syntax Description**

- `interface interface-number`:
  - Interface type; valid values are `fastethernet` and `gigabitethernet`.
  - Module and port number.

**Defaults**
This command has no default settings.

**Command Modes**
Privileged EXEC mode

**Usage Guidelines**
The TDR test is supported on Catalyst 4500 series switches for the following line cards only:

- WS-X4548-GB-RJ45
- WS-X4548-GB-RJ45V
- WS-X4524-GB-RJ45V
- WS-X4013+TS
- WS-C4948
- WS-C4948-10GE

Do not start the test at the same time on both ends of the cable. Starting the test at both ends of the cable at the same time can lead to false test results.

Do not change the port configuration during any cable diagnostics test. This action may result in incorrect test results.

The interface must be operating before starting the TDR test. If the port is down, the results of the test will be invalid. Issue the `no shutdown` command on the port.

**Examples**

This example shows how to start the TDR test on port 1 on module 2:

```
Switch# test cable-diagnostics tdr int gi2/1
```

This example shows the message that displays when the TDR test is not supported on a module:

```
Switch# test cable-diagnostics tdr int gi2/1
00:03:15:%C4K_IOSDIAGMAN-4-TESTNOTSUPPORTEDONMODULE: Online cable interface Interface type; valid values are fastethernet and gigabitethernet.
```

Note: The command `interface number` used in the example is incorrect. It should be `interface interface-number` for the command to work properly.
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:
- `show cable-diagnostic tdr`: Displays the test results for the TDR cable diagnostics.
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**

- **Defaults**: This command has no default settings.
- **Command Modes**: Privileged EXEC mode
- **Usage Guidelines**:
  - Do not use leading zeros when entering a VLAN ID.
  - For Layer 2 traceroute to functional properly, Cisco Discovery Protocol (CDP) must be enabled on all of the switches in the network. Do not disable CDP.
  - When the switch detects a device in the Layer 2 path that does not support Layer 2 traceroute, the switch continues to send Layer 2 trace queries and lets them time out.
  - The maximum number of hops identified in the path is ten.
  - Layer 2 traceroute supports only unicast traffic. If you specify a multicast source or destination MAC address, the physical path is not identified, and a message appears.
  - The `traceroute mac` command output shows the Layer 2 path when the specified source and destination addresses belong to the same VLAN. If you specify source and destination addresses that belong to different VLANs, the Layer 2 path is not identified, and a message appears.
  - If the source or destination MAC address belongs to multiple VLANs, you must specify the VLAN to which both the source and destination MAC addresses belong. If the VLAN is not specified, the path is not identified, and a message appears.
  - Layer 2 traceroute is not supported when multiple devices are attached to one port through hubs (for example, multiple CDP neighbors are detected on a port). When 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.

- **interface interface-id** (Optional) Specifies the source or destination switch interface.
- **source-mac-address** MAC address of the source switch in hexadecimal format.
- **destination-mac-address** MAC address of the destination switch in hexadecimal format.
- **vlan vlan-id** (Optional) Specifies the VLAN on which to trace the Layer 2 path that the packets take from the source switch to the destination switch; valid VLAN IDs are from 1 to 4094. Do not enter leading zeros.
- **detail** (Optional) Displays detail information.
Examples

This example shows how to display the Layer 2 path by specifying the source and destination MAC addresses:

```
Switch# traceroute mac 0000.0201.0601 0000.0201.0201
Source 0000.0201.0601 found on con6[WS-C2950G-24-EI] (2.2.6.6)
con6 (2.2.6.6) :Fa0/1 =>Fa0/3
con5                 (2.2.5.5        )  :    Fa0/3 =>Gi0/1
con1                 (2.2.1.1        )  :    Gi0/1 =>Gi0/2
con2                 (2.2.2.2        )  :    Gi0/2 =>Fa0/1
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed
Switch#```

This example shows how to display the detailed Layer 2 path:

```
Switch# traceroute mac 0000.0201.0601 0000.0201.0201 detail
Source 0000.0201.0601 found on con6[WS-C2950G-24-EI] (2.2.6.6)
con6 / WS-C2950G-24-EI / 2.2.6.6 :
    Fa0/1 [auto, auto] =>Fa0/3 [auto, auto]
con5 / WS-C2950G-24-EI / 2.2.5.5 :
    Fa0/3 [auto, auto] =>Gi0/1 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
    Gi0/1 [auto, auto] =>Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
    Gi0/2 [auto, auto] =>Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
Switch#```

This example shows the Layer 2 path when the switch is not connected to the source switch:

```
Switch# traceroute mac 0000.0201.0501 0000.0201.0201 detail
Source not directly connected, tracing source ......
Source 0000.0201.0501 found on con5[WS-C2950G-24-EI] (2.2.5.5)
con5 / WS-C2950G-24-EI / 2.2.5.5 :
    Fa0/1 [auto, auto] =>Gi0/1 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
    Gi0/1 [auto, auto] =>Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
    Gi0/2 [auto, auto] =>Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
Switch#```

This example shows the Layer 2 path when the switch cannot find the destination port for the source MAC address:

```
Switch# traceroute mac 0000.0011.1111 0000.0201.0201
Error:Source Mac address not found.
Layer2 trace aborted.
Switch#```

This example shows the Layer 2 path when the source and destination devices are in different VLANs:

```
Switch# traceroute mac 0000.0201.0601 0000.0301.0201
Error:Source and destination macs are on different vlans.
Layer2 trace aborted.
Switch#```

This example shows the Layer 2 path when the destination MAC address is a multicast address:

```
Switch# traceroute mac 0000.0201.0601 0100.0201.0201
Invalid destination mac address
Switch#```
This example shows the Layer 2 path when the source and destination switches belong to multiple VLANs:

```
Switch# traceroute mac 0000.0201.0601 0000.0201.0201
Error: Mac found on multiple vlans.
Layer2 trace aborted.
Switch#
```

This example shows how to display the Layer 2 path by specifying the interfaces on the source and destination switches:

```
Switch# traceroute mac interface fastethernet0/1 0000.0201.0601 interface fastethernet0/3 0000.0201.0201
Source 0000.0201.0601 found on 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#
```
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

trace route  mac  i p

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 `trace route  mac` command.

```
trace route  mac  ip
```

### Syntax Description

- **source-ip-address**
  - IP address of the source switch as a 32-bit quantity in dotted-decimal format.
- **source-hostname**
  - IP hostname of the source switch.
- **destination-ip-address**
  - IP address of the destination switch as a 32-bit quantity in dotted-decimal format.
- **destination-hostname**
  - IP hostname of the destination switch.
- **detail**
  - (Optional) Displays detailed traceroute MAC IP information.

### Defaults

This command has no default settings.

### Command Modes

- Privileged EXEC mode

### Usage Guidelines

For Layer 2 traceroute to function properly, Cisco Discovery Protocol (CDP) must be enabled on all the switches in the network. Do not disable CDP.

When the switch detects a device in the Layer 2 path that does not support Layer 2 traceroute, the switch continues to send Layer 2 trace queries and lets them time out.

The maximum number of hops identified in the path is ten.

The `trace route  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

This example shows how to display the Layer 2 path by specifying the source and destination IP addresses and by using the `detail` keyword:
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

traceroute mac ip
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#

This example shows how to display the Layer 2 path by specifying the source and destination hostnames:
Switch#
traceroute
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#

This example shows the Layer 2 path when Address Resolution Protocol (ARP) cannot associate the source IP address with the corresponding MAC address:
Switch#
traceroute mac ip 2.2.66.66 2.2.77.77
Arp failed for destination 2.2.77.77.
Layer2 trace aborted.
Switch#
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

trust

To define a trust state for traffic classified through the class 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

- **Defaults**: The action is not trusted.
- **Command Modes**: Policy-map class configuration
- **Usage Guidelines**: Use this command to distinguish the quality of service (QoS) trust behavior for certain traffic from other traffic. For example, inbound traffic with certain DSCP values can be trusted. You can configure a class map to match and trust the DSCP values in the inbound traffic.

Trust values set with this command supersede trust values set with the qos trust interface configuration command.

- If you specify **trust cos**, QoS uses the received or default port CoS value and the CoS-to-DSCP map to generate a DSCP value for the packet.
- If you specify **trust dscp**, QoS uses the DSCP value from the ingress packet. For non-IP packets that are tagged, QoS uses the received CoS value; for non-IP packets that are untagged, QoS uses the default port CoS value. In either case, the DSCP value for the packet is derived from the CoS-to-DSCP map.

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

**Examples**

This example shows how to define a port trust state to trust inbound DSCP values for traffic classified with "class1":

```
Switch# 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#
```

- **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.
trust

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

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>class</td>
<td>Specifies the name of the class whose traffic policy you want to create or change.</td>
</tr>
<tr>
<td>police</td>
<td>Configures the Traffic Policing feature.</td>
</tr>
<tr>
<td>policy-map</td>
<td>Creates a policy map that can be attached to multiple ports to specify a service policy and to enter policy-map configuration mode.</td>
</tr>
<tr>
<td>set</td>
<td>Marks IP traffic by setting a class of service (CoS), a Differentiated Services Code Point (DSCP), or IP-precedence in the packet.</td>
</tr>
<tr>
<td>show policy-map</td>
<td>Displays information about the policy map.</td>
</tr>
</tbody>
</table>
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 })
```

**Defaults**

- Encapsulation type is dependent on the platform or interface hardware.
- QoS enabled bandwidth rate is 4:255.
- QoS disabled bandwidth rate is 255:1.

**Command Modes**

Interface configuration mode

**Usage Guidelines**

- The bandwidth and shape rates cannot exceed the maximum speed of the interface.
- The bandwidth can be configured only on the following:
  - Ports on the WS-X4306-GB module
  - The two 1000BASE-X ports on the WS-X4232-GB-RJ module
  - The first two ports on the WS-X4418-GB module
  - The two 1000BASE-X ports on the WS-X4412-2GB-TX module
- Only transmit queue 3 can be configured to be a high-priority transmit queue.

**Examples**

- This example shows how to allocate bandwidth on queue 1 to 100 Mbps:
  ```
  Switch(config-if)#
  tx-queue 1
  Switch(config-if-tx-queue)#
  bandwidth 1000000000
  Switch(config-if-tx-queue)#
  ```
- This 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
  ```
This example shows how to configure the traffic shaping rate of 64 kbps to transmit queue 1:

```
Switch(config-if)#
tx-queue 1
Switch(config-if-tx-queue)#
shape 64000
Switch(config-if-tx-queue)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show qos interface</code></td>
<td>Displays queueing information.</td>
</tr>
</tbody>
</table>
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
udld aggressive
udld message time message-timer-time
udld fast-hello error-reporting
```

**Syntax Description**

**Defaults**

All fiber-optic interfaces are disabled and the message timer for UDLD is set to 15 seconds.

Fast UDLD is disabled on all interfaces.

**Command Modes**

Global configuration

`enable`

Enables UDLD in normal mode by default on all the fiber-optic interfaces.

`aggressive`

Enables UDLD in aggressive mode by default on all the fiber-optic interfaces.

`message time message-timer-time`

Sets the period of time between the UDLD probe messages on the ports that are in advertisement mode and are currently determined to be bidirectional; valid values are from 1 to 90 seconds.

If Fast UDLD is enabled and a link failure is detected, reports the link failure through a log message instead of errdisabling the port.
udld (global configuration mode)

Usage Guidelines
If you enable aggressive mode, once all the switch port's neighbors have aged out either in the advertisement or in the detection phase, UDLD and Fast UDLD restart the linkup sequence. They can resynchronize with any potentially out-of-sync neighbor and shut down the port if the UDLD messages from the neighbor indicate that the link state is still undetermined.

This command affects fiber interfaces only. Use the udld (interface configuration mode) command to enable UDLD on other interface types.

Examples
This example shows how to enable UDLD on all the fiber interfaces:

Switch (config)# udld enable
Switch (config)##

Related Commands
<table>
<thead>
<tr>
<th>Command Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show udld</td>
</tr>
<tr>
<td>udld (interface configuration mode)</td>
</tr>
</tbody>
</table>
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
no udld fast-hello
```

**Syntax Description**

- **Defaults**
  - 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

**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.
udld (interface configuration mode)

Examples

This 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)#

This 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)#

This 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)#

This example shows how to enable Fast UDLD on a port interface with a timer value of 200 ms. To enable Fast UDLD on a port, you must first enable UDLD in normal or aggressive mode:

Switch (config-if)#
udld port
Switch (config-if)#
udld fast-hello 200
Switch (config-if)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show udld</td>
<td>Displays the administrative and operational UDLD and Fast UDLD status.</td>
</tr>
<tr>
<td>udld (global configuration mode)</td>
<td>Enables aggressive or normal mode in the UDLD protocol and sets the configurable message timer time.</td>
</tr>
</tbody>
</table>
To reset all the UDLD ports in the shut down state (that is, errdisabled by UDLD), use the `udld reset` privileged EXEC command.

### Syntax Description

This command has no arguments or keywords.

### Defaults

This command has no default settings.

### Command Modes

Privileged EXEC

### Usage Guidelines

If the interface configuration is still enabled for UDLD, those ports will begin to run UDLD again and may shut down if the reason for the shut down 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

This example shows how to reset all the ports that are shut down by UDLD:

```
Switch# udld reset
Switch# 
```
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 unidirectional` command.

```
unidirectional {receive-only | send-only}
no unidirectional {receive-only | send-only}
```

**Syntax Description**

- `receive-only`: Specifies the unidirectional reception.
- `send-only`: Specifies the unidirectional transmission.

**Defaults**

Disabled

**Command Modes**

Interface configuration mode

**Usage Guidelines**

Enabling port unidirectional mode automatically disables port UDLD. You must manually ensure that the unidirectional link does not create a spanning-tree loop in the network.

**Examples**

This example shows how to set Gigabit Ethernet interface 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**

- `receive-only`: Specifies the unidirectional reception.
- `send-only`: Specifies the unidirectional transmission.

**Command Description**

- `show interfaces switchport`: Displays the administrative and operational status of a switching (nonrouting) port.
To establish a username-based authentication system, use the `username` command.

```
username name secret {0 | 5} password
```

**Syntax Description**

- **name**: User ID of the user.
- **secret**: 0 | 5 Specifies the authentication system for the user; valid values are 0 (text immediately following is not encrypted) and 5 (text immediately following is encrypted using an MD5-type encryption method).
- **password**: Password of the user.

**Defaults**

No username-based authentication system is established.

**Command Modes**

Global configuration mode

**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**

This example shows how to specify an MD5 encryption on a password (warrior) for a username (xena):

```
Switch(config)# username xena secret 5 warrior
```

**Related Commands**

- `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.
To verify the checksum of a file on a flash memory file system, use the `verify` command.

```
[md5] [flash-filesystem:] [filename] [expected-md5-signature]
```

**Syntax Description**

- `/md5` (Optional) Verifies the MD5 signatures.
- `flash-filesystem:` (Optional) Device where the flash resides; valid values are `bootflash:`, `slot0:`, `flash:`, or `sup-bootflash:`.
- `filename` (Optional) Name of the Cisco IOS image.
- `expected-md5-signature` (Optional) MD5 signature.

**Defaults**

The current working device is specified.

**Command Modes**

Privileged EXEC mode

**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

This example shows how to use the `verify` command:
```
Switch# verify cat6k_r47_1.cbi
..........................................................
File cat6k_r47_1.cbi verified OK.
Switch#
```

This example shows how to manually verify the MD5 signature:
```
Switch# verify /md5 c4-jsv-mz
.................................................
.................................................
.................................................
.................................................
.................................................
............................................Done!
```

```
verify /md5 (slot0:c4-jsv-mz) = 0f369ed9e98756f179d4f29d6e7755d3
```

This 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show file system (Flash file system)</td>
<td>Displays available file systems.</td>
</tr>
<tr>
<td>show flash</td>
<td>Displays the contents of flash memory.</td>
</tr>
</tbody>
</table>
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] [tb-vlan1 tb-vlan1-id] [tb-vlan2 tb-vlan2-id]
```

**Syntax Description**

- `vlan_id`: Number of the VLAN; valid values are from 1 to 4094.
- `are hops`: (Optional) Specifies the maximum number of All Route Explorer hops for this VLAN; valid values are from 0 to 13. Zero is assumed if no value is specified.
- `backupcrf mode`: (Optional) Enables or disables the backup CRF mode of the VLAN; valid values are `enable` and `disable`.
- `bridge type`: (Optional) Specifies the bridging characteristics of the VLAN or identification number of the bridge; valid `type` values are `srb` and `srt`.
- `bridge_num`: (Optional) Valid bridge_num values are from 0 to 15.
- `media type`: (Optional) Specifies the media type of the VLAN; valid values are `fast ethernet`, `fd-net`, `fddi`, `trcrf`, and `trbrf`.
- `mtu mtu-size`: (Optional) Specifies the maximum transmission unit (packet size, in bytes) that the VLAN can use; valid values are from 576 to 18190.
- `name vlan-name`: (Optional) Defines a text string used as the name of the VLAN (1 to 32 characters).
- `parent parent-vlan-id`: (Optional) Specifies the ID number of the parent VLAN of FDDI or Token Ring-type VLANs; valid values are from 2 to 1001.
- `ring ring-number`: (Optional) Specifies the ring number of FDDI or Token Ring-type VLANs; valid values are from 2 to 1001.
- `said said-value`: (Optional) Specifies the security association identifier; valid values are from 1 to 4294967294.
- `state`: (Optional) Specifies the state of the VLAN.
  - `suspend`: Specifies that the state of the VLAN is suspended. VLANs in the suspended state do not pass packets.
  - `active`: Specifies that the state of the VLAN is active.
- `stp type`: (Optional) Specifies the STP type; valid values are `ieee`, `ibm`, and `auto`.
- `tb-vlan1 tb-vlan1-id`: (Optional) Specifies the ID number of the first translational VLAN for this VLAN; valid values are from 2 to 1001. Zero is assumed if no value is specified.
- `tb-vlan2 tb-vlan2-id`: (Optional) Specifies the ID number of the second translational VLAN for this VLAN; valid values are from 2 to 1001. Zero is assumed if no value is specified.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

vlan (VLAN Database mode)

Defaults
The defaults are as follows:

- The vlan-name is “VLANxxxx” where “xxxx” represents four numeric digits (including leading zeroes) equal to the VLAN ID number.
- The media type is Fast Ethernet.
- The state is active.
- The said-value is 100,000 plus the VLAN ID number.
- The mtu-size default is dependent upon the VLAN type:
  - 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

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
This example shows how to add a new VLAN with all the default parameters to the new VLAN database:

Switch(vlan)#
vlan 2
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

Vlan (VLAN Database mode)

Note
If the VLAN already exists, no action occurs.

This example shows how to cause the device to add a new VLAN, specify the media type and parent VLAN ID number 3, and set all the other parameters to the defaults:

```
Switch(vlan)# vlan 2 media fastethernet parent 3
VLAN 2 modified:
Media type FASTETHERNET
Parent VLAN 3
```

This example shows how to delete VLAN 2:

```
Switch(vlan)# no vlan 2
```

This example shows how to return the MTU to the default for its type and the translational bridging VLANs to the default:

```
Switch(vlan)# no vlan 2 mtu tb-vlan1 tb-vlan2
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show vlan</td>
<td>Displays VLAN information.</td>
</tr>
</tbody>
</table>
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#]
```

### Syntax Description

- **Defaults**: This command has no default settings.

### Command Modes

- **Global configuration mode**

### 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

This example shows how to enter VLAN access-map mode:

```
Switch(config)##
vlan access-map cisco
Switch(config-access-map)#
```

### Related Commands

- **name**: VLAN access-map tag.
- **seq#**: (Optional) Map sequence number; valid values are from 0 to 65535.
- **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.
To configure a service-policy on a VLAN, use the `vlan configuration` command to enter the VLAN feature configuration mode.

```
vlan configuration
```

**Syntax Description**

This command has no default settings.

**Defaults**

This command has no default settings.

**Command Modes**

Global configuration mode

**Usage Guidelines**

Even though an SVI is not needed in all cases, such as when you use your Catalyst 4500 series switch as a pure Layer 2 switch, you are required to create an SVI. VLAN configuration mode has 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**

This example shows how to configure a service policy while in VLAN configuration mode and display the new service policy:

```
Switch# configure terminal
Switch(config)# vlan configuration 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#
```

This example shows how to display the new service policy:

```
Switch# show policy-map vlan 30
vlan 30
Service-policy input: p1
Class-map: class-default (match-any)
0 packets
Match: any
```
vlan configuration

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.
To enter VLAN configuration mode, use the `vlan database` command.

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

This command has no default settings.

**Command Modes**

Privileged EXEC mode

**Usage Guidelines**

From VLAN configuration mode, you can access the VLAN database editing buffer manipulation commands, including:

- `ab` or `t` — Exits mode without applying the changes.
- `apply` — Applies the current changes and bumps the revision number.
- `exit` — Applies the changes, bumps the revision number, and exits VLAN configuration mode.
- `no` — Negates a command or sets its defaults; valid values are `vlan` and `vtp`.
- `reset` — Abandons the current changes and rereads the current database.
- `show` — Displays the database information.
- `vlan` — Accesses the subcommands to add, delete, or modify values that are associated with a single VLAN. For information about the `vlan` subcommands, see the `vlan (VLAN Database mode)` command.
- `vtp` — Accesses the subcommands to perform VTP administrative functions. For information about the `vtp` subcommands, see the `vtp client` command.

**Examples**

This example shows how to enter VLAN configuration mode:

```
Switch# vlan database
```

```
Switch(vlan)#
```

This example shows how to exit VLAN configuration mode without applying changes after you are in VLAN configuration mode:

```
Switch(vlan)# abort
```

```
Aborting....
Switch#
```

This example shows how to delete a VLAN after you are in VLAN configuration mode:

```
Switch(vlan)# no vlan 100
```

```
Deleting VLAN 100...
Switch(vlan)#
```
This example shows how to turn off pruning after you are in VLAN configuration mode:

Switch(vlan)#
no vtp pruning
Pruning switched OFF
Switch(vlan)#

Related Commands

Command Description
show vlan
Displays VLAN information.
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.

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

802.1Q native VLAN tagging is disabled.

**Command Modes**

Global configuration mode

**Usage Guidelines**

When enabled, the native VLAN packets exiting all 802.1Q trunk ports are tagged unless the port is explicitly configured to disable native VLAN tagging.

When disabled, the native VLAN packets exiting all 802.1Q trunk ports are not tagged.

You can use this command with 802.1Q tunneling. This feature operates on an edge switch of a service-provider network and expands VLAN space by using a VLAN-in-VLAN hierarchy and by tagging the tagged packets. You must use the 802.1Q trunk ports for sending out the packets to the service-provider network. However, the packets going through the core of the service-provider network might also be carried on the 802.1Q trunks. If the native VLANs of an 802.1Q trunk match the native VLAN of a tunneling port on the same switch, the traffic on the native VLAN is not tagged on the sending trunk port. This command ensures that the native VLAN packets on all 802.1Q trunk ports are tagged.

**Examples**

This example shows how to enable 802.1Q tagging on the native VLAN frames and verify the configuration:

```
Switch# config terminal
Switch (config)# vlan dot1q tag native
Switch (config)# end
Switch# show vlan dot1q tag native
dot1q native vlan tagging is enabled
```

**Related Commands**

- `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.
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**

This command has no default settings.

**Defaults**

This command has no default settings.

**Command Modes**

Global configuration mode

**Usage Guidelines**

When configuring an action clause in a VLAN access map, note the following:

- You can apply the VLAN access map to one or more VLANs.
- The `vlan-list` parameter can be a single VLAN ID, a list of VLAN IDs, or VLAN ID ranges (`vlan-id - vlan-id`). Multiple entries are separated by (-), (hyphen), or (,) (comma).
- You can apply only one VLAN access map to each VLAN.
- When entering the `no` form of this command, the `vlan-list` parameter is optional (but the keyword `vlan-list` is required). If you do not enter the `vlan-list` parameter, the VACL is removed from all the VLANs where the `map-name` is applied.

**Examples**

This example shows how to apply a VLAN access map on VLANs 7 through 9:

```
Switch(config)#
vlan filter ganymede vlan-list 7-9
```
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

no vlan group
  group-name
  vlan-list
```

**Syntax Description**

- **Defaults**: This command has no arguments or keywords.
- **Command Modes**: Global configuration

**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 (e.g., `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**

- This 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
  ```

- This example shows how to remove VLAN 7 from the VLAN group:
  ```
  Switch(config)# no vlan group ganymede vlan-list 7
  ```

**Related Commands**

- `group-name`: Specifies the VLAN group name.
- `vlan-list`: Specifies a VLAN list name. See the Usage Guidelines section below for additional information about this argument.
- `Command Description`:
  - `show vlan group`: Displays the VLANs mapped to VLAN groups.
To configure the internal VLAN allocation scheme, use the \texttt{vlan internal allocation policy} command. To return to the default setting, use the \texttt{no} form of this command.

\texttt{vlan internal allocation policy} \{\texttt{ascending} | \texttt{descending}\}

\texttt{no vlan internal allocation policy}

\textbf{Syntax Description}

\textbf{Defaults}

The default is the ascending allocation scheme.

\textbf{Command Modes}

Global configuration mode

\textbf{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 \texttt{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 \texttt{write mem} command and the system reloads, the reconfigured allocation scheme is used by the port manager.

\textbf{Examples}

This example shows how to configure the VLANs in a descending order as the internal VLAN allocation policy:

\begin{verbatim}
Switch(config)\# vlan internal allocation policy descending
Switch(config)\#
\end{verbatim}

\textbf{Related Commands}

- \texttt{ascending} Specifies to allocate internal VLANs from 1006 to 4094.
- \texttt{descending} Specifies to allocate internal VLANs from 4094 to 1006.

\textbf{Command Description}

- \texttt{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

Syntax Description

- `interval`: Queries to the VLAN Membership Policy Server (VMPS) to reconfirm dynamic VLAN assignments; valid values are from 1 to 120 minutes.

Defaults

The reconfirmation interval is 60 minutes.

Command Modes

- Global configuration mode

Examples

This example shows how to set the VQP client to reconfirm dynamic VLAN entries every 20 minutes:

```
Switch(config) # vmps reconfirm 20
```

You can verify your setting by entering the `show vmps` command and examining information in the `Reconfirm Interval` row.

Related Commands

- `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).
To immediately send VLAN Query Protocol (VQP) queries to reconfirm all the dynamic VLAN assignments with the VLAN Membership Policy Server (VMPS), use the `vmps reconfirm` command.

```plaintext
vmps reconfirm
```

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

**Defaults**
This command has no default settings.

**Command Modes**
Privileged EXEC mode

**Usage Guidelines**
You can verify your setting by entering the `show vmps` command and examining the VMPS Action row of the Reconfirmation Status section. The `show vmps` command shows the result of the last time that the assignments were reconfirmed either because the reconfirmation timer expired or because the `vmps reconfirm` command was entered.

**Examples**
This example shows how to immediately send VQP queries to the VMPS:
```
Switch# vmps reconfirm
Switch# 
```

**Related Commands**
- `show vmps` - Displays the VLAN Query Protocol (VQP) version, reconfirmation interval, retry count, VLAN Membership Policy Server (VMPS) IP addresses, current servers, and primary servers.
- `vmps reconfirm (global configuration)` - Changes the reconfirmation interval for the VLAN Query Protocol (VQP) client.
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
```

**Syntax Description**

- **count**
  - Number of attempts to contact the VLAN Membership Policy Server (VMPS) by the client before querying the next server in the list; valid values are from 1 to 10.

**Defaults**

- The retry count is 3.

**Command Modes**

- Global configuration mode

**Usage Guidelines**

You can verify your setting by entering the `show vmps` command and examining information in the `Server Retry Count` row.

**Examples**

This example shows how to set the retry count to 7:

```
Switch(config) #
vmps retry 7
```

**Related Commands**

- `count` Command Description
  - Displays the VLAN Query Protocol (VQP) version, reconfirmation interval, retry count, VLAN Membership Policy Server (VMPS) IP addresses, current servers, and primary servers.
To configure the primary VLAN Membership Policy Server (VMPS) and up to three secondary servers, use the `vmps server` command. To remove a VMPS server, use the `no` form of this command.

```
vmps server ipaddress [primary]
```

**Syntax Description**

- `ipaddress`: 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.

**Defaults**

No primary or secondary VMPS servers are defined.

**Command Modes**

Global configuration mode

**Usage Guidelines**

The first server that you entered is automatically selected as the primary server whether or not `primary` is entered. You can override the first server address by using `primary` in a subsequent command.

If a member switch in a cluster configuration does not have an IP address, the cluster does not use the VMPS server that is configured for that member switch. Instead, the cluster uses the VMPS server on the command switch, and the command switch proxies the VMPS requests. The VMPS server treats the cluster as a single switch and uses the IP address of the command switch to respond to requests.

When using the `no` form without specifying the `ipaddress`, all configured servers are deleted. If you delete all servers when dynamic-access ports are present, the switch cannot forward the packets from the new sources on these ports because it cannot query the VMPS.

You can verify your setting by entering the `show vmps` command and examining information in the VMPS Domain Server row.

**Examples**

This example shows how to configure the server with IP address 191.10.49.20 as the primary VMPS server. The servers with IP addresses 191.10.49.21 and 191.10.49.22 are configured as secondary servers:

```
Switch(config) #
vmps server 191.10.49.20 primary
Switch(config) #
vmps server 191.10.49.21
Switch(config) #
vmps server 191.10.49.22
```

This example shows how to delete the server with IP address 191.10.49.21:

```
Switch(config) #
no vmps server 191.10.49.21
Switch(config) #
```
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

vmps server

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.
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}}
```

**Syntax Description**

- **Defaults**: Disabled
- **Command Modes**: Global configuration mode

**Usage Guidelines**

You cannot use the `vtp file` command to load a new database. You can use it only to rename the file in which the existing database is stored.

You can use the `vtp if-id` command to specify the name of the interface providing the VTP updater ID for this device. The VTP updater is the device that adds, deletes, or modifies VLANs to a network, and triggers a VTP updater to inform the rest of the system of the changes.

**Examples**

This example shows how to specify the IFS file system file where VTP configuration is stored:

```
Switch(config)#
vtp file vtpconfig
```

Setting device to store VLAN database at filename vtpconfig.

```
Switch(config)#
```

This example shows how to specify the name of the interface providing the VTP updater ID:

```
Switch(config)#
vtp if-id fastethernet
```

Related Commands

- `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 Description**

- `show vtp`: Displays VTP statistics and domain information.
To place a device in VTP client mode, use the `vtp client` command. To return to VTP server mode, use the `no vtp client` command.

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

Disabled

**Command Modes**

VLAN configuration mode

**Usage Guidelines**

If the receiving switch is in client mode, the client switch changes its configuration to duplicate the configuration of the server. If you have switches in client mode, make sure to make all VTP or VLAN configuration changes on a switch in server mode.

The `vtp server` command is the functional equivalent of `no vtp client` except that it does not return an error if the device is not in client mode.

**Examples**

This example shows how to place the device in VTP client mode:

```
Switch(vlan-config)# vtp client
Switch(vlan-config)#
```
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

vtp domain

to configure the administrative domain name for a device, use the vtp domain command.

Syntax Description

vtp domain domain-name

This command has no default settings.

Defaults

Command Modes

VLAN configuration mode

Usage Guidelines

When you define the domain-name, the domain name is case sensitive and can be from 1 to 32 characters. You must set a domain name before you can transmit any VTP advertisements. Even if you do not set a domain name, the device will leave the no-management-domain state upon receiving the first VTP summary packet on any port that is currently trunking. If the device receives its domain from a summary packet, it resets its configuration revision number to zero. Once the device leaves the no-management-domain state, it can never be configured to reenter the number except by cleaning NVRAM and reloading.

Examples

This example shows how to set the device's administrative domain:

Switch(vlan-config)# vtp domain DomainChandon
Switch(vlan-config)#

Related Commands

domain-name

Name of the domain.

Command Description

show vtp

Displays VTP statistics and domain information.

vtp (global configuration mode)

Configures the name of a VTP configuration storage file.
To create a VTP domain password, use the `vtp password` command. To delete the password, use the `no vtp password` command.

**Syntax Description**

**password-value**

An ASCII string, from 1 to 32 characters, identifying the administrative domain for the device.

**Command Modes**

VLAN configuration mode

**Examples**

This example shows how to create a VTP domain password:

```
Switch(vlan-config)# vtp password DomainChandon
```

This example shows how to delete the VTP domain password:

```
Switch(vlan-config)# no vtp password
```

Clearing device VLAN database password.

**Related Commands**

- `show vtp`
  - Displays VTP statistics and domain information.
- `vtp (global configuration mode)`
  - Configures the name of a VTP configuration storage file.
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

vtp pruning

To enable pruning in the VLAN database, use the **vtp pruning** command. To disable pruning in the VLAN database, use the **no** form of this command.

vtp pruning
no vtp pruning

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

Disabled

**Command Modes**

VLAN configuration mode

**Usage Guidelines**

VTP pruning causes information about each pruning-eligible VLAN to be removed from VTP updates if there are no stations belonging to that VLAN.

**Examples**

This example shows how to enable pruning in the VLAN database:

```
Switch(vlan-config)# vtp pruning
Pruning switched ON
Switch(vlan-config)#
```

This example shows how to disable pruning in the VLAN database:

```
Switch(vlan-config)# no vtp pruning
Pruning switched OFF
Switch(vlan-config)#
```

**Related Commands**

<table>
<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>
</tbody>
</table>
To place the device in VTP server mode, use the `vtp server` command.

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

Enabled

**Command Modes**

VLAN configuration mode

**Usage Guidelines**

If you make a change to the VTP or VLAN configuration on a switch in server mode, that change is propagated to all the switches in the same VTP domain.

You can set VTP to either server or client mode only when you disable dynamic VLAN creation.

If the receiving switch is in server mode, the configuration is not changed.

The `vtp server` command is the functional equivalent of `no vtp client`, except that it does not return an error if the device is not in client mode.

**Examples**

This example shows how to place the device in VTP server mode:

```
Switch(vlan-config)#
vtp server
Switch(vlan-config)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show vtp</code></td>
<td>Displays VTP statistics and domain information.</td>
</tr>
<tr>
<td><code>vtp (global configuration mode)</code></td>
<td>Configures the name of a VTP configuration storage file.</td>
</tr>
</tbody>
</table>
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
```

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

Disabled

**Command Modes**

VLAN configuration mode

**Usage Guidelines**

The `vtp transparent` command disables VTP from the domain but does not remove the domain from the switch. If the receiving switch is in transparent mode, the configuration is not changed. The switches in transparent mode do not participate in VTP. If you make VTP or VLAN configuration changes on a switch in transparent mode, the changes are not propagated to the other switches in the network.

The `vtp server` command is similar to the `no vtp transparent` command, except that it does not return an error if the device is not in transparent mode.

**Examples**

This example shows how to place the device in VTP transparent mode:

```
Switch(vlan-config)# vtp transparent
```

This example shows how to return the device to VTP server mode:

```
Switch(vlan-config)# no vtp transparent
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show vtp</code></td>
<td>Displays VTP statistics and domain information.</td>
</tr>
<tr>
<td><code>vtp (global configuration mode)</code></td>
<td>Configures the name of a VTP configuration storage file.</td>
</tr>
</tbody>
</table>
Chapter 2      Cisco IOS Commands for the Catalyst 4500 Series Switches

vtp v2-mode

To enable version 2 mode, use the `vtp v2-mode` command. To disable version 2 mode, use the `no vtp v2-mode` command.

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

VLAN configuration mode

Usage Guidelines

All switches in a VTP domain must run the same version of VTP. VTP version 1 and VTP version 2 do not operate on switches in the same VTP domain.

If all switches in a domain are VTP version 2-capable, you only need to enable VTP version 2 on one switch; the version number is then propagated to the other version 2-capable switches in the VTP domain.

If you toggle the version 2 mode, the parameters of certain default VLANs will be modified.

Examples

This example shows how to enable version 2 mode in the VLAN database:

```
Switch(vlan-config)# vtp v2-mode
Switch(vlan-config)#
```

This example shows how to disable version 2 mode in the VLAN database:

```
Switch(vlan-config)# no vtp v2-mode
Switch(vlan-config)#
```

Related Commands

<table>
<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>
## 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
Appendix A: Abbreviations

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
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEC</td>
<td>Digital Equipment Corporation</td>
</tr>
<tr>
<td>DFI</td>
<td>Domain-Specific Part Format Identifier</td>
</tr>
<tr>
<td>DFP</td>
<td>Dynamic Feedback Protocol</td>
</tr>
<tr>
<td>DISL</td>
<td>Dynamic Inter-Switch Link</td>
</tr>
<tr>
<td>DLC</td>
<td>Data Link Control</td>
</tr>
<tr>
<td>DLSw</td>
<td>Data Link Switching</td>
</tr>
<tr>
<td>DMP</td>
<td>data movement processor</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>DoD</td>
<td>Department of Defense</td>
</tr>
<tr>
<td>DOS</td>
<td>denial of service</td>
</tr>
<tr>
<td>DRAM</td>
<td>dynamic RAM</td>
</tr>
<tr>
<td>DRiP</td>
<td>Dual Ring Protocol</td>
</tr>
<tr>
<td>DSAP</td>
<td>destination service access point</td>
</tr>
<tr>
<td>DSCP</td>
<td>differentiated services code point</td>
</tr>
<tr>
<td>DSPU</td>
<td>downstream SNA Physical Units</td>
</tr>
<tr>
<td>DTP</td>
<td>Dynamic Trunking Protocol</td>
</tr>
<tr>
<td>DTR</td>
<td>data terminal ready</td>
</tr>
<tr>
<td>DVMRP</td>
<td>Distance Vector Multicast Routing Protocol</td>
</tr>
<tr>
<td>DXI</td>
<td>data exchange interface</td>
</tr>
<tr>
<td>E</td>
<td>Extensible Authentication Protocol</td>
</tr>
<tr>
<td>EARL</td>
<td>Enhanced Address Recognition Logic</td>
</tr>
<tr>
<td>EEPROM</td>
<td>electrically erasable programmable read-only memory</td>
</tr>
<tr>
<td>EHSA</td>
<td>enhanced high system availability</td>
</tr>
</tbody>
</table>
Appendix A     Abbreviations

- EIA: Electronic Industries Association
- ELAN: Emulated Local Area Network
- EOBC: Ethernet out-of-band channel
- ESI: end-system identifier
- FECN: forward explicit congestion notification
- FM: feature manager
- FRU: field replaceable unit
- FSM: feasible successor metrics
- GARP: General Attribute Registration Protocol
- GMRP: GARP Multicast Registration Protocol
- GVRP: GARP VLAN Registration Protocol
- 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
Appendix A  Abbreviations

ILMI Integrated Local Management Interface
IP Internet Protocol
IPX Internetwork Packet Exchange
ISL Inter-Switch Link
ISO International Organization of Standardization
ISR Integrated SONET router
ISSU In Service Software Upgrade
L 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
Appendix A      Abbreviations

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
MV AP 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
Appendix A      Abbreviations

NMP       Network Management Processor
NSAP      network service access point
NTP       Network Time Protocol
NVRAM     nonvolatile RAM
O          Operation, Administration, and Maintenance
OSI       Open System Interconnection
OSPF      open shortest path first
PAE       port access entity
PAgP      Port Aggregation Protocol
PBD       packet buffer daughterboard
PC        Personal Computer (formerly PCMCI A)
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
Appendix A     Abbreviations

PPP Point-to-Point Protocol
PR C Parser Return Code
PRID Policy Rule Identifiers
PVLAN Private VLAN
PVST+ Per VLAN Spanning Tree+
QM QoS manager
QoS Quality of Service
RAC L Router Interface Access Control List
RADIUS Remote Access Dial-In User Service
RAM random-access memory
RCP Remote Copy Protocol
RGMP Router Group Management Protocol
RIF Routing Information Field
RMON Remote Network Monitor
ROM read-only memory
RP route processor or rendezvous point
RPC remote procedure call
RPF reverse path forwarding
RPR Router Processor Redundancy
RSPAN remote SPAN
RST reset
Appendix A      Abbreviations

RSVP ReSerVation Protocol
Rx Receive
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 sourc e-route br idging
SRT source-route transparent bridging
SSTP Cisco Shared Spanning Tree
STP Spanning Tree Protocol
Appendix A      Abbreviations

SVC switched virtual circuit
SVI switched virtual interface
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
UDLD UniDirectional Link Detection Protocol
UDP User Datagram Protocol
UNI User-Network Interface
UTC Coordinated Universal Time
Appendix A      Abbreviations

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
VMPVS VLAN Membership Policy Server
VTP VLAN Trunking Protocol
VVID voice VLAN ID
WFQ weighted fair queueing
WRED weighted random early detection
WRR weighted round-robin
XNS Xerox Network System
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>display mac interface</td>
<td>2-67</td>
<td>Displays MAC address information.</td>
</tr>
<tr>
<td>show mode interface</td>
<td>2-44</td>
<td>Displays interface mode information.</td>
</tr>
<tr>
<td>access groups</td>
<td>2-6</td>
<td>Managed access list configuration.</td>
</tr>
<tr>
<td>IP</td>
<td>2-172</td>
<td>IP access list configuration.</td>
</tr>
<tr>
<td>access lists</td>
<td>2-94</td>
<td>Clearing access list configuration.</td>
</tr>
<tr>
<td>defining ARP</td>
<td>2-18</td>
<td>ARP configuration.</td>
</tr>
<tr>
<td>displaying ARP information</td>
<td>2-517</td>
<td>Displays ARP configuration information.</td>
</tr>
<tr>
<td>See also ACLs, MAC ACLs, and VACLs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>access maps</td>
<td>2-911</td>
<td>Applying access maps with VLAN filter.</td>
</tr>
<tr>
<td>access-node-identifier, setting for the switch</td>
<td>2-442</td>
<td>Setting access node identifier.</td>
</tr>
<tr>
<td>access-policies, applying using host-mode</td>
<td>2-26</td>
<td>Applying access policies with host-mode.</td>
</tr>
<tr>
<td>ACLs</td>
<td>2-327</td>
<td>Applying ACLs with MAC ACLs naming conventions.</td>
</tr>
<tr>
<td>action clause, specifying drop or forward action in a VACL</td>
<td>2-12</td>
<td>Clause for VACL action.</td>
</tr>
<tr>
<td>addresses, configuring a maximum</td>
<td>2-427</td>
<td>Configuring maximum addresses.</td>
</tr>
<tr>
<td>adjacency</td>
<td>2-124</td>
<td>Debugging adjacency table configuration.</td>
</tr>
<tr>
<td>displaying information about the adjacency table</td>
<td>2-514</td>
<td>Displaying adjacency table information.</td>
</tr>
<tr>
<td>displaying IPC table entries</td>
<td>2-124</td>
<td>Displaying IPC table entries.</td>
</tr>
<tr>
<td>aggregate policer</td>
<td>2-742</td>
<td>Displaying aggregate policer information.</td>
</tr>
<tr>
<td>aging time</td>
<td>2-674</td>
<td>Displaying MAC address aging time.</td>
</tr>
<tr>
<td>MAC address table</td>
<td>2-330</td>
<td>MAC address table configuration.</td>
</tr>
<tr>
<td>alarms, displaying operational status</td>
<td>2-556</td>
<td>Displaying alarm status.</td>
</tr>
<tr>
<td>authentication control-direction command</td>
<td>2-20</td>
<td>Setting control direction for authentication.</td>
</tr>
<tr>
<td>authentication critical recovery delay command</td>
<td>2-22</td>
<td>Critical recovery delay setting.</td>
</tr>
<tr>
<td>authentication event command</td>
<td>2-23</td>
<td>Setting event command.</td>
</tr>
<tr>
<td>authentication fallback command</td>
<td>2-25</td>
<td>Setting fallback command.</td>
</tr>
<tr>
<td>authentication host-mode</td>
<td>2-26</td>
<td>Setting host-mode authentication.</td>
</tr>
<tr>
<td>authentication methods, setting priority</td>
<td>2-33</td>
<td>Setting priority of authentication methods.</td>
</tr>
<tr>
<td>authentication methods, setting username</td>
<td>2-899</td>
<td>Setting username for authentication methods.</td>
</tr>
<tr>
<td>authentication methods, specifying order of methods</td>
<td>2-29</td>
<td>Specifying order of authentication methods.</td>
</tr>
<tr>
<td>using an MD5-type encryption method</td>
<td>2-899</td>
<td>Using MD5-type encryption method.</td>
</tr>
<tr>
<td>verifying MD5 signature</td>
<td>2-900</td>
<td>Verifying MD5 signature.</td>
</tr>
<tr>
<td>verifying the checksum for Flash memory</td>
<td>2-900</td>
<td>Verifying checksum for Flash memory.</td>
</tr>
<tr>
<td>authentication control-direction command, authentication critical recovery delay command, authentication event command, authentication fallback command, authentication host-mode, authentication methods, setting priority, authentication methods, setting username, authentication methods, specifying order of methods, using an MD5-type encryption method, verifying MD5 signature, verifying the checksum for Flash memory, authentication control-direction command, authentication critical recovery delay command, authentication event command, authentication fallback command, authentication host-mode, authentication methods, setting priority, authentication methods, setting username, authentication methods, specifying order of methods, using an MD5-type encryption method, verifying MD5 signature, verifying the checksum for Flash memory</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Index

authentication methods, specifying the order of attempts 2-29
authentication open command 2-28
authentication order command 2-29
authentication periodic command 2-30
authentication port-control command 2-31
authentication priority command 2-33
authentication timer, setting 2-35
authentication timer command 2-35
authentication violation command 2-37
auth fail VLAN enable on a port 2-176
set max number of attempts 2-175
Auth Manager configuring authentication timer 2-35
authorization state enabling manual control 2-191
authorization state of a controlled port 2-191
automatic installation displaying status 2-523
automatic medium-dependent interface crossover See Auto-MDIX
Auto-MDIX disabling 2-374
enabling 2-374
auto-negotiate interface speed example 2-834
auto-QoS configuring for VoIP 2-59
displaying configuration 2-524
auto qos srnd4 command 2-47
B
baby giants displaying the system MTU setting 2-770
setting the maximum Layer 2 payload size 2-881
BackboneFast displaying debugging messages 2-153
displaying spanning tree status 2-762
enabling debugging 2-153
bandwidth command 2-67
bindings store for DHCP snooping 2-244
BOOT environment variable displaying information 2-527
bootflash displaying information 2-525
BPDUs debugging spanning tree activities 2-151
bridge protocol data units See BPDUs
broadcast suppression level configuring 2-835, 2-837
enabling 2-835, 2-837
C
cable diagnostics TDR displaying test results 2-528
testing conditions of copper cables 2-882
call home displaying information 2-530
e-mailing output 2-75
entering configuration submode 2-70
executing 2-75
manually send test message 2-78
receiving information 2-73
sending alert group message 2-76
submitting information 2-73
call home destination profiles displaying 2-532
Catalyst 4507R 2-425
CDP configuring tunneling encapsulation rate 2-315
displaying
Index

IN-5

Catalyst 4500 Series Switch Cisco IOS Command Reference—Release IOS XE 3.3.0X

2-493  displaying policy-map class information
2-119  entering configuration mode
2-493  removing service policy from control plane
2-313  assigning to Layer 2 protocol packets
2-121  counter command
2-89  clearing interface counters
2-22  critical authentication, configure 802.1X parameters
2-22  critical recovery, configuring 802.1X parameter
2-96  clear statistics
2-743  displaying qos dbl
2-125  debugging backup events
2-136  debugging DHCP snooping events
2-137  debugging DHCP snooping messages
2-132  debugging EtherChannel/PAgP/shim
2-135  debugging IPC activity
2-138  debugging IP DHCP snooping security messages
2-142  debugging NVRAM activities
2-143  debugging PAgP activities
2-146  debugging port manager activities
2-151  debugging spanning tree activities
2-153  debugging spanning tree BackboneFast events
2-156  debugging spanning tree UplinkFast events
2-150  debugging supervisor redundancy
2-157  debugging VLAN manager activities
2-140  displaying monitor activity
2-124  displaying the adjacency table
2-131  enabling debug dot1x
2-160  enabling debugging messages for ISL VLAN IDs
2-161  enabling debugging messages for VTP
2-162  enabling debugging of UDLD activity
2-154  enabling switch shim debugging
2-158  enabling VLAN manager file system error tests
2-129  limiting debugging output for VLANs
2-126  limiting interface debugging output
2-127  limiting output for debugging standby state changes
2-134  shortcut to the debug condition interface
2-140  debugging activity monitoring
2-136  DHCP snooping events
2-137  DHCP snooping packets
2-135  IPC activities
2-138  IP DHCP snooping security packets
2-142  NVRAM activities
2-143  PAgP activities
2-132  PAgP shim
2-146  PM activities
2-148  PPoE Intermediate Agent
2-153  spanning tree BackboneFast events
2-154  spanning tree switch shim
2-161  spanning tree UplinkFast events
2-157  VLAN manager activities
2-158  VLAN manager IOS file system error tests
2-161  VTP protocol debug messages
2-141  debug nmsp command
2-154  debug spanning tree switch
2-161  debug sw-vlan vtp
1-6  default form of a command, using
2-100  clearing database statistics
2-243  configuring bindings
2-166  deny ARP packet based on matches
2-407  permit ARP packet based on matches
2-243  configuring bindings
2-166  deny ARP packet based on matches
2-407  permit ARP packet based on matches
enabling error disable detection
2-90, 2-204
enabling per-VLAN on BPDU guard
2-204
error-disabled state
displaying
2-586
error disable recovery
configuring recovery mechanism variables
2-206
displaying recovery timer information
2-560
enabling ARP inspection timeout
2-206
specifying recovery cause
2-206
EtherChannel
assigning interfaces to EtherChannel groups
2-79
debugging EtherChannel
2-132
debugging PAgP shim
2-132
debugging spanning tree activities
2-151
displaying information for a channel
2-561
removing interfaces from EtherChannel groups
2-79
EtherChannel guard
detecting STP misconfiguration
2-807
Explicit Host Tracking
clearing the database
2-103
enabling per-VLAN
2-265
expressions
matching multiple expression occurrences
1-9
multiple-character patterns
1-8
multiplying pattern occurrence
1-11
single-character patterns
1-7
Extensible Authentication Protocol
See EAP
F
fallback profile, specifying
2-25
field replaceable unit (FRU)
displaying status information
2-556
filters
EIGRP
routing updates, preventing
2-404
Flash memory file system
displaying file system information
2-525
verifying checksum
2-900
flow control
configuring a gigabit interface for pause frames
2-209
displaying per-interface statistics for flow control
2-565
G
GBIC
displaying SEEPROM information
2-567
generic-error-message, setting for the switch
2-442
Gigabit Ethernet interface
clearing the hardware logic
2-92
Gigabit Ethernet uplink
showing the mode
2-567
global configuration mode
using
1-5
H
hardware module
resetting a module by toggling the power
2-214
hardware statistics
disabling
2-212
enabling
2-212
hardware uplink
showing the mode
2-567
helper addresses, IP
2-619
hot standby protocol
debugging
2-127
disabling debugging
2-127
limiting output
2-127
hw-module beacon command
2-213
I
identifier-string, setting for the switch
2-442
ID mapping, creating an ANCP client
2-14
IDPROMs
configuring

default setting

displaying allocation information

Internet Group Management Protocol
See IGMP

IP address of remote ANCP server, setting

IP AR P
applying ARP ACL to VLAN

clearing inspection statistics

clearing status of log buffer

controlling packet logging

enabling dynamic inspection

limit rate of incoming requests

set per-port config trust state

showing status of dynamic ARP inspection

showing status of log buffer

IP C
debugging IPC activities

IP DHCP Snooping
See DHCP snooping

IP header validation

disabling

enabling

IP interfaces
displaying usability status

IP multicast
displaying multicast routing table information

ip multicast multipath command

IP packets
enable DSCP rewrite

IP phone and standard desktop
enabling Cisco-recommended features

IP Port Security
enabling

IP source binding
adding or deleting

displaying bindingstagging

IP source guard
debugging messages

displaying configuration and filters

enabling on DHCP snooping

IPv4 statistics, enabling collection

IPv6 statistics, enabling collection

ip wccp check services all command

ip wccp command

ip wccp group-address command

ip wccp group-list command

ip wccp group-listen command

ip wccp password command

ip wccp redirect command

ip wccp redirect exclude in command

ip wccp redirect-list command

IS SU
canceling process

configuring rollback timer

displaying capability

displaying client information

displaying compatibility matrix

displaying endpoint information

displaying entities

displaying FSM session

displaying messages

displaying negotiated

displaying rollback-timer
MAC address table
adding static entries
2-365
clearing dynamic entries
2-108, 2-110
configuring aging time
2-330
displaying dynamic table entry information
2-676
displaying entry count
2-675
displaying information
2-672
displaying interface-based information
2-678
displaying multicast information
2-681
displaying notification information
2-683
displaying protocol-based information
2-685
displaying static table entry information
2-687
displaying the MAC address aging time
2-674
displaying VLAN-based information
2-689
enabling authentication bypass
2-188
enabling notifications
2-336
learning in the protocol buckets
2-331
removing static entries
2-365
mac address-table learning vlan command
2-334
MAC address tables
adding static entries
2-338
deleting secure or specific addresses
2-113
disabling IGMP snooping on static MAC addresses
2-338
removing static entries
2-338
mac-address-table static
2-338
MAC address unicast filtering
dropping unicast traffic
2-338
MAC authentication bypass (MAB), display information
2-669
MAC authorization bypass (MAB), enable and configure
2-326
macro
displaying descriptions
2-364
macro auto global processing command
2-347, 2-349, 2-352, 2-353, 2-355, 2-357, 2-359, 2-361, 2-691
macro auto monitor command
2-358
macro keywords
help strings
2-2
macros
adding a global description
2-364
cisco global
2-362
system-cpp
2-363
mapping secondary VLANs to MST instance
2-457
mapping VLAN(s) to an MST instance
2-216
match (class-map configuration) command
2-13, 2-168, 2-169, 2-170, 2-171, 2-367, 2-838, 2-839, 2-841, 2-843, 2-847
maximum transmission unit (MTU)
displaying the system MTU setting
2-770
setting the maximum Layer 2 payload size
2-881
MD5
verifying MD5 signature
2-900
message digest 5
See MD5
MFIB
clearing ip mfib counters
2-104
clearing ip mfib fastdrop
2-105
displaying all active MFIB routes
2-621
displaying MFIB fastdrop table entries
2-623
enabling IP MFIB fastdrops
2-271
MLD
configuring snooping
last-listener-query-intervals
2-295
configuring snooping
listener-message-suppression
2-297
configuring snooping robustness-variables
2-298
configuring topology change notifications
2-300
counting snooping last-listener-queries
2-293
enabling snooping
2-291
enabling snooping on a VLAN
2-301
MLD snooping
displaying
2-645
modes
access-group
2-6
show access-group interface
2-440, 2-513, 2-741
switching between PVST+, MST, and Rapid PVST
2-812
See also command modes
module password clearing
2-91
module reset
bootup, displaying results
ongoing, displaying results
PACL
access-group mode
paging prompt
see --More-- prompt
PAgP
clearing port channel information
debugging PAgP activity
deselecting channeling protocol
displaying port channel information
hot standby mode
returning to defaults
selecting ports
input interface of incoming packets
learning
returning to defaults
setting channeling protocol
parentheses
1-11
password
clearing on an intelligent line module
establishing enhanced password security
setting username
PBR
displaying route maps
redistributing route maps
PM activities
debugging
disabling debugging
PoE policing
configure on an interface
PoE policing and monitoring
displaying status
police (percent) command
police (two rates) command
police command
policing, configure PoE
policing and monitoring status
Policy Based Routing
See PBR
policy maps
creating
marking
See also QoS, hierarchical policies
traffic classification
defining the class
defining trust states
port, dual-capable
selecting the connector
Port Aggregation Protocol
See PAgP
port-based authentication
displaying debug messages
displaying statistics and status
enabling 802.1X
host modes
manual control of authorization state
periodic re-authentication
enabling
re-authenticating 802.1X-enabled ports
switch-to-client frame-retransmission number
port channel
accessing
creating
displaying information
load distribution method
resetting to defaults
setting
port-channel standalone-disable command
port control, changing from unidirectional or bidirectional
port-control value, configuring
port range
executing
port security
debugging ports security
deleting secure or specific addresses
Index

Catalyst 4500 Series Switch Cisco IOS Command Reference—Release IOS XE 3.3.0XO(15.1(1)XO)

IN-17

displaying information about the system

SNMP

debugging spanning tree activities

ifIndex persistence

clearing SNMP ifIndex commands

compress SNMP ifIndex table format

disabling globally

disabling on an interface

enabling globally

enabling on an interface

informs

disabling

enabling

traps

configuring to send when storm occurs

disabling

enabling

mac-notification

adding

removing

SPAN commands

configuring a SPAN session to monitor

displaying SPAN session information

SPAN enhancements

displaying status

Spanning Tree Protocol

See STP

SPAN session

displaying session information

filter ACLs

specify encap type

turn off host learning based on ingress packets

special characters

anchoring, table

SSO

standard desktop

enabling Cisco-recommended features

standard desktop and Cisco IP phone

enabling Cisco-recommended features

sticky address, configuring

sticky-ARP

disabling on PVLANs

enabling on PVLANs

sticky port

deleting

enabling security

storm control

configuring for action when storm occurs

disabling suppression mode

displaying settings

enabling

enabling broadcast

enabling multicast

enabling suppression mode

enabling timer to recover from error disable

enabling unicast

multicast, enabling

setting high and low levels

setting suppression level

STP

configuring link type for a port

configuring tunneling encapsulation rate

debugging all activities

debugging spanning tree activities

debugging spanning tree BackboneFast events

debugging spanning tree UplinkFast

detecting misconfiguration

displaying active interfaces only

displaying BackboneFast status

displaying bridge status and configuration

displaying spanning tree debug messages

displaying summary of interface information

enabling BPDU filtering by default on all PortFast ports

enabling BPDU filtering on an interface

enabling BPDU guard by default on all PortFast ports

enabling BPDU guard on an interface

enabling RSTP port mode on an interface
enabling extended system ID
2-808
enabling loop guard as a default on all ports
2-811
enabling PortFast by default on all access ports
2-826
enabling PortFast mode
2-822
enabling protocol tunneling for
2-312
enabling root guard
2-809
enabling spanning tree BackboneFast
2-802
enabling spanning tree on a per VLAN basis
2-830
enabling spanning tree UplinkFast
2-828
setting an interface priority
2-827
setting drop threshold for
2-314
setting pathcost
2-806
setting the default pathcost calculation method
2-821
subinterface configuration mode, summary
1-6
SVI
creating a Layer 3 interface on a VLAN
2-224
switching characteristics
excluding from link-up calculation
2-853
modifying
2-853
returning to interfaces
2-853
capture function
2-853
switchport
2-876
switchport interfaces
2-876
displaying status of Layer 3 port
2-588
displaying status of native VLAN tagging
2-588
switchport vlan mapping command
2-879
switch shim
debugging
2-154
disabling debugging
2-154
switch to router connection
enabling Cisco-recommended features
2-343
switch to switch connection
enabling Cisco-recommended features
2-345
switch virtual interface
See SVI
sw-vlan
2-157
system prompts
1-5
Tab key
command completion
1-1
tables
characters with special meaning
1-7
mac access-list extended subcommands
2-327
multipliers
1-9
relationship between duplex and speed
commands
2-833
show cable-diagnostics tdr command output
fields
2-529
show cdp neighbors detail field descriptions
2-537
show cdp neighbors field descriptions
2-536
show ip dhcp snooping command output
2-519, 2-669
show ip interface field descriptions
2-619
show policy-map control-plane field descriptions
2-717
show vlan command output fields
2-787
show vtp command output fields
2-791
special characters
1-9
special characters used for anchoring
1-10
speed command options
2-370, 2-832
valid interface types
2-219
TAC
displaying information useful to TAC
2-771
TCAM
debugging spanning tree activities
2-151
TDR
displaying cable diagnostic test results
2-528
test condition of copper cables
2-882
temperature readings
displaying information
2-556
timer information
2-560
traffic monitor
display status
2-669
traffic shaping
enable on an interface
2-510
traps, enabling
2-795
trunk encapsulation
Index

IN-19

Catalyst 4500 Series Switch Cisco IOS Command Reference—Release IOS XE 3.3.0XO(15.1(1)XO)

OL_2 873 8 - 01

setting format

trunk interfaces

displaying trunk interfaces information

trunk port, configuring VLAN mapping

trunk ports, display VLAN mapping information

trust configuration, setting on an interface

trust state

setting

tunnel ports

displaying information about Layer 2 protocol

TX queues

allocating bandwidth

returning to default values

setting priority to high

specifying burst size

specifying traffic rate

U

UDLD

displaying administrative and operational status

enabling by default on all fiber interfaces

enabling on an individual interface

preventing a fiber interface from being enabled

resetting all shutdown ports

setting the message timer

Unidirectional Link Detection

See UDLD

unidirection port control, changing from bidirectional

unknown multicast traffic, preventing

unknown unicast traffic, preventing

user EXEC mode, summary

username

setting password and privilege level

V

VACLs

access-group mode

applying VLAN access maps

displaying VLAN access map information

specifying an action in a VLAN access map sequence

specifying the match clause for a VLAN access-map sequence

using a VLAN filter

VLAN

applying an ARP ACL

configuring

configuring service policies

converting to RSPAN VLAN

displaying CEF information

displaying CEF next-hop information

displaying information on switch interfaces

displaying information on VLAN switch interfaces

displaying information sorted by group IP address

displaying IP address and version information

displaying Layer 2 VLAN information

displaying statistical information

displaying VLAN information

enabling dynamic ARP inspection

enabling Explicit Host Tracking

enabling guest per-port

enabling guest VLAN supplicant

entering VLAN configuration mode

native frames

enabling tagging on all 802.1Q trunk ports

pruning the list for VTP

setting the list of allowed

VLAN, create or modify a group

VLAN Access Control Lists

See VACLs
Index

IN-20
Catalyst 4500 Series Switch Cisco IOS Command Reference—Release IOS XE 3.3.0XO(15.1(1)XO)

VLAN access map
See VACLs
VLAN database
resetting
VLAN debugging
limiting output
vlan group command
2-912
VLAN groups, display VLANs mapped
2-782
VLAN link-up calculation
excluding a switch port
2-853
including a switch port
2-853
VLAN manager
debugging
disabling debugging
2-157
IOS file system error tests
debugging
disabling debugging
2-158
VLAN mapping
configuring
displaying
VLAN mapping, configure on trunk port
2-879
VLAN mapping on trunk ports, display information
2-784
VLAN Query Protocol
See VQP
VLAN query protocol (VQPC)
debugging
VLANs
clearing
counters
clearing hardware logic
configuring
internal allocation scheme
displaying
internal VLAN allocation information
2-783
RSPAN VLANs
2-788
entering VLAN configuration mode
2-908
VMPS
configuring servers
reconfirming dynamic VLAN assignments
2-915
voice VLANs
enabling
VoIP
configuring auto-QoS
VQP
per-server retry count
reconfirming dynamic VLAN assignments
2-915
VTP
configuring the administrative domain name
calculating IP addresses
configuring the device in VTP client mode
calculating IP addresses
configuring the device in VTP server mode
calculating IP addresses
configuring the device in VTP transparent mode
calculating IP addresses
configuring tunnel encapsulation rate
2-315
creating a VTP domain password
2-922
displaying domain information
2-790
displaying statistics information
2-790
enabling protocol tunneling for
2-312
enabling pruning in the VLAN database
2-923
enabling VTP version 2 mode
2-926
modifying the VTP configuration storage file
name
2-919
set drop threshold for
2-314
VTP protocol code
activating debug messages
debugging
deactivating debug messages
debugging
Webauth fallback, enabling
2-25