

You'll be entered into a quarterly drawing for **free** Cisco Press books by returning this survey! Cisco is dedicated to customer satisfaction and would like to hear your thoughts on these printed manuals. Please visit the Cisco Product Comments on-line survey at **www.cisco.com/go/crc** to submit your comments about accessing Cisco technical manuals. Thank you for your time.

General Information

1	Years of networking experience:	_____	Years of experience with Cisco products:	_____
2	I have these network types:	_____ LAN	_____ Backbone	_____ WAN
	Other:	_____		
3	I have these Cisco products:	_____ Switches	_____ Routers	
	Other (specify models):	_____		
4	I perform these types of tasks:	_____ H/W installation and/or maintenance	_____ S/W configuration	
	Network management	_____ Other:	_____	
5	I use these types of documentation:	_____ H/W installation	_____ H/W configuration	_____ S/W configuration
	Command reference	_____ Quick reference	_____ Release notes	_____ Online help
	Other:	_____		
6	I access this information through:	_____ % Cisco.com	_____ % CD-ROM	_____ % Printed manuals
	% Other:	_____		
7	I prefer this access method:	_____ Cisco.com	_____ CD-ROM	_____ Printed manuals
	Other:	_____		
8	I use the following three product features the most:	_____		

Document Information

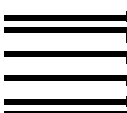
Document Title:	Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide		
Part Number:	78-15523-01	S/W Release (if applicable):	12.1(19)EW
On a scale of 1–5 (5 being the best), please let us know how we rate in the following areas:			
_____ The document is complete.	_____ The information is accurate.		
_____ The information is well organized.	_____ The information I wanted was easy to find.		
_____ The document is written at my technical level of understanding.	_____ The information I found was useful to my job.		
Please comment on our lowest scores: _____			

Mailing Information

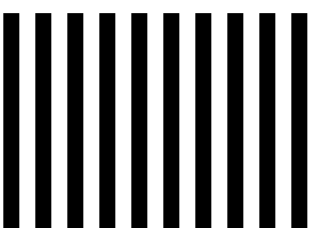
Organization	Date	
Contact Name	_____	
Mailing Address	_____	
City	State/Province	Zip/Postal Code
Country	Phone ()	Extension
E-mail	Fax ()	
May we contact you further concerning our documentation? Yes No		

You can also send us your comments by e-mail to **bug-doc@cisco.com**, or by fax to **408-527-8089**.

When mailing this card from outside of the United States, please enclose in an envelope addressed to the location on the back of this card with the required postage or fax to 1-408-527-8089.



NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES



BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 4631 SAN JOSE CA

POSTAGE WILL BE PAID BY ADDRESSEE

DOCUMENT RESOURCE CONNECTION
CISCO SYSTEMS INC
170 WEST TASMAN DR
SAN JOSE CA 95134-9916





Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide

Release 12.1(19)EW

Corporate Headquarters

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

Customer Order Number: DOC-7815523=
Text Part Number: 78-15523-01



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

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

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

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

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

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0304R)

Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide
Copyright © 1999–2003 Cisco Systems, Inc. All rights reserved.



Preface xix

Audience	xix
Organization	xix
Related Documentation	xxi
Conventions	xxii
Commands in Task Tables	xxii
Obtaining Documentation	xxiii
Cisco.com	xxiii
Documentation CD-ROM	xxiii
Ordering Documentation	xxiii
Documentation Feedback	xxiii
Obtaining Technical Assistance	xxiv
Cisco.com	xxiv
Technical Assistance Center	xxiv
Obtaining Additional Publications and Information	xxv

CHAPTER 1

Product Overview 1-1

Layer 2 Software Features	1-1
Storm Control	1-2
CDP	1-2
DHCP Snooping	1-2
EtherChannel Bundles	1-2
IP Source Guard	1-3
Jumbo Frames	1-3
Layer 2 Traceroute	1-3
MST	1-3
PVRST+	1-3
Spanning Tree Protocol	1-4
UDLD	1-4
Unidirectional Ethernet	1-4
VLANs	1-4
Layer 3 Software Features	1-5
CEF	1-6
HSRP	1-6

IP Routing Protocols	1-6
Multicast Services	1-8
Network Security with ACLs	1-8
Policy-Based Routing	1-9
Unidirectional Link Routing	1-9
QoS Features	1-9
Management and Security Features	1-10

CHAPTER 2

Command-Line Interfaces 2-1

Accessing the Switch CLI	2-1
Accessing the CLI Using the EIA/TIA-232 Console Interface	2-1
Accessing the CLI Through Telnet	2-2
Performing Command-Line Processing	2-3
Performing History Substitution	2-3
Understanding Cisco IOS Command Modes	2-4
Getting a List of Commands and Syntax	2-5
ROMMON Command-Line Interface	2-6

CHAPTER 3

Configuring the Switch for the First Time 3-1

Default Switch Configuration	3-1
Configuring the Switch	3-2
Using Configuration Mode to Configure Your Switch	3-2
Checking the Running Configuration Settings	3-3
Saving the Running Configuration Settings to Your Start-up File	3-3
Reviewing the Configuration in NVRAM	3-4
Configuring a Default Gateway	3-4
Configuring a Static Route	3-5
Controlling Access to Privileged EXEC Commands	3-7
Setting or Changing a Static enable Password	3-7
Using the enable Password and enable secret Commands	3-7
Setting or Changing a Privileged Password	3-8
Setting TACACS+ Password Protection for Privileged EXEC Mode	3-8
Encrypting Passwords	3-9
Configuring Multiple Privilege Levels	3-10
Recovering a Lost Enable Password	3-12
Modifying the Supervisor Engine Startup Configuration	3-12
Understanding the Supervisor Engine Boot Configuration	3-12
Configuring the Software Configuration Register	3-13

Specifying the Startup System Image	3-17
Controlling Environment Variables	3-18

CHAPTER 4**Configuring Interfaces 4-1**

Overview of Interface Configuration	4-1
Using the interface Command	4-2
Configuring a Range of Interfaces	4-4
Defining and Using Interface-Range Macros	4-5
Configuring Optional Interface Features	4-6
Configuring Ethernet Interface Speed and Duplex Mode	4-6
Configuring Jumbo Frame Support	4-9
Interacting with the Baby Giants Feature	4-11
Understanding Online Insertion and Removal	4-12
Monitoring and Maintaining the Interface	4-12
Monitoring Interface and Controller Status	4-12
Clearing and Resetting the Interface	4-13
Shutting Down and Restarting an Interface	4-13

CHAPTER 5**Checking Port Status and Connectivity 5-1**

Checking Module Status	5-1
Checking Interfaces Status	5-2
Checking MAC Addresses	5-3
Using Telnet	5-3
Changing the Logout Timer	5-4
Monitoring User Sessions	5-4
Using Ping	5-5
Understanding How Ping Works	5-5
Running Ping	5-6
Using IP Traceroute	5-7
Understanding How IP Traceroute Works	5-7
Running IP Traceroute	5-7
Using Layer 2 Traceroute	5-8
Understanding Layer 2 Traceroute	5-8
Layer 2 Traceroute Usage Guidelines	5-8
Running Layer 2 Traceroute	5-9
Configuring ICMP	5-10
Enabling ICMP Protocol Unreachable Messages	5-10

Enabling ICMP Redirect Messages	5-11
Enabling ICMP Mask Reply Messages	5-11

CHAPTER 6**Configuring Layer 2 Ethernet Interfaces 6-1**

Overview of Layer 2 Ethernet Switching	6-1
Understanding Layer 2 Ethernet Switching	6-1
Understanding VLAN Trunks	6-3
Layer 2 Interface Modes	6-4
Default Layer 2 Ethernet Interface Configuration	6-4
Layer 2 Interface Configuration Guidelines and Restrictions	6-5
Configuring Ethernet Interfaces for Layer 2 Switching	6-5
Configuring an Ethernet Interface as a Layer 2 Trunk	6-6
Configuring an Interface as a Layer 2 Access Port	6-8
Clearing Layer 2 Configuration	6-9

CHAPTER 7**Configuring Unidirectional Ethernet 7-1****CHAPTER 8****Understanding and Configuring VLANs 8-1**

Overview of VLANs	8-1
VLAN Configuration Guidelines and Restrictions	8-3
VLAN Ranges	8-3
Configurable Normal-Range VLAN Parameters	8-4
VLAN Default Configuration	8-4
Configuring VLANs	8-4
Configuring VLANs in Global Configuration Mode	8-5
Configuring VLANs in VLAN Database Mode	8-7
Assigning a Layer 2 LAN Interface to a VLAN	8-8

CHAPTER 9**Configuring Dynamic VLAN Membership 9-1**

Understanding VMPS	9-1
Entering Port Names in the VMPS	9-2
Dynamic Port VLAN Membership	9-2
VMPS Configuration Guidelines	9-3
Default VMPS Configuration	9-3
Configuring Dynamic VLAN Membership	9-4
Entering the IP Address of the VMPS	9-4
Configuring Dynamic Ports on VMPS Clients	9-5
Administering and Monitoring the VMPS	9-5

Configuring the Reconfirmation Interval	9-7
Reconfirming VLAN Memberships	9-7
Troubleshooting Dynamic Port VLAN Membership	9-8
VMPS Database Configuration File Example	9-8
Dynamic Port VLAN Membership Configuration Example	9-9

CHAPTER 10**Configuring Private VLANs 10-1**

Overview of PVLANS	10-1
PVLAN Trunks	10-2
PVLANS and VLAN ACL/QoS	10-2
PVLAN Configuration Restrictions	10-3
How to Configure PVLANS	10-3
PVLAN Configuration Guidelines	10-4
Configuring a VLAN as a PVLAN	10-5
Associating a Secondary VLAN with a Primary VLAN	10-6
Configuring a Layer 2 Interface as a PVLAN Promiscuous Port	10-7
Configuring a Layer 2 Interface as a PVLAN Host Port	10-8
Configuring a Layer 2 Interface as a PVLAN Trunk Port	10-9
Permitting Routing of Secondary VLAN Ingress Traffic	10-10

CHAPTER 11**Understanding and Configuring VTP 11-1**

Overview of VTP	11-1
Understanding the VTP Domain	11-2
Understanding VTP Modes	11-2
Understanding VTP Advertisements	11-3
Understanding VTP Version 2	11-3
Understanding VTP Pruning	11-3
VTP Configuration Guidelines and Restrictions	11-5
VTP Default Configuration	11-5
Configuring VTP	11-6
Configuring VTP Global Parameters	11-6
Configuring the Switch as a VTP Server	11-7
Configuring the Switch as a VTP Client	11-8
Disabling VTP (VTP Transparent Mode)	11-9
Displaying VTP Statistics	11-10

CHAPTER 12**Understanding and Configuring STP 12-1**

Overview of STP	12-1

Understanding the Bridge ID	12-2
Bridge Protocol Data Units	12-3
Election of the Root Bridge	12-4
STP Timers	12-4
Creating the STP Topology	12-4
STP Port States	12-5
MAC Address Allocation	12-5
STP and IEEE 802.1Q Trunks	12-6
Per-VLAN Rapid Spanning Tree	12-6
Default STP Configuration	12-6
Configuring STP	12-7
Enabling STP	12-7
Enabling the Extended System ID	12-8
Configuring the Root Bridge	12-9
Configuring a Secondary Root Switch	12-12
Configuring STP Port Priority	12-13
Configuring STP Port Cost	12-15
Configuring the Bridge Priority of a VLAN	12-16
Configuring the Hello Time	12-17
Configuring the Maximum Aging Time for a VLAN	12-18
Configuring the Forward-Delay Time for a VLAN	12-18
Disabling Spanning Tree Protocol	12-19
Enabling Per-VLAN Rapid Spanning Tree	12-20

CHAPTER 13

Configuring STP Features	13-1
Overview of Root Guard	13-2
Overview of Loop Guard	13-2
Overview of PortFast	13-3
Overview of BPDU Guard	13-4
Overview of PortFast BPDU Filtering	13-4
Overview of UplinkFast	13-5
Overview of BackboneFast	13-6
Enabling Root Guard	13-8
Enabling Loop Guard	13-9
Enabling PortFast	13-11
Enabling BPDU Guard	13-12
Enabling PortFast BPDU Filtering	13-12
Enabling UplinkFast	13-14

Enabling BackboneFast 13-15

CHAPTER 14

Understanding and Configuring Multiple Spanning Trees 14-1

- Overview of MST 14-1
 - IEEE 802.1s MST 14-2
 - IEEE 802.1w RSTP 14-3
 - MST-to-SST Interoperability 14-4
 - Common Spanning Tree 14-5
 - MST Instances 14-5
 - MST Configuration Parameters 14-5
 - MST Regions 14-6
 - Message Age and Hop Count 14-7
 - MST-to-PVST+ Interoperability 14-8
- MST Configuration Restrictions and Guidelines 14-8
- Configuring MST 14-9
 - Enabling MST 14-9
 - Configuring MST Instance Parameters 14-10
 - Configuring MST Instance Port Parameters 14-11
 - Restarting Protocol Migration 14-12
 - Displaying MST Configurations 14-13

CHAPTER 15

Configuring IGMP Snooping and Filtering 15-1

- Overview of IGMP Snooping 15-1
 - Immediate-Leave Processing 15-2
 - IGMPv3 Snooping 15-3
- Configuring IGMP Snooping 15-3
 - Default IGMP Snooping Configuration 15-3
 - Enabling IGMP Snooping 15-4
 - Configuring Learning Methods 15-5
 - Configuring a Multicast Router Port Statically 15-6
 - Enabling IGMP Immediate-Leave Processing 15-6
 - Configuring a Host Statically 15-7
 - Suppressing Multicast Flooding 15-7
- Displaying IGMP Snooping Information 15-10
 - Displaying Multicast Router Interfaces 15-10
 - Displaying MAC Address Multicast Entries 15-11
 - Displaying IGMP Snooping Information for a VLAN Interface 15-11
- Configuring IGMP Filtering 15-12
 - Default IGMP Filtering Configuration 15-12

Configuring IGMP Profiles	15-12
Applying IGMP Profiles	15-13
Setting the Maximum Number of IGMP Groups	15-14
Displaying IGMP Filtering Configuration	15-16

CHAPTER 16

Understanding and Configuring CDP 16-1

Overview of CDP	16-1
Configuring CDP	16-1
Enabling CDP Globally	16-2
Displaying the CDP Global Configuration	16-2
Enabling CDP on an Interface	16-2
Displaying the CDP Interface Configuration	16-3
Monitoring and Maintaining CDP	16-3

CHAPTER 17

Understanding and Configuring EtherChannel 17-1

Overview of EtherChannel	17-1
Understanding Port-Channel Interfaces	17-2
Understanding How EtherChannels Are Configured	17-2
Understanding Load Balancing	17-5
EtherChannel Configuration Guidelines and Restrictions	17-5
Configuring EtherChannel	17-6
Configuring Layer 3 EtherChannels	17-6
Configuring Layer 2 EtherChannel	17-9
Configuring the LACP System Priority and System ID	17-11
Configuring EtherChannel Load Balancing	17-12
Removing an Interface from an EtherChannel	17-13
Removing an EtherChannel	17-13

CHAPTER 18

Configuring UDLD 18-1

Overview of UDLD	18-1
Default UDLD Configuration	18-2
Configuring UDLD on the Switch	18-2
Enabling UDLD Globally	18-3
Enabling UDLD on Individual Interfaces	18-3
Disabling UDLD on Nonfiber-Optic Interfaces	18-3
Disabling UDLD on Fiber-Optic Interfaces	18-4
Resetting Disabled Interfaces	18-4

CHAPTER 19**Configuring DHCP Snooping and IP Source Guard 19-1**

- Overview of DHCP Snooping 19-1
 - Overview of the DHCP Snooping Database Agent 19-2
- Configuring DHCP Snooping on the Switch 19-3
 - Default Configuration for DHCP Snooping 19-3
 - Enabling DHCP Snooping 19-4
 - Enabling DHCP Snooping on Private VLAN 19-5
 - Enabling the DHCP Snooping Database Agent 19-5
 - Configuration Examples for the Database Agent 19-6
- Displaying DHCP Snooping Information 19-9
 - Displaying a Binding Table 19-9
 - Displaying the DHCP Snooping Configuration 19-10
- Overview of IP Source Guard 19-10
- Configuring IP Source Guard on the Switch 19-11
 - Configuring IP Source Guard on Private VLANs 19-12
- Displaying IP Source Guard Information 19-12
- Displaying IP Source Binding Information 19-13

CHAPTER 20**Configuring Layer 3 Interfaces 20-1**

- Overview of Layer 3 Interfaces 20-1
 - Logical Layer 3 VLAN Interfaces 20-2
 - Physical Layer 3 Interfaces 20-2
- Configuration Guidelines 20-3
- Configuring Logical Layer 3 VLAN Interfaces 20-3
- Configuring Physical Layer 3 Interfaces 20-4

CHAPTER 21**Configuring Cisco Express Forwarding 21-1**

- Overview of CEF 21-1
 - Benefits of CEF 21-1
 - Forwarding Information Base 21-2
 - Adjacency Tables 21-2
- Catalyst 4500 Series Switch Implementation of CEF 21-3
 - Hardware and Software Switching 21-4
 - Load Balancing 21-6
 - Software Interfaces 21-6
- CEF Configuration Restrictions 21-6
- Configuring CEF 21-6
 - Enabling CEF 21-6

Configuring Load Balancing for CEF	21-7
Monitoring and Maintaining CEF	21-8
Displaying IP Statistics	21-9

CHAPTER 22

Configuring Policy-Based Routing 22-1

Overview of Policy-Based Routing	22-1
Understanding PBR	22-2
Using Policy-Based Routing	22-2
Policy-Based Routing Configuration Task List	22-2
Enabling PBR	22-2
Enabling Local PBR	22-4
Unsupported Commands	22-4
Policy-Based Routing Configuration Examples	22-4
Equal Access Example	22-4
Differing Next Hops Example	22-5
Deny ACE Example	22-5

CHAPTER 23

Understanding and Configuring IP Multicast 23-1

Overview of IP Multicast	23-1
IP Multicast Protocols	23-2
IP Multicast on the Catalyst 4500 Series Switch	23-4
Unsupported Features	23-12
Configuring IP Multicast Routing	23-12
Default Configuration in IP MULTicast Routing	23-13
Enabling IP Multicast Routing	23-13
Enabling PIM on an Interface	23-13
Monitoring and Maintaining IP Multicast Routing	23-15
Displaying System and Network Statistics	23-15
Displaying the Multicast Routing Table	23-16
Displaying IP MFIB	23-18
Displaying IP MFIB Fast Drop	23-19
Displaying PIM Statistics	23-20
Clearing Tables and Databases	23-20
Configuration Examples	23-21
PIM Dense Mode Example	23-21
PIM Sparse Mode Example	23-21
BSR Configuration Example	23-21

CHAPTER 24**Configuring Network Security with ACLs 24-1**

- Understanding ACLs 24-1
 - ACL Overview 24-2
 - Supported Features That Use ACLs 24-2
 - Router ACLs 24-3
 - Port ACLs 24-4
 - VLAN Maps 24-5
- Hardware and Software ACL Support 24-5
- Layer 4 Operators in ACLs 24-6
 - Restrictions for Layer 4 Operations 24-6
 - Configuration Guidelines for Layer 4 Operations 24-6
 - How ACL Processing Impacts CPU 24-8
- Configuring Unicast MAC Address Filtering 24-9
- Configuring Named MAC Extended ACLs 24-9
- Configuring VLAN Maps 24-10
 - VLAN Map Configuration Guidelines 24-11
 - Creating and Deleting VLAN Maps 24-12
 - Applying a VLAN Map to a VLAN 24-14
 - Using VLAN Maps in Your Network 24-15
- Displaying VLAN Access Map Information 24-17
- Using VLAN Maps with Router ACLs 24-18
 - Guidelines for Using Router ACLs and VLAN Maps 24-18
 - Examples of Router ACLs and VLAN Maps Applied to VLANs 24-18
- Configuring PACLs 24-20
 - Creating a PACL 24-20
 - PACL Configuration Guidelines 24-21
 - Configuring IP and MAC ACLs on a Layer 2 interface 24-21
 - Using PACL with Access-group Mode 24-22
 - Configuring Access-group Mode on Layer 2 Interface 24-22
 - Applying ACLs to a Layer 2 Interface 24-23
 - Displaying an ACL Configuration on a Layer 2 Interface 24-23
- Using PACL with VLAN Maps and Router ACLs 24-24

CHAPTER 25**Configuring Port Security 25-1**

- Understanding Port Security 25-1
- Default Port Security Configuration 25-2
- Port Security Guidelines and Restrictions 25-3
- Configuring Port Security 25-3

Configuring Port Security on an Interface	25-3
Configuring Port Security Aging	25-5
Displaying Port Security Settings	25-7

CHAPTER 26

Configuring 802.1x Port-Based Authentication 26-1

Understanding 802.1x Port-Based Authentication	26-1
Device Roles	26-2
Authentication Initiation and Message Exchange	26-3
Ports in Authorized and Unauthorized States	26-4
Using 802.1X with VLAN Assignment	26-4
Using 802.1x Authentication for Guest VLANs	26-5
Supported Topologies	26-6
How to Configure 802.1x	26-6
Default 802.1x Configuration	26-7
802.1x Configuration Guidelines	26-8
Enabling 802.1x Authentication	26-8
Configuring 802.1x with Guest-VLANs	26-10
Configuring Switch-to-RADIUS-Server Communication	26-10
Enabling Periodic Re-Authentication	26-11
Manually Re-Authenticating a Client Connected to a Port	26-12
Changing the Quiet Period	26-12
Changing the Switch-to-Client Retransmission Time	26-13
Setting the Switch-to-Client Frame-Retransmission Number	26-14
Enabling Multiple Hosts	26-15
Resetting the 802.1x Configuration to the Default Values	26-15
Displaying 802.1x Statistics and Status	26-16

CHAPTER 27

Port Unicast and Multicast Flood Blocking 27-1

Overview of Flood Blocking	27-1
Configuring Port Blocking	27-1
Blocking Flooded Traffic on an Interface	27-2
Resuming Normal Forwarding on a Port	27-3

CHAPTER 28

Configuring Port-Based Traffic Control 28-1

Overview of Storm Control	28-1
Hardware-based Storm Control Implementation	28-2
Software-based Storm Control Implementation	28-2
Enabling Storm Control	28-3

Disabling Storm Control	28-4
Displaying Storm Control	28-5

CHAPTER 29

Configuring QoS 29-1

Overview of QoS	29-1
Prioritization	29-2
QoS Terminology	29-3
Basic QoS Model	29-5
Classification	29-5
Policing and Marking	29-9
Mapping Tables	29-12
Queueing and Scheduling	29-13
Packet Modification	29-14
Configuring Auto-QoS	29-15
Generated Auto-QoS Configuration	29-15
Effects of Auto-QoS on the Configuration	29-16
Configuration Guidelines	29-16
Enabling Auto-QoS for VoIP	29-17
Displaying Auto-QoS Information	29-18
Auto-QoS Configuration Example	29-19
Configuring QoS	29-21
Default QoS Configuration	29-21
Configuration Guidelines	29-22
Enabling QoS Globally	29-23
Configuring a Trusted Boundary to Ensure Port Security	29-23
Enabling Dynamic Buffer Limiting	29-25
Creating Named Aggregate Policers	29-25
Configuring a QoS Policy	29-27
Enabling or Disabling QoS on an Interface	29-34
Configuring VLAN-Based QoS on Layer 2 Interfaces	29-34
Configuring the Trust State of Interfaces	29-35
Configuring the CoS Value for an Interface	29-36
Configuring DSCP Values for an Interface	29-37
Configuring Transmit Queues	29-37
Configuring DSCP Maps	29-40

CHAPTER 30

Configuring NetFlow Statistics Collection 30-1

Overview of NetFlow Statistics Collection	30-1
Information Derived from Hardware	30-2

Information Derived from Software	30-2
Determining the Input and Output interface and AS Numbers	30-2
VLAN Statistics	30-3
Caveat for the NetFlow Feature	30-3
Configuring NetFlow Statistics Collection	30-4
Checking for Required Hardware	30-4
Enabling NetFlow Statistics Collection	30-5
Exporting NetFlow Statistics	30-5
Managing NetFlow Statistics Collection	30-6
Configuring an Aggregation Cache	30-6
Configuring a NetFlow Minimum Prefix Mask for Router-Based Aggregation	30-7
Configuring Netflow Aging Parameters	30-9
NetFlow Statistics Collection Configuration Example	30-9
NetFlow Configuration Examples	30-10
Sample Netflow Enabling Schemes	30-10
Sample NetFlow Aggregation Configurations	30-10
Sample NetFlow Minimum Prefix Mask Router-Based Aggregation Schemes	30-12

CHAPTER 31

Understanding and Configuring Dynamic ARP Inspection 31-1

Overview of Dynamic ARP Inspection	31-1
ARP Cache Poisoning	31-2
Dynamic ARP Inspection	31-2
Interface Trust state, Security Coverage and Network Configuration	31-3
Relative Priority of Static Bindings and DHCP Snooping Entries	31-4
Logging of Denied Packets	31-4
Rate Limiting of ARP Packets	31-4
Port Channels and Their Behavior	31-4
Configuring Dynamic ARP Inspection	31-5
Scenario One: Two Switches Support Dynamic ARP Inspection	31-5
Scenario Two: One Switch Supports Dynamic ARP Inspection	31-9
	31-10

CHAPTER 32

Configuring SPAN 32-1

Overview of SPAN	32-1
SPAN Session	32-2
Destination Interface	32-2
Source Interface	32-3
Traffic Types	32-3

VLAN-Based SPAN	32-3
SPAN Traffic	32-3
SPAN Configuration Guidelines and Restrictions	32-4
Configuring SPAN	32-4
Configuring SPAN Sources	32-5
Configuring SPAN Destinations	32-5
Monitoring Source VLANs on a Trunk Interface	32-6
Configuration Scenario	32-6
Verifying a SPAN Configuration	32-6
CPU Port Sniffing	32-7
Encapsulation Configuration	32-7
Ingress Packets	32-7
Packet Type Filtering	32-8
Configuration Example	32-9

CHAPTER 33

Environmental Monitoring and Power Management 33-1

Understanding Environmental Monitoring	33-1
Using CLI Commands to Monitor your Environment	33-1
System Alarms	33-2
Power Management	33-3
Power Management for the Catalyst 4500 Series Switches	33-3
Power Management for the Catalyst 4006 Switch	33-10
Power Consumption of Chassis Components	33-15
Configuring Inline Power	33-16
Power Management Modes	33-16
Configuring Power Allocation for an Interface	33-18
Displaying the Operational Status for an Interface	33-19

CHAPTER 34

Configuring Supervisor Engine Redundancy on the Catalyst 4507R Switch 34-1

Overview of Supervisor Engine Redundancy	34-1
Understanding Supervisor Engine Redundancy	34-2
Operation	34-2
Supervisor Engine Synchronization	34-3
Supervisor Engine Redundancy Guidelines and Restrictions	34-3
Configuring Supervisor Engine Redundancy	34-4
Synchronizing the Supervisor Engine Configurations	34-4
Performing a Software Upgrade	34-5

Copying Files to the Standby Supervisor Engine 34-7

CHAPTER 35

Configuring Voice Interfaces 35-1

Overview of Voice Interfaces 35-1

Configuring a Port to Connect to a Cisco 7690 IP Phone 35-2

Configuring Voice Ports for Voice and Data Traffic 35-2

Overriding the CoS Priority of Incoming Frames 35-3

Configuring Inline Power 35-4

APPENDIX A

Acronyms A-1

INDEX



Preface

This preface describes who should read this document, how it is organized, and its conventions. The book also tells you how to obtain Cisco documents as well as how to obtain technical assistance.

Audience

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

Organization

This guide is organized into the following chapters:

Chapter	Title	Description
Chapter 1	Product Overview	Presents an overview of the Cisco IOS software for the Catalyst 4500 series switches
Chapter 2	Command-Line Interfaces	Describes how to use the CLI
Chapter 3	Configuring the Switch for the First Time	Describes how to perform a baseline configuration of the switch
Chapter 4	Configuring Interfaces	Describes how to configure non-layer-specific features on Fast Ethernet and Gigabit Ethernet interfaces
Chapter 5	Checking Port Status and Connectivity	Describes how to check module and interface status
Chapter 6	Configuring Layer 2 Ethernet Interfaces	Describes how to configure interfaces to support Layer 2 features, including VLAN trunks
Chapter 7	Configuring Unidirectional Ethernet	Describes how to configure unidirectional Ethernet
Chapter 8	Understanding and Configuring VLANs	Describes how to set up and modify VLANs
Chapter 9	Configuring Dynamic VLAN Membership	Describes how to configure dynamic VLAN membership

Chapter	Title	Description
Chapter 10	Configuring Private VLANs	Describes how to set up and modify private VLANs
Chapter 11	Understanding and Configuring VTP	Describes how to configure the VLAN Trunking Protocol
Chapter 12	Understanding and Configuring STP	Describes how to configure the Spanning Tree Protocol (STP) and explains how spanning tree works
Chapter 13	Configuring STP Features	Describes how to configure the spanning-tree PortFast, UplinkFast, BackboneFast, and other STP features
Chapter 14	Understanding and Configuring Multiple Spanning Trees	Describes how to configure the Multiple Spanning Tree (MST) protocol and explains how it works
Chapter 15	Configuring IGMP Snooping and Filtering	Describes how to configure Internet Group Management Protocol (IGMP) snooping
Chapter 16	Understanding and Configuring CDP	Describes how to configure the Cisco Discovery Protocol (CDP)
Chapter 17	Understanding and Configuring EtherChannel	Describes how to configure Layer 2 and Layer 3 EtherChannel port bundles
Chapter 18	Configuring UDLD	Describes how to configure the UniDirectional Link Detection (UDLD) protocol
Chapter 19	Configuring DHCP Snooping and IP Source Guard	Describes how to configure DHCP snooping and display DHCP snooping information
Chapter 20	Configuring Layer 3 Interfaces	Describes how to configure interfaces to support Layer 3 features
Chapter 21	Configuring Cisco Express Forwarding	Describes how to configure Cisco Express Forwarding (CEF) for IP unicast traffic
Chapter 22	Configuring Policy-Based Routing	Describes how to configure policy-based routing
Chapter 23	Understanding and Configuring IP Multicast	Describes how to configure IP Multicast Multilayer Switching (MMLS)
Chapter 24	Configuring Network Security with ACLs	Describes how to configure ACLs, VACLs, and MACs
Chapter 25	Configuring Port Security	Describes how to configure the port security feature
Chapter 26	Configuring 802.1x Port-Based Authentication	Describes how to configure 802.1x port-based authentication
Chapter 27	Port Unicast and Multicast Flood Blocking	Describes how to configure unicast flood blocking on the Catalyst 4000 family switches.
Chapter 28	Configuring Port-Based Traffic Control	Describes how to configure storm control suppression on the Catalyst 4500 series switches.
Chapter 29	Configuring QoS	Describes how to configure quality of service (QoS)
Chapter 30	Configuring NetFlow Statistics Collection	Describes how to configure NetFlow statistics gathering
Chapter 31	Understanding and Configuring Dynamic ARP Inspection	Describes how to configure Dynamic ARP Inspection.

Chapter	Title	Description
Chapter 32	Configuring SPAN	Describes how to configure the Switched Port Analyzer (SPAN)
Chapter 33	Environmental Monitoring and Power Management	Describes how to configure environmental monitoring, power redundancy, and inline power features
Chapter 34	Configuring Supervisor Engine Redundancy on the Catalyst 4507R Switch	Describes how to configure RPR on the Catalyst 4507R
Chapter 35	Configuring Voice Interfaces	Describes how to configure multi-VLAN access ports for use with Cisco IP phones
Appendix A	Acronyms	Defines acronyms used in this book

Related Documentation

The following publications are available for the Catalyst 4000 family and Catalyst 4500 series switches:

- *Catalyst 4000 Series Switch Cisco IOS Installation Guide*
- *Catalyst 4500 Series Switch Cisco IOS Installation Guide*
- *Catalyst 4500 Series Switch Cisco IOS Module Installation Guide*
- *Catalyst 4500 Series Switch Cisco IOS Command Reference*
- *Catalyst 4500 Series Switch Cisco IOS System Message Guide*
- Release Notes for the Catalyst 4500 Series
- Cisco IOS configuration guides and command references—Use these publications to help you configure Cisco IOS software features not described in the preceding publications:
 - *Configuration Fundamentals Configuration Guide*
 - *Configuration Fundamentals Command Reference*
 - *Interface Configuration Guide*
 - *Interface Command Reference*
 - *Network Protocols Configuration Guide*, Part 1, 2, and 3
 - *Network Protocols Command Reference*, Part 1, 2, and 3
 - *Security Configuration Guide*
 - *Security Command Reference*
 - *Switching Services Configuration Guide*
 - *Switching Services Command Reference*
 - *Voice, Video, and Fax Applications Configuration Guide*
 - *Voice, Video, and Fax Applications Command Reference*
 - *Cisco IOS IP Configuration Guide*
 - *Cisco IOS IP Command Reference*

The Cisco IOS configuration guides and command references are at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/index.htm>

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

Conventions

This document uses the following typographical conventions:

Convention	Description
boldface font	Commands, command options, and keywords are in boldface .
<i>italic</i> font	Command arguments for which you supply values are in <i>italics</i> .
[]	Command elements in square brackets are optional.
{ x y z }	Alternative keywords in command lines are grouped in braces and separated by vertical bars.
[x y z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string because the string will include the quotation marks.
screen font	System displays are in screen font.
boldface screen font	Information you must enter verbatim is in boldface screen font.
<i>italic screen</i> font	Arguments for which you supply values are in <i>italic screen</i> font.
→	This pointer highlights an important line of text in an example.
^	Represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters such as passwords are in angle brackets.

Notes use the following conventions:



Note

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

Cautions use the following conventions:



Caution

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

Commands in Task Tables

Commands listed in task tables show only the relevant information for completing the task and not all available options for the command. For a complete description of a command, please refer to the command in the *Catalyst 4500 Series Switch Cisco IOS Command Reference*.

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco websites can be accessed from this URL:

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

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order monthly or quarterly subscriptions through the online Subscription Store:

<http://www.cisco.com/go/subscription>

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products Marketplace:
<http://www.cisco.com/en/US/partner/ordering/index.shtml>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can e-mail your comments to bug-doc@cisco.com.

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

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

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

To obtain customized information and service, you can self-register on Cisco.com at this URL:

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

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The type of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration. There is little or no impact to your business operations.
- Priority level 3 (P3)—Operational performance of the network is impaired, but most business operations remain functional. You and Cisco are willing to commit resources during normal business hours to restore service to satisfactory levels.

- Priority level 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively impacted by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.
- Priority level 1 (P1)—An existing network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Cisco TAC Website

The Cisco TAC website provides online documents and tools to help troubleshoot and resolve technical issues with Cisco products and technologies. To access the Cisco TAC website, go to this URL:

<http://www.cisco.com/tac>

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC website. Some services on the Cisco TAC website require a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

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

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

<http://www.cisco.com/tac/caseopen>

If you have Internet access, we recommend that you open P3 and P4 cases online so that you can fully describe the situation and attach any necessary files.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

Before calling, please check with your network operations center to determine the Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

Obtaining Additional Publications and Information

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

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:

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

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary*, *Internetworking Technology Handbook*, *Internetworking Troubleshooting Guide*, and the *Internetworking Design Guide*. For current Cisco Press titles and other information, go to Cisco Press online at this URL:
<http://www.ciscopress.com>
- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access *Packet* magazine at this URL:
<http://www.cisco.com/go/packet>
- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:
<http://www.cisco.com/go/iqmagazine>
- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:
http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html
- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:
http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html



Product Overview

This chapter provides an overview of Catalyst 4500 series switches and includes the following major sections:

- Layer 2 Software Features, page 1-1
- Layer 3 Software Features, page 1-5
- QoS Features, page 1-9
- Management and Security Features, page 1-10



Note

For more information about the chassis, modules, and software features supported by the Catalyst 4500 series switch, refer to the *Release Notes for the Catalyst 4500 Series Switch, 12.1(19)EW* at <http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4500/relnotes/>

Layer 2 Software Features

The following subsections describe the key Layer 2 switching software features on the Catalyst 4500 series switch:

- Storm Control, page 1-2
- CDP, page 1-2
- DHCP Snooping, page 1-2
- EtherChannel Bundles, page 1-2
- IP Source Guard, page 1-3
- Jumbo Frames, page 1-3
- Layer 2 Traceroute, page 1-3
- MST, page 1-3
- PVRST+, page 1-3
- Spanning Tree Protocol, page 1-4
- UDLD, page 1-4
- Unidirectional Ethernet, page 1-4
- VLANs, page 1-4

Storm Control

Broadcast suppression is used to prevent LANs from being disrupted by a broadcast storm on one or more switch ports. A LAN broadcast storm occurs when broadcast packets flood the LAN, creating excessive traffic and degrading network performance. Errors in the protocol-stack implementation or in the network configuration can cause a broadcast storm. Broadcast suppression measures how much broadcast traffic is passing through a port and compares the broadcast traffic with some configurable threshold value within a specific time interval. If the amount of broadcast traffic reaches the threshold during this interval, broadcast frames are dropped, and optionally the port is shut down.

For information on configuring broadcast suppression, see Chapter 28, “Configuring Port-Based Traffic Control.”

CDP

The Cisco Discovery Protocol (CDP) is a device-discovery protocol that is both media- and protocol-independent. CDP is available on all Cisco products, including routers, switches, bridges, and access servers. Using CDP, a device can advertise its existence to other devices and receive information about other devices on the same LAN. CDP enables Cisco switches and routers to exchange information, such as their MAC addresses, IP addresses, and outgoing interfaces. CDP runs over the data-link layer only, allowing two systems that support different network-layer protocols to learn about each other. Each device configured for CDP sends periodic messages to a multicast address. Each device advertises at least one address at which it can receive Simple Network Management Protocol (SNMP) messages.

For information on configuring CDP, see Chapter 16, “Understanding and Configuring CDP.”

DHCP Snooping

Dynamic Host Configuration Protocol (DHCP) snooping is a security feature that is a component of a DHCP server. DHCP snooping provides security by intercepting untrusted DHCP messages and by building and maintaining a DHCP snooping binding table. An untrusted message is a message that is received from outside the network or firewall that can cause traffic attacks within your network.

DHCP snooping acts like a firewall between untrusted hosts and DHCP servers. It also provides a way to differentiate between untrusted interfaces connected to the end-user and trusted interfaces connected to the DHCP server or another switch.

For DHCP server configuration information, refer to the chapter, “Configuring DHCP,” in the *Cisco IOS IP and IP Routing Configuration Guide* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgr/ip_c/ipcprt1/1cddhcp.htm

For information on configuring DHCP snooping, see Chapter 19, “Configuring DHCP Snooping and IP Source Guard.”

EtherChannel Bundles

EtherChannel port bundles allow you to create high-bandwidth connections between two switches by grouping multiple ports into a single logical transmission path.

For information on configuring EtherChannel, see Chapter 17, “Understanding and Configuring EtherChannel.”

IP Source Guard

Similar to DHCP snooping, this feature is enabled on an untrusted 12 port that is configured for DHCP snooping. Initially all IP traffic on the port is blocked except for the DHCP packets, which are captured by the DHCP snooping process. When a client receives a valid IP address from the DHCP server, a PVACL is installed on the port, which restricts the client IP traffic only to clients with assigned IP addresses; so any IP traffic with source IP addresses other than those assigned by the DHCP server will be filtered out. This filtering prevents a malicious host from attacking a network by hijacking neighbor host's IP address.

For information on configuring IP Source Guard, see Chapter 19, “Configuring DHCP Snooping and IP Source Guard.”

Jumbo Frames

The jumbo frames feature allows the switch to forward packets as large as 9216 bytes (larger than the IEEE Ethernet MTU), rather than declare those frames “oversize” and discard them. This feature is typically used for large data transfers. The jumbo feature can be configured on a per-port basis on Layer 2 and Layer 3 interfaces and is supported only on non-blocking GB front ports.

For information on Jumbo Frames, see Chapter 4, “Configuring Interfaces.”

Layer 2 Traceroute

The Layer 2 traceroute feature allows the switch to identify the physical path that a packet takes from a source device to a destination device. Layer 2 traceroute supports only unicast source and destination MAC addresses.

For information about Layer 2 Traceroute, see Chapter 5, “Checking Port Status and Connectivity.”

MST

IEEE 802.1s Multiple Spanning Tree (MST) allows for multiple spanning tree instantiations within a single 802.1q or Inter-Switch Link (ISL) VLAN trunk. MST extends the IEEE 802.1w Rapid Spanning Tree (RST) algorithm to multiple spanning trees. This extension provides both rapid convergence and load balancing in a VLAN environment.

MST allows you to build multiple spanning trees over trunks. You can group and associate VLANs to spanning tree instances. Each instance can have a topology independent of other spanning tree instances. This new architecture provides multiple forwarding paths for data traffic and enables load balancing. Network fault tolerance is improved because a failure in one instance (forwarding path) does not affect other instances (forwarding paths).

For information on configuring MST, see Chapter 14, “Understanding and Configuring Multiple Spanning Trees.”

PVRST+

Per-VLAN Rapid Spanning Tree (PVRST+) is the implementation of 802.1w on a per-VLAN basis. It is the same as PVST+ with respect to STP mode and runs RSTP protocol based on 802.1w.

For information on configuring PVRST+, see Chapter 12, “Understanding and Configuring STP.”

Spanning Tree Protocol

The Spanning Tree Protocol (STP) allows you to create fault-tolerant internetworks that ensure an active, loop-free data path between all nodes in the network. STP uses an algorithm to calculate the best loop-free path throughout a switched network.

For information on configuring STP, see Chapter 12, “Understanding and Configuring STP.”

The Catalyst 4500 series switch supports the following STP enhancements:

- Spanning tree PortFast—PortFast allows a port with a directly attached host to transition to the forwarding state directly, bypassing the listening and learning states.
- Spanning tree UplinkFast—UplinkFast provides fast convergence after a spanning-tree topology change and achieves load balancing between redundant links using uplink groups. Uplink groups provide an alternate path in case the currently forwarding link fails. UplinkFast is designed to decrease spanning-tree convergence time for switches that experience a direct link failure.
- Spanning tree BackboneFast—BackboneFast reduces the time needed for the spanning tree to converge after a topology change caused by an indirect link failure. BackboneFast decreases spanning-tree convergence time for any switch that experiences an indirect link failure.
- Spanning tree root guard—Root guard forces a port to become a designated port so that no switch on the other end of the link can become a root switch.

For information on the STP enhancements, see Chapter 13, “Configuring STP Features.”

UDLD

The UniDirectional Link Detection (UDLD) protocol allows devices connected through fiber-optic or copper Ethernet cables to monitor the physical configuration of the cables and detect a unidirectional link.

For information about UDLD, see Chapter 18, “Configuring UDLD.”

Unidirectional Ethernet

Unidirectional Ethernet uses only one strand of fiber for either transmitting or receiving one-way traffic for the Gigaport, instead of two strands of fiber for a full-duplex Gigaport Ethernet.

For information about Unidirectional Ethernet, see Chapter 7, “Configuring Unidirectional Ethernet.”

VLANs

A VLAN configures switches and routers according to logical, rather than physical, topologies. Using VLANs, a network administrator can combine any collection of LAN segments within an internetwork into an autonomous user group, such that the segments appear as a single LAN in the network. VLANs logically segment the network into different broadcast domains so that packets are switched only between ports within the VLAN. Typically, a VLAN corresponds to a particular subnet, although not necessarily.

For more information about VLANs, see Chapter 8, “Understanding and Configuring VLANs.”

The following VLAN-related features are also supported.

- **VLAN Trunking Protocol (VTP)**—VTP maintains VLAN naming consistency and connectivity between all devices in the VTP management domain. You can have redundancy in a domain by using multiple VTP servers, through which you can maintain and modify the global VLAN information. Only a few VTP servers are required in a large network.

For more information about VTP, see Chapter 11, “Understanding and Configuring VTP.”

- **Private VLANs**—Private VLANs are sets of ports that have the features of normal VLANs and also provide some Layer 2 isolation from other ports on the switch.

For information about private VLANs, see Chapter 10, “Configuring Private VLANs.”

- **Private VLAN Trunk Ports**—Private VLAN trunk ports allow a secondary port on a private VLAN to carry multiple secondary VLANs.
- **Dynamic VLAN Membership**—Dynamic VLAN Membership allows you to assign switch ports to VLANs dynamically, based on the source Media Access Control (MAC) address of the device connected to the port. When you move a host from a port on one switch in the network to a port on another switch in the network, that switch dynamically assigns the new port to the proper VLAN for that host.

For more information about Dynamic VLAN Membership, see Chapter 9, “Configuring Dynamic VLAN Membership.”

Layer 3 Software Features

A Layer 3 switch is a high-performance switch that has been optimized for a campus LAN or intranet and that provides both wirespeed Ethernet routing and switching services. Layer 3 switching improves network performance with two software functions—route processing and intelligent network services.

Compared to conventional software-based switches, Layer 3 switches process more packets faster; they do so by using application-specific integrated circuit (ASIC) hardware instead of microprocessor-based engines.

The following subsections describe the key Layer 3 switching software features on the Catalyst 4000 family switch:

- CEF, page 1-6
- HSRP, page 1-6
- IP Routing Protocols, page 1-6
- Multicast Services, page 1-8
- Network Security with ACLs, page 1-8
- Policy-Based Routing, page 1-9
- Unidirectional Link Routing, page 1-9

CEF

Cisco Express Forwarding (CEF) is an advanced Layer 3 IP-switching technology. CEF optimizes network performance and scalability in networks with large and dynamic traffic patterns, such as the Internet, and on networks that use intensive web-based applications, or interactive sessions. Although you can use CEF in any part of a network, it is designed for high-performance, highly resilient Layer 3 IP-backbone switching.

For information on configuring CEF, see Chapter 21, “Configuring Cisco Express Forwarding.”

HSRP

The Hot Standby Router Protocol (HSRP) provides high network availability by routing IP traffic from hosts on Ethernet networks without relying on the availability of any single Layer 3 switch. This feature is particularly useful for hosts that do not support a router discovery protocol and do not have the functionality to switch to a new router when their selected router reloads or loses power.

For information on configuring HSRP, refer to the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cger/ip_c/ipcprt1/1cdip.htm

IP Routing Protocols

The following routing protocols are supported on the Catalyst 4000 family switch:

- RIP
- OSPF
- IS-IS
- IGRP
- EIGRP
- BGP

RIP

The Routing Information Protocol (RIP) is a distance-vector, intradomain routing protocol. RIP works well in small, homogeneous networks. In large, complex internetworks, it has many limitations, such as a maximum hop count of 15, lack of support for variable-length subnet masks (VLSMs), inefficient use of bandwidth, and slow convergence. (RIP II does support VLSMs.)

OSPF

The Open Shortest Path First (OSPF) protocol is a standards-based IP routing protocol designed to overcome the limitations of RIP. Because OSPF is a link-state routing protocol, it sends link-state advertisements (LSAs) to all other routers within the same hierarchical area. Information on the attached interfaces and their metrics is used in OSPF LSAs. As routers accumulate link-state information, they use the shortest path first (SPF) algorithm to calculate the shortest path to each node. Additional OSPF features include equal-cost multipath routing and routing based on the upper-layer type of service (ToS) requests.

OSPF employs the concept of an area, which is a group of contiguous OSPF networks and hosts. OSPF areas are logical subdivisions of OSPF autonomous systems in which the internal topology is hidden from routers outside the area. Areas allow an additional level of hierarchy different from that provided by IP network classes, and they can be used to aggregate routing information and mask the details of a network. These features make OSPF particularly scalable for large networks.

IS-IS

The IS-IS protocol uses a link-state routing algorithm. It closely follows the Open Shortest Path First (OSPF) routing protocol used within the TCP/IP environment. The operation of ISO IS-IS requires each router to maintain a full topology map of the network (that is, which ISs and ESs are connected to which other ISs and ESs). Periodically, the router runs an algorithm over its map to calculate the shortest path to all possible destinations.

IS-IS is a two-level hierarchy. Intermediate Systems (or routers) are classified as Level 1 and Level 2. Level 1 ISs deal with a single routing area. Traffic is relayed only within their area. Any other internetwork traffic is sent to nearest Level 2 ISs, which also acts as a Level 1 ISs. Level 2 ISs move traffic between different routing areas within the same domain.

An IS-IS with multiarea support allows multiple Level 1 areas within in a single IS, thus allowing an IS to be in multiple areas. A single Level 2 area is used as backbone for interarea traffic.

Only Ethernet frames are supported. The IS-IS does not support IPX.

IGRP

The Interior Gateway Routing Protocol (IGRP) is a robust distance-vector Interior Gateway Protocol (IGP) developed by Cisco to provide for routing within an autonomous system (AS). Distance vector routing protocols request that a switch send all or a portion of its routing table data in a routing update message at regular intervals to each of its neighboring routers. As routing information proliferates through the network, routers can calculate distances to all nodes within the internetwork. IGRP uses a combination of metrics: internetwork delay, bandwidth, reliability, and load are all factored into the routing decision.

EIGRP

The Enhanced Interior Gateway Routing Protocol (EIGRP) is a version of IGRP that combines the advantages of link-state protocols with distance-vector protocols. EIGRP incorporates the Diffusing Update Algorithm (DUAL). EIGRP includes fast convergence, variable-length subnet masks, partially bounded updates, and multiple network-layer support. When a network topology change occurs, EIGRP checks its topology table for a suitable new route to the destination. If such a route exists in the table, EIGRP updates the routing table instantly. You can use the fast convergence and partial updates that EIGRP provides to route Internetwork Packet Exchange (IPX) packets.

EIGRP saves bandwidth by sending routing updates only when routing information changes. The updates contain information only about the link that changed, not the entire routing table. EIGRP also takes into consideration the available bandwidth when determining the rate at which it transmits updates.



Note

Layer 3 switching does not support the Next Hop Resolution Protocol (NHRP).

BGP

The Border Gateway Protocol (BGP) is an exterior gateway protocol that allows you to set up an interdomain routing system to automatically guarantee the loop-free exchange of routing information between autonomous systems. In BGP, each route consists of a network number, a list of autonomous systems that information has passed through (called the autonomous system path), and a list of other path attributes.

The Catalyst 4500 series switch supports BGP version 4, including classless interdomain routing (CIDR). CIDR lets you reduce the size of your routing tables by creating aggregate routes, resulting in supernets. CIDR eliminates the concept of network classes within BGP and supports the advertising of IP prefixes. CIDR routes can be carried by OSPF, EIGRP, and RIP.

For BGP configuration information, refer to the chapter “Configuring BGP” in the *Cisco IOS IP and IP Routing Configuration Guide* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_c/ipcprt2/1cdbgp.htm

For a complete description of the BGP commands, refer to the chapter “BGP Commands” in the *Cisco IOS IP and IP Routing Command Reference* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_r/iprprt2/1rdbgp.htm

Multicast Services

Multicast services save bandwidth by forcing the network to replicate packets only when necessary and by allowing hosts to join and leave groups dynamically. The following multicast services are supported:

- Cisco Group Management Protocol (CGMP) server—CGMP server manages multicast traffic. Multicast traffic is forwarded only to ports with attached hosts that request the multicast traffic.
- Internet Group Management Protocol (IGMP) snooping—IGMP snooping manages multicast traffic. The switch software examines IP multicast packets and makes forwarding decisions based on their content. Multicast traffic is forwarded only to ports with attached hosts that request multicast traffic. Support for IGMPv3 allows a user to establish a reporting interest in a specific channel rather than just a multicast group.
- Protocol Independent Multicast (PIM)—PIM is protocol-independent because it can leverage whichever unicast routing protocol is used to populate the unicast routing table, including EIGRP, OSPF, BGP, or static route. PIM also uses a unicast routing table to perform the Reverse Path Forwarding (RPF) check function instead of building a completely independent multicast routing table.

For information on configuring multicast services, see Chapter 23, “Understanding and Configuring IP Multicast.”

Network Security with ACLs

An access control list (ACL) filters network traffic by controlling whether routed packets are forwarded or blocked at the router interfaces. The Catalyst 4000 family switch examines each packet to determine whether to forward or drop the packet, based on the criteria you specified within the access lists.

MAC access control lists (MACLS) and VLAN access control lists (VACLs) are supported. VACLs are also known as VLAN maps in Cisco IOS.

The following security features are supported:

- MAC address filtering, which enables you to block unicast traffic for a MAC address on a VLAN interface.
- Port ACLs, which enable you to apply ACLs to Layer 2 interfaces on a switch for inbound traffic.

For information on ACLs, MACs, VLAN maps, MAC address filtering, and Port ACLs, see Chapter 24, “Configuring Network Security with ACLs.”

Policy-Based Routing

Traditional IP forwarding decisions are based purely on the destination IP address of the packet being forwarded. Policy Based Routing (PBR) enables forwarding based upon other information associated with a packet, such as the source interface, IP source address, Layer 4 ports, etc. This feature allows network managers more flexibility in how they configure and design their networks.

For more information on policy-based routing, see Chapter 22, “Configuring Policy-Based Routing.”

Unidirectional Link Routing

Unidirectional link routing (UDLR) provides a way to forward multicast packets over a physical unidirectional interface (such as a satellite link of high bandwidth) to stub networks that have a back channel.

For information on configuring unidirectional link routing, refer to the chapter “Configuring Unidirectional Link Routing” in the *Cisco IP and IP Routing Configuration Guide*.

QoS Features

The quality of service (QoS) features prevent congestion by selecting network traffic and prioritizing it according to its relative importance. Implementing QoS in your network makes network performance more predictable and bandwidth use more effective.

The Catalyst 4500 series switch supports the following QoS features:

- Classification and marking
- Ingress and egress policing
- Sharing and shaping

Catalyst 4500 series switch supports trusted boundary, which uses the Cisco Discovery Protocol (CDP) to detect the presence of a Cisco IP phone (such as the Cisco IP Phone 7910, 7935, 7940, and 7960) on a switch port. If the telephone is not detected, the trusted boundary feature disables the trusted setting on the switch port and prevents misuse of a high-priority queue.

The Catalyst 4500 series switch also supports QoS Automation (Auto QoS), which simplifies the deployment of existing QoS features via automatic configuration.

For information on QoS and Auto QoS, see Chapter 29, “Configuring QoS.”

Management and Security Features

The Catalyst 4500 series switch offers network management and control through the CLI or through alternative access methods, such as SNMP. The switch software supports these network management and security features:

- 802.1x protocol—This feature provides a means for a host connected to a switch port to be authenticated before it is given access to the switch services.
- 802.1x with VLAN assignment—This feature allows you to enable non-802.1x capable hosts to access networks that use 802.1x authentication.
- 802.1x authentication for guest VLANs—This feature allows you to use VLAN assignment to limit network access for certain users.
- Dynamic ARP inspection—This feature intercepts all ARP requests, replies on untrusted ports, and verifies each intercepted packet for valid IP to MAC bindings. Dynamic ARP Inspection helps to prevent attacks on a network by not relaying invalid ARP replies out to other ports in the same VLAN. Denied ARP packets are logged by the switch for auditing.
- Password-protected access (read-only and read-write)—This feature protects management interfaces against unauthorized configuration changes.
- Flood Blocking— This feature enables users to disable the flooding of unicast and multicast packets on a per-port basis. Occasionally, unknown unicast or multicast traffic from an unprotected port is flooded to a protected port because a MAC address has timed out or has not been learned by the switch.
- Port Security—This feature restricts traffic on a port based upon the MAC address of the workstation that accesses the port.
- Local Authentication, Remote Authentication Dial-In User Service (RADIUS), and Terminal Access Controller Access Control System Plus (TACACS+) authentication—These authentication methods control access to the switch. For additional information, refer to the chapter “Authentication, Authorization, and Accounting (AAA),” in *Cisco IOS Security Configuration Guide*, Release 12.1, at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cger/secur_c/scprt1/index.htm
- Visual port status information—The switch LEDs provide visual management of port- and switch-level status.
- Secure Shell—Secure Shell (SSH) is a program that enables you to log into another computer over a network, to execute commands remotely, and to move files from one machine to another. The implementation will be limited to providing a remote login session to the switch, and will only function as a server; that is, the switch may not initiate SSH connections.
- NetFlow statistics—This feature is a global traffic monitoring feature that allows flow-level monitoring of all IPv4-routed traffic through the switch.
- Switched Port Analyzer (SPAN)—SPAN allows you to monitor traffic on any port for analysis by a network analyzer or Remote Monitoring (RMON) probe. You also can do the following:
 - Allow incoming traffic on SPAN destination ports to be switched normally.
 - Explicitly configure the encapsulation type of packets that are spanned out of a destination port.
 - Restrict ingress sniffing depending on whether the packet is unicast, multicast, or broadcast, and depending on whether the packet is valid.
 - For troubleshooting purposes, mirror packets sent to or from the CPU out of a SPAN destination port.

For information on SPAN, see Chapter 32, “Configuring SPAN.”

- Simple Network Management Protocol—SNMP facilitates the exchange of management information between network devices. The Catalyst 4500 series switch supports these SNMP types and enhancements:
 - SNMP—A full Internet standard
 - SNMP v2—Community-based administrative framework for version 2 of SNMP
 - SNMP trap message enhancements—Additional information with certain SNMP trap messages, including spanning-tree topology change notifications and configuration change notifications

For information on SNMP, refer to the *Cisco IOS Configuration Fundamentals Configuration Guide* and *Cisco IOS Configuration Fundamentals Command Reference* at the following URL:
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/index.htm>

- Dynamic Host Control Protocol server—DHCP server enables you to automatically assign reusable IP addresses to DHCP clients. The Cisco IOS DHCP server feature is a full DHCP server implementation that assigns and manages IP addresses from specified address pools within the router to DHCP clients. If the Cisco IOS DHCP server cannot satisfy a DHCP request from its own database, it can forward the request to one or more secondary DHCP servers defined by the network administrator.

For more information on configuring the DHCP server, refer to the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t1/easyip2.htm>

- Debugging features—The Catalyst 4500 series switch has several commands to help you debug your initial setup. These commands include the following groups:
 - **platform**
 - **debug platform**

For more information on these commands, refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference*.



Command-Line Interfaces

This chapter describes the CLIs you use to configure the Catalyst 4500 series switch. This chapter includes the following major sections:

- Accessing the Switch CLI, page 2-1
- Performing Command-Line Processing, page 2-3
- Performing History Substitution, page 2-3
- Understanding Cisco IOS Command Modes, page 2-4
- Getting a List of Commands and Syntax, page 2-5
- ROMMON Command-Line Interface, page 2-6



Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference* and related publications at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/index.htm>

Accessing the Switch CLI

The following sections describe how to access the switch CLI:

- Accessing the CLI Using the EIA/TIA-232 Console Interface, page 2-1
- Accessing the CLI Through Telnet, page 2-2

Accessing the CLI Using the EIA/TIA-232 Console Interface



Note

EIA/TIA-232 was known as recommended standard 232 (RS-232) before its acceptance as a standard by the Electronic Industries Alliance (EIA) and Telecommunications Industry Association (TIA).

Perform the initial switch configuration over a connection to the EIA/TIA-232 console interface. Refer to the *Catalyst 4500 Series Switch Module Installation Guide* for console interface cable connection procedures.

To access the switch through the console interface, perform this task:

	Command	Purpose
Step 1	Switch> enable	From the user EXEC prompt (>), enter enable to change to enable mode (also known as privileged mode or privileged EXEC mode).
Step 2	Password: <i>password</i> Switch#	At the password prompt, enter the system password. The prompt (#) appears, indicating that you have accessed the CLI in enabled mode.
Step 3	Switch# quit	When you are finished executing the task command, exit the session.

After accessing the switch through the EIA/TIA-232 interface, you see this display:

Press Return for Console prompt

```
Switch> enable
Password:< >
Switch#
```

Accessing the CLI Through Telnet



Note

Before you make a Telnet connection to the switch, you must set the IP address for the switch. See the “Configuring Physical Layer 3 Interfaces” section on page 20-4.

The switch supports up to eight simultaneous Telnet sessions. Telnet sessions disconnect automatically after remaining idle for the period specified by the **exec-timeout** command.

To make a Telnet connection to the switch, perform this task:

	Command	Purpose
Step 1	telnet { <i>hostname</i> <i>ip_addr</i> }	From the remote host, enter the telnet command and the name or IP address of the switch you want to access.
Step 2	Password: <i>password</i> Switch#	At the prompt, enter the password for the CLI. If no password has been configured, press Return .
Step 3		Enter the necessary commands to complete your desired tasks.
Step 4	Switch# quit	When finished, exit the Telnet session.

This example shows how to open a Telnet session to the switch:

```
unix_host% telnet Switch_1
Trying 172.20.52.40...
Connected to 172.20.52.40.
Escape character is '^]'.
User Access Verification
Password:< >
Switch_1> enable
Password:
Switch_1#
```

Performing Command-Line Processing

Switch commands are not case sensitive. You can abbreviate commands and parameters if the abbreviations contain enough letters to be different from any other currently available commands or parameters.

You can scroll through the last 20 commands stored in the history buffer and enter or edit a command at the prompt. Table 2-1 lists the keyboard shortcuts for entering and editing switch commands.

Table 2-1 Keyboard Shortcuts

Keystrokes	Result
Press Ctrl-B or press the Left Arrow key ¹	Moves the cursor back one character.
Press Ctrl-F or press the Right Arrow key ¹	Moves the cursor forward one character.
Press Ctrl-A	Moves the cursor to the beginning of the command line.
Press Ctrl-E	Moves the cursor to the end of the command line.
Press Esc-B	Moves the cursor back one word.
Press Esc-F	Moves the cursor forward one word.

1. The Arrow keys function only on ANSI-compatible terminals, such as VT100s.

Performing History Substitution

The history buffer stores the last 20 command lines you entered. History substitution allows you to access these command lines without retyping them. Table 2-2 lists the history substitution commands.

Table 2-2 History Substitution Commands

Command	Purpose
Ctrl-P or the Up Arrow key ¹	Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall older commands successively.

Table 2-2 History Substitution Commands (continued)

Command	Purpose
Ctrl-N or the Down Arrow key ¹	Returns to more recent commands in the history buffer after commands have been recalled with Ctrl-P or the Up Arrow key. Repeat the key sequence to recall more recent commands.
Switch# show history	Lists the last several commands you have entered in EXEC mode.

1. The Arrow keys function only on ANSI-compatible terminals such as VT100s.

Understanding Cisco IOS Command Modes



Note

For complete information about Cisco IOS command modes, refer to the *Cisco IOS Configuration Fundamentals Configuration Guide* and the *Cisco IOS Configuration Fundamentals Command Reference* at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/index.htm>

The Cisco IOS user interface has many different modes: user EXEC, privileged EXEC (enable), global configuration, interface, subinterface, and protocol-specific. The commands available to you depend on which mode you are in. To get a list of the commands in a given mode, enter a question mark (?) at the system prompt. See the “Getting a List of Commands and Syntax” section on page 2-5 for more information.

When you start a session on the switch, you begin in user mode, also called user EXEC mode. Only a small subset of commands are available in EXEC mode. To have access to all commands, you must enter privileged EXEC mode, also called enable mode. To access the privileged EXEC mode, you must enter a password. When you are in the privileged EXEC mode, you can enter any EXEC command or access global configuration mode. Most EXEC commands are one-time commands, such as **show** commands, which display the current configuration status, and **clear** commands, which reset counters or interfaces. The EXEC commands are not saved when the switch is rebooted.

The configuration modes allow you to make changes to the running configuration. If you save the configuration, these commands are stored when you reboot the switch. You must start in global configuration mode. From global configuration mode, you can enter interface configuration mode, subinterface configuration mode, and a variety of protocol-specific modes.

You would use a separate mode called ROMMON when the switch cannot boot up properly. For example, the switch might enter ROMMON mode if it does not find a valid system image when it is booting, or if its configuration file is corrupted. For more information, see the “ROMMOM Command-Line Interface” section on page 2-6.

Table 2-3 lists and describes frequently used Cisco IOS modes.

Table 2-3 Frequently Used Cisco IOS Command Modes

Mode	What You Use It For	How to Access	Prompt
User EXEC	To connect to remote devices, change terminal settings on a temporary basis, perform basic tests, and display system information.	Log in.	Switch>
Privileged EXEC (enable)	To set operating parameters. The privileged command set includes the commands in user EXEC mode, as well as the configure command. Use the configure command to access the other command modes.	From user EXEC mode, enter the enable command and the enable password (if a password has been configured).	Switch#
Global configuration	To configure features that affect the system as a whole, such as the system time or switch name.	From privileged EXEC mode, enter the configure terminal command.	Switch(config)#
Interface configuration	To enable or modify the operation of a Gigabit Ethernet or Fast Ethernet interface with interface commands.	From global configuration mode, enter the interface <i>type location</i> command.	Switch(config-if)#
Console configuration	To configure the console interface; from the directly connected console or the virtual terminal; used with Telnet.	From global configuration mode, enter the line console 0 command.	Switch(config-line)#

The Cisco IOS command interpreter, called the EXEC, interprets and runs the commands you enter. You can abbreviate commands and keywords by entering just enough characters to make the command unique from other commands. For example, you can abbreviate the **show** command to **sh** and the **configure terminal** command to **conf t**.

When you type **exit**, the switch backs out one level. To exit configuration mode completely and return to privileged EXEC mode, press **Ctrl-Z**.

Getting a List of Commands and Syntax

In any command mode, you can get a list of available commands by entering a question mark (?).

```
Switch> ?
```

To obtain a list of commands that begin with a particular character sequence, enter those characters followed by the question mark (?). Do not include a space before the question mark. This form of help is called word help, because it completes a word for you.

To list keywords or arguments, enter a question mark in place of a keyword or argument. Include a space before the question mark. This form of help is called command syntax help, because it reminds you which keywords or arguments are applicable based on the command, keywords, and arguments you have already entered.

```
Switch# configure ?
memory          Configure from NV memory
network          Configure from a TFTP network host
overwrite-network Overwrite NV memory from TFTP network host
terminal         Configure from the terminal
<cr>
```

To redisplay a command you previously entered, press the **Up Arrow** key or **Ctrl-P**. You can continue to press the **Up Arrow** key to see the last 20 commands you entered.

**Tip**

If you are having trouble entering a command, check the system prompt and enter the question mark (?) for a list of available commands. You might be in the wrong command mode or using incorrect syntax.

Type **exit** to return to the previous mode. Press **Ctrl-Z** or enter the **end** command in any mode to immediately return to privileged EXEC mode.

ROMMON Command-Line Interface

ROMMON is a ROM-based program that is involved at power-up or reset, or when a fatal exception error occurs. The switch enters ROMMON mode if the switch does not find a valid software image, if the NVRAM configuration is corrupted, or if the configuration register is set to enter ROMMON mode. From the ROMMON mode, you can load a software image manually from Flash memory, from a network server file, or from bootflash.

You can also enter ROMMON mode by restarting the switch and pressing **Ctrl-C** during the first five seconds of startup.

**Note**

Ctrl-C is always enabled for 60 seconds after you reboot the switch, even if **Ctrl-C** is configured to be off in the configuration register settings.

When you enter ROMMON mode, the prompt changes to **rommon 1>**. Use the **?** command to see the available ROMMON commands.

For more information about the ROMMON commands, see *Catalyst 4500 Series Switch Cisco IOS Command Reference*.



Configuring the Switch for the First Time

This chapter describes how to initially configure a Catalyst 4500 series switch. The information presented here supplements the administration information and procedures in these publications:

- *Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.1, at this URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/fun_c/index.htm
- *Cisco IOS Configuration Fundamentals Configuration Command Reference*, Release 12.1, at this URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/fun_r/index.htm

This chapter includes the following major sections:

- Default Switch Configuration, page 3-1
- Configuring the Switch, page 3-2
- Controlling Access to Privileged EXEC Commands, page 3-7
- Recovering a Lost Enable Password, page 3-12
- Modifying the Supervisor Engine Startup Configuration, page 3-12



Note

For complete syntax and usage information for the switch commands used in this chapter, refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference* and related publications at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/index.htm>

Default Switch Configuration

This section describes the default configurations for the Catalyst 4500 series switch. Table 3-1 shows the default configuration settings for each feature.

Table 3-1 Default Switch Configuration

Feature	Default Settings
Administrative connection	Normal mode
Global switch information	No default value for system name, system contact, and location
System clock	No value for system clock time
Passwords	No passwords are configured for normal mode or enable mode (press the Return key)

Table 3-1 Default Switch Configuration (continued)

Feature	Default Settings
Switch prompt	Switch>
Interfaces	Enabled, with speed and flow control autonegotiated, and without IP addresses

Configuring the Switch

The following sections describe how to configure your switch:

- Using Configuration Mode to Configure Your Switch, page 3-2
- Checking the Running Configuration Settings, page 3-3
- Saving the Running Configuration Settings to Your Start-up File, page 3-3
- Reviewing the Configuration in NVRAM, page 3-4
- Configuring a Default Gateway, page 3-4
- Configuring a Static Route, page 3-5

Using Configuration Mode to Configure Your Switch

To configure your switch from configuration mode, perform this procedure:

- Step 1** Connect a console terminal to the console interface of your supervisor engine.
- Step 2** After a few seconds, you will see the user EXEC prompt (Switch>). Now, you may want to enter privileged EXEC mode, also known as enable mode. Type **enable** to enter enable mode:
- ```
Switch> enable
```



**Note** You must be in enable mode to make configuration changes.

The prompt will change to the enable prompt (#):

```
Switch#
```

- Step 3** At the enable prompt (#), enter the **configure terminal** command to enter global configuration mode:
- ```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
```
- Step 4** At the global configuration mode prompt, enter the **interface type slot/interface** command to enter interface configuration mode:
- ```
Switch(config)# interface fastethernet 5/1
Switch(config-if)#
```
- Step 5** In either of these configuration modes, enter changes to the switch configuration.



- Step 6** Enter the **end** command to exit configuration mode.
- Step 7** Save your settings. (See the “Saving the Running Configuration Settings to Your Start-up File” section on page 3-3.)
- 

Your switch is now minimally configured and can boot with the configuration you entered. To see a list of the configuration commands, enter **?** at the prompt or press the **help** key in configuration mode.

## Checking the Running Configuration Settings

To verify the configuration settings you entered or the changes you made, enter the **show running-config** command at the enable prompt (**#**), as shown in this example:

```
Switch# show running-config
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Switch

<...output truncated...>

!
line con 0
 transport input none
line vty 0 4
 exec-timeout 0 0
 password lab
 login
 transport input lat pad dsipcon mop telnet rlogin udptn nasi
!
end
Switch#
```

## Saving the Running Configuration Settings to Your Start-up File



### Caution

This command saves the configuration settings that you created in configuration mode. If you fail to do this step, your configuration will be lost the next time you reload the system.

To store the configuration, changes to the configuration, or changes to the startup configuration in NVRAM, enter the **copy running-config startup-config** command at the enable prompt (**#**), as follows:

```
Switch# copy running-config startup-config
```

## Reviewing the Configuration in NVRAM

To display information stored in NVRAM, enter the **show startup-config** EXEC command.

The following example shows a typical system configuration:

```
Switch# show startup-config
Using 1579 out of 491500 bytes, uncompressed size = 7372 bytes
Uncompressed configuration from 1579 bytes to 7372 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service compress-config
!
hostname Switch
!
!
ip subnet-zero
!
!
!
interface GigabitEthernet1/1
 no snmp trap link-status
!
interface GigabitEthernet1/2
 no snmp trap link-status
!--More--

<...output truncated...>

!
line con 0
 exec-timeout 0 0
 transport input none
line vty 0 4
 exec-timeout 0 0
 password lab
 login
 transport input lat pad dsipcon mop telnet rlogin udptn nasi
!
end

Switch#
```

## Configuring a Default Gateway

**Note**

---

The switch uses the default gateway only when it is not configured with a routing protocol.

---

Configure a default gateway to send data to subnets other than its own when the switch is not configured with a routing protocol. The default gateway must be the IP address of an interface on a router that is directly connected to the switch.

To configure a default gateway, perform this task:

|        | Command                                                     | Purpose                                                                           |
|--------|-------------------------------------------------------------|-----------------------------------------------------------------------------------|
| Step 1 | Switch(config)# <b>ip default-gateway</b> <i>IP-address</i> | Configures a default gateway.                                                     |
| Step 2 | Switch# <b>show ip route</b>                                | Verifies that the default gateway is correctly displayed in the IP routing table. |

This example shows how to configure a default gateway and how to verify the configuration:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip default-gateway 172.20.52.35
Switch(config)# end
3d17h: %SYS-5-CONFIG_I: Configured from console by console
Switch# show ip route
Default gateway is 172.20.52.35

Host Gateway Last Use Total Uses Interface
ICMP redirect cache is empty
Switch#
```

## Configuring a Static Route

If your Telnet station or SNMP network management workstation is on a different network from your switch and a routing protocol has not been configured, you might need to add a static routing table entry for the network where your end station is located.

To configure a static route, perform this task:

|        | Command                                                                                    | Purpose                                                |
|--------|--------------------------------------------------------------------------------------------|--------------------------------------------------------|
| Step 1 | Switch(config)# <b>ip route</b> <i>dest_IP_address mask {forwarding_IP   vlan vlan_ID}</i> | Configures a static route to the remote network.       |
| Step 2 | Switch# <b>show running-config</b>                                                         | Verifies that the static route is displayed correctly. |

This example shows how to use the **ip route** command to configure a static route to a workstation at IP address 171.10.5.10 on the switch with a subnet mask and IP address 172.20.3.35 of the forwarding router:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip route 171.10.5.10 255.255.255.255 172.20.3.35
Switch(config)# end
Switch#
```

This example shows how to use the **show running-config** command to confirm the configuration of the static route:

```
Switch# show running-config
Building configuration...
.
<...output truncated...>
.
ip default-gateway 172.20.52.35
ip classless
ip route 171.10.5.10 255.255.255.255 172.20.3.35
no ip http server
!
line con 0
 transport input none
line vty 0 4
 exec-timeout 0 0
 password lab
 login
 transport input lat pad dsipcon mop telnet rlogin udptn nasi
!
end

Switch#
```

This example shows how to use the **ip route** command to configure the static route IP address 171.20.5.3 with subnet mask and connected over VLAN 1 to a workstation on the switch:

```
Switch# configure terminal
Switch(config)# ip route 171.20.5.3 255.255.255.255 vlan 1
Switch(config)# end
Switch#
```

This example shows how to use the **show running-config** command to confirm the configuration of the static route:

```
Switch# show running-config
Building configuration...
.
<...output truncated...>
.
ip default-gateway 172.20.52.35
ip classless
ip route 171.20.5.3 255.255.255.255 Vlan1
no ip http server
!
!
x25 host z
!
line con 0
 transport input none
line vty 0 4
 exec-timeout 0 0
 password lab
 login
 transport input lat pad dsipcon mop telnet rlogin udptn nasi
!
end

Switch#
```

# Controlling Access to Privileged EXEC Commands

The procedures in these sections let you control access to the system configuration file and privileged EXEC commands:

- Setting or Changing a Static enable Password, page 3-7
- Using the enable Password and enable secret Commands, page 3-7
- Setting or Changing a Privileged Password, page 3-8
- Setting TACACS+ Password Protection for Privileged EXEC Mode, page 3-8
- Encrypting Passwords, page 3-9
- Configuring Multiple Privilege Levels, page 3-10

## Setting or Changing a Static enable Password

To set or change a static password that controls access to the enable mode, perform this task:

| Command                                                | Purpose                                                                           |
|--------------------------------------------------------|-----------------------------------------------------------------------------------|
| Switch(config)# <b>enable password</b> <i>password</i> | Sets a new password or changes an existing password for the privileged EXEC mode. |

This example shows how to configure an enable password as “lab” at the privileged EXEC mode:

```
Switch# configure terminal
Switch(config)# enable password lab
Switch(config)#
```

For instructions on how to display the password or access level configuration, see the “Displaying the Password, Access Level, and Privilege Level Configuration” section on page 3-11.

## Using the enable Password and enable secret Commands

To provide an additional layer of security, particularly for passwords that cross the network or that are stored on a TFTP server, you can use either the **enable password** or **enable secret** commands. Both commands configure an encrypted password that you must enter to access the enable mode (the default) or any other privilege level that you specify.

We recommend that you use the **enable secret** command.

If you configure the **enable secret** command, it takes precedence over the **enable password** command; the two commands cannot be in effect simultaneously.

To configure the switch to require an enable password, perform either one of these tasks:

| Command                                                                                              | Purpose                                                                                                                                                                                                          |
|------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Switch(config)# <b>enable password</b> [level level] {password   encryption-type encrypted-password} | Establishes a password for the privileged EXEC mode.                                                                                                                                                             |
| Switch(config)# <b>enable secret</b> [level level] {password   encryption-type encrypted-password}   | Specifies a secret password that will be saved using a nonreversible encryption method. (If <b>enable password</b> and <b>enable secret</b> commands are both set, users must enter the enable secret password.) |

When you enter either of these password commands with the **level** option, you define a password for a specific privilege level. After you specify the level and set a password, give the password only to users who need to have access at this level. Use the **privilege level** configuration command to specify commands accessible at various levels.

If you enable the **service password-encryption** command, the password you enter is encrypted. When you display the password with the **more system:running-config** command, the password displays the password in encrypted form.

If you specify an encryption type, you must provide an encrypted password—an encrypted password you copy from another Catalyst 4500 series switch configuration.



#### Note

You cannot recover a lost encrypted password. You must clear NVRAM and set a new password. See the “Recovering a Lost Enable Password” section on page 3-12 for more information.

For information on how to display the password or access level configuration, see the “Displaying the Password, Access Level, and Privilege Level Configuration” section on page 3-11.

## Setting or Changing a Privileged Password

To set or change a privileged password, perform this task:

| Command                                       | Purpose                                                                       |
|-----------------------------------------------|-------------------------------------------------------------------------------|
| Switch(config-line)# <b>password</b> password | Sets a new password or changes an existing password for the privileged level. |

For information on how to display the password or access level configuration, see the “Displaying the Password, Access Level, and Privilege Level Configuration” section on page 3-11.

## Setting TACACS+ Password Protection for Privileged EXEC Mode

For complete information about TACACS+ and RADIUS, refer to these publications:

- The “Authentication, Authorization, and Accounting (AAA)” chapter in the *Cisco IOS Security Configuration Guide*, Release 12.1, at the following URL:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur\\_c/scprt1/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur_c/scprt1/index.htm)

- *Cisco IOS Security Command Reference*, Release 12.1, at the following URL:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur\\_r/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur_r/index.htm)

To set the TACACS+ protocol to determine whether a user can access privileged EXEC mode, perform this task:

| Command                                  | Purpose                                                                                     |
|------------------------------------------|---------------------------------------------------------------------------------------------|
| Switch(config)# <b>enable use-tacacs</b> | Sets the TACACS-style user ID and password-checking mechanism for the privileged EXEC mode. |

When you set TACACS password protection at the privileged EXEC mode, the **enable EXEC** command prompts you for a new username and a new password. This information is then passed to the TACACS+ server for authentication. If you are using the extended TACACS, another extension to the older TACACS protocol that provides additional functionality, it also passes any existing UNIX user identification code to the TACACS+ server.

An extension to the older TACACS protocol, supplying additional functionality to TACACS. Extended TACACS provides information about protocol translator and router use. This information is used in UNIX auditing trails and accounting files.

**Note**

When used without extended TACACS, the **enable use-tacacs** command allows anyone with a valid username and password to access the privileged EXEC mode, creating a potential security risk. This problem occurs because the query resulting from entering the **enable** command is indistinguishable from an attempt to log in without extended TACACS.

## Encrypting Passwords

Because protocol analyzers can examine packets (and read passwords), you can increase access security by configuring the Cisco IOS software to encrypt passwords. Encryption prevents the password from being readable in the configuration file.

To configure the Cisco IOS software to encrypt passwords, perform this task:

| Command                                            | Purpose              |
|----------------------------------------------------|----------------------|
| Switch(config)# <b>service password-encryption</b> | Encrypts a password. |

Encryption occurs when the current configuration is written or when a password is configured. Password encryption is applied to all passwords, including authentication key passwords, the privileged command password, console and virtual terminal line access passwords, and Border Gateway Protocol (BGP) neighbor passwords. The **service password-encryption** command keeps unauthorized individuals from viewing your password in your configuration file.

**Caution**

The **service password-encryption** command does not provide a high level of network security. If you use this command, you should also take additional network security measures.

Although you cannot recover a lost encrypted password (that is, you cannot get the original password back), you can regain control of the switch after having lost or forgotten the encrypted password. See the “Recovering a Lost Enable Password” section on page 3-12 for more information.

For information on how to display the password or access level configuration, see the “Displaying the Password, Access Level, and Privilege Level Configuration” section on page 3-11.

## Configuring Multiple Privilege Levels

By default, the Cisco IOS software has two modes of password security: user EXEC mode and privileged EXEC mode. You can configure up to 16 hierarchical levels of commands for each mode. By configuring multiple passwords, you can allow different sets of users to have access to specified commands.

For example, if you want many users to have access to the **clear line** command, you can assign it level 2 security and distribute the level 2 password fairly widely. If you want more restricted access to the **configure** command, you can assign it level 3 security and distribute that password to fewer users.

The procedures in the following sections describe how to configure additional levels of security:

- Setting the Privilege Level for a Command, page 3-10
- Changing the Default Privilege Level for Lines, page 3-10
- Logging In to a Privilege Level, page 3-11
- Exiting a Privilege Level, page 3-11
- Displaying the Password, Access Level, and Privilege Level Configuration, page 3-11

### Setting the Privilege Level for a Command

To set the privilege level for a command, perform this task:

|        | Command                                                                          | Purpose                                              |
|--------|----------------------------------------------------------------------------------|------------------------------------------------------|
| Step 1 | Switch(config)# <b>privilege</b> mode level level<br>command                     | Sets the privilege level for a command.              |
| Step 2 | Switch(config)# <b>enable password</b> level level<br>[encryption-type] password | Specifies the enable password for a privilege level. |

For information on how to display the password or access level configuration, see the “Displaying the Password, Access Level, and Privilege Level Configuration” section on page 3-11.

### Changing the Default Privilege Level for Lines

To change the default privilege level for a given line or a group of lines, perform this task:

| Command                                           | Purpose                                           |
|---------------------------------------------------|---------------------------------------------------|
| Switch(config-line)# <b>privilege</b> level level | Changes the default privilege level for the line. |

For information on how to display the password or access level configuration, see the “Displaying the Password, Access Level, and Privilege Level Configuration” section on page 3-11.



## Logging In to a Privilege Level

To log in at a specified privilege level, perform this task:

| Command                            | Purpose                                 |
|------------------------------------|-----------------------------------------|
| Switch# <b>enable</b> <i>level</i> | Logs in to a specified privilege level. |

## Exiting a Privilege Level

To exit to a specified privilege level, perform this task:

| Command                             | Purpose                               |
|-------------------------------------|---------------------------------------|
| Switch# <b>disable</b> <i>level</i> | Exits to a specified privilege level. |

## Displaying the Password, Access Level, and Privilege Level Configuration

To display detailed password information, perform this task:

|        | Command                            | Purpose                                               |
|--------|------------------------------------|-------------------------------------------------------|
| Step 1 | Switch# <b>show running-config</b> | Displays the password and access level configuration. |
| Step 2 | Switch# <b>show privilege</b>      | Shows the privilege level configuration.              |

This example shows how to display the password and access level configuration:

```
Switch# show running-config
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug datetime localtime
service timestamps log datetime localtime
no service password-encryption
!
hostname Switch
!
boot system flash sup-bootflash
enable password lab
!
<...output truncated...>
```

This example shows how to display the privilege level configuration:

```
Switch# show privilege
Current privilege level is 15
Switch#
```

# Recovering a Lost Enable Password

**Note**

For more information on the configuration register which is preconfigured in NVRAM, see “Configuring the Software Configuration Register” section on page 3-13.

Perform these steps to recover a lost enable password:

- 
- |               |                                                                                                              |
|---------------|--------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Connect to the console interface.                                                                            |
| <b>Step 2</b> | Stop the boot sequence and enter ROM monitor by pressing <b>Ctrl-C</b> during the first 5 seconds of bootup. |
| <b>Step 3</b> | Configure the switch to boot-up without reading the configuration memory (NVRAM).                            |
| <b>Step 4</b> | Reboot the system.                                                                                           |
| <b>Step 5</b> | Access enable mode (this can be done without a password if a password has not been configured).              |
| <b>Step 6</b> | View or change the password, or erase the configuration.                                                     |
| <b>Step 7</b> | Reconfigure the switch to boot-up and read the NVRAM as it normally does.                                    |
| <b>Step 8</b> | Reboot the system.                                                                                           |
- 

## Modifying the Supervisor Engine Startup Configuration

These sections describe how the startup configuration on the supervisor engine works and how to modify the configuration register and BOOT variable:

- Understanding the Supervisor Engine Boot Configuration, page 3-12
- Configuring the Software Configuration Register, page 3-13
- Specifying the Startup System Image, page 3-17
- Controlling Environment Variables, page 3-18

## Understanding the Supervisor Engine Boot Configuration

The supervisor engine boot process involves two software images: ROM monitor and supervisor engine software. When the switch is booted or reset, the ROMMON code is executed. Depending on the NVRAM configuration, the supervisor engine either stays in ROMMON mode or loads the supervisor engine software.

Two user-configurable parameters determine how the switch boots: the configuration register and the BOOT environment variable. The configuration register is described in the “Modifying the Boot Field and Using the boot Command” section on page 3-14. The BOOT environment variable is described in the “Specifying the Startup System Image” section on page 3-17.

## Understanding the ROM Monitor

The ROM monitor (ROMMON) is invoked at switch bootup, reset, or when a fatal exception occurs. The switch enters ROMMON mode if the switch does not find a valid software image, if the NVRAM configuration is corrupted, or if the configuration register is set to enter ROMMON mode. From ROMMON mode, you can manually load a software image from bootflash or a Flash disk, or you can boot up from the management interface. ROMMON mode loads a primary image from which you can configure a secondary image to boot up from a specified source either locally or through the network using the BOOTLDR environment variable. This variable is described in the “Switch#” section on page 3-18.

You can also enter ROMMON mode by restarting the switch and then pressing **Ctrl-C** during the first five seconds of startup. If you are connected through a terminal server, you can escape to the Telnet prompt and enter the **send break** command to enter ROMMON mode.



### Note

**Ctrl-C** is always enabled for five seconds after you reboot the switch, regardless of whether the configuration-register setting has **Ctrl-C** disabled.

The ROM monitor has these features:

- Power-on confidence test
- Hardware initialization
- Boot capability (manual bootup and autoboot)
- File system (read-only while in ROMMON)

## Configuring the Software Configuration Register

The switch uses a 16-bit software configuration register, which allows you to set specific system parameters. Settings for the software configuration register are preconfigured in NVRAM.

Following are some reasons you might want to change the software configuration register settings:

- To select a boot source and default boot filename
- To control broadcast addresses
- To set the console terminal baud rate
- To load operating software from Flash memory
- To recover a lost password
- To manually boot the system using the **boot** command at the bootstrap program prompt
- To force an automatic bootup from the system bootstrap software (boot image) or from a default system image in onboard Flash memory, and read any **boot system** commands that are stored in the configuration file in NVRAM



### Caution

To avoid possibly halting the Catalyst 4006 switch with Supervisor Engine III switch, remember that valid configuration register settings might be combinations of settings and not just the individual settings listed in Table 3-2. For example, the factory default value of 0x0102 is a combination of settings.

Table 3-2 lists the meaning of each of the software configuration memory bits. Table 3-3 defines the *boot* field.

**Table 3-2 Software Configuration Register Bits**

| Bit Number <sup>1</sup> | Hexadecimal      | Meaning                                                        |
|-------------------------|------------------|----------------------------------------------------------------|
| 00 to 03                | 0x0000 to 0x000F | Boot field (see Table 3-3)                                     |
| 04                      | 0x0010           | Unused                                                         |
| 05                      | 0x0020           | Bit two of console line speed                                  |
| 06                      | 0x0040           | Causes system software to ignore NVRAM contents                |
| 07                      | 0x0080           | OEM <sup>2</sup> bit enabled                                   |
| 08                      | 0x0100           | Unused                                                         |
| 09                      | 0x0200           | Unused                                                         |
| 10                      | 0x0400           | IP broadcast with all zeros                                    |
| 11 to 12                | 0x0800 to 0x1000 | Bits one and zero of Console line speed (default is 9600 baud) |
| 13                      | 0x2000           | Loads ROM monitor after netboot fails                          |
| 14                      | 0x4000           | IP broadcasts do not have network numbers                      |

1. The factory default value for the configuration register is 0x0102. This value is a combination of the following: binary bit 8 = 0x0100 and binary bits 00 through 03 = 0x0002 (see Table 3-3).
2. OEM = original equipment manufacturer.

**Table 3-3 Explanation of Boot Field (Configuration Register Bits 00 to 03)**

| Boot Field | Meaning                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 00         | Stays at the system bootstrap prompt (does not autoboot).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 01         | Boots the first system image in onboard Flash memory.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 02 to 0F   | Autoboots using image(s) specified by the BOOT environment variable. If more than one image is specified, the switch attempts to boot the first image specified in the BOOT variable. As long as the switch can successfully boot from this image, the same image will be used on a reboot. If the switch fails to boot from the image specified in the BOOT variable, the switch will try to boot from the next image listed in the BOOT variable. If the end of the BOOT variable is reached without the switch booting successfully, the switch attempts the boot from the beginning of the BOOT variable. The autoboot continues until the switch successfully boots from one of the images specified in the BOOT variable. |

## Modifying the Boot Field and Using the boot Command

The configuration register boot field determines whether the switch loads an operating system image and, if so, where it obtains this system image. The following sections describe how to use and set the configuration register boot field and the procedures you must perform to modify the configuration register boot field. In ROMMON, you can use the **confreg** command to modify the configuration register and change boot settings.

Bits 0 through 3 of the software configuration register contain the boot field.



### Note

The factory default configuration register setting for systems and spares is 0x0102.

When the boot field is set to either 00 or 01 (0-0-0-0 or 0-0-0-1), the system ignores any boot instructions in the system configuration file and the following occurs:

- When the boot field is set to 00, you must boot up the operating system manually by issuing the **boot** command at the system bootstrap or ROMMON prompt.
- When the boot field is set to 01, the system boots the first image in the bootflash single in-line memory module (SIMM).
- When the entire boot field equals a value between 0-0-1-0 and 1-1-1-1, the switch loads the system image specified by **boot system** commands in the startup configuration file.

You can enter the **boot** command only, or enter the command and include additional boot instructions, such as the name of a file stored in Flash memory, or a file that you specify for booting from a network server. If you use the **boot** command without specifying a file or any other boot instructions, the system boots from the default Flash image (the first image in onboard Flash memory). Otherwise, you can instruct the system to boot up from a specific Flash image (using the **boot system flash filename** command).

You can also use the **boot** command to boot up images stored in the compact Flash cards located in slot 0 on the supervisor engine.

## Modifying the Boot Field

Modify the boot field from the software configuration register. To modify the software configuration register boot field, perform this task:

|        | Command                                      | Purpose                                                                                                             |
|--------|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch# <b>show version</b>                  | Determines the current configuration register setting.                                                              |
| Step 2 | Switch# <b>configure terminal</b>            | Enters configuration mode, and specify the <b>terminal</b> option.                                                  |
| Step 3 | Switch(config)# <b>config-register value</b> | Modifies the existing configuration register setting to reflect the way you want the switch to load a system image. |
| Step 4 | Switch(config)# <b>end</b>                   | Exits configuration mode.                                                                                           |
| Step 5 | Switch# <b>reload</b>                        | Reboots the switch to make your changes take effect.                                                                |

To modify the configuration register while the switch is running the Cisco IOS operating system, follow these steps:

- Step 1** Enter the **enable** command and your password to enter privileged level, as follows:

```
Switch> enable
Password:
Switch#
```

- Step 2** Enter the **configure terminal** command at the EXEC mode prompt (#), as follows:

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

- Step 3** Configure the configuration register to 0x102 as follows:

```
Switch(config)# config-register 0x102
```

Set the contents of the configuration register by specifying the *value* command variable, where *value* is a hexadecimal number preceded by 0x (see Table 3-2 on page 3-14).

- Step 4** Enter the **end** command to exit configuration mode. The new value settings are saved to memory; however, the new settings do not take effect until the system is rebooted.

- Step 5** Enter the **show version EXEC** command to display the configuration register value currently in effect; it will be used at the next reload. The value is displayed on the last line of the screen display, as shown in this sample output:

```
Configuration register is 0x141 (will be 0x102 at next reload)
```

- Step 6** Save your settings. (See the “Saving the Running Configuration Settings to Your Start-up File” section on page 3-3. Note that configuration register changes take effect only after the system reloads, such as when you enter a **reload** command from the console.)

- Step 7** Reboot the system. The new configuration register value takes effect with the next system boot up.

---

This completes the procedure for making configuration register changes.

## Verifying the Configuration Register Setting

Enter the **show version EXEC** command to verify the current configuration register setting. In ROMMON mode, enter the **show version** command to verify the value of the configuration register boot field.

To verify the configuration register setting for the switch, perform this task:

| Command                     | Purpose                                      |
|-----------------------------|----------------------------------------------|
| Switch# <b>show version</b> | Displays the configuration register setting. |

In this example, the **show version** command indicates that the current configuration register is set so that the switch does not automatically load an operating system image. Instead, it enters ROMMON mode and waits for you to enter ROM monitor commands.

```
Switch#show version
Cisco Internetwork Operating System Software
IOS (tm) Catalyst 4000 L3 Switch Software (cat4000-IS-M), Experimental
Version 12.1(20010828:211314) [cisco 105]
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Thu 06-Sep-01 15:40 by
Image text-base:0x00000000, data-base:0x00ADF444

ROM:1.15
Switch uptime is 10 minutes
System returned to ROM by reload
Running default software
```

```
cisco Catalyst 4000 (MPC8240) processor (revision 3) with 262144K bytes
of memory.
Processor board ID Ask SN 12345
Last reset from Reload
Bridging software.
49 FastEthernet/IEEE 802.3 interface(s)
20 Gigabit Ethernet/IEEE 802.3 interface(s)
271K bytes of non-volatile configuration memory.

Configuration register is 0xEC60

Switch#
```

## Specifying the Startup System Image

You can enter multiple boot commands in the startup configuration file or in the BOOT environment variable to provide backup methods for loading a system image.

The BOOT environment variable is also described in the “Specify the Startup System Image in the Configuration File” section in the “Loading and Maintaining System Images and Microcode” chapter of the *Cisco IOS Configuration Fundamentals Configuration Guide*.

Use the following sections to configure your switch to boot from Flash memory. Flash memory can be either single in-line memory modules (SIMMs) or Flash disks. Check the appropriate hardware installation and maintenance guide for information about types of Flash memory.

## Using Flash Memory

Flash memory allows you to do the following:

- Copy the system image to Flash memory using TFTP
- Boot the system from Flash memory either automatically or manually
- Copy the Flash memory image to a network server using TFTP or RCP

## Flash Memory Features

Flash memory allows you to do the following:

- Remotely load multiple system software images through TFTP or RCP transfers (one transfer for each file loaded)
- Boot a switch manually or automatically from a system software image stored in Flash memory (you can also boot directly from ROM)

## Security Precautions

Note the following security precaution when loading from Flash memory:



### Caution

You can only change the system image stored in Flash memory from privileged EXEC level on the console terminal.

## Configuring Flash Memory

To configure your switch to boot from Flash memory, perform this procedure. Refer to the appropriate hardware installation and maintenance publication for complete instructions on installing the hardware.

- 
- Step 1** Copy a system image to Flash memory using TFTP or other protocols. Refer to the “Cisco IOS File Management” and “Loading and Maintaining System Images” chapters in the *Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.1, at the following URL:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgr/fun\\_c/fcprt2/fcd203.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgr/fun_c/fcprt2/fcd203.htm)
  - Step 2** Configure the system to boot automatically from the desired file in Flash memory. You might need to change the configuration register value. See the “Modifying the Boot Field and Using the boot Command” section on page 3-14, for more information on modifying the configuration register.
  - Step 3** Save your configurations.
  - Step 4** Power cycle and reboot your system to verify that all is working as expected.
- 

## Controlling Environment Variables

Although the ROM monitor controls environment variables, you can create, modify, or view them with certain commands. To create or modify the BOOT and BOOTLDR variables, use the **boot system** and **boot bootldr** global configuration commands, respectively.

Refer to the “Specify the Startup System Image in the Configuration File” section in the “Loading and Maintaining System Images and Microcode” chapter of the *Configuration Fundamentals Configuration Guide* for details on setting the BOOT environment variable.



### Note

When you use the **boot system** and **boot bootldr** global configuration commands, you affect only the running configuration. To save the configuration for future use, you must save the environment variable settings to your startup configuration, which places the information under ROM monitor control. Enter the **copy system:running-config nvram:startup-config** command to save the environment variables from your running configuration to your startup configuration.

You can view the contents of the BOOT and BOOTLDR variables using the **show bootvar** command. This command displays the settings for these variables as they exist in the startup configuration and in the running configuration if a running configuration setting differs from a startup configuration setting. This example shows how to check the BOOT and BOOTLDR variables on the switch:

```
Switch# show bootvar
BOOTLDR variable = bootflash:cat4000-is-mz,1;
Configuration register is 0x0

Switch#
```





## Configuring Interfaces

---

This chapter describes how to configure interfaces for the Catalyst 4500 series switches. It also provides guidelines, procedures, and configuration examples.

This chapter includes the following major sections:

- Overview of Interface Configuration, page 4-1
- Using the interface Command, page 4-2
- Configuring a Range of Interfaces, page 4-4
- Defining and Using Interface-Range Macros, page 4-5
- Configuring Optional Interface Features, page 4-6
- Understanding Online Insertion and Removal, page 4-12
- Monitoring and Maintaining the Interface, page 4-12



### Note

For complete syntax and usage information for the switch commands used in this chapter, refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference* and related publications at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/index.htm>.

## Overview of Interface Configuration

By default, all interfaces are enabled. The 10/100-Mbps Ethernet interfaces autonegotiate connection speed and duplex. The 10/100/1000-Mbps Ethernet interfaces negotiate speed, duplex, and flow control. The 1000-Mbps Ethernet interfaces negotiate flow control only. Autonegotiation automatically selects the fastest speed possible on that port for the given pair. If a speed is explicitly stated for an interface, that interface will default to half duplex unless it is explicitly set for full duplex.

Many features are enabled on a per-interface basis. When you enter the **interface** command, you must specify the following:

- Interface type:
  - Fast Ethernet (use the **fastethernet** keyword)
  - Gigabit Ethernet (use the **gigabitethernet** keyword)
- Slot number—The slot in which the interface module is installed. Slots are numbered starting with 1, from top to bottom.

- Interface number—The interface number on the module. The interface numbers always begin with 1. When you are facing the front of the switch, the interfaces are numbered from left to right.

You can identify interfaces by physically checking the slot/interface location on the switch. You can also use the Cisco IOS **show** commands to display information about a specific interface or all the interfaces.

## Using the interface Command

These general instructions apply to all interface configuration processes.

- Step 1** At the privileged EXEC prompt, enter the **configure terminal** command to enter global configuration mode:

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

- Step 2** In global configuration mode, enter the **interface** command. Identify the interface type and the number of the connector on the interface card. The following example shows how to select Fast Ethernet, slot 5, interface 1:

```
Switch(config)# interface fastethernet 5/1
Switch(config-if)#
```

- Step 3** Interface numbers are assigned at the factory at the time of installation or when modules are added to a system. Enter the **show interfaces** EXEC command to see a list of all interfaces installed on your switch. A report is provided for each interface that your switch supports, as shown in this display:

```
Switch(config-if)#Ctrl-Z
Switch#show interfaces
Vlan1 is up, line protocol is down
 Hardware is Ethernet SVI, address is 0004.dd46.7aff (bia 0004.dd46.7aff)
 MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
 reliability 255/255, txload 1/255, rxload 1/255
 Encapsulation ARPA, loopback not set
 ARP type: ARPA, ARP Timeout 04:00:00
 Last input never, output never, output hang never
 Last clearing of "show interface" counters never
 Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
 Queueing strategy: fifo
 Output queue: 0/40 (size/max)
 5 minute input rate 0 bits/sec, 0 packets/sec
 5 minute output rate 0 bits/sec, 0 packets/sec
 0 packets input, 0 bytes, 0 no buffer
 Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
 0 packets output, 0 bytes, 0 underruns
 0 output errors, 0 interface resets
 0 output buffer failures, 0 output buffers swapped out
GigabitEthernet1/1 is up, line protocol is down
 Hardware is Gigabit Ethernet Port, address is 0004.dd46.7700 (bia 0004.dd46.7700)
 MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
 reliability 255/255, txload 1/255, rxload 1/255
 Encapsulation ARPA, loopback not set
 Keepalive set (10 sec)
 Auto-duplex, Auto-speed
 ARP type: ARPA, ARP Timeout 04:00:00
 Last input never, output never, output hang never
 Last clearing of "show interface" counters never
 Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
```

```

Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
 0 packets input, 0 bytes, 0 no buffer
 Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
 0 input packets with dribble condition detected
 0 packets output, 0 bytes, 0 underruns
 0 output errors, 0 collisions, 0 interface resets
 0 babbles, 0 late collision, 0 deferred
 0 lost carrier, 0 no carrier
 0 output buffer failures, 0 output buffers swapped out
GigabitEthernet1/2 is up, line protocol is down
 Hardware is Gigabit Ethernet Port, address is 0004.dd46.7701 (bia 0004.dd46.7701)
 MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
 reliability 255/255, txload 1/255, rxload 1/255
 Encapsulation ARPA, loopback not set
 Keepalive set (10 sec)
 Auto-duplex, Auto-speed
 ARP type: ARPA, ARP Timeout 04:00:00
 Last input never, output never, output hang never
 Last clearing of "show interface" counters never
 Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
 Queueing strategy: fifo
 Output queue: 0/40 (size/max)
 5 minute input rate 0 bits/sec, 0 packets/sec
 5 minute output rate 0 bits/sec, 0 packets/sec
 0 packets input, 0 bytes, 0 no buffer
 Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
 0 input packets with dribble condition detected
 0 packets output, 0 bytes, 0 underruns
 0 output errors, 0 collisions, 0 interface resets
 0 babbles, 0 late collision, 0 deferred
 0 lost carrier, 0 no carrier
 0 output buffer failures, 0 output buffers swapped out
--More--
<...output truncated...>

```

- Step 4** To begin configuring Fast Ethernet interface 5/5, as shown in the following example, enter the **interface** keyword, interface type, slot number, and interface number in global configuration mode:

```

Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 5/5
Switch(config-if)#

```



**Note** You do not need to add a space between the interface type and interface number. For example, in the preceding line you can specify either **fastethernet 5/5** or **fastethernet5/5**.

- Step 5** Follow each **interface** command with the interface configuration commands your particular interface requires. The commands you enter define the protocols and applications that will run on the interface. The commands are collected and applied to the **interface** command until you enter another **interface** command or press **Ctrl-Z** to exit interface configuration mode and return to privileged EXEC mode.
- Step 6** After you configure an interface, check its status by using the EXEC **show** commands listed in “Monitoring and Maintaining the Interface” section on page 4-12.

# Configuring a Range of Interfaces

The interface-range configuration mode allows you to configure multiple interfaces with the same configuration parameters. When you enter the interface-range configuration mode, all command parameters you enter are attributed to all interfaces within that range until you exit interface-range configuration mode.

To configure a range of interfaces with the same configuration, perform this task:

| Command                                                                                                                                                                                                                                                              | Purpose                                                                                                                                                                                                                                                                                                              |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>Switch(config)# interface range {vlan vlan_ID - vlan_ID}   {{fastethernet   gigabitethernet   macro macro_name} slot/interface - interface} [, {vlan vlan_ID - vlan_ID} {{fastethernet   gigabitethernet   macro macro_name} slot/interface - interface}]</pre> | <p>Selects the range of interfaces to be configured. Note the following:</p> <ul style="list-style-type: none"> <li>You are required to enter a space before the dash.</li> <li>You can enter up to five comma-separated ranges.</li> <li>You are not required to enter spaces before or after the comma.</li> </ul> |



## Note

When you use the **interface range** command, you must add a space between the **vlan**, **fastethernet**, **gigabitethernet**, or **macro** keyword and the dash. For example, the command **interface range fastethernet 5/1 - 5** specifies a valid range; the command **interface range fastethernet 1-5** does not contain a valid range command.



## Note

The **interface range** command works only with VLAN interfaces that have been configured with the **interface vlan** command (the **show running-configuration** command displays the configured VLAN interfaces). VLAN interfaces that are not displayed by the **show running-configuration** command cannot be used with the **interface range** command.

This example shows how to reenoble all Fast Ethernet interfaces 5/1 to 5/5:

```
Switch(config)# interface range fastethernet 5/1 - 5
Switch(config-if-range)# no shutdown
Switch(config-if-range)#
*Oct 6 08:24:35: %LINK-3-UPDOWN: Interface FastEthernet5/1, changed state to up
*Oct 6 08:24:35: %LINK-3-UPDOWN: Interface FastEthernet5/2, changed state to up
*Oct 6 08:24:35: %LINK-3-UPDOWN: Interface FastEthernet5/3, changed state to up
*Oct 6 08:24:35: %LINK-3-UPDOWN: Interface FastEthernet5/4, changed state to up
*Oct 6 08:24:35: %LINK-3-UPDOWN: Interface FastEthernet5/5, changed state to up
*Oct 6 08:24:36: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet5/
5, changed state to up
*Oct 6 08:24:36: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet5/
3, changed state to up
*Oct 6 08:24:36: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet5/
4, changed state to up
Switch(config-if)#
```

This example shows how to use a comma to add different interface type strings to the range to reenoble all Fast Ethernet interfaces in the range 5/1 to 5/5 and both Gigabit Ethernet interfaces 1/1 and 1/2:

```
Switch(config-if)# interface range fastethernet 5/1 - 5, gigabitethernet 1/1 - 2
Switch(config-if)# no shutdown
```

```
Switch(config-if)#
*Oct 6 08:29:28: %LINK-3-UPDOWN: Interface FastEthernet5/1, changed state to up
*Oct 6 08:29:28: %LINK-3-UPDOWN: Interface FastEthernet5/2, changed state to up
*Oct 6 08:29:28: %LINK-3-UPDOWN: Interface FastEthernet5/3, changed state to up
*Oct 6 08:29:28: %LINK-3-UPDOWN: Interface FastEthernet5/4, changed state to up
*Oct 6 08:29:28: %LINK-3-UPDOWN: Interface FastEthernet5/5, changed state to up
*Oct 6 08:29:28: %LINK-3-UPDOWN: Interface GigabitEthernet1/1, changed state to
up
*Oct 6 08:29:28: %LINK-3-UPDOWN: Interface GigabitEthernet1/2, changed state to
up
*Oct 6 08:29:29: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet5/
5, changed state to up
*Oct 6 08:29:29: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet5/
3, changed state to up
*Oct 6 08:29:29: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet5/
4, changed state to up
Switch(config-if)#
```

If you enter multiple configuration commands while you are in interface-range configuration mode, each command is run as it is entered (they are not batched together and run after you exit interface-range configuration mode). If you exit interface-range configuration mode while the commands are being run, some commands might not be run on all interfaces in the range. Wait until the command prompt is displayed before exiting interface-range configuration mode.

## Defining and Using Interface-Range Macros

You can define an interface-range macro to automatically select a range of interfaces for configuration. Before you can use the **macro** keyword in the **interface-range** macro command string, you must define the macro.

To define an interface-range macro, perform this task:

| Command                                                                                                                                                                                                                                                                                                                                                                     | Purpose                                                                           |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| Switch(config)# <b>define interface-range</b> <i>macro_name</i><br>{ <b>vlan</b> <i>vlan_ID</i> - <i>vlan_ID</i> }   {{ <b>fastethernet</b>  <br><b>gigabitethernet</b> } <i>slot/interface</i> - <i>interface</i> }<br>[, { <b>vlan</b> <i>vlan_ID</i> - <i>vlan_ID</i> } {{ <b>fastethernet</b>  <br><b>gigabitethernet</b> } <i>slot/interface</i> - <i>interface</i> }] | Defines the interface-range macro and saves it in the running configuration file. |

This example shows how to define an interface-range macro named **enet\_list** to select Fast Ethernet interfaces 5/1 through 5/4:

```
Switch(config)# define interface-range enet_list fastethernet 5/1 - 4
```

To show the defined interface-range macro configuration, perform this task:

| Command                            | Purpose                                                |
|------------------------------------|--------------------------------------------------------|
| Switch# <b>show running-config</b> | Shows the defined interface-range macro configuration. |

This example shows how to display the defined interface-range macro named **enet\_list**:

```
Switch# show running-config | include define
 define interface-range enet_list FastEthernet5/1 - 4
 Switch#
```

To use an interface-range macro in the **interface range** command, perform this task:

| Command                                                   | Purpose                                                                                               |
|-----------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| Switch(config) # <b>interface range macro</b> <i>name</i> | Selects the interface range to be configured using the values saved in a named interface-range macro. |

This example shows how to change to the interface-range configuration mode using the interface-range macro **enet\_list**:

```
Switch(config) # interface range macro enet_list
Switch(config-if) #
```

## Configuring Optional Interface Features

The following subsections describe optional procedures:

- Configuring Ethernet Interface Speed and Duplex Mode, page 4-6
- Configuring Jumbo Frame Support, page 4-9
- Interacting with the Baby Giants Feature, page 4-11

## Configuring Ethernet Interface Speed and Duplex Mode

- Speed and Duplex Mode Configuration Guidelines, page 4-6
- Setting the Interface Speed, page 4-7
- Setting the Interface Duplex Mode, page 4-7
- Displaying the Interface Speed and Duplex Mode Configuration, page 4-8
- Adding a Description for an Interface, page 4-8

### Speed and Duplex Mode Configuration Guidelines

You can configure the interface speed and duplex mode parameters to **auto** and allow the Catalyst 4500 series switch to negotiate the interface speed and duplex mode between interfaces. If you decide to configure the interface **speed** and **duplex** commands manually, consider the following:

- If you set the interface **speed** to **auto**, the switch automatically sets the **duplex** mode to **auto**.
- If you enter the **no speed** command, the switch automatically configures both interface **speed** and **duplex** to **auto**.
- When you set the interface speed to 1000 Mbps, the duplex mode is full duplex. You cannot change the duplex mode.
- If the interface speed is set to 10 or 100 mbps, the duplex mode is set to half duplex by default unless you explicitly configure it.



#### Caution

Changing the interface speed and duplex mode configuration might shut down and restart the interface during the reconfiguration.

## Setting the Interface Speed

If you set the interface speed to **auto** on a 10/100-Mbps Ethernet interface, speed and duplex are autonegotiated.

To set the port speed for a 10/100-Mbps Ethernet interface, perform this task:

|        | Command                                                      | Purpose                                   |
|--------|--------------------------------------------------------------|-------------------------------------------|
| Step 1 | Switch(config)# <b>interface fastethernet slot/interface</b> | Specifies the interface to be configured. |
| Step 2 | Switch(config-if)# <b>speed [10   100   auto]</b>            | Set the interface speed of the interface. |

This example shows how to set the interface speed to 100 Mbps on the Fast Ethernet interface 5/4:

```
Switch(config)# interface fastethernet 5/4
Switch(config-if)# speed 100
```

Turning off autonegotiation on a Gigabit Ethernet interface will result in the port being forced into 1000 Mbps and full-duplex mode. To turn off the port speed autonegotiation for Gigabit Ethernet interface 1/1, perform this task:

|        | Command                                             | Purpose                                    |
|--------|-----------------------------------------------------|--------------------------------------------|
| Step 1 | Switch(config)# <b>interface gigabitethernet1/1</b> | Specifies the interface to be configured.  |
| Step 2 | Switch(config-if)# <b>speed nonegotiate</b>         | Disables autonegotiation on the interface. |

To restore autonegotiation, enter the **no speed nonegotiate** command in the interface configuration mode.



### Note

For the blocking ports on the WS-X4416 module, do not set the speed to autonegotiate.

## Setting the Interface Duplex Mode



### Note

When the interface is set to 1000 Mbps, you cannot change the duplex mode from full duplex to half duplex.



### Note

If you set the port speed to **auto** on a 10/100-Mbps Ethernet interface, both speed and duplex mode are autonegotiated. The configured duplex mode is not applied on autonegotiation interfaces.

To set the duplex mode of a Fast Ethernet interface, perform this task:

|        | Command                                                      | Purpose                                   |
|--------|--------------------------------------------------------------|-------------------------------------------|
| Step 1 | Switch(config)# <b>interface fastethernet slot/interface</b> | Specifies the interface to be configured. |
| Step 2 | Switch(config-if)# <b>duplex [auto   full   half]</b>        | Sets the duplex mode of the interface.    |

This example shows how to set the interface duplex mode to full on Fast Ethernet interface 5/4:

```
Switch(config)# interface fastethernet 5/4
Switch(config-if)# duplex full
```

## Displaying the Interface Speed and Duplex Mode Configuration

To display the interface speed and duplex mode configuration for an interface, perform this task:

| Command                                                                                               | Purpose                                                     |
|-------------------------------------------------------------------------------------------------------|-------------------------------------------------------------|
| Switch# <b>show interfaces</b> [ <b>fastethernet</b>   <b>gigabitethernet</b> ] <i>slot/interface</i> | Displays the interface speed and duplex mode configuration. |

This example shows how to display the interface speed and duplex mode of Fast Ethernet interface 6/1:

```
Switch# show interface fastethernet 6/1
FastEthernet6/1 is up, line protocol is up
 Hardware is Fast Ethernet Port, address is 0050.547a.dee0 (bia 0050.547a.dee0)
 MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
 reliability 255/255, txload 1/255, rxload 1/255
 Encapsulation ARPA, loopback not set
 Keepalive set (10 sec)
 Full-duplex, 100Mb/s
 ARP type: ARPA, ARP Timeout 04:00:00
 Last input 00:00:54, output never, output hang never
 Last clearing of "show interface" counters never
 Input queue: 50/2000/0/0 (size/max/drops/flushes); Total output drops: 0
 Queueing strategy: fifo
 Output queue: 0/40 (size/max)
 5 minute input rate 0 bits/sec, 0 packets/sec
 5 minute output rate 0 bits/sec, 0 packets/sec
 50 packets input, 11300 bytes, 0 no buffer
 Received 50 broadcasts, 0 runts, 0 giants, 0 throttles
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
 0 input packets with dribble condition detected
 1456 packets output, 111609 bytes, 0 underruns
 0 output errors, 0 collisions, 0 interface resets
 0 babbles, 0 late collision, 0 deferred
 1 lost carrier, 0 no carrier
 0 output buffer failures, 0 output buffers swapped out
Switch#
```

## Adding a Description for an Interface

You can add a description about an interface to help you remember its function. The description appears in the output of the following commands: **show configuration**, **show running-config**, and **show interfaces**.

To add a description for an interface, enter the following command:

| Command                                             | Purpose                              |
|-----------------------------------------------------|--------------------------------------|
| Switch(config-if)# <b>description</b> <i>string</i> | Adds a description for an interface. |

This example shows how to add a description on Fast Ethernet interface 5/5:

```
Switch(config)# interface fastethernet 5/5
Switch(config-if)# description Channel-group to "Marketing"
```



## Configuring Jumbo Frame Support

These subsections describe jumbo frame support:

- Ports and Modules that Support Jumbo Frames, page 4-9
- Understanding Jumbo Frame Support, page 4-9
- Configuring MTU Sizes, page 4-11

### Ports and Modules that Support Jumbo Frames

The following ports and modules support jumbo frames:

- Supervisor uplink ports
- WS-X4306-GB: all ports
- WS-X4232-GB-RJ: ports 1-2
- WS-X4418-GB: ports 1-2
- WS-X4412-2GB-TX: ports 13-14

Each of the last three modules has two non-blocking ports that can support jumbo frames. Other ports are over-subscribed ports and cannot support jumbo frames.

### Understanding Jumbo Frame Support

These sections describe jumbo frame support:

- Jumbo Frame Support Overview, page 4-9
- Ethernet Ports, page 4-10
- VLAN Interfaces, page 4-10

#### Jumbo Frame Support Overview

A jumbo frame is a frame larger than the default Ethernet size. Enable jumbo frame support by configuring a larger-than-default maximum transmission unit (MTU) size on a port or interface.

Catalyst 4000 family switch Ethernet LAN ports configured with a nondefault MTU size accept frames containing packets with a size between 1500 and 9198 bytes. With a nondefault MTU size configured, the packet size of ingress frames is checked. If the packet is larger than the configured MTU, it is dropped.

For traffic that needs to be routed, the MTU of the egress port is checked. If the MTU is smaller than the packet size, the packet is forwarded to the CPU. If the “do not fragment bit” is not set, it is fragmented. Otherwise, the packet is dropped.

**Note**

---

Jumbo frame support does not fragment Layer 2 switched packets.

---

The Catalyst 4000 family switch does not compare the packet size with the MTU at the egress port, but jumbo frames are dropped in ports that do not support them. The frames can be transmitted in ports that do support jumbo frames, even though the MTU is not configured to jumbo size.

**Note**

Jumbo frame support is only configured per interface; jumbo frame support cannot be configured globally.

## Ethernet Ports

These sections describe configuring nondefault MTU sizes on Ethernet ports:

- Ethernet Port Overview, page 4-10
- Layer 3 and Layer 2 EtherChannels, page 4-10

### Ethernet Port Overview

With Cisco IOS Release 12.1(11)EW, configuring a nondefault MTU size on certain Ethernet port limits the size of ingress packets. The MTU does not impact the egress packets.

With releases earlier than Cisco IOS Release 12.1(13)EW, you can configure the MTU size only on Gigabit Ethernet and 10-Gigabit Ethernet ports.

### Layer 3 and Layer 2 EtherChannels

With Release Cisco IOS Release 12.1(11)EW and later releases, you can configure all the interfaces in an EtherChannel provided that they have the same MTU. Changing the MTU of an EtherChannel changes the MTU of all member ports. If the MTU of a member port cannot be changed to the new value, that port is suspended (administratively shut down). A port cannot join an EtherChannel if the port has a different MTU. If a member port of an EtherChannel changes MTU, the member port is suspended.

## VLAN Interfaces

If switch ports reside in the same VLAN, either configure all of the switch ports to handle jumbo frames and support the same MTU size, or configure none of them. However, such uniformity of MTU size in the same VLAN is not enforced.

When a VLAN has switch ports with different MTU size, packets received from a port with a larger MTU might be dropped when they are forwarded to a port with a smaller MTU.

If the switch ports in a VLAN have jumbo frames enabled, the corresponding SVI can have jumbo frames enabled. The MTU of an SVI should always be smaller than the smallest MTU among all the switch ports in the VLAN, but this condition is not enforced.

The MTU of a packet is not checked on the ingress side for an SVI; it is checked on the egress side of an SVI. If the MTU of a packet is larger than the MTU of the egress SVI, the packet will be sent to the CPU for fragmentation processing. If the “do not fragment” bit is not set, the packet is fragmented. Otherwise, the packet is dropped.

## Configuring MTU Sizes

To configure the MTU size, perform this task:

|        | Command                                                                                                                            | Purpose                                                                       |
|--------|------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|
| Step 1 | Router(config)# <b>interface</b> {{vlan vlan_ID}   {{type <sup>1</sup> slot/port}   {port-channel port_channel_number} slot/port}} | Selects the interface to configure.                                           |
| Step 2 | Router(config-if)# <b>mtu</b> mtu_size<br><br>Router(config-if)# <b>no mtu</b>                                                     | Configures the MTU size.<br><br>Reverts to the default MTU size (1500 bytes). |
| Step 3 | Router(config-if)# <b>end</b>                                                                                                      | Exits configuration mode.                                                     |
| Step 4 | Router# <b>show running-config interface</b> [{fastethernet   gigabitethernet} slot/port]                                          | Displays the running configuration.                                           |

1. *type* = fastethernet or gigabitethernet



### Note

When configuring the MTU size for VLAN interfaces and Layer 3 and Layer 2 Ethernet ports, note that the supported MTU values are from 1500 to 9198 bytes.

This example shows how to configure the MTU size on Gigabit Ethernet port 1/2:

```
switch# conf t
switch(config)# int gi1/1
switch(config-if)# mtu 9198
switch(config-if)# end
```

This example shows how to verify the configuration:

```
switch# show interface gigabitethernet 1/2
GigabitEthernet1/2 is administratively down, line protocol is down
 Hardware is C6k 1000Mb 802.3, address is 0030.9629.9f88 (bia 0030.9629.9f88)
 MTU 9216 bytes, BW 1000000 Kbit, DLY 10 usec,
 <...Output Truncated...>
switch#
```

## Interacting with the Baby Giants Feature

The baby giants feature, introduced in Cisco IOS Release 12.1(12c)EW, uses the global command **system mtu <size>** to set the global baby giant MTU. This feature also allows certain interfaces to support Ethernet payload size of up to 1552 bytes.

Both the **system mtu** command and the per-interface **mtu** command can operate on interfaces that can support jumbo frames, but the per-interface **mtu** command takes precedence.

For example, let's say that before setting the per-interface MTU for interface gi1/1, you issue the **system mtu 1550** command to change the MTU for gi1/1 to 1550 bytes. Next, you issue the per-interface **mtu** command to change the MTU for gi1/1 to 9198 bytes. Now, if you change the baby giant MTU to 1540 bytes with the command **system mtu 1540**, the MTU for gi1/1 remains unchanged at 9198 bytes.

# Understanding Online Insertion and Removal

The online insertion and removal (OIR) feature supported on the Catalyst 4500 series switch allows you to remove and replace modules while the system is online. You can shut down the module before removal and restart it after insertion without causing other software or interfaces to shut down.

You do not need to enter a command to notify the software that you are going to remove or install a module. The system notifies the supervisor engine that a module has been removed or installed and scans the system for a configuration change. The newly installed module is initialized, and each interface type is verified against the system configuration; then the system runs diagnostics on the new interface. There is no disruption to normal operation during module insertion or removal.

If you remove a module and then replace it, or insert a different module of the same type into the same slot, no change to the system configuration is needed. An interface of a type that has been configured previously will be brought online immediately. If you remove a module and insert a module of a different type, the interface(s) on that module will be administratively up with the default configuration for that module.

## Monitoring and Maintaining the Interface

The following sections describe how to monitor and maintain the interfaces:

- Monitoring Interface and Controller Status, page 4-12
- Clearing and Resetting the Interface, page 4-13
- Shutting Down and Restarting an Interface, page 4-13

## Monitoring Interface and Controller Status

The Cisco IOS software for the Catalyst 4500 series switch contains commands that you can enter at the EXEC prompt to display information about the interface, including the version of the software and the hardware, the controller status, and statistics about the interfaces. The following table lists some of the interface monitoring commands. (You can display the full list of **show** commands by entering the **show ?** command at the EXEC prompt.) These commands are fully described in the *Interface Command Reference*.

To display information about the interface, perform this task:

|        | Command                                                       | Purpose                                                                                                                   |
|--------|---------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch# <b>show interfaces</b> [ <i>type slot/interface</i> ] | Displays the status and configuration of all interfaces or of a specific interface.                                       |
| Step 2 | Switch# <b>show running-config</b>                            | Displays the configuration currently running in RAM.                                                                      |
| Step 3 | Switch# <b>show protocols</b> [ <i>type slot/interface</i> ]  | Displays the global (system-wide) and interface-specific status of any configured protocol.                               |
| Step 4 | Switch# <b>show version</b>                                   | Displays the hardware configuration, software version, the names and sources of configuration files, and the boot images. |

This example shows how to display the status of Fast Ethernet interface 5/5:

```
Switch# show protocols fastethernet 5/5
FastEthernet5/5 is up, line protocol is up
Switch#
```

## Clearing and Resetting the Interface

To clear the interface counters shown with the **show interfaces** command, enter the following command:

| Command                                             | Purpose                    |
|-----------------------------------------------------|----------------------------|
| Switch# <b>clear counters</b> {type slot/interface} | Clears interface counters. |

This example shows how to clear and reset the counters on Fast Ethernet interface 5/5:

```
Switch# clear counters fastethernet 5/5
Clear "show interface" counters on this interface [confirm] y
Switch#
*Sep 30 08:42:55: %CLEAR-5-COUNTERS: Clear counter on interface FastEthernet5/5
by vty1 (171.69.115.10)
Switch#
```

The **clear counters** command (without any arguments) clears all the current interface counters from all interfaces.



### Note

The **clear counters** command does not clear counters retrieved with SNMP; it clears only those counters displayed with the EXEC **show interfaces** command.

## Shutting Down and Restarting an Interface

You can disable an interface, which disables all functions on the specified interface and marks the interface as unavailable on all monitoring command displays. This information is communicated to other network servers through all dynamic routing protocols. The interface will not be mentioned in any routing updates.

To shut down an interface and then restart it, perform this task:

|        | Command                                                                                                                                 | Purpose                                   |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|
| Step 1 | Switch(config)# <b>interface</b> {vlan vlan_ID}  <br>{fastethernet   gigabitethernet} slot/port  <br>{port-channel port_channel_number} | Specifies the interface to be configured. |
| Step 2 | Switch(config-if)# <b>shutdown</b>                                                                                                      | Shuts down the interface.                 |
| Step 3 | Switch(config-if)# <b>no shutdown</b>                                                                                                   | Reenables the interface.                  |

This example shows how to shut down Fast Ethernet interface 5/5:

```
Switch(config)# interface fastethernet 5/5
Switch(config-if)# shutdown
Switch(config-if)#
*Sep 30 08:33:47: %LINK-5-CHANGED: Interface FastEthernet5/5, changed state to a
administratively down
Switch(config-if)#
```

This example shows how to reenabale Fast Ethernet interface 5/5:

```
Switch(config-if)# no shutdown
Switch(config-if)#
*Sep 30 08:36:00: %LINK-3-UPDOWN: Interface FastEthernet5/5, changed state to up
Switch(config-if)#
```

To check whether or not an interface is disabled, enter the EXEC **show interfaces** command. An interface that has been shut down is shown as being administratively down when you enter the **show interfaces** command.



## Checking Port Status and Connectivity

---

This chapter describes how to check switch port status and connectivity on the Catalyst 4500 series switch.

This chapter includes the following major sections:

- Checking Module Status, page 5-1
- Checking Interfaces Status, page 5-2
- Checking MAC Addresses, page 5-3
- Using Telnet, page 5-3
- Changing the Logout Timer, page 5-4
- Monitoring User Sessions, page 5-4
- Using Ping, page 5-5
- Using IP Traceroute, page 5-7
- Using Layer 2 Traceroute, page 5-8
- Configuring ICMP, page 5-10



### Note

For complete syntax and usage information for the commands used in this publication, refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference* and the publications at: <http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/index.htm>.

## Checking Module Status

The Catalyst 4500 series switch is a multimodule system. You can see which modules are installed, as well as the MAC address ranges and version numbers for each module, by using the **show module** command. You can use the `[mod_num]` argument to specify a particular module number to see detailed information on that module.

This example shows how to check module status for all modules on your switch:

```
Switch# show module all
```

| Mod | Ports | Card Type                          | Model            | Serial No.  |
|-----|-------|------------------------------------|------------------|-------------|
| 1   | 2     | 1000BaseX (GBIC) Supervisor Module | WS-X4014         | JAB012345AB |
| 5   | 24    | 10/100/1000BaseTX (RJ45)           | WS-X4424-GB-RJ45 | JAB045304EY |
| 6   | 48    | 10/100BaseTX (RJ45)                | WS-X4148         | JAB023402QK |

| M | MAC addresses                    | Hw  | Fw                | Sw            | Stat |
|---|----------------------------------|-----|-------------------|---------------|------|
| 1 | 0004.dd46.9f00 to 0004.dd46.a2ff | 0.0 | 12.1(10r)EW(1.21) | 12.1(10)EW(1) | Ok   |
| 5 | 0050.3e7e.1d70 to 0050.3e7e.1d87 | 0.0 |                   |               | Ok   |
| 6 | 0050.0f10.2370 to 0050.0f10.239f | 1.0 |                   |               | Ok   |

```
Switch#
```

## Checking Interfaces Status

You can view summary or detailed information on the switch ports using the **show interfaces status** command. To see summary information on all of the ports on the switch, enter the **show interfaces status** command with no arguments. Specify a particular module number to see information on the ports on that module only. Enter both the module number and the port number to see detailed information about the specified port.

To apply configuration commands to a particular port, you must specify the appropriate logical module. For more information, see the “Checking Module Status” section on page 5-1.

This example shows how to display the status of all interfaces on a Catalyst 4500 series switch:

```
Switch#show interfaces status
```

| Port  | Name | Status     | Vlan | Duplex | Speed | Type           |
|-------|------|------------|------|--------|-------|----------------|
| Gi1/1 |      | notconnect | 1    | auto   | auto  | No Gbic        |
| Gi1/2 |      | notconnect | 1    | auto   | auto  | No Gbic        |
| Gi5/1 |      | notconnect | 1    | auto   | auto  | 10/100/1000-TX |
| Gi5/2 |      | notconnect | 1    | auto   | auto  | 10/100/1000-TX |
| Gi5/3 |      | notconnect | 1    | auto   | auto  | 10/100/1000-TX |
| Gi5/4 |      | notconnect | 1    | auto   | auto  | 10/100/1000-TX |
| Fa6/1 |      | connected  | 1    | a-full | a-100 | 10/100BaseTX   |
| Fa6/2 |      | connected  | 2    | a-full | a-100 | 10/100BaseTX   |
| Fa6/3 |      | notconnect | 1    | auto   | auto  | 10/100BaseTX   |
| Fa6/4 |      | notconnect | 1    | auto   | auto  | 10/100BaseTX   |

```
Switch#
```

This example shows how to display the status of interfaces in error-disabled state:

```
Switch# show interfaces status err-disabled
```

| Port  | Name | Status       | Reason    |
|-------|------|--------------|-----------|
| Fa9/4 |      | err-disabled | link-flap |

informational error message when the timer expires on a cause

```

5d04h:%PM-SP-4-ERR_RECOVER:Attempting to recover from link-flap err-disable state on Fa9/4
Switch#
```



## Checking MAC Addresses

In addition to displaying the MAC address range for a module using the **show module** command, you can display the MAC address table information of a specific MAC address or a specific interface in the switch using the **show mac-address-table address** and **show mac-address-table interface** commands.

This example shows how to display MAC address table information for a specific MAC address:

```
Switch# show mac-address-table address 0050.3e8d.6400
vlan mac address type protocol qos ports
-----+-----+-----+-----+-----+-----
200 0050.3e8d.6400 static assigned -- Switch
100 0050.3e8d.6400 static assigned -- Switch
5 0050.3e8d.6400 static assigned -- Switch
4 0050.3e8d.6400 static ipx -- Switch
1 0050.3e8d.6400 static ipx -- Switch
1 0050.3e8d.6400 static assigned -- Switch
4 0050.3e8d.6400 static assigned -- Switch
5 0050.3e8d.6400 static ipx -- Switch
100 0050.3e8d.6400 static ipx -- Switch
200 0050.3e8d.6400 static ipx -- Switch
100 0050.3e8d.6400 static other -- Switch
200 0050.3e8d.6400 static other -- Switch
5 0050.3e8d.6400 static other -- Switch
4 0050.3e8d.6400 static ip -- Switch
1 0050.3e8d.6400 static ip -- Route
1 0050.3e8d.6400 static other -- Switch
4 0050.3e8d.6400 static other -- Switch
5 0050.3e8d.6400 static ip -- Switch
200 0050.3e8d.6400 static ip -- Switch
100 0050.3e8d.6400 static ip -- Switch
Switch#
```

This example shows how to display MAC address table information for a specific interface:

```
Switch# show mac-address-table interface gigabit 1/1
Multicast Entries
vlan mac address type ports
-----+-----+-----+-----
1 ffff.ffff.ffff system Switch,Gi6/1,Gi6/2,Gi6/9,Gi1/1
Switch#
```

## Using Telnet

You can access the switch command-line interface (CLI) using Telnet. In addition, you can use Telnet from the switch to access other devices in the network. You can have up to eight simultaneous Telnet sessions.

Before you can open a Telnet session to the switch, you must first set the IP address (and in some cases the default gateway) for the switch. For information about setting the IP address and default gateway, see Chapter 3, “Configuring the Switch for the First Time.”



### Note

To **telnet** to a host using the hostname, configure and enable DNS.

To **telnet** to another device on the network from the switch, perform this task:

| Command                                           | Purpose                                  |
|---------------------------------------------------|------------------------------------------|
| Switch# <b>telnet</b> <i>host</i> [ <i>port</i> ] | Opens a Telnet session to a remote host. |

This example shows how to **telnet** from the switch to the remote host named labsparc:

```
Switch# telnet labsparc
Trying 172.16.10.3...
Connected to labsparc.
Escape character is '^]'.

UNIX(r) System V Release 4.0 (labsparc)

login:
```

## Changing the Logout Timer

The logout timer automatically disconnects a user from the switch when the user is idle for longer than the specified time. To set the logout timer, perform this task:

| Command                                    | Purpose                                                                                                                                                                          |
|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Switch# <b>logoutwarning</b> <i>number</i> | Changes the logout timer value (a timeout value of 0 prevents idle sessions from being disconnected automatically).<br>Use the <b>no</b> keyword to return to the default value. |

## Monitoring User Sessions

You can display the currently active user sessions on the switch using the **show users** command. The command output lists all active console port and Telnet sessions on the switch.

To display the active user sessions on the switch, perform this task in privileged EXEC mode:

| Command                                  | Purpose                                                    |
|------------------------------------------|------------------------------------------------------------|
| Switch# <b>show users</b> [ <i>all</i> ] | Displays the currently active user sessions on the switch. |

This example shows the output of the **show users** command when local authentication is enabled for console and Telnet sessions (the asterisk [\*] indicates the current session):

```
Switch#show users
 Line User Host(s) Idle Location
* 0 con 0 idle 00:00:00

 Interface User Mode Idle Peer Address

Switch#show users all
 Line User Host(s) Idle Location
* 0 con 0 idle 00:00:00
 1 vty 0 idle 00:00:00
 2 vty 1 idle 00:00:00
 3 vty 2 idle 00:00:00
 4 vty 3 idle 00:00:00
 5 vty 4 idle 00:00:00

 Interface User Mode Idle Peer Address
Switch#
```

To disconnect an active user session, perform this task:

| Command                                       | Purpose                                           |
|-----------------------------------------------|---------------------------------------------------|
| Switch# <b>disconnect</b> {console   ip_addr} | Disconnects an active user session on the switch. |

This example shows how to disconnect an active console port session and an active Telnet session:

```
Switch> disconnect console
Console session disconnected.
Console> (enable) disconnect tim-nt.bigcorp.com
Telnet session from tim-nt.bigcorp.com disconnected. (1)
Switch# show users
 Session User Location
 ----- -
telnet jake jake-mac.bigcorp.com
* telnet suzy suzy-pc.bigcorp.com
Switch#
```

## Using Ping

These sections describe how to use IP ping:

- Understanding How Ping Works, page 5-5
- Running Ping, page 5-6

## Understanding How Ping Works

You can use the **ping** command to verify connectivity to remote hosts. If you attempt to ping a host in a different IP subnetwork, you must define a static route to the network or configure a router to route between those subnets.

The **ping** command is configurable from normal executive and privileged EXEC mode. Ping returns one of the following responses:

- Normal response—The normal response (*hostname* is alive) occurs in 1 to 10 seconds, depending on network traffic.
- Destination does not respond—If the host does not respond, a No Answer message is returned.
- Unknown host—If the host does not exist, an Unknown Host message is returned.
- Destination unreachable—If the default gateway cannot reach the specified network, a Destination Unreachable message is returned.
- Network or host unreachable—If there is no entry in the route table for the host or network, a Network or Host Unreachable message is returned.

To stop a ping in progress, press **Ctrl-C**.

## Running Ping

To ping another device on the network from the switch, perform this task:

| Command                         | Purpose                               |
|---------------------------------|---------------------------------------|
| Switch# <b>ping</b> <i>host</i> | Checks connectivity to a remote host. |

This example shows how to ping a remote host from normal executive mode:

```
Switch# ping labsparc
labsparc is alive
Switch> ping 72.16.10.3
72.16.10.3 is alive
Switch#
```

This example shows how to enter a **ping** command in privileged EXEC mode specifying the number of packets, the packet size, and the timeout period:

```
Switch# ping
Target IP Address []: 12.20.5.19
Number of Packets [5]: 10
Datagram Size [56]: 100
Timeout in seconds [2]: 10
Source IP Address [12.20.2.18]: 12.20.2.18
!!!!!!!!!!

---12.20.2.19 PING Statistics---
10 packets transmitted, 10 packets received, 0% packet loss
round-trip (ms) min/avg/max = 1/1/1
Switch
```

# Using IP Traceroute

These sections describe how to use IP traceroute feature:

- Understanding How IP Traceroute Works, page 5-7
- Running IP Traceroute, page 5-7

## Understanding How IP Traceroute Works

You can use IP traceroute to identify the path that packets take through the network on a hop-by-hop basis. The command output displays all network layer (Layer 3) devices, such as routers, that the traffic passes through on the way to the destination.

Layer 2 switches can participate as the source or destination of the **trace** command but will not appear as a hop in the **trace** command output.

The **trace** command uses the Time To Live (TTL) field in the IP header to cause routers and servers to generate specific return messages. Traceroute starts by sending a User Datagram Protocol (UDP) datagram to the destination host with the TTL field set to 1. If a router finds a TTL value of 1 or 0, it drops the datagram and sends back an Internet Control Message Protocol (ICMP) Time-Exceeded message to the sender. Traceroute determines the address of the first hop by examining the source address field of the ICMP Time-Exceeded message.

To identify the next hop, traceroute sends a UDP packet with a TTL value of 2. The first router decrements the TTL field by 1 and sends the datagram to the next router. The second router sees a TTL value of 1, discards the datagram, and returns the Time-Exceeded message to the source. This process continues until the TTL is incremented to a value large enough for the datagram to reach the destination host or until the maximum TTL is reached.

To determine when a datagram reaches its destination, traceroute sets the UDP destination port in the datagram to a very large value that the destination host is unlikely to be using. When a host receives a datagram with an unrecognized port number, it sends an ICMP Port Unreachable error message to the source. The Port Unreachable error message indicates to traceroute that the destination has been reached.

## Running IP Traceroute

To trace the path that packets take through the network, perform this task in EXEC or privileged EXEC mode:

| Command                                                         | Purpose                                                                     |
|-----------------------------------------------------------------|-----------------------------------------------------------------------------|
| Switch# <b>trace</b> [ <i>protocol</i> ] [ <i>destination</i> ] | Runs IP traceroute to trace the path that packets take through the network. |

This example shows use the **trace** command to display the route a packet takes through the network to reach its destination:

```
Switch# trace ip ABA.NYC.mil

Type escape sequence to abort.
Tracing the route to ABA.NYC.mil (26.0.0.73)
 0 DEBRIS.CISCO.COM (192.180.1.6) 1000 msec 8 msec 4 msec
 1 BARRNET-GW.CISCO.COM (192.180.16.2) 8 msec 8 msec 8 msec
 2 EXTERNAL-A-GATEWAY.STANFORD.EDU (192.42.110.225) 8 msec 4 msec 4 msec
 3 BB2.SU.BARRNET.NET (192.200.254.6) 8 msec 8 msec 8 msec
 4 SU.ARC.BARRNET.NET (192.200.3.8) 12 msec 12 msec 8 msec
 5 MOFFETT-FLD-MB.in.MIL (192.52.195.1) 216 msec 120 msec 132 msec
 6 ABA.NYC.mil (26.0.0.73) 412 msec 628 msec 664 msec
Switch#
```

## Using Layer 2 Traceroute

These sections describe how to use the Layer 2 traceroute feature:

- Understanding Layer 2 Traceroute, page 5-8
- Layer 2 Traceroute Usage Guidelines, page 5-8
- Running Layer 2 Traceroute, page 5-9

## Understanding Layer 2 Traceroute

The Layer 2 traceroute feature allows the switch to identify the physical path that a packet takes from a source device to a destination device. Layer 2 traceroute supports only unicast source and destination MAC addresses. It determines the path by using the MAC address tables of the switches in the path. When the switch detects a device in the path that does not support Layer 2 traceroute, the switch continues to send Layer 2 trace queries and lets them time out.

If you want the switch to trace the path from a host on a source device to a host on a destination device, the switch can identify only the path from the source device to the destination device. It cannot identify the path that a packet takes from source host to the source device or from the destination device to the destination host.

## Layer 2 Traceroute Usage Guidelines

These are the Layer 2 traceroute usage guidelines:

- CDP must be enabled on all the devices in the network. For Layer 2 traceroute to functional properly, do not disable CDP.

If any devices in the physical path are transparent to CDP, the switch cannot identify the path through these devices.



### Note

For more information about enabling CDP, see Chapter 16, “Understanding and Configuring CDP.”

- All switches in the physical path must have IP connectivity. When a switch is reachable from another switch, you can test connectivity by using the **ping** command in privileged EXEC mode.

- The maximum number of hops identified in the path is ten.
- You can enter the **traceroute mac** or the **traceroute mac ip** command in privileged EXEC mode on a switch that is not in the physical path from the source device to the destination device. All switches in the path must be reachable from this switch.
- The **traceroute mac** command output shows the Layer 2 path only when the specified source and destination MAC addresses belong to the same VLAN. If you specify source and destination MAC addresses that belong to different VLANs, the Layer 2 path is not identified, and an error message appears.
- If you specify a multicast source or destination MAC address, the path is not identified, and an error message appears.
- If the source or destination MAC address belongs to multiple VLANs, you must specify the VLAN to which both the source and destination MAC addresses belong. If the VLAN is not specified, the path is not identified, and an error message appears.
- The **traceroute mac ip** command output shows the Layer 2 path when the specified source and destination IP addresses belong to the same subnet. When you specify the IP addresses, the switch uses Address Resolution Protocol (ARP) to associate the IP address with the corresponding MAC address and the VLAN ID.
  - If an ARP entry exists for the specified IP address, the switch uses the associated MAC address and identifies the physical path.
  - If an ARP entry does not exist, the switch sends an ARP query and tries to resolve the IP address. If the IP address is not resolved, the path is not identified, and an error message appears.
- When multiple devices are attached to one port through hubs (for example, multiple CDP neighbors are detected on a port), the Layer 2 traceroute feature is not supported. 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.

## Running Layer 2 Traceroute

To display the physical path that a packet takes from a source device to a destination device, perform either one of these tasks in privileged EXEC mode:

| Command                                                                         | Purpose                                                                          |
|---------------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| Switch# <b>traceroute mac</b> {source-mac-address}<br>{destination-mac-address} | Runs Layer 2 traceroute to trace the path that packets take through the network. |

or

| Command                                                                            | Purpose                                                                     |
|------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| Switch# <b>traceroute mac ip</b> {source-mac-address}<br>{destination-mac-address} | Runs IP traceroute to trace the path that packets take through the network. |

These examples show how to use the **tracert mac** and **tracert mac ip** commands to display the physical path a packet takes through the network to reach its destination:

```
Switch# tracert 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#

Switch# tracert 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#
```

# Configuring ICMP

Internet Control Message Protocol (ICMP) provides many services that control and manage IP connections. ICMP messages are sent by routers or access servers to hosts or other routers when a problem is discovered with the Internet header. For detailed information on ICMP, refer to RFC 792.

## Enabling ICMP Protocol Unreachable Messages

If the Cisco IOS software receives a nonbroadcast packet that uses an unknown protocol, it sends an ICMP Protocol Unreachable message back to the source.

Similarly, if the software receives a packet that it is unable to deliver to the ultimate destination because it knows of no route to the destination address, it sends an ICMP Host Unreachable message to the source. This feature is enabled by default.

To enable the generation of ICMP Protocol Unreachable and Host Unreachable messages, enter the following command in interface configuration mode:

| Command                                 | Purpose                                                                                                                           |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| Switch (config-if)# [no] ip unreachable | Enables ICMP destination unreachable messages.<br>Use the <b>no</b> keyword to disable the ICMP destination unreachable messages. |



To limit the rate that Internet Control Message Protocol (ICMP) destination unreachable messages are generated, perform this task:

| Command                                                                | Purpose                                                                                                                                           |
|------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| Switch (config)# [no] ip icmp rate-limit unreachable [df] milliseconds | Limits the rate that ICMP destination messages are generated.<br><br>Use the <b>no</b> keyword to remove the rate limit and reduce the CPU usage. |

## Enabling ICMP Redirect Messages

Data routes are sometimes less than optimal. For example, it is possible for the router to be forced to resend a packet through the same interface on which it was received. If this occurs, the Cisco IOS software sends an ICMP Redirect message to the originator of the packet telling the originator that the router is on a subnet directly connected to the receiving device, and that it must forward the packet to another system on the same subnet. The software sends an ICMP Redirect message to the packet's originator because the originating host presumably could have sent that packet to the next hop without involving this device at all. The Redirect message instructs the sender to remove the receiving device from the route and substitute a specified device representing a more direct path. This feature is enabled by default.

However, when Hot Standby Router Protocol (HSRP) is configured on an interface, ICMP Redirect messages are disabled (by default) for the interface. For more information on HSRP, refer to the following URL:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip\\_c/ipcprt1/1cdip.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_c/ipcprt1/1cdip.htm)

To enable the sending of ICMP Redirect messages if the Cisco IOS software is forced to resend a packet through the same interface on which it was received, enter the following command in interface configuration mode:

| Command                               | Purpose                                                                                                                      |
|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| Switch (config-if)# [no] ip redirects | Enables ICMP Redirect messages.<br><br>Use the <b>no</b> keyword to disable the ICMP Redirect messages and reduce CPU usage. |

## Enabling ICMP Mask Reply Messages

Occasionally, network devices must know the subnet mask for a particular subnetwork in the internetwork. To obtain this information, devices can send ICMP Mask Request messages. These messages are responded to by ICMP Mask Reply messages from devices that have the requested information. The Cisco IOS software can respond to ICMP Mask Request messages if the ICMP Mask Reply function is enabled.

To have the Cisco IOS software respond to ICMP mask requests by sending ICMP Mask Reply messages, perform this task:

| Command                                        | Purpose                                                                                                         |
|------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| Switch (config-if) # [no] <b>ip mask-reply</b> | Enables response to ICMP destination mask requests.<br>Use the <b>no</b> keyword to disable this functionality. |



## Configuring Layer 2 Ethernet Interfaces

This chapter describes how to use the command-line interface (CLI) to configure Fast Ethernet and Gigabit Ethernet interfaces for Layer 2 switching on Catalyst 4500 series switches. It also provides guidelines, procedures, and configuration examples. The configuration tasks in this chapter apply to Fast Ethernet and Gigabit Ethernet interfaces on any module, including the uplink ports on the supervisor engine.

This chapter includes the following major sections:

- Overview of Layer 2 Ethernet Switching, page 6-1
- Default Layer 2 Ethernet Interface Configuration, page 6-4
- Layer 2 Interface Configuration Guidelines and Restrictions, page 6-5
- Configuring Ethernet Interfaces for Layer 2 Switching, page 6-5



**Note**

To configure Layer 3 interfaces, see Chapter 20, “Configuring Layer 3 Interfaces.”



**Note**

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference* and related publications at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/index.htm>

## Overview of Layer 2 Ethernet Switching

The following sections describe how Layer 2 Ethernet switching works on Catalyst 4500 series switches:

- Understanding Layer 2 Ethernet Switching, page 6-1
- Understanding VLAN Trunks, page 6-3
- Layer 2 Interface Modes, page 6-4

## Understanding Layer 2 Ethernet Switching

Catalyst 4500 series switches support simultaneous, parallel connections between Layer 2 Ethernet segments. Switched connections between Ethernet segments last only for the duration of the packet. New connections can be made between different segments for successive packets.

**Note**

With release 12.1(13)EW, the Catalyst 4500 series switches can handle packets of 1600 bytes, rather than treat them as “oversized” and discard them. This size is larger than the usual IEEE Ethernet Maximum Transmission Unit (MTU) (1518 bytes) and 802.1q MTU (1522 bytes). The ability to handle larger packets is required to support two nested 802.1q headers and Multiprotocol Label Switching (MPLS) on a network.

The Catalyst 4500 series solves congestion problems caused by high-bandwidth devices and a large number of users by assigning each device (for example, a server) to its own 10-, 100-, or 1000-Mbps segment. Because each Ethernet interface on the switch represents a separate Ethernet segment, servers in a properly configured switched environment achieve full access to the bandwidth.

Because collisions are a major bottleneck in Ethernet networks, an effective solution is full-duplex communication. Normally, Ethernet operates in half-duplex mode, which means that stations can either receive or transmit. In full-duplex mode, two devices can transmit and receive at the same time. When packets can flow in both directions simultaneously, effective Ethernet bandwidth doubles to 20 Mbps for 10-Mbps interfaces and to 200 Mbps for Fast Ethernet interfaces. Gigabit Ethernet interfaces on the Catalyst 4500 series switch are full-duplex mode only, providing 2-Gbps effective bandwidth.

## Switching Frames Between Segments

Each Ethernet interface on a Catalyst 4500 series switch can connect to a single workstation or server, or to a hub through which workstations or servers connect to the network.

On a typical Ethernet hub, all ports connect to a common backplane within the hub, and the bandwidth of the network is shared by all devices attached to the hub. If two devices establish a session that uses a significant level of bandwidth, the network performance of all other stations attached to the hub is degraded.

To reduce degradation, the switch treats each interface as an individual segment. When stations on different interfaces need to communicate, the switch forwards frames from one interface to the other at wire speed to ensure that each session receives full bandwidth.

To switch frames between interfaces efficiently, the switch maintains an address table. When a frame enters the switch, it associates the MAC address of the sending station with the interface on which it was received.

## Building the MAC Address Table

The Catalyst 4500 series builds the MAC address table by using the source address of the frames received. When the switch receives a frame for a destination address not listed in its MAC address table, it floods the frame to all interfaces of the same VLAN except the interface that received the frame. When the destination device replies, the switch adds its relevant source address and interface ID to the address table. The switch then forwards subsequent frames to a single interface without flooding to all interfaces.

The address table can store at least 32,000 address entries without flooding any entries. The switch uses an aging mechanism, defined by a configurable aging timer, so if an address remains inactive for a specified number of seconds, it is removed from the address table.

## Understanding VLAN Trunks

A trunk is a point-to-point link between one or more Ethernet switch interfaces and another networking device such as a router or a switch. Trunks carry the traffic of multiple VLANs over a single link and allow you to extend VLANs across an entire network.

Two trunking encapsulations are available on all Ethernet interfaces:

- Inter-Switch Link (ISL) Protocol—ISL is a Cisco-proprietary trunking encapsulation.

**Note**

The blocking Gigabit ports on the WS-X4418-GB and WS-X4412-2GB-T modules do not support ISL. Ports 3 to 18 are blocking Gigabit ports on the WS-X4418-GB module. Ports 1 to 12 are blocking Gigabit ports on the WS-X4412-2GB-T module.

- 802.1Q—802.1Q is an industry-standard trunking encapsulation.

You can configure a trunk on a single Ethernet interface or on an EtherChannel bundle. For more information about EtherChannel, see Chapter 17, “Understanding and Configuring EtherChannel.”

Ethernet trunk interfaces support different trunking modes (see Table 6-2). You can specify whether the trunk uses ISL encapsulation, 802.1Q encapsulation, or if the encapsulation type is autonegotiated.

To autonegotiate trunking, make sure your interfaces are in the same VTP domain. Use the **trunk** or **nonegotiate** keywords to force interfaces in different domains to trunk. For more information on VTP domains, see Chapter 11, “Understanding and Configuring VTP.”

Trunk negotiation is managed by the Dynamic Trunking Protocol (DTP). DTP supports autonegotiation of both ISL and 802.1Q trunks.

## Encapsulation Types

Table 6-1 lists the Ethernet trunk encapsulation types.

**Table 6-1** Ethernet Trunk Encapsulation Types

| Encapsulation Type | Encapsulation Command                           | Purpose                                                                                                                                                                                           |
|--------------------|-------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ISL                | <b>switchport trunk encapsulation isl</b>       | Specifies ISL encapsulation on the trunk link.                                                                                                                                                    |
| 802.1Q             | <b>switchport trunk encapsulation dot1q</b>     | Specifies 802.1Q encapsulation on the trunk link.                                                                                                                                                 |
| Negotiate          | <b>switchport trunk encapsulation negotiate</b> | Specifies that the interface negotiate with the neighboring interface to become an ISL (preferred) or 802.1Q trunk, depending on the configuration and capabilities of the neighboring interface. |

The trunking mode, the trunk encapsulation type, and the hardware capabilities of the two connected interfaces determine whether a link becomes an ISL or 802.1Q trunk.

## Layer 2 Interface Modes

Table 6-2 lists the Layer 2 interface modes and describes how they function on Ethernet interfaces.

**Table 6-2** *Layer 2 Interface Modes*

| Mode                              | Purpose                                                                                                                                                                                                                                                                  |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| switchport mode access            | Puts the interface into permanent nontrunking mode and negotiates to convert the link into a nontrunking link. The interface becomes a nontrunk interface even if the neighboring interface does not change.                                                             |
| switchport mode dynamic desirable | Makes the interface actively attempt to convert the link to a trunking link. The interface becomes a trunk interface if the neighboring interface is set to <b>trunk</b> , <b>desirable</b> , or <b>auto</b> mode. This is the default mode for all Ethernet interfaces. |
| switchport mode dynamic auto      | Makes the interface convert the link to a trunking link if the neighboring interface is set to <b>trunk</b> or <b>desirable</b> mode. This is the default mode for all Ethernet interfaces.                                                                              |
| switchport mode trunk             | Puts the interface into permanent trunking mode and negotiates to convert the link into a trunking link. The interface becomes a trunk interface even if the neighboring interface does not change.                                                                      |
| switchport nonegotiate            | Puts the interface into permanent trunking mode but prevents the interface from generating DTP frames. You must configure the neighboring interface manually as a trunk interface to establish a trunking link.                                                          |



**Note**

DTP is a point-to-point protocol. However, some internetworking devices might forward DTP frames improperly. To avoid this problem, ensure that interfaces connected to devices that do not support DTP are configured with the **access** keyword if you do not intend to trunk across those links. To enable trunking to a device that does not support DTP, use the **nonegotiate** keyword to cause the interface to become a trunk without generating DTP frames.

## Default Layer 2 Ethernet Interface Configuration

Table 6-3 shows the Layer 2 Ethernet interface default configuration.

**Table 6-3** *Layer 2 Ethernet Interface Default Configuration*

| Feature                         | Default Value                            |
|---------------------------------|------------------------------------------|
| Interface mode                  | switchport mode dynamic auto             |
| Trunk encapsulation             | switchport trunk encapsulation negotiate |
| Allowed VLAN range              | VLANs 1–1005                             |
| VLAN range eligible for pruning | VLANs 2–1001                             |
| Default VLAN (for access ports) | VLAN 1                                   |

**Table 6-3 Layer 2 Ethernet Interface Default Configuration (continued)**

| Feature                              | Default Value                                                                                                                                                                                          |
|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Native VLAN (for 802.1Q only trunks) | VLAN 1                                                                                                                                                                                                 |
| STP <sup>1</sup>                     | Enabled for all VLANs                                                                                                                                                                                  |
| STP port priority                    | 128                                                                                                                                                                                                    |
| STP port cost                        | <ul style="list-style-type: none"><li>• 19 for 10/100-Mbps Fast Ethernet interfaces</li><li>• 19 for 100-Mbps Fast Ethernet interfaces</li><li>• 4 for 1000-Mbps Gigabit Ethernet interfaces</li></ul> |

1. STP = Spanning Tree Protocol

## Layer 2 Interface Configuration Guidelines and Restrictions

Keep the following guidelines and restrictions in mind when you configure Layer 2 interfaces:

- In a network of Cisco switches connected through 802.1Q trunks, the switches maintain one instance of spanning tree for each VLAN allowed on the trunks. Non-Cisco 802.1Q switches maintain only one instance of spanning tree for all VLANs allowed on the trunks.

When you connect a Cisco switch to a non-Cisco device through an 802.1Q trunk, the Cisco switch combines the spanning tree instance of the native VLAN of the trunk with the spanning tree instance of the non-Cisco 802.1Q switch. However, spanning tree information for each VLAN is maintained by Cisco switches separated by a cloud of non-Cisco 802.1Q switches. The non-Cisco 802.1Q cloud separating the Cisco switches is treated as a single trunk link between the switches.

- Make sure the native VLAN for an 802.1Q trunk is the same on both ends of the trunk link. If the VLAN on one end of the trunk is different from the VLAN on the other end, spanning tree loops might result.
- Disabling spanning tree on any VLAN of an 802.1Q trunk can cause spanning tree loops.

## Configuring Ethernet Interfaces for Layer 2 Switching

The following sections describe how to configure Layer 2 switching on a Catalyst 4500 series switch:

- Configuring an Ethernet Interface as a Layer 2 Trunk, page 6-6
- Configuring an Interface as a Layer 2 Access Port, page 6-8
- Clearing Layer 2 Configuration, page 6-9

## Configuring an Ethernet Interface as a Layer 2 Trunk



### Note

The default for Layer 2 interfaces is **switchport mode dynamic auto**. If the neighboring interface supports trunking and is configured to trunk mode or dynamic desirable mode, the link becomes a Layer 2 trunk. By default, trunks negotiate encapsulation. If the neighboring interface supports ISL and 802.1Q encapsulation and both interfaces are set to negotiate the encapsulation type, the trunk uses ISL encapsulation.

To configure an interface as a Layer 2 trunk, perform this task:

|         | Command                                                                                                                                                             | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1  | Switch(config)# <b>interface</b> { <b>fastethernet</b>   <b>gigabitethernet</b> } <i>slot/port</i>                                                                  | Specifies the interface to configure.                                                                                                                                                                                                                                                                                                                                                                                                 |
| Step 2  | Switch(config-if)# <b>shutdown</b>                                                                                                                                  | (Optional) Shuts down the interface to prevent traffic flow until configuration is complete.                                                                                                                                                                                                                                                                                                                                          |
| Step 3  | Switch(config-if)# <b>switchport trunk encapsulation</b> { <b>isl</b>   <b>dot1q</b>   <b>negotiate</b> }                                                           | (Optional) Specifies the encapsulation.<br><br><b>Note</b> You must enter this command with either the <b>isl</b> or <b>dot1q</b> keyword to support the <b>switchport mode trunk</b> command, which is not supported by the default mode ( <b>negotiate</b> ).                                                                                                                                                                       |
| Step 4  | Switch(config-if)# <b>switchport mode</b> { <b>dynamic</b> { <b>auto</b>   <b>desirable</b> }   <b>trunk</b> }                                                      | Configures the interface as a Layer 2 trunk. (Required only if the interface is a Layer 2 access port or to specify the trunking mode.)                                                                                                                                                                                                                                                                                               |
| Step 5  | Switch(config-if)# <b>switchport access vlan</b> <i>vlan_num</i>                                                                                                    | (Optional) Specifies the access VLAN, which is used if the interface stops trunking. The access VLAN is not used as the native VLAN.<br><br><b>Note</b> The <i>vlan_num</i> parameter is either a single VLAN number from 1 to 1005 or a range of VLANs described by two VLAN numbers, the lesser one first, separated by a dash. Do not enter any spaces between comma-separated <i>vlan</i> parameters or in dash-specified ranges. |
| Step 6  | Switch(config-if)# <b>switchport trunk native vlan</b> <i>vlan_num</i>                                                                                              | For 802.1Q trunks, specifies the native VLAN.<br><br><b>Note</b> If you do not set the native VLAN, the default is used (VLAN 1).                                                                                                                                                                                                                                                                                                     |
| Step 7  | Switch(config-if)# <b>switchport trunk allowed vlan</b> { <b>add</b>   <b>except</b>   <b>all</b>   <b>remove</b> }<br><i>vlan_num[,vlan_num[,vlan_num[,...]]]</i>  | (Optional) Configures the list of VLANs allowed on the trunk. All VLANs are allowed by default. You cannot remove any of the default VLANs from a trunk.                                                                                                                                                                                                                                                                              |
| Step 8  | Switch(config-if)# <b>switchport trunk pruning vlan</b> { <b>add</b>   <b>except</b>   <b>none</b>   <b>remove</b> }<br><i>vlan_num[,vlan_num[,vlan_num[,...]]]</i> | (Optional) Configures the list of VLANs allowed to be pruned from the trunk (see the “Understanding VTP Pruning” section on page 11-3). The default list of VLANs allowed to be pruned contains all VLANs, except for VLAN 1.                                                                                                                                                                                                         |
| Step 9  | Switch(config-if)# <b>no shutdown</b>                                                                                                                               | Activates the interface. (Required only if you shut down the interface.)                                                                                                                                                                                                                                                                                                                                                              |
| Step 10 | Switch(config-if)# <b>end</b>                                                                                                                                       | Exits interface configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                   |



|         | Command                                                                                                               | Purpose                                                  |
|---------|-----------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|
| Step 11 | Switch# <b>show running-config interface</b><br>{ <b>fastethernet</b>   <b>gigabitethernet</b> }<br><i>slot/port</i>  | Displays the running configuration of the interface.     |
| Step 12 | Switch# <b>show interfaces</b> [ <b>fastethernet</b>  <br><b>gigabitethernet</b> ] <i>slot/port</i> <b>switchport</b> | Displays the switch port configuration of the interface. |
| Step 13 | Switch# <b>show interfaces</b> [{ <b>fastethernet</b>  <br><b>gigabitethernet</b> } <i>slot/port</i> ] <b>trunk</b>   | Displays the trunk configuration of the interface.       |

This example shows how to configure the Fast Ethernet interface 5/8 as an 802.1Q trunk. This example assumes that the neighbor interface is configured to support 802.1Q trunking and that the native VLAN defaults to VLAN 1:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 5/8
Switch(config-if)# shutdown
Switch(config-if)# switchport mode dynamic desirable
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# no shutdown
Switch(config-if)# end
Switch# exit
```

This example shows how to verify the running configuration:

```
Switch# show running-config interface fastethernet 5/8
Building configuration...
Current configuration:
!
interface FastEthernet5/8
 switchport mode dynamic desirable
 switchport trunk encapsulation dot1q
end
```

This example shows how to verify the switch port configuration:

```
Switch# show interfaces fastethernet 5/8 switchport
Name: Fa5/8
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: trunk
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Enabled
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
```

This example shows how to verify the trunk configuration:

```
Switch# show interfaces fastethernet 5/8 trunk

Port Mode Encapsulation Status Native vlan
Fa5/8 desirable n-802.1q trunking 1

Port Vlans allowed on trunk
Fa5/8 1-1005

Port Vlans allowed and active in management domain
Fa5/8 1-6,10,20,50,100,152,200,300,303-305,349-351,400,500,521,524,570,801-8
02,850,917,999,1002-1005
```

```

Port Vlans in spanning tree forwarding state and not pruned
Fa5/8 1-6,10,20,50,100,152,200,300,303-305,349-351,400,500,521,524,570,801-8
02,850,917,999,1002-1005

Switch#

```

## Configuring an Interface as a Layer 2 Access Port



**Note**

If you assign an interface to a VLAN that does not exist, the interface is not operational until you create the VLAN in the VLAN database (see the “Configuring VLANs in Global Configuration Mode” section on page 8-5).

To configure an interface as a Layer 2 access port, perform this task:

|               | Command                                                                                                               | Purpose                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------|-----------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Switch(config)# <b>interface</b> { <b>fastethernet</b>   <b>gigabitethernet</b> } <i>slot/port</i>                    | Specifies the interface to configure.                                                                                                                                                                                                                                                                                                                                                                |
| <b>Step 2</b> | Switch(config-if)# <b>shutdown</b>                                                                                    | (Optional) Shuts down the interface to prevent traffic flow until configuration is complete.                                                                                                                                                                                                                                                                                                         |
| <b>Step 3</b> | Switch(config-if)# <b>switchport</b>                                                                                  | Configures the interface for Layer 2 switching: <ul style="list-style-type: none"> <li>You must enter the <b>switchport</b> command once without any keywords to configure the interface as a Layer 2 port before you can enter additional <b>switchport</b> commands with keywords.</li> <li>Required only if you previously entered the <b>no switchport</b> command for the interface.</li> </ul> |
| <b>Step 4</b> | Switch(config-if)# <b>switchport mode access</b>                                                                      | Configures the interface as a Layer 2 access port.                                                                                                                                                                                                                                                                                                                                                   |
| <b>Step 5</b> | Switch(config-if)# <b>switchport access vlan</b> <i>vlan_num</i>                                                      | Place the interface in a VLAN.                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Step 6</b> | Switch(config-if)# <b>no shutdown</b>                                                                                 | Activates the interface. (Required only if you had shut down the interface.)                                                                                                                                                                                                                                                                                                                         |
| <b>Step 7</b> | Switch(config-if)# <b>end</b>                                                                                         | Exits interface configuration mode.                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Step 8</b> | Switch# <b>show running-config interface</b> { <b>fastethernet</b>   <b>gigabitethernet</b> } <i>slot/port</i>        | Displays the running configuration of the interface.                                                                                                                                                                                                                                                                                                                                                 |
| <b>Step 9</b> | Switch# <b>show interfaces</b> [{ <b>fastethernet</b>   <b>gigabitethernet</b> } <i>slot/port</i> ] <b>switchport</b> | Displays the switch port configuration of the interface.                                                                                                                                                                                                                                                                                                                                             |

This example shows how to configure the Fast Ethernet interface 5/6 as an access port in VLAN 200:

```

Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 5/6
Switch(config-if)# shutdown
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 200
Switch(config-if)# no shutdown
Switch(config-if)# end
Switch# exit

```

This example shows how to verify the running configuration:

```
Switch# show running-config interface fastethernet 5/6
Building configuration...
!
Current configuration :33 bytes
interface FastEthernet 5/6
 switchport access vlan 200
 switchport mode access
end
```

This example shows how to verify the switch port configuration:

```
Switch# show running-config interface fastethernet 5/6 switchport
Name:Fa5/6
Switchport:Enabled
Administrative Mode:dynamic auto
Operational Mode:static access
Administrative Trunking Encapsulation:negotiate
Operational Trunking Encapsulation:native
Negotiation of Trunking:On
Access Mode VLAN:1 (default)
Trunking Native Mode VLAN:1 (default)
Administrative private-vlan host-association:none
Administrative private-vlan mapping:none
Operational private-vlan:none
Trunking VLANs Enabled:ALL
Pruning VLANs Enabled:2-1001
Switch#
```

## Clearing Layer 2 Configuration

To clear the Layer 2 configuration on an interface, perform this task:

|        | Command                                                                                                               | Purpose                                                  |
|--------|-----------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|
| Step 1 | Switch(config)# <b>default interface</b> { <b>fastethernet</b>   <b>gigabitethernet</b> } <i>slot/port</i>            | Specifies the interface to clear.                        |
| Step 2 | Switch(config-if)# <b>end</b>                                                                                         | Exits interface configuration mode.                      |
| Step 3 | Switch# <b>show running-config interface</b> { <b>fastethernet</b>   <b>gigabitethernet</b> } <i>slot/port</i>        | Displays the running configuration of the interface.     |
| Step 4 | Switch# <b>show interfaces</b> [{ <b>fastethernet</b>   <b>gigabitethernet</b> } <i>slot/port</i> ] <b>switchport</b> | Displays the switch port configuration of the interface. |

This example shows how to clear the Layer 2 configuration on the Fast Ethernet interface 5/6:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# default interface fastethernet 5/6
Switch(config)# end
Switch# exit
```

This example shows how to verify that the Layer 2 configuration was cleared:

```
Switch# show running-config interface fastethernet 5/6
Building configuration...
Current configuration:
!
interface FastEthernet5/6
end
```

This example shows how to verify the switch port configuration:

```
Switch# show interfaces fastethernet 5/6 switchport
Name: Fa5/6
Switchport: Enabled
Switch#
```



## Configuring Unidirectional Ethernet

This chapter describes how to configure Unidirectional Ethernet on the Catalyst 4500 series switch.



### Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference* and the publications at this URL: <http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/index.htm>

You can set non-blocking GigaPorts to unidirectionally transmit or receive traffic. Unidirectional Ethernet uses only one strand of fiber for either transmitting or receiving one-way traffic for the GigaPort, instead of two strands of fiber for a full-duplex GigaPort Ethernet. Configuring your GigaPorts either to transmit or receive traffic effectively doubles the amount of traffic capabilities for applications, such as video streaming, where most traffic is sent as unacknowledged unidirectional video broadcast streams.



### Note

Enabling Unidirectional Ethernet on the non blocking GigaPort will automatically disable UDLD on the port.

To enable Unidirectional Ethernet, perform this task:

|        | Command                                                                                                                 | Purpose                                                                                           |
|--------|-------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| Step 1 | Switch(config)# <b>interface</b> {vlan vlan_ID   {fastethernet   gigabitethernet} slot/interface   Port-channel number} | Selects the interface to configure.                                                               |
| Step 2 | Switch(config-if)# [no] <b>unidirectional</b> {send-only   receive-only}                                                | Enables Unidirectional Ethernet.<br>Use the <b>no</b> keyword to disable Unidirectional Ethernet. |
| Step 3 | Switch(config-if)# <b>end</b>                                                                                           | Exits configuration mode.                                                                         |
| Step 4 | Switch# <b>show interface</b> {vlan vlan_ID   {fastethernet   gigabitethernet} slot/interface} <b>unidirectional</b>    | Verifies the configuration.                                                                       |

This example shows how to set Gigabit Ethernet interface 1/1 to unidirectionally send traffic:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet 1/1
Switch(config-if)# unidirectional send-only
Switch(config-if)# end
```

Warning!

Enable 12 port unidirectional mode will automatically disable port uddl. You must manually ensure that the unidirectional link does not create a spanning tree loop in the network.

Enable 13 port unidirectional mode will automatically disable ip routing on the port. You must manually configure static ip route and arp entry in order to route ip traffic.

This example shows how to set Gigabit Ethernet interface 1/1 to receive traffic unidirectionally:

```
Switch# configure 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
```

Warning!

Enable 12 port unidirectional mode will automatically disable port uddl. You must manually ensure that the unidirectional link does not create a spanning tree loop in the network.

Enable 13 port unidirectional mode will automatically disable ip routing on the port. You must manually configure static ip route and arp entry in order to route ip traffic.

This example shows how to verify the configuration

```
Switch>show interface gigabitethernet 1/1 unidirectional
show interface gigabitethernet 1/1 unidirectional
Unidirectional configuration mode: send only
CDP neighbour unidirectional configuration mode: receive only
```

This example shows how to disable Unidirectional Ethernet on Gigabit Ethernet interface 1/1:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet 1/1
Switch(config-if)# no unidirectional
Switch(config-if)# end
```

This example shows the result of issuing the **show interface** command for a port that does not support unidirectional ethernet:

```
Switch#show interface f6/1 unidirectional
Unidirectional Ethernet is not supported on FastEthernet6/1
```



# Understanding and Configuring VLANs

This chapter describes VLANs on Catalyst 4500 series switches. It also provides guidelines, procedures, and configuration examples.

This chapter includes the following major sections:

- Overview of VLANs, page 8-1
- VLAN Configuration Guidelines and Restrictions, page 8-3
- VLAN Default Configuration, page 8-4
- Configuring VLANs, page 8-4



**Note**

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference* and related publications at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/index.htm>

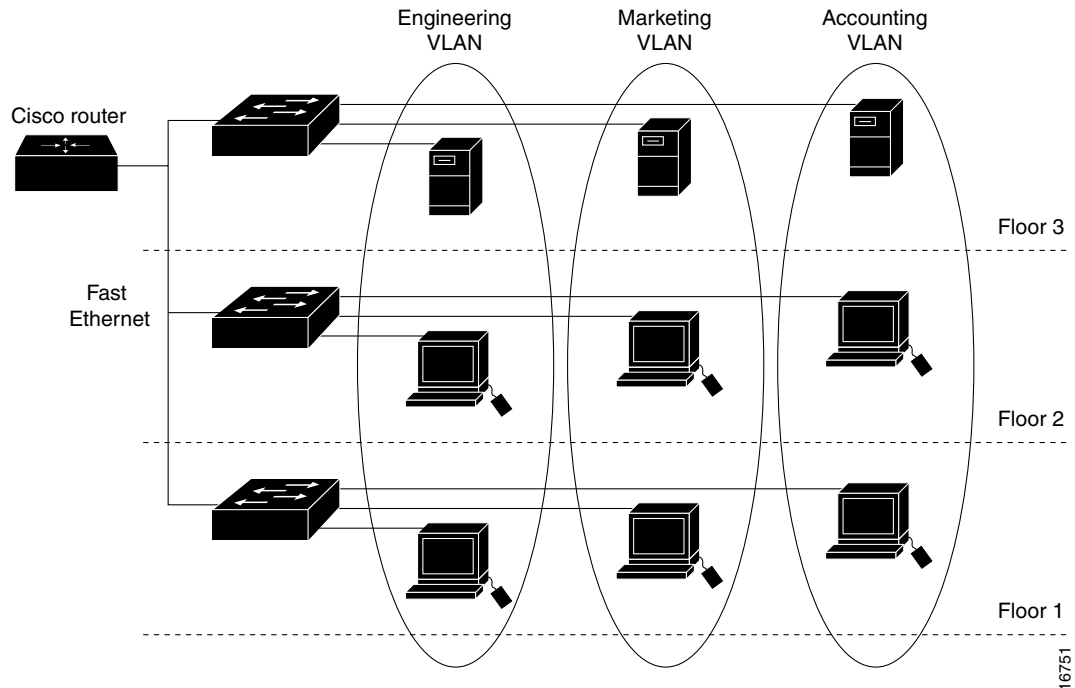
## Overview of VLANs

A VLAN is a group of devices on one or more LANs that are configured to communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

VLANs define broadcast domains in a Layer 2 network. A broadcast domain is the set of all devices that will receive broadcast frames originating from any device within the set. Broadcast domains are typically bounded by routers because routers do not forward broadcast frames. Layer 2 switches create broadcast domains based on the configuration of the switch. Switches are multiport bridges that allow you to create multiple broadcast domains. Each broadcast domain is like a distinct virtual bridge within a switch.

You can define one or many virtual bridges within a switch. Each virtual bridge you create in the switch defines a new broadcast domain (VLAN). Traffic cannot pass directly to another VLAN (between broadcast domains) within the switch or between two switches. To interconnect two different VLANs, you must use routers or Layer 3 switches. See the “Overview of Layer 3 Interfaces” section on page 20-1 for information on inter-VLAN routing on Catalyst 4500 series switches.

Figure 8-1 shows an example of three VLANs that create logically defined networks.

**Figure 8-1 Sample VLANs**

VLANs are often associated with IP subnetworks. For example, all of the end stations in a particular IP subnet belong to the same VLAN. Traffic between VLANs must be routed. You must assign LAN interface VLAN membership on an interface-by-interface basis (this is known as interface-based or static VLAN membership).

You can set the following parameters when you create a VLAN in the management domain:

- VLAN number
- VLAN name
- VLAN type
- VLAN state (active or suspended)
- Maximum transmission unit (MTU) for the VLAN
- Security Association Identifier (SAID)
- VLAN number to use when translating from one VLAN type to another


**Note**

When the software translates from one VLAN type to another, it requires a different VLAN number for each media type.



# VLAN Configuration Guidelines and Restrictions

Follow these guidelines and restrictions when creating and modifying VLANs in your network:

- Before creating a VLAN, put the Catalyst 4500 series switch in VTP server mode or VTP transparent mode. If the Catalyst 4500 series switch is a VTP server, you must define a VTP domain. For information on configuring VTP, see Chapter 11, “Understanding and Configuring VTP.”
- The Cisco IOS **end** command is not supported in VLAN database mode.
- You cannot use **Ctrl-Z** to exit VLAN database mode.

## VLAN Ranges



### Note

You must enable the extended system ID to use 4094 VLANs. See the “Understanding the Bridge ID” section on page 12-2.

With Cisco IOS Release 12.1(11)EW and later, Catalyst 4500 series switches support 4096 VLANs in compliance with the IEEE 802.1Q standard. These VLANs are organized into three ranges: reserved, normal, and extended.

Some of these VLANs are propagated to other switches in the network when you use the VLAN Trunking Protocol (VTP). The extended-range VLANs are not propagated, so you must configure extended-range VLANs manually on each network device.

Table 8-1 describes the uses for VLAN ranges.

**Table 8-1 VLAN Ranges**

| VLANs     | Range    | Usage                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Propagated by VTP |
|-----------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|
| 0, 4095   | Reserved | For system use only. You cannot see or use these VLANs.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | N/A               |
| 1         | Normal   | Cisco default. You can use this VLAN but you cannot delete it.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Yes               |
| 2–1001    | Normal   | Used for Ethernet VLANs; you can create, use, and delete these VLANs.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Yes               |
| 1002–1005 | Normal   | Cisco defaults for FDDI and Token Ring. You cannot delete VLANs 1002–1005.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Yes               |
| 1006–4094 | Extended | For Ethernet VLANs only. When configuring extended-range VLANs, note the following: <ul style="list-style-type: none"> <li>• Layer 3 ports and some software features require internal VLANs. Internal VLANs are allocated from 1006 and up. You cannot use a VLAN that has been allocated for such use. To display the VLANs used internally, enter the <b>show vlan internal usage</b> command.</li> <li>• Switches running Catalyst product family software do not support configuration of VLANs 1006–1024. If you configure VLANs 1006–1024, ensure that the VLANs do not extend to any switches running Catalyst product family software.</li> <li>• You must enable the extended system ID to use extended range VLANs. See the “Enabling the Extended System ID” section on page 12-8.</li> </ul> | No                |

## Configurable Normal-Range VLAN Parameters

**Note**

Ethernet VLANs 1 and 1006 through 4094 use only default values.

You can configure the following parameters for VLANs 2 through 1001:

- VLAN name
- VLAN type
- VLAN state (active or suspended)
- SAID
- STP type for VLANs

## VLAN Default Configuration

Table 8-2 shows the default VLAN configuration values.

**Table 8-2 Ethernet VLAN Defaults and Ranges**

| Parameter              | Default                                                    | Valid Values              |
|------------------------|------------------------------------------------------------|---------------------------|
| VLAN ID                | 1                                                          | 1–4094                    |
| VLAN name              | VLAN $x$ , where $x$ is a number assigned by the software. | No range                  |
| 802.10 SAID            | 100,001                                                    | 1–4,294,967,294           |
| MTU size               | 1500                                                       | 1500–18,190               |
| Translational bridge 1 | 1002                                                       | 0–1005                    |
| Translational bridge 2 | 1003                                                       | 0–1005                    |
| VLAN state             | active                                                     | active; suspend; shutdown |

**Note**

Catalyst 4500 series switches do not support Token Ring or FDDI media. The switch does not forward FDDI, FDDI-NET, TrCRF, or TrBRF traffic, but it does propagate the VLAN configuration via VTP. The software reserves parameters for these media types, but they are not truly supported.

## Configuring VLANs

**Note**

Before you configure VLANs, you must use VLAN Trunking Protocol (VTP) to maintain global VLAN configuration information for your network. For complete information on VTP, see Chapter 11, “Understanding and Configuring VTP.”

**Note**

VLANs support a number of parameters that are not discussed in detail in this section. For complete information, refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference*.

**Note**

The VLAN configuration is stored in the **vlan.dat** file, which is stored in nonvolatile memory. You can cause inconsistency in the VLAN database if you manually delete the **vlan.dat** file. If you want to modify the VLAN configuration or VTP, use the commands described in the following sections and in the *Catalyst 4500 Series Switch Cisco IOS Command Reference*.

These sections describe how to configure VLANs:

- Configuring VLANs in Global Configuration Mode, page 8-5
- Configuring VLANs in VLAN Database Mode, page 8-7
- Assigning a Layer 2 LAN Interface to a VLAN, page 8-8

## Configuring VLANs in Global Configuration Mode

If the switch is in VTP server or transparent mode (see the “Configuring VTP” section on page 11-6), you can configure VLANs in global and VLAN configuration modes. When you configure VLANs in global and config-vlan configuration modes, the VLAN configuration is saved in the **vlan.dat** files, not the **running-config** or **startup-config** files. To display the VLAN configuration, enter the **show vlan** command.

If the switch is in VLAN transparent mode, use the **copy running-config startup-config** command to save the VLAN configuration to the **startup-config** file. After you save the running configuration as the startup configuration, the **show running-config** and **show startup-config** commands display the VLAN configuration.

**Note**

When the switch boots, if the VTP domain name and VTP mode in the **startup-config** and **vlan.dat** files do not match, the switch uses the configuration in the **vlan.dat** file.

You use the interface configuration command mode to define the port membership mode and add and remove ports from a VLAN. The results of these commands are written to the **running-config** file, and you can display the contents of the file by entering the **show running-config** command.

User-configured VLANs have unique IDs from 1 to 4094. To create a VLAN, enter the **vlan** command with an unused ID. To verify whether a particular ID is in use, enter the **show vlan id ID** command. To modify a VLAN, enter the **vlan** command for an existing VLAN.

See the “VLAN Default Configuration” section on page 8-4 for the list of default parameters that are assigned when you create a VLAN. If you do not use the **media** keyword when specifying the VLAN type, the VLAN is an Ethernet VLAN.

To create a VLAN, perform this task:

|        | Command                                                               | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------|-----------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch# <b>configure terminal</b>                                     | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Step 2 | Switch(config)# <b>vlan</b> <i>vlan_ID</i><br>Switch(config-vlan)#    | <p>Adds an Ethernet VLAN.</p> <p><b>Note</b> You cannot delete the default VLANs for these media types: Ethernet VLAN 1 and FDDI or Token Ring VLANs 1002 to 1005.</p> <p>When you delete a VLAN, any LAN interfaces configured as access ports assigned to that VLAN become inactive. They remain associated with the VLAN (and thus inactive) until you assign them to a new VLAN.</p> <p>You can use the <b>no</b> keyword to delete a VLAN.</p> <p>When the prompt reads <code>Switch(config-vlan)#</code>, you are in vlan-configuration mode. If you wish to change any of the parameters for the newly created VLAN, use this mode.</p> |
| Step 3 | Switch(config-vlan)# <b>end</b>                                       | Returns to enable mode from vlan-configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Step 4 | Switch# <b>show vlan</b> [ <i>id</i>   <i>name</i> ] <i>vlan_name</i> | Verifies the VLAN configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

When you create or modify an Ethernet VLAN, note the following:

- Because Layer 3 ports and some software features require internal VLANs allocated from 1006 and up, configure extended-range VLANs starting with 4094 and work downward.
- You can configure extended-range VLANs only in global configuration mode. You cannot configure extended-range VLANs in VLAN database mode.
- Layer 3 ports and some software features use extended-range VLANs. If the VLAN you are trying to create or modify is being used by a Layer 3 port or a software feature, the switch displays a message and does not modify the VLAN configuration.

This example shows how to create an Ethernet VLAN in global configuration mode and verify the configuration:

```
Switch# configure terminal
Switch(config)# vlan 3
Switch(config-vlan)# end
Switch# show vlan id 3
```

| VLAN Name  | Status | Ports |
|------------|--------|-------|
| 3 VLAN0003 | active |       |

```

VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2

3 enet 100003 1500 - - - - - 0 0
Primary Secondary Type Interfaces

Switch#
```

## Configuring VLANs in VLAN Database Mode

When the switch is in VTP server or transparent mode, you can configure VLANs in the VLAN database mode. When you configure VLANs in VLAN database mode, the VLAN configuration is saved in the **vlan.dat** file, not the **running-config** or **startup-config** files. To display the VLAN configuration, enter the **show running-config vlan** command.

User-configurable VLANs have unique IDs from 1 to 4094. Database mode supports configuration of IDs from 1 to 1001, but not the extended addresses from 1006 to 4094. To create a VLAN, enter the **vlan** command with an unused ID. To verify whether a particular ID is in use, enter the **show vlan id ID** command. To modify a VLAN, enter the **vlan** command for an existing VLAN.

See the “VLAN Default Configuration” section on page 8-4 for a listing of the default parameters that are assigned when you create a VLAN. If you do not use the **media** keyword when specifying the VLAN type, the VLAN is an Ethernet VLAN.

To create a VLAN, perform this task:

|        | Command                                                               | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------|-----------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch# <b>vlan database</b>                                          | Enters VLAN database mode.                                                                                                                                                                                                                                                                                                                                                                                                               |
| Step 2 | Switch(vlan)# <b>vlan</b> <i>vlan_ID</i>                              | Adds an Ethernet VLAN.<br><br><b>Note</b> You cannot delete the default VLANs for these media types: Ethernet VLAN 1 and FDDI or Token Ring VLANs 1002 to 1005.<br>When you delete a VLAN, any LAN interfaces configured as access ports assigned to that VLAN become inactive. They remain associated with the VLAN (and thus inactive) until you assign them to a new VLAN.<br><br>You can use the <b>no</b> keyword to delete a VLAN. |
| Step 3 | Switch(vlan)# <b>exit</b>                                             | Returns to enable mode.                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Step 4 | Switch# <b>show vlan</b> [ <i>id</i>   <i>name</i> ] <i>vlan_name</i> | Verifies the VLAN configuration.                                                                                                                                                                                                                                                                                                                                                                                                         |

This example shows how to create an Ethernet VLAN in VLAN database mode and verify the configuration:

```
Switch# vlan database
Switch(vlan)# vlan 3
VLAN 3 added:
 Name: VLAN0003
Switch(vlan)# exit
APPLY completed.
Exiting...
Switch# show vlan name VLAN0003
VLAN Name Status Ports

3 VLAN0003 active

VLAN Type SAID MTU Parent RingNo BridgeNo Stp Trans1 Trans2

3 enet 100003 1500 - - - - 0 0
Switch#
```

## Assigning a Layer 2 LAN Interface to a VLAN

A VLAN created in a management domain remains unused until you assign one or more LAN interfaces to the VLAN.

**Note**

---

Makes sure you assign LAN interfaces to a VLAN of the proper type. Assign Fast Ethernet and Gigabit Ethernet interfaces to Ethernet-type VLANs.

---

To assign one or more LAN interfaces to a VLAN, complete the procedures in the “Configuring Ethernet Interfaces for Layer 2 Switching” section on page 6-5.



## Configuring Dynamic VLAN Membership

This chapter describes how to configure dynamic port VLAN membership by using the VLAN Membership Policy Server (VMPS).

This chapter includes the following major sections:

- Understanding VMPS, page 9-1
- Configuring Dynamic VLAN Membership, page 9-4
- VMPS Database Configuration File Example, page 9-8



**Note**

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference* and related publications at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/index.htm>

## Understanding VMPS

With the VMPS, you can dynamically assign switch ports to VLANs based on the source Media Access Control (MAC) address of the device connected to the port. When you move a host from a port on one switch in the network to a port on another switch in the network, that switch dynamically assigns the new port to the proper VLAN for that host.

A Catalyst 4500 series switch can be a member switch or a command switch in a cluster of switches managed as a single entity. The communication between VMPS and a member switch is managed by the command switch. In this description, the VMPS client is always the command switch.

A Catalyst 4500 series switch acts as a client to the VMPS and communicates with it by using the VLAN Query Protocol (VQP). When the VMPS receives a VQP request from a client switch, the VMPS searches its database for a MAC address-to-VLAN mapping. The server response is based on this mapping. If the server is in secure mode, the server shuts down the port when a VLAN is not allowed on it, or the server simply denies the port access to the VLAN.

In response to a request, the VMPS takes one of the following actions:

- If the assigned VLAN is restricted to a group of ports, the VMPS verifies the requesting port against this group and responds as follows:
  - If the VLAN is allowed on the port, the VMPS sends the VLAN name to the client in response.
  - If the VLAN is not allowed on the port, and the VMPS is not in secure mode, the VMPS sends an *access-denied* response.

- If the VLAN is not allowed on the port, and the VMPS is in secure mode, the VMPS sends a *port-shutdown* response.
- If the VLAN in the database does not match the current VLAN on the port, and there are active hosts on the port, the VMPS sends an *access-denied* or a *port-shutdown* response, depending on the secure mode of the VMPS.

If the switch receives an *access-denied* response from the VMPS, the switch continues to block traffic from the MAC address to or from the port. The switch continues to monitor the packets directed to the port and sends a query to the VMPS when it identifies a new address. If the switch receives a *port-shutdown* response from the VMPS, the switch disables the port. The port must be manually reenabled by using the CLI, Cisco Visual Switch Manager (CVSM), or SNMP.

You can also use an explicit entry in the configuration table to deny access to specific MAC addresses for security reasons. If you enter the **none** keyword for the VLAN name, the VMPS sends an *access-denied* or *port-shutdown* response.

## Entering Port Names in the VMPS

A VMPS database configuration file must use the Catalyst 4500 series convention for naming ports. For example, Fa0/5 is fixed-port number 5.

If the switch is a cluster member, the command switch adds the name of the switch before the “Fa” in the port name. For example, es3%Fa02 refers to fixed 10/100 port 2 on member switch 3. These naming conventions must be used in the VMPS database configuration file when the VMPS is configured to support a cluster.

You can configure a fallback VLAN name. If you connect a device with a MAC address that is not in the database, the VMPS sends the fallback VLAN name to the client. If you do not configure a fallback VLAN name and the MAC address does not exist in the database, the VMPS sends an *access-denied* response. If the VMPS is in secure mode, it sends a *port-shutdown* response.

## Dynamic Port VLAN Membership

A dynamic (nontrunking) port can belong to only one VLAN. When the link comes up, the switch does not forward traffic to or from this port until the port is assigned to a VLAN. The source MAC address from the first packet of a new host on the dynamic port is sent to the VMPS, which attempts to match the MAC address to a VLAN in the VMPS database. If there is a match, the VMPS sends the VLAN number for that port. If there is no match, the VMPS either denies the request or shuts down the port (depending on the VMPS secure mode setting). See the “Understanding VMPS” section on page 9-1 for a complete description of possible VMPS responses.

Multiple hosts (MAC addresses) can be active on a dynamic port if they are all in the same VLAN. If the link goes down on a dynamic port, the port returns to an isolated state and does not belong to a VLAN. Any hosts that come online through the port are checked again with the VMPS before the port is assigned to a VLAN.



### Note

The VMPS shuts down a dynamic port if more than 20 hosts are active on that port.



## VMPS Configuration Guidelines

The following guidelines and restrictions apply to dynamic port VLAN membership:

- You must configure the VMPS before you configure ports as dynamic.
- The communication between a cluster of switches and the VMPS is managed by the command switch and includes port-naming conventions that are different from standard port names. See “Entering Port Names in the VMPS” section on page 9-2 for the cluster-based port-naming conventions.
- When you configure a port as dynamic, the spanning-tree PortFast feature is automatically enabled for that port. The PortFast mode accelerates the process of bringing the port into the forwarding state. You can disable PortFast mode on a dynamic port.
- Secure ports cannot be dynamic ports. You must disable port security on the port before it becomes dynamic.
- Trunk ports cannot be dynamic ports, but it is possible to enter the **switchport access VLAN dynamic** command for a trunk port. In this case, the switch retains the setting and applies it if the port is later configured as an access port.

You must turn off trunking on the port before the dynamic access setting takes effect.

- Dynamic ports cannot be network ports or monitor ports.



**Note**

The VTP management domain of the VMPS client and the VMPS server must match.

## Default VMPS Configuration

Table 9-1 shows the default VMPS and dynamic port configuration on client switches.

**Table 9-1** Default VMPS Client and Dynamic Port Configuration

| Feature                 | Default Configuration |
|-------------------------|-----------------------|
| VMPS domain server      | None                  |
| VMPS reconfirm interval | 60 minutes            |
| VMPS server retry count | 3                     |
| Dynamic ports           | None configured       |

# Configuring Dynamic VLAN Membership

These subsections describe how to configure a switch as a VMPS client and configure its ports for dynamic VLAN membership.

The following topics are included:

- Entering the IP Address of the VMPS, page 9-4
- Configuring Dynamic Ports on VMPS Clients, page 9-5
- Administering and Monitoring the VMPS, page 9-5
- Configuring the Reconfirmation Interval, page 9-7
- Reconfirming VLAN Memberships, page 9-7
- Troubleshooting Dynamic Port VLAN Membership, page 9-8

## Entering the IP Address of the VMPS

To configure the switch as a client, you must enter the IP address of the Catalyst 4500 series switch or the other device acting as the VMPS.

To define a VMPS for a cluster of switches, perform this task:

|        | Command                                               | Purpose                                                                 |
|--------|-------------------------------------------------------|-------------------------------------------------------------------------|
| Step 1 | Switch# <b>configure terminal</b>                     | Enters global configuration mode.                                       |
| Step 2 | Switch(config)# <b>vmips server ipaddress primary</b> | Enters the IP address of the switch acting as the primary VMPS server.  |
| Step 3 | Switch(config)# <b>vmips server ipaddress</b>         | Enters the IP address for the switch acting as a secondary VMPS server. |
| Step 4 | Switch(config)# <b>end</b>                            | Returns to privileged EXEC mode.                                        |
| Step 5 | Switch# <b>show vmips</b>                             | Verifies the VMPS server entry.                                         |

This example shows how to enter the primary and backup VMPS devices:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# vmips server 172.20.128.179 primary
Switch(config)# vmips server 172.20.128.178
Switch(config)# end

Switch# show vmips
VQP Client Status:

VMPS VQP Version: 1
Reconfirm Interval: 60 min
Server Retry Count: 3
VMPS domain server: 172.20.128.179 (primary, current)
 172.20.128.178

Reconfirmation status

VMPS Action: No Dynamic Port
```

## Configuring Dynamic Ports on VMPS Clients

If you are configuring a port on a member switch as a dynamic port, first log in to the member switch by using the **rcommand** command in privileged EXEC mode. See the *Catalyst 4500 Series Switch Cisco IOS Command Reference* for more information on how to use this command.

To configure dynamic ports on the VMPS client switches, perform this task:

|        | Command                                               | Purpose                                                            |
|--------|-------------------------------------------------------|--------------------------------------------------------------------|
| Step 1 | Switch# <b>configure terminal</b>                     | Enters global configuration mode.                                  |
| Step 2 | Switch(config)# <b>interface interface</b>            | Enters interface configuration mode and the port to be configured. |
| Step 3 | Switch(config)# <b>switchport mode access</b>         | Sets the port to access mode.                                      |
| Step 4 | Switch(config)# <b>switchport access vlan dynamic</b> | Configures the port as eligible for dynamic VLAN access.           |
| Step 5 | Switch(config-if)# <b>end</b>                         | Returns to privileged EXEC mode.                                   |
| Step 6 | Switch# <b>show interface interface switchport</b>    | Verifies the entry.                                                |

This example shows how to configure a port as a dynamic access port and then verify the entry:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fa0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan dynamic
Switch(config-if)# end
```

```
Switch# show interface fa0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative mode: dynamic access
Operational Mode: dynamic access
Administrative Trunking Encapsulation: isl
Operational Trunking Encapsulation: isl
Negotiation of Trunking: Disabled
Access Mode VLAN: 0 ((Inactive))
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: NONE
Pruning VLANs Enabled: NONE
```

## Administering and Monitoring the VMPS

You can display information about the VMPS by using the **show vmps** command in mode privileged EXEC.

The switch displays the following information about the VMPS:

|                    |                                                                                                                                                                                                                                                  |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VMPS VQP Version   | The version of VQP used to communicate with the VMPS. The switch queries the VMPS using version 1 of VQP.                                                                                                                                        |
| Reconfirm Interval | The number of minutes the switch waits before reconfirming the VLAN-to-MAC-address assignments.                                                                                                                                                  |
| Server Retry Count | The number of times VQP resends a query to the VMPS. If no response is received after this many tries, the switch starts to query the secondary VMPS.                                                                                            |
| VMPS domain server | The IP address of the configured VLAN membership policy servers. The switch currently sends queries to the one marked <i>current</i> . The one marked <i>primary</i> is the primary server.                                                      |
| VMPS Action        | The result of the most-recent reconfirmation attempt. This can happen automatically when the reconfirmation interval expired, or you can force it by entering the privileged EXEC <b>vmpls reconfirm</b> command or its CVSM or SNMP equivalent. |

The following example shows how to display VMPS information. You can enter this information on a command or member switch:

```
Switch# show vmpls
VQP Client Status:

VMPS VQP Version: 1
Reconfirm Interval: 60 min
Server Retry Count: 3
VMPS domain server:
```

```
Reconfirmation status

VMPS Action: other
```

The following example shows how to display VMPS statistics:

```
Switch# show vmpls 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
```



#### Note

Refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference* for details on the VMPS statistics.

## Configuring the Reconfirmation Interval

VMPS clients periodically reconfirm the VLAN membership information received from the VMPS. You can set the interval at which the reconfirmation will occur.

If you are configuring a member switch in a cluster, the parameter must be equal to or greater than the reconfirmation setting on the command switch. In addition, you must first log in to the member switch by using the **recommand** command in privileged EXEC mode. See the *Catalyst 4500 Series Switch Cisco IOS Command Reference* for more information on how to use this command.

To configure the reconfirmation interval, perform this task:

|        | Command                                               | Purpose                                                                              |
|--------|-------------------------------------------------------|--------------------------------------------------------------------------------------|
| Step 1 | Switch# <b>configure terminal</b>                     | Enters global configuration mode.                                                    |
| Step 2 | Switch(config)# <b>vmpls reconfirm</b> <i>minutes</i> | Enters the number of minutes between reconfirmations of the dynamic VLAN membership. |
| Step 3 | Switch(config)# <b>end</b>                            | Returns to privileged EXEC mode.                                                     |
| Step 4 | Switch# <b>show vmpls</b>                             | Verifies the dynamic VLAN reconfirmation status.                                     |

This example shows how to change the reconfirmation interval to 60 minutes and verify the change by displaying the VMPS information:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# vmpls reconfirm 60
Switch(config)# end

Switch# show vmpls
VQP Client Status:

VMPS VQP Version: 1
Reconfirm Interval: 60 min
Server Retry Count: 10
VMPS domain server: 172.20.130.50 (primary, current)

Reconfirmation status

VMPS Action: No Host
```

## Reconfirming VLAN Memberships

To confirm the dynamic port VLAN membership assignments that the switch has received from the VMPS, perform this task in privileged EXEC mode:

|        | Command                                | Purpose                                          |
|--------|----------------------------------------|--------------------------------------------------|
| Step 1 | Switch(config)# <b>vmpls reconfirm</b> | Reconfirms dynamic port VLAN membership.         |
| Step 2 | Switch# <b>show vmpls</b>              | Verifies the dynamic VLAN reconfirmation status. |

## Troubleshooting Dynamic Port VLAN Membership

The VMPS shuts down a dynamic port under these conditions:

- The VMPS is in secure mode, and it will not allow the host to connect to the port. The VMPS shuts down the port to prevent the host from connecting to the network.
- More than 20 active hosts reside on a dynamic port.

To reenable a shut-down dynamic port, enter the **no shutdown** command in interface configuration mode.

## VMPS Database Configuration File Example

This example shows a sample VMPS database configuration file as it appears on a Catalyst 4500 series switch. A VMPS database configuration file is an ASCII text file that is stored on a TFTP server accessible to the switch that functions as the VMPS server.

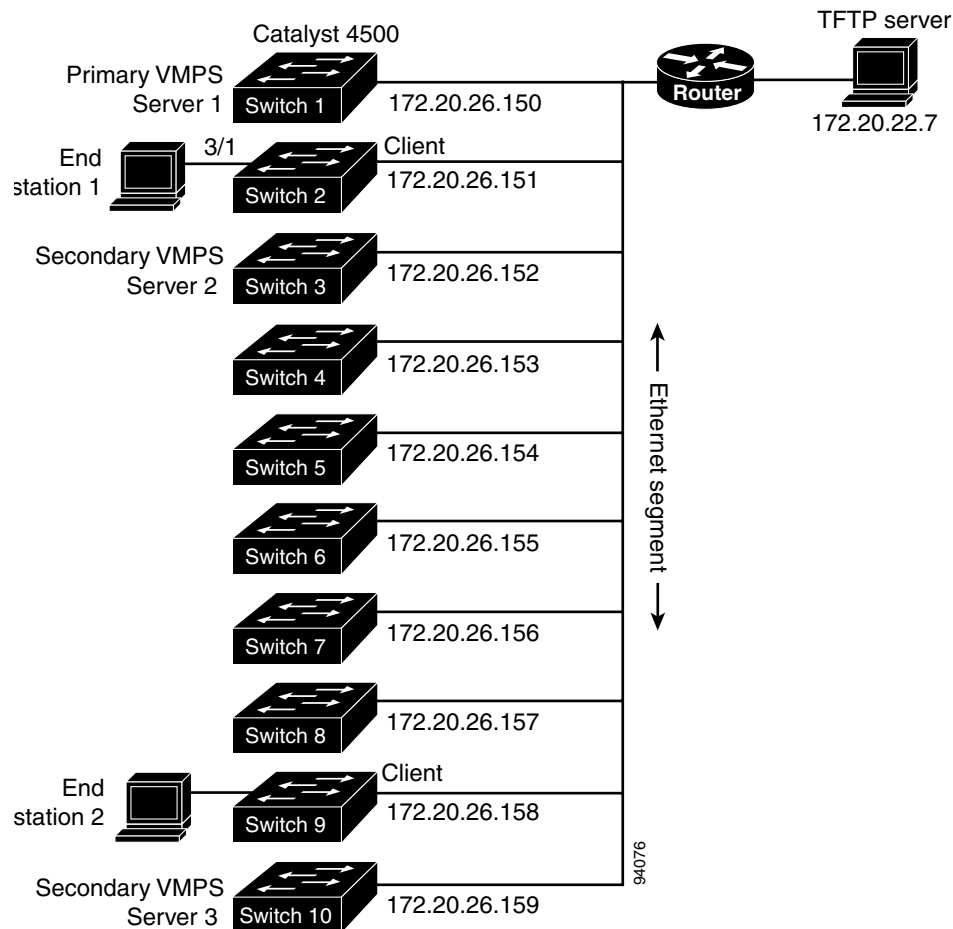
```
!vmps domain <domain-name>
! The VMPS domain must be defined.
!vmps mode { open | secure }
! The default mode is open.
!vmps fallback <vlan-name>
!vmps no-domain-req { allow | deny }
!
! The default value is allow.
vmps domain WBU
vmps mode open
vmps fallback default
vmps no-domain-req deny
!
!
!MAC Addresses
!
vmps-mac-addr
!
! address <addr> vlan-name <vlan_name>
!
address 0012.2233.4455 vlan-name hardware
address 0000.6509.a080 vlan-name hardware
address aabb.ccdd.eeff vlan-name Green
address 1223.5678.9abc vlan-name ExecStaff
address fedc.ba98.7654 vlan-name --NONE--
address fedc.ba23.1245 vlan-name Purple
!
!Port Groups
!
!vmps-port-group <group-name>
! device <device-id> { port <port-name> | all-ports }
!
vmps-port-group WiringCloset1
device 198.92.30.32 port Fa1/3
device 172.20.26.141 port Fa1/4
vmps-port-group "Executive Row"
device 198.4.254.222 port es5%Fa0/1
device 198.4.254.222 port es5%Fa0/2
device 198.4.254.223 all-ports
!
!VLAN groups
```

```
!
!vmmps-vlan-group <group-name>
! vlan-name <vlan-name>
!
vmmps-vlan-group Engineering
vlan-name hardware
vlan-name software
!
!VLAN port Policies
!
!vmmps-port-policies {vlan-name <vlan_name> | vlan-group <group-name> }
! { port-group <group-name> | device <device-id> port <port-name> }
!
vmmps-port-policies vlan-group Engineering
 port-group WiringCloset1
vmmps-port-policies vlan-name Green
 device 198.92.30.32 port Fa0/9
vmmps-port-policies vlan-name Purple
 device 198.4.254.22 port Fa0/10
 port-group "Executive Row"
```

## Dynamic Port VLAN Membership Configuration Example

Figure 9-1 on page 9-10 shows a network with a VMPS server switch and VMPS client switches with dynamic ports. In this example, these assumptions apply:

- The VMPS server and the VMPS client are separate switches.
- The Catalyst 4500 family Switch 1 is the primary VMPS server.
- The Catalyst 4500 family Switch 3 and Switch 10 are secondary VMPS servers.
- End stations are connected to these clients:
  - Catalyst 2900 series XL Switch 2
  - Catalyst 2900 series XL Switch 9
- The database configuration file is called Bldg-G.db and is stored on the TFTP server with the IP address 172.20.22.7.

**Figure 9-1** Dynamic Port VLAN Membership Configuration

In the following procedure, the Catalyst 4500 series switches are the VMPS servers. Use this procedure to configure the Catalyst 4500 series and Catalyst 2900 XL series clients in the network:

**Step 1** Configure the VMPS server addresses on Switch 2, the client switch.

- a. Starting from privileged EXEC mode, enter global configuration mode:

```
switch# configuration terminal
```

- b. Enter the primary VMPS server IP address:

```
switch(config)# vmps server 172.20.26.150 primary
```

- c. Enter the secondary VMPS server IP addresses:

```
switch(config)# vmps server 172.20.26.152
```

- d. To verify your entry of the VMPS IP addresses, return to privileged EXEC mode:

```
switch#(config) exit
```



- e. Display VMPS information configured for the switch:

```
switch# show vmps
VQP Client Status:

VMPS VQP Version: 1
Reconfirm Interval: 60 min
Server Retry Count: 3
VMPS domain server: 172.20.26.152
 172.20.26.150 (primary, current)
```

**Step 2** Configure port Fa0/1 on Switch 2 as a dynamic port.

- a. Return to global configuration mode:

```
switch# configure terminal
```

- b. Enter interface configuration mode:

```
switch(config)# interface fa0/1
```

- c. Configure the VLAN membership mode for static-access ports:

```
switch(config-if)# switchport mode access
```

- d. Assign the port dynamic VLAN membership:

```
switch(config-if)# switchport access vlan dynamic
```

- e. Return to privileged EXEC mode:

```
switch(config-if)# exit
switch#
```

**Step 3** Connect End Station 2 on port Fa0/1. When End Station 2 sends a packet, Switch 2 sends a query to the primary VMPS server, Switch 1. Switch 1 responds with the VLAN ID for port Fa0/1. Because spanning-tree PortFast mode is enabled by default on dynamic ports, port Fa0/1 connects immediately and begins forwarding.

**Step 4** Set the VMPS reconfirmation period to 60 minutes. The reconfirmation period is the number of minutes the switch waits before reconfirming the VLAN to MAC address assignments.

```
switch# config terminal
switch(config)# vmps reconfirm 60
```

**Step 5** Confirm the entry from privileged EXEC mode:

```
switch# show vmps
VQP Client Status:

VMPS VQP Version: 1
Reconfirm Interval: 60 min
Server Retry Count: 3
VMPS domain server:

Reconfirmation status

VMPS Action: No Dynamic Port
```

**Step 6** Repeat Steps 1 and 2 to configure the VMPS server addresses, and assign dynamic ports on each VMPS client switch.





## Configuring Private VLANs

This chapter describes private VLANs (PVLANS) on Catalyst 4500 series switches. It also provides restrictions, procedures, and configuration examples.

This chapter includes the following major sections:

- Overview of PVLANS, page 10-1
- PVLAN Configuration Restrictions, page 10-3
- How to Configure PVLANS, page 10-3



**Note**

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference* and related publications at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/index.htm>

## Overview of PVLANS

PVLANS provide Layer 2 isolation between ports within the same PVLAN. There are three types of PVLAN ports:

- Promiscuous—A promiscuous port can communicate with all interfaces, including the isolated and community ports within a PVLAN.
- Isolated—An isolated port has complete Layer 2 separation from the other ports within the same PVLAN, but not from the promiscuous ports. PVLANS block all traffic to isolated ports except traffic from promiscuous ports. Traffic from isolated port is forwarded only to promiscuous ports.
- Community—Community ports communicate among themselves and with their promiscuous ports. These interfaces are separated at Layer 2 from all other interfaces in other communities or isolated ports within their PVLAN.

Because trunks can support the VLANs carrying traffic between isolated, community, and promiscuous ports, isolated and community port traffic might enter or leave the switch through a trunk interface.

PVLAN ports are associated with a set of supporting VLANs that are used to create the PVLAN structure. A PVLAN uses VLANs three ways:

- As a primary VLAN—Carries traffic from promiscuous ports to isolated, community, and other promiscuous ports in the same primary VLAN.

- As an isolated VLAN—Carries traffic from isolated ports to a promiscuous port.
- As a community VLAN—Carries traffic between community ports and to promiscuous ports. You can configure multiple community VLANs in a PVLAN.

Isolated and community VLANs are called secondary VLANs. You can extend PVLANs across multiple devices by trunking the primary, isolated, and community VLANs to other devices that support PVLANs.

In a switched environment, you can assign an individual PVLAN and associated IP subnet to each individual or common group of end stations. The end stations need to communicate with a default gateway only to gain access outside the PVLAN. With end stations in a PVLAN, you can do the following:

- Designate which ports will be connected to end stations. For example, interfaces connected to servers as isolated ports prevent any communication at Layer 2. Or, if the end stations are servers, this configuration prevents Layer 2 communication between the servers.
- Designate the interfaces to which the default gateway(s) and selected end stations (for example, backup servers or LocalDirector) are attached as promiscuous ports to allow all end stations access.
- Reduce VLAN and IP subnet consumption, because you can prevent traffic between end stations even though they are in the same VLAN and IP subnet.

**Note**

A promiscuous port can service only one primary VLAN. A promiscuous port can service one isolated or many community VLANs.

With a promiscuous port, you can connect a wide range of devices as access points to a PVLAN. For example, you can connect a promiscuous port to the server port of a LocalDirector to connect an isolated VLAN or a number of community VLANs to the server. LocalDirector can load balance the servers present in the isolated or community VLANs, or you can use a promiscuous port to monitor or back up all the PVLAN servers from an administration workstation.

## PVLAN Trunks

A PVLAN trunkport can carry multiple secondary and non-PVLANs. Packets are received and transmitted with secondary or regular VLAN tags on the PVLAN trunk ports.

PVLAN trunk port behavior is the same as PVLAN isolated or community port behavior, except that PVLANs can tag packets and carry multiple secondary and regular VLANs.

**Note**

Only IEEE 802.1q encapsulation is supported.

## PVLANs and VLAN ACL/QoS

PVLAN ports use primary and secondary VLANs, as follows:

- A packet received on a PVLAN host port belongs to the secondary VLAN.
- A packet received on a PVLAN trunk port belongs to the secondary VLAN, if the packet is tagged with a secondary VLAN or the packet is untagged and the port's native VLAN is a secondary VLAN.

A packet received on a PVLAN host or trunk port and assigned to secondary VLAN is bridged on the secondary VLAN. Because of this bridging, the secondary VLAN ACL as well as the secondary VLAN QoS (on input direction) apply.

When a packet is transmitted out of a PVLAN host or trunk port, the packet logically belongs to the primary VLAN. This relationship applies even though the packet may be transmitted with the secondary VLAN tagging for PVLAN trunk ports. In this situation, the primary VLAN ACL and the primary VLAN QoS on output applies to the packet.

## PVLAN Configuration Restrictions

Keep the following restrictions in mind when configuring PVLANs correctly:

- PVLAN trunk ports support only IEEE 802.1q encapsulation.
- Community VLANs are not supported in this release.
- You cannot change the VTP mode to client or server for PVLANs.
- An isolated or community VLAN can have only one primary VLAN associated with it.
- VTP does not support PVLANs. You must configure PVLANs on each device where you want PVLAN ports.

## How to Configure PVLANs

To configure a PVLAN, follow this procedure:

- 
- |               |                                                                                                                                    |
|---------------|------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Set VTP mode to transparent. See the “Disabling VTP (VTP Transparent Mode)” section on page 11-9.                                  |
| <b>Step 2</b> | Create the secondary VLANs. See the “Configuring a VLAN as a PVLAN” section on page 10-5.                                          |
| <b>Step 3</b> | Create the primary VLAN. See the “Configuring a VLAN as a PVLAN” section on page 10-5.                                             |
| <b>Step 4</b> | Associate the secondary VLAN to the primary VLAN. See the “Associating a Secondary VLAN with a Primary VLAN” section on page 10-6. |



---

|             |                                                                                                                           |
|-------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>Note</b> | Only one isolated VLAN can be mapped to a primary VLAN, but more than one community VLAN can be mapped to a primary VLAN. |
|-------------|---------------------------------------------------------------------------------------------------------------------------|

---

- |               |                                                                                                                                                                    |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 5</b> | Configure an interface to an isolated or community port. See the “Configuring a Layer 2 Interface as a PVLAN Host Port” section on page 10-8.                      |
| <b>Step 6</b> | Associate the isolated port or community port to the primary-secondary VLAN pair. See the “Associating a Secondary VLAN with a Primary VLAN” section on page 10-6. |
| <b>Step 7</b> | Configure an interface as a promiscuous port. See the “Configuring a Layer 2 Interface as a PVLAN Promiscuous Port” section on page 10-7.                          |
| <b>Step 8</b> | Map the promiscuous port to the primary-secondary VLAN pair. See the “Configuring a Layer 2 Interface as a PVLAN Promiscuous Port” section on page 10-7.           |
-

These sections describe how to configure PVLANS:

- “PVLAN Configuration Guidelines” section on page 10-4
- “Configuring a VLAN as a PVLAN” section on page 10-5
- “Associating a Secondary VLAN with a Primary VLAN” section on page 10-6
- “Configuring a Layer 2 Interface as a PVLAN Promiscuous Port” section on page 10-7
- “Configuring a Layer 2 Interface as a PVLAN Host Port” section on page 10-8
- “Permitting Routing of Secondary VLAN Ingress Traffic” section on page 10-10

## PVLAN Configuration Guidelines

Follow these guidelines when configuring PVLANS:

- To configure a PVLAN correctly, enable VTP in transparent mode.
- Do not include VLAN 1 or VLANs 1002–1005 in PVLANS.
- Use only PVLAN commands to assign ports to primary, isolated, or community VLANs.  
Layer 2 interfaces on primary, isolated, or community VLANs are inactive in PVLANS. Layer 2 trunk interfaces remain in the STP forwarding state.
- You cannot configure Layer 3 VLAN interfaces for secondary VLANs.  
Layer 3 VLAN interfaces for isolated and community (secondary) VLANs are inactive while the VLAN is configured as an isolated or community VLAN.
- Do not configure PVLAN ports as EtherChannel.  
EtherChannel ports in PVLANS are inactive.
- Do not configure a destination SPAN port in a PVLAN.  
Destination SPAN ports are inactive in PVLANS.
- If you delete a VLAN in a PVLAN, the PVLAN ports in the VLAN become inactive.
- Do not apply Cisco IOS ACLs to isolated or community VLANs.  
Cisco IOS ACL configuration applied to isolated and community VLANs is inactive while the VLANs are part of the PVLAN configuration.
- Do not apply dynamic access control entries (ACEs) to primary VLANs.  
Cisco IOS dynamic ACL configuration applied to a primary VLAN is inactive while the VLAN is part of the PVLAN configuration.
- Do not apply Cisco IOS ACLs to isolated or community VLANs.  
Cisco IOS ACL configuration applied to isolated and community VLANs is inactive while the VLANs are part of the PVLAN configuration.
- Do not apply dynamic access control entries (ACEs) to primary VLANs.  
Dynamic ACLs applied to a primary VLAN are inactive in PVLANS.
- Enable PortFast on the PVLAN trunk ports with the **spanning-tree portfast trunk** command.
- Any VLAN ACL configured on an isolated VLAN is effective in the input direction, and any VLAN ACL configured on the primary VLAN associated with the isolated VLAN is effective in the output direction.

- You can stop Layer 3 switching on an isolated VLAN by deleting the mapping of that VLAN with its primary VLAN.
- PVLAN ports do not have to be on the same network device as long as the devices are trunk connected and the primary and secondary VLANs have not been removed from the trunk.
- You can use VLAN-based SPAN (VSPAN) on primary, isolated, and community VLANs, or use SPAN on only one VLAN to separately monitor egress or ingress traffic.
- Enable PortFast and bridge packet data unit (BPDU) guard on isolated and community ports to prevent spanning tree loops due to misconfigurations.

When PortFast and BPDU guard enabled, STP applies the BPDU guard to all PortFast-configured Layer 2 LAN ports.

- To maintain the security of your PVLAN configuration and avoid other use of the VLANs configured as PVLANS, configure PVLANS on all intermediate devices, even if devices have no PVLAN ports.
- Prune the PVLANS from the trunks on devices that carry no traffic in the PVLANS.
- To apply Cisco IOS output ACLs to all outgoing PVLAN traffic, configure them on the Layer 3 VLAN interface of the primary VLAN.
- You can apply different quality of service (QoS) configuration to primary, isolated, and community VLANs.
- On a PVLAN trunk port, a secondary VLAN ACL is applied on ingress traffic and a primary VLAN ACL is applied on egress traffic.
- On a promiscuous port the primary VLAN ACL is applied on ingress traffic.
- Cisco IOS ACLs applied to the Layer 3 VLAN interface of a primary VLAN automatically apply to the associated isolated and community VLANs.

## Configuring a VLAN as a PVLAN

To configure a VLAN as a PVLAN, perform this task:

|        | Command                                                                                                                     | Purpose                                                                                                                                                                                                                           |
|--------|-----------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch# <b>configure terminal</b>                                                                                           | Enters configuration mode.                                                                                                                                                                                                        |
| Step 2 | Switch(config)# <b>vlan</b> <i>vlan_ID</i><br>Switch(config-vlan)# <b>private-vlan</b> { <i>isolated</i>   <i>primary</i> } | Configures a VLAN as a PVLAN. <ul style="list-style-type: none"> <li>• The command does not take effect until you exit VLAN configuration submenu.</li> <li>• You can use the <b>no</b> keyword to clear PVLAN status.</li> </ul> |
| Step 3 | Switch(config-vlan)# <b>end</b>                                                                                             | Exits VLAN configuration mode.                                                                                                                                                                                                    |
| Step 4 | Switch# <b>show vlan private-vlan</b> [ <i>type</i> ]                                                                       | Verifies the configuration.                                                                                                                                                                                                       |

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 type
```

```
Vlan Type

202 primary
440 isolated
```

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 type
```

```
Vlan Type

202 primary
440 isolated
```

## Associating a Secondary VLAN with a Primary VLAN

To associate secondary VLANs with a primary VLAN, perform this task:

|        | Command                                                                                                                                                                              | Purpose                                                                                                                                                                         |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch# <b>configure terminal</b>                                                                                                                                                    | Enters configuration mode.                                                                                                                                                      |
| Step 2 | Switch(config)# <b>vlan</b> <i>primary_vlan_ID</i>                                                                                                                                   | Enters VLAN configuration mode for the primary VLAN.                                                                                                                            |
| Step 3 | Switch(config-vlan)# [ <b>no</b> ] <b>private-vlan association</b> { <i>secondary_vlan_list</i>   <b>add</b> <i>secondary_vlan_list</i>   <b>remove</b> <i>secondary_vlan_list</i> } | Associates the secondary VLAN with the primary VLAN. The list can contain only one VLAN.<br>You can use the <b>no</b> keyword to delete all associations from the primary VLAN. |
| Step 4 | Switch(config-vlan)# <b>end</b>                                                                                                                                                      | Exits VLAN configuration mode.                                                                                                                                                  |
| Step 5 | Switch# <b>show vlan private-vlan</b> [ <i>type</i> ]                                                                                                                                | Verifies the configuration.                                                                                                                                                     |

When you associate secondary VLANs with a primary VLAN, note the following:

- The *secondary\_vlan\_list* parameter contains only one isolated VLAN ID.
- Use the **remove** keyword with the *secondary\_vlan\_list* variable to clear the association between the secondary VLAN and the primary VLAN. The list can contain only one VLAN.
- The command does not take effect until you exit VLAN configuration submode.

This example shows how to associate isolated VLAN 440 with primary VLAN 202 and verify the configuration:

```
Switch# configure terminal
Switch(config)# vlan 202
Switch(config-vlan)# private-vlan association 440
Switch(config-vlan)# end
Switch# show vlan private-vlan
```

```
Primary Secondary Type Interfaces

202 440 isolated
```



## Configuring a Layer 2 Interface as a PVLAN Promiscuous Port

To configure a Layer 2 interface as a PVLAN promiscuous port, perform this task:

|        | Command                                                                                                                                                                                                          | Purpose                                                                                                                                                                       |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch# <b>configure terminal</b>                                                                                                                                                                                | Enters global configuration mode.                                                                                                                                             |
| Step 2 | Switch(config)# <b>interface</b> { <i>fastethernet</i>   <i>gigabitethernet</i> } <i>slot/port</i>                                                                                                               | Specifies the LAN interface to configure.                                                                                                                                     |
| Step 3 | Switch(config-if)# <b>switchport mode private-vlan</b> { <i>host</i>   <i>promiscuous</i>   <i>trunk</i> }                                                                                                       | Configures a Layer 2 interface as a PVLAN promiscuous port.                                                                                                                   |
| Step 4 | Switch(config-if)# [ <b>no</b> ] <b>switchport private-vlan mapping</b> <i>primary_vlan_ID</i> { <i>secondary_vlan_list</i>   <b>add</b> <i>secondary_vlan_list</i>   <b>remove</b> <i>secondary_vlan_list</i> } | Maps the PVLAN promiscuous port to a primary VLAN and to selected secondary VLANs.<br><br>You can use the <b>no</b> keyword to delete all associations from the primary VLAN. |
| Step 5 | Switch(config-if)# <b>end</b>                                                                                                                                                                                    | Exits configuration mode.                                                                                                                                                     |
| Step 6 | Switch# <b>show interfaces</b> { <i>fastethernet</i>   <i>gigabitethernet</i> } <i>slot/port</i> <b>switchport</b>                                                                                               | Verifies the configuration.                                                                                                                                                   |

When you configure a Layer 2 interface as a PVLAN promiscuous port, note the following:

- 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 hyphenated range of PVLAN IDs.
- Enter a *secondary\_vlan\_list* or use the **add** keyword with a *secondary\_vlan\_list* to map the secondary VLANs to the PVLAN promiscuous port.
- Use the **remove** keyword with a *secondary\_vlan\_list* to clear the mapping between secondary VLANs and the PVLAN promiscuous port.

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 202 440
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
```

## Configuring a Layer 2 Interface as a PVLAN Host Port

To configure a Layer 2 interface as a PVLAN host port, perform this task:

|        | Command                                                                                                                          | Purpose                                                                                                                               |
|--------|----------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch# <b>configure terminal</b>                                                                                                | Enters configuration mode.                                                                                                            |
| Step 2 | Switch(config)# <b>interface</b> { <b>fastethernet</b>   <b>gigabitethernet</b> } <i>slot/port</i>                               | Specifies the LAN port to configure.                                                                                                  |
| Step 3 | Switch(config-if)# <b>switchport mode private-vlan</b> { <b>host</b>   <b>promiscuous</b> }   <b>trunk</b>                       | Configures a Layer 2 interface as a PVLAN host port.                                                                                  |
| Step 4 | Switch(config-if)# [ <b>no</b> ] <b>switchport private-vlan host-association</b> <i>primary_vlan_ID</i> <i>secondary_vlan_ID</i> | Associates the Layer 2 interface with a PVLAN.<br>You can use the <b>no</b> keyword to delete all associations from the primary VLAN. |
| Step 5 | Switch(config-if)# <b>end</b>                                                                                                    | Exits configuration mode.                                                                                                             |
| Step 6 | Switch# <b>show interfaces</b> { <b>fastethernet</b>   <b>gigabitethernet</b> } <i>slot/port</i> <b>switchport</b>               | Verifies the configuration.                                                                                                           |

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):
 2 (VLAN0202) 3 (VLAN0440)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
```

## Configuring a Layer 2 Interface as a PVLAN Trunk Port

To configure a Layer 2 interface as a PVLAN trunk port, perform this task:

|        | Command                                                                                                                                           | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch> <b>enable</b>                                                                                                                             | Enters privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Step 2 | Switch# <b>configure terminal</b>                                                                                                                 | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Step 3 | Switch(config)# <b>interface</b> {fastethernet   gigabitethernet} slot/port                                                                       | Specifies the LAN port to configure.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Step 4 | Switch(config-if)# <b>switchport mode private-vlan</b> {host   promiscuous   trunk}                                                               | Configures a Layer 2 interface as a PVLAN trunk port for multiple secondary VLANs.                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Step 5 | Switch(config-if)# [no] <b>switchport private-vlan association trunk</b> primary_vlan_ID secondary_vlan_ID                                        | <p>Configures association between primary VLANs and secondary VLANs the PVLAN trunk port with a PVLAN.</p> <p><b>Note</b> Multiple PVLAN pairs can be specified using this command so that a PVLAN trunk port can carry multiple secondary VLANs. If an association is specified for the existing primary VLAN, the existing association is replaced. If there is no trunk association, any packets received on secondary VLANs are dropped.</p> <p>You can use the <b>no</b> keyword to delete all associations from the primary VLAN.</p> |
| Step 6 | Switch(config-if)# [no] <b>switchport private-vlan trunk allowed vlan</b> vlan_list all   none   [add   remove   except] vlan_atom[,vlan_atom...] | <p>Configures a list of allowed normal VLANs on a PVLAN trunk port.</p> <p>You can use the <b>no</b> keyword to remove all allowed normal VLANs on a PVLAN trunk port.</p>                                                                                                                                                                                                                                                                                                                                                                  |
| Step 7 | Switch(config-if)# [no] <b>switchport private-vlan trunk native vlan</b> vlan_id                                                                  | <p>Configures a VLAN to which untagged packets (as in IEEE 802.1Q tagging) are assigned on a PVLAN trunk port.</p> <p>If there is no native VLAN configured, all untagged packets are dropped.</p> <p>If the native VLAN is a secondary VLAN and the port does not have the association for the secondary VLAN, the untagged packets are dropped.</p> <p>You can use the <b>no</b> keyword to remove all native VLANs on a PVLAN trunk port.</p>                                                                                            |
| Step 8 | Switch(config-if)# <b>end</b>                                                                                                                     | Exits configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Step 9 | Switch# <b>show interfaces</b> {fastethernet   gigabitethernet} slot/port <b>switchport</b>                                                       | Verifies the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

This example shows how to configure interface FastEthernet 5/1 as a PVLAN trunk port, maps VLAN0202 to VLAN0440, and configures the PVLAN trunk:

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/1
Switch(config-if)# switchport private-vlan association trunk 202 440
Switch(config-if)# switchport mode private-vlan trunk
Switch(config-if)# end

Switch#show interfaces fastethernet 5/1 switchport
Name: Fa5/1
Switchport: Enabled
Administrative Mode: private-vlan trunk
Operational Mode: private-vlan trunk
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
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:
 202 (VLAN0202) 440 (VLAN0440)
Operational private-vlan(s):
 202 (VLAN0202) 440 (VLAN0440)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
```

## Permitting Routing of Secondary VLAN Ingress Traffic

To permit routing of secondary VLAN ingress traffic, perform this task:

|        | Command                                                                                                                                                              | Purpose                                                                                                                                                                                     |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch# <b>configure terminal</b>                                                                                                                                    | Enters global configuration mode.                                                                                                                                                           |
| Step 2 | Switch(config)# <b>interface</b> <i>vlan primary_vlan_ID</i>                                                                                                         | Enters interface configuration mode for the primary VLAN.                                                                                                                                   |
| Step 3 | Switch(config-if)# <b>[no] private-vlan mapping</b><br><i>primary_vlan_ID {secondary_vlan_list   add</i><br><i>secondary_vlan_list   remove secondary_vlan_list}</i> | To permit routing on the secondary VLAN ingress traffic, map the secondary VLAN to the primary VLAN.<br>You can use the <b>no</b> keyword to delete all associations from the primary VLAN. |
| Step 4 | Switch(config-if)# <b>end</b>                                                                                                                                        | Exits configuration mode.                                                                                                                                                                   |
| Step 5 | Switch# <b>show interface private-vlan mapping</b>                                                                                                                   | Verifies the configuration.                                                                                                                                                                 |

When you permit routing on the secondary VLAN ingress traffic, note the following:

- Enter a value for the *secondary\_vlan\_list* variable or use the **add** keyword with the *secondary\_vlan\_list* variable to map the secondary VLANs to the primary VLAN.
- Use the **remove** keyword with the *secondary\_vlan\_list* variable to clear the mapping between secondary VLANs and the primary VLAN.

This example shows how to permit routing of secondary VLAN ingress traffic from PVLAN 440 and verify the configuration:

```
Switch# configure terminal
Switch(config)# interface vlan 202
Switch(config-if)# private-vlan mapping add 440
Switch(config-if)# end
Switch# show interfaces private-vlan mapping
Interface Secondary VLAN Type

vlan202 440 isolated

Switch#
```





## Understanding and Configuring VTP

This chapter describes the VLAN Trunking Protocol (VTP) on the Catalyst 4500 series switch. It also provides guidelines, procedures, and configuration examples.

This chapter includes the following major sections:

- Overview of VTP, page 11-1
- VTP Configuration Guidelines and Restrictions, page 11-5
- VTP Default Configuration, page 11-5
- Configuring VTP, page 11-6



### Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference* and the publications at: <http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/index.htm>

## Overview of VTP

VTP is a Layer 2 messaging protocol that maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs within a VTP domain. A VTP domain (also called a VLAN management domain) is made up of one or more network devices that share the same VTP domain name and that are interconnected with trunks. VTP minimizes misconfigurations and configuration inconsistencies that can result in a number of problems, such as duplicate VLAN names, incorrect VLAN-type specifications, and security violations.

Before you create VLANs, you must decide whether you want to use VTP in your network. With VTP, you can make configuration changes centrally on one or more network devices and have those changes automatically communicated to all the other network devices in the network.



### Note

For complete information on configuring VLANs, see Chapter 8, “Understanding and Configuring VLANs.”

These sections describe how VTP works:

- Understanding the VTP Domain, page 11-2
- Understanding VTP Modes, page 11-2
- Understanding VTP Advertisements, page 11-3

- Understanding VTP Version 2, page 11-3
- Understanding VTP Pruning, page 11-3

## Understanding the VTP Domain

A VTP domain is made up of one or more interconnected network devices that share the same VTP domain name. A network device can be configured to be in only one VTP domain. You make global VLAN configuration changes for the domain using either the command-line interface (CLI) or Simple Network Management Protocol (SNMP).

By default, the Catalyst 4500 series switch is in VTP server mode and is in the no-management domain state until the switch receives an advertisement for a domain over a trunk link or you configure a management domain. You cannot create or modify VLANs on a VTP server until the management domain name is specified or learned.

If the switch receives a VTP advertisement over a trunk link, it inherits the management domain name and the VTP configuration revision number. The switch ignores advertisements with a different management domain name or an earlier configuration revision number.

If you configure the switch as VTP transparent, you can create and modify VLANs, but the changes affect only the individual switch.

When you make a change to the VLAN configuration on a VTP server, the change is propagated to all network devices in the VTP domain. VTP advertisements are transmitted out all Inter-Switch Link (ISL) and IEEE 802.1Q trunk connections.

VTP maps VLANs dynamically across multiple LAN types with unique names and internal index associations. Mapping eliminates unnecessary device administration for network administrators.

## Understanding VTP Modes

You can configure a Catalyst 4500 series switch to operate in any one of these VTP modes:

- **Server**—In VTP server mode, you can create, modify, and delete VLANs and specify other configuration parameters (such as VTP version and VTP pruning) for the entire VTP domain. VTP servers advertise their VLAN configuration to other network devices in the same VTP domain and synchronize their VLAN configuration with other network devices based on advertisements received over trunk links. VTP server is the default mode.
- **Client**—VTP clients behave the same way as VTP servers, but you cannot create, change, or delete VLANs on a VTP client.
- **Transparent**—VTP transparent network devices do not participate in VTP. A VTP transparent network device does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements. However, in VTP version 2, transparent network devices do forward VTP advertisements that they receive on their trunking LAN interfaces.



### Note

Catalyst 4500 series switch automatically change from VTP server mode to VTP client mode if the switch detects a failure while writing configuration to NVRAM. If this happens, the switch cannot be returned to VTP server mode until the NVRAM is functioning.



## Understanding VTP Advertisements

Each network device in the VTP domain sends periodic advertisements out each trunking LAN interface to a reserved multicast address. VTP advertisements are received by neighboring network devices, which update their VTP and VLAN configurations as necessary.

The following global configuration information is distributed in VTP advertisements:

- VLAN IDs (ISL and 802.1Q)
- Emulated LAN names (for ATM LANE)
- 802.10 SAID values (FDDI)
- VTP domain name
- VTP configuration revision number
- VLAN configuration, including maximum transmission unit (MTU) size for each VLAN
- Frame format

## Understanding VTP Version 2

If you use VTP in your network, you must decide whether to use VTP version 1 or version 2.

**Note**

Catalyst 4500 series switch do not support Token Ring or FDDI media. The switch does not forward FDDI, FDDI-Net, Token Ring Concentrator Relay Function [TrCRF], or Token Ring Bridge Relay Function [TrBRF] traffic, but it does propagate the VLAN configuration via VTP.

VTP version 2 supports the following features, which are not supported in version 1:

- Token Ring support—VTP version 2 supports Token Ring LAN switching and VLANs (TrBRF and TrCRF).
- Unrecognized Type-Length-Value (TLV) Support—A VTP server or client propagates configuration changes to its other trunks, even for TLVs it is not able to parse. The unrecognized TLV is saved in NVRAM.
- Version-Dependent Transparent Mode—In VTP version 1, a VTP transparent network device inspects VTP messages for the domain name and version, and forwards a message only if the version and domain name match. Because only one domain is supported in the supervisor engine software, VTP version 2 forwards VTP messages in transparent mode, without checking the version.
- Consistency Checks—In VTP version 2, VLAN consistency checks (such as VLAN names and values) are performed only when you enter new information through the CLI or SNMP. Consistency checks are not performed when new information is obtained from a VTP message or when information is read from NVRAM. If the digest on a received VTP message is correct, its information is accepted without consistency checks.

## Understanding VTP Pruning

VTP pruning enhances network bandwidth use by reducing unnecessary flooded traffic, such as broadcast, multicast, and unicast packets. VTP pruning increases available bandwidth by restricting flooded traffic to those trunk links that the traffic must use to access the appropriate network devices. By default, VTP pruning is disabled.

For VTP pruning to be effective, all devices in the management domain must either support VTP pruning or, on devices that do not support VTP pruning, you must manually configure the VLANs allowed on trunks.

Figure 11-1 shows a switched network without VTP pruning enabled. Interface 1 on Switch 1 and Interface 2 on Switch 4 are assigned to the Red VLAN. A broadcast is sent from the host connected to Switch 1. Switch 1 floods the broadcast and every network device in the network receives it, even though Switches 3, 5, and 6 have no interfaces in the Red VLAN.

You can enable pruning globally on the Catalyst 4500 series switch (see the “Enabling VTP Pruning” section on page 11-6).

**Figure 11-1 Flooding Traffic without VTP Pruning**

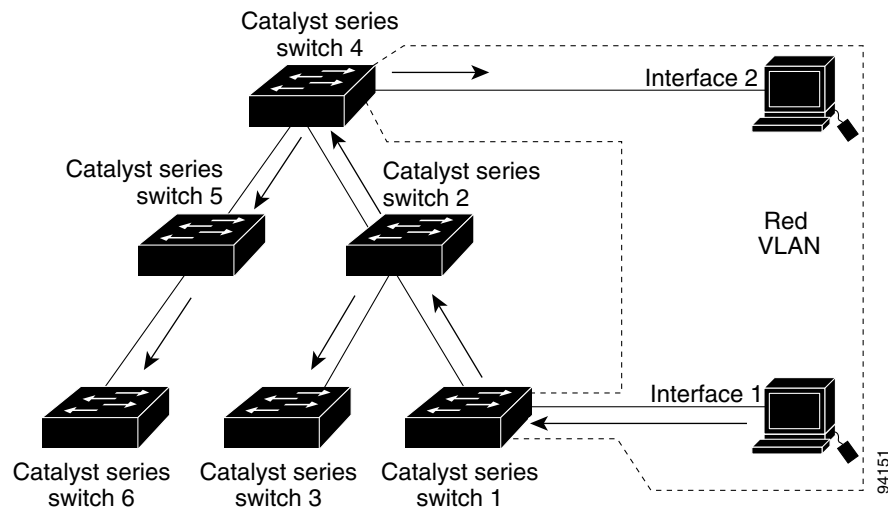
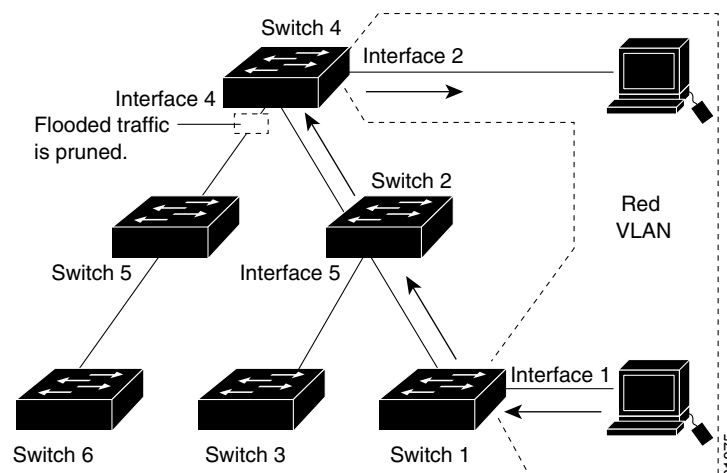


Figure 11-2 shows the same switched network with VTP pruning enabled. The broadcast traffic from Switch 1 is not forwarded to Switches 3, 5, and 6 because traffic for the Red VLAN has been pruned on the links indicated (Interface 5 on Switch 2 and Interface 4 on Switch 4).

**Figure 11-2 Flooding Traffic with VTP Pruning**



Enabling VTP pruning on a VTP server enables pruning for the entire management domain. VTP pruning takes effect several seconds after you enable it. By default, VLANs 2 through 1000 are eligible for pruning. VTP pruning does not prune traffic from pruning-eligible VLANs. VLAN 1 is always ineligible for pruning; traffic from VLAN 1 cannot be pruned.

To configure VTP pruning on a trunking LAN interface, use the **switchport trunk pruning vlan** command. VTP pruning operates when a LAN interface is trunking. You can set VLAN pruning eligibility regardless of whether VTP pruning is enabled or disabled for the VTP domain, whether any given VLAN exists, and regardless of whether the LAN interface is currently trunking.

## VTP Configuration Guidelines and Restrictions

Follow these guidelines and restrictions when implementing VTP in your network:

- All network devices in a VTP domain must run the same VTP version.
- You must configure a password on each network device in the management domain when VTP is in secure mode.



### Caution

If you configure VTP in secure mode, the management domain will not function properly if you do not assign a management domain password to each network device in the domain.

- A VTP version 2-capable network device can operate in the same VTP domain as a network device running VTP version 1 if VTP version 2 is disabled on the VTP version 2-capable network device (VTP version 2 is disabled by default).
- Do not enable VTP version 2 on a network device unless all of the network devices in the same VTP domain are version 2-capable. When you enable VTP version 2 on a server, all of the version 2-capable network devices in the domain enable VTP version 2.
- Enabling or disabling VTP pruning on a VTP server enables or disables VTP pruning for the entire management domain.
- Configuring VLANs as eligible for pruning on a Catalyst 4500 series switch affects pruning eligibility for those VLANs on that switch only, not on all network devices in the VTP domain.

## VTP Default Configuration

Table 11-1 shows the default VTP configuration.

**Table 11-1 VTP Default Configuration**

| Feature                    | Default Value         |
|----------------------------|-----------------------|
| VTP domain name            | Null                  |
| VTP mode                   | Server                |
| VTP version 2 enable state | Version 2 is disabled |
| VTP password               | None                  |
| VTP pruning                | Disabled              |

# Configuring VTP

The following sections describe how to configure VTP:

- Configuring VTP Global Parameters, page 11-6
- Configuring the Switch as a VTP Server, page 11-7
- Configuring the Switch as a VTP Client, page 11-8
- Disabling VTP (VTP Transparent Mode), page 11-9
- Displaying VTP Statistics, page 11-10

## Configuring VTP Global Parameters

The following sections describe configuring the VTP global parameters:

- Configuring a VTP Password, page 11-6
- Enabling VTP Pruning, page 11-6
- Enabling VTP Version 2, page 11-7

### Configuring a VTP Password

To configure the VTP password, perform this task:

| Command                                   | Purpose                                                                          |
|-------------------------------------------|----------------------------------------------------------------------------------|
| Switch# [no] vtp password password_string | Sets a password for the VTP domain. The password can be from 8 to 64 characters. |
|                                           | Uses the <b>no</b> keyword to remove the password.                               |

This example shows how to configure a VTP password:

```
Switch#vtp password WATER
Setting device VLAN database password to WATER.
Switch#show vtp password
VTP Password:WATER
Switch#
```

### Enabling VTP Pruning

To enable VTP pruning in the management domain, perform this task:

|        | Command                  | Purpose                                                                                                                         |
|--------|--------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch# [no] vtp pruning | Enables VTP pruning in the management domain.<br><br>Use the <b>no</b> keyword to disable VTP pruning in the management domain. |
| Step 2 | Switch# show vtp status  | Verifies the configuration.                                                                                                     |

This example shows how to enable VTP pruning in the management domain:

```
Switch# vtp pruning
Pruning switched ON
```

This example shows how to verify the configuration:

```
Switch# show vtp status | include Pruning
VTP Pruning Mode : Enabled
Switch#
```

## Enabling VTP Version 2

By default, VTP version 2 is disabled on VTP version 2-capable network devices. When you enable VTP version 2 on a server, every VTP version 2-capable network device in the VTP domain enables version 2.



### Caution

VTP version 1 and VTP version 2 are not interoperable on network devices in the same VTP domain. Every network device in the VTP domain must use the same VTP version. Do not enable VTP version 2 unless every network device in the VTP domain supports version 2.

To enable VTP version 2, perform this task:

|        | Command                          | Purpose                                                                       |
|--------|----------------------------------|-------------------------------------------------------------------------------|
| Step 1 | Switch# [no] vtp version {1   2} | Enables VTP version 2.<br>Use the <b>no</b> keyword to revert to the default. |
| Step 2 | Switch# show vtp status          | Verifies the configuration.                                                   |

This example shows how to enable VTP version 2:

```
Switch# vtp version 2
V2 mode enabled.
Switch#
```

This example shows how to verify the configuration:

```
Switch# show vtp status | include V2
VTP V2 Mode : Enabled
Switch#
```

## Configuring the Switch as a VTP Server

To configure the Catalyst 4500 series switch as a VTP server, perform this task:

|        | Command                                | Purpose                                                             |
|--------|----------------------------------------|---------------------------------------------------------------------|
| Step 1 | Switch# configuration terminal         | Enters configuration mode.                                          |
| Step 2 | Switch(config)# vtp mode server        | Configures the switch as a VTP server.                              |
| Step 3 | Switch(config)# vtp domain domain_name | Defines the VTP domain name, which can be up to 32 characters long. |

|        | Command                        | Purpose                        |
|--------|--------------------------------|--------------------------------|
| Step 4 | Switch(config)# <b>end</b>     | Exits VLAN configuration mode. |
| Step 5 | Switch# <b>show vtp status</b> | Verifies the configuration.    |

This example shows how to configure the switch as a VTP server:

```
Switch# configuration terminal
Switch(config)# vtp mode server
Setting device to VTP SERVER mode.
Switch(config)# vtp domain Lab_Network
Setting VTP domain name to Lab_Network
Switch(config)# end
Switch#
```

This example shows how to verify the configuration:

```
Switch# show vtp status
VTP Version : 2
Configuration Revision : 247
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 : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0x45 0x52 0xB6 0xFD 0x63 0xC8 0x49 0x80
Configuration last modified by 0.0.0.0 at 8-12-99 15:04:49
Local updater ID is 172.20.52.34 on interface Gi1/1 (first interface found)
Switch#
```

## Configuring the Switch as a VTP Client

To configure the Catalyst 4500 series switch as a VTP client, perform this task:

|        | Command                                              | Purpose                                                                                                            |
|--------|------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch# <b>configuration terminal</b>                | Enters configuration mode.                                                                                         |
| Step 2 | Switch(config)# [ <b>no</b> ] <b>vtp mode client</b> | Configure the switch as a VTP client.<br>Use the <b>no</b> keyword to return to the default setting (server mode). |
| Step 3 | Switch(config)# <b>end</b>                           | Exits configuration mode.                                                                                          |
| Step 4 | Switch# <b>show vtp status</b>                       | Verifies the configuration.                                                                                        |

This example shows how to configure the switch as a VTP client:

```
Switch# configuration terminal
Switch(config)# vtp mode client
Setting device to VTP CLIENT mode.
Switch(config)# exit
Switch#
```

This example shows how to verify the configuration:

```
Switch# show vtp status
VTP Version : 2
Configuration Revision : 247
Maximum VLANs supported locally : 1005
Number of existing VLANs : 33
VTP Operating Mode : Client
VTP Domain Name : Lab_Network
VTP Pruning Mode : Enabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0x45 0x52 0xB6 0xFD 0x63 0xC8 0x49 0x80
Configuration last modified by 0.0.0.0 at 8-12-99 15:04:49
Switch#
```

## Disabling VTP (VTP Transparent Mode)

To disable VTP on the Catalyst 4500 series switch, perform this task:

|        | Command                                          | Purpose                                                                                               |
|--------|--------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| Step 1 | Switch# <b>configuration terminal</b>            | Enters configuration mode.                                                                            |
| Step 2 | Switch(config)# <b>[no] vtp mode transparent</b> | Disables VTP on the switch. Use the <b>no</b> keyword to return to the default setting (server mode). |
| Step 3 | Switch(config)# <b>end</b>                       | Exits configuration mode.                                                                             |
| Step 4 | Switch# <b>show vtp status</b>                   | Verifies the configuration.                                                                           |

This example shows how to disable VTP on the switch:

```
Switch# configuration terminal
Switch(config)# vtp transparent
Setting device to VTP mode.
Switch(config)# end
Switch#
```

This example shows how to verify the configuration:

```
Switch# show vtp status
VTP Version : 2
Configuration Revision : 247
Maximum VLANs supported locally : 1005
Number of existing VLANs : 33
VTP Operating Mode : Transparent
VTP Domain Name : Lab_Network
VTP Pruning Mode : Enabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0x45 0x52 0xB6 0xFD 0x63 0xC8 0x49 0x80
Configuration last modified by 0.0.0.0 at 8-12-99 15:04:49
Switch#
```

## Displaying VTP Statistics

To display VTP statistics, including VTP advertisements sent and received and VTP errors, perform this task:

| Command                          | Purpose                  |
|----------------------------------|--------------------------|
| Switch# <b>show vtp counters</b> | Displays VTP statistics. |

This example shows how to display VTP statistics:

```
Switch# show vtp counters
```

```
VTP statistics:
```

```
Summary advertisements received : 7
Subset advertisements received : 5
Request advertisements received : 0
Summary advertisements transmitted : 997
Subset advertisements transmitted : 13
Request advertisements transmitted : 3
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<br>non-pruning-capable device |
|-------|------------------|---------------|-----------------------------------------------------------|
| ----- | -----            | -----         | -----                                                     |
| Fa5/8 | 43071            | 42766         | 5                                                         |





## Understanding and Configuring STP

This chapter describes how to configure the Spanning Tree Protocol (STP) on a Catalyst 4500 series switch. It also provides guidelines, procedures, and configuration examples.

This chapter includes the following major sections:

- Overview of STP, page 12-1
- Default STP Configuration, page 12-6
- Configuring STP, page 12-7



### Note

For information on configuring the PortFast, UplinkFast, and BackboneFast, and other spanning tree enhancements, see Chapter 13, “Configuring STP Features.”



### Note

For complete syntax and usage information for the switch commands used in this chapter, refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference* and related publications at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/index.htm>

## Overview of STP

STP is a Layer 2 link management protocol that provides path redundancy while preventing undesirable loops in the network. For a Layer 2 Ethernet network to function properly, only one active path can exist between any two stations. A loop-free subset of a network topology is called a spanning tree. The operation of a spanning tree is transparent to end stations, which cannot detect whether they are connected to a single LAN segment or a switched LAN of multiple segments.

A Catalyst 4500 series switch use STP (the IEEE 802.1D bridge protocol) on all VLANs. By default, a single spanning tree runs on each configured VLAN (provided you do not manually disable the spanning tree). You can enable and disable a spanning tree on a per-VLAN basis.

When you create fault-tolerant internetworks, you must have a loop-free path between all nodes in a network. The spanning tree algorithm calculates the best loop-free path throughout a switched Layer 2 network. Switches send and receive spanning tree frames at regular intervals. The switches do not forward these frames, but use the frames to construct a loop-free path.

Multiple active paths between end stations cause loops in the network. If a loop exists in the network, end stations might receive duplicate messages and switches might learn end station MAC addresses on multiple Layer 2 interfaces. These conditions result in an unstable network.

A spanning tree defines a tree with a root switch and a loop-free path from the root to all switches in the Layer 2 network. A spanning tree forces redundant data paths into a standby (blocked) state. If a network segment in the spanning tree fails and a redundant path exists, the spanning tree algorithm recalculates the spanning tree topology and activates the standby path.

When two ports on a switch are part of a loop, the spanning tree port priority and port path cost setting determine which port is put in the forwarding state and which port is put in the blocking state. The spanning tree port priority value represents the location of an interface in the network topology and how well located it is to pass traffic. The spanning tree port path cost value represents media speed.

## Understanding the Bridge ID

Each VLAN on each network device has a unique 64-bit bridge ID consisting of a bridge priority value, an extended system ID, and an STP MAC address allocation.

### Bridge Priority Value

The bridge priority value determines whether a given redundant link will be given priority and considered part of a given span in a spanning tree. Preference is given to lower values, and if you want to manually configure a preference, assign a lower bridge priority value to a link than to its redundant possibility. With releases prior to 12.1(12c)EW, the bridge priority is a 16-bit value (see Table 12-1). With Release 12.1(12c)EW and later releases, the bridge priority is a 4-bit value when the extended system ID is enabled (see Table 12-2). See the “Configuring the Bridge Priority of a VLAN” section on page 12-16.

### Extended System ID

Extended system IDs are VLAN IDs between 1025 and 4096. Releases 12.1(12c)EW and later releases support a 12-bit extended system ID field as part of the bridge ID (see Table 12-2). Chassis that support only 64 MAC addresses always use the 12-bit extended system ID. On chassis that support 1024 MAC addresses, you can enable use of the extended system ID. STP uses the VLAN ID as the extended system ID. See the “Enabling the Extended System ID” section on page 12-8.

**Table 12-1 Bridge Priority Value with the Extended System ID Disabled**

| Bridge Priority Value |        |        |        |        |        |        |       |       |       |       |       |       |       |       |       |
|-----------------------|--------|--------|--------|--------|--------|--------|-------|-------|-------|-------|-------|-------|-------|-------|-------|
| Bit 16                | Bit 15 | Bit 14 | Bit 13 | Bit 12 | Bit 11 | Bit 10 | Bit 9 | Bit 8 | Bit 7 | Bit 6 | Bit 5 | Bit 4 | Bit 3 | Bit 2 | Bit 1 |
| 32768                 | 16384  | 8192   | 4096   | 2048   | 1024   | 512    | 256   | 128   | 64    | 32    | 16    | 8     | 4     | 2     | 1     |

**Table 12-2 Bridge Priority Value and Extended System ID with the Extended System ID Enabled**

| Bridge Priority Value |        |        |        | Extended System ID (Set Equal to the VLAN ID) |        |        |       |       |       |       |       |       |       |       |       |
|-----------------------|--------|--------|--------|-----------------------------------------------|--------|--------|-------|-------|-------|-------|-------|-------|-------|-------|-------|
| Bit 16                | Bit 15 | Bit 14 | Bit 13 | Bit 12                                        | Bit 11 | Bit 10 | Bit 9 | Bit 8 | Bit 7 | Bit 6 | Bit 5 | Bit 4 | Bit 3 | Bit 2 | Bit 1 |
| 32768                 | 16384  | 8192   | 4096   | VLAN ID                                       |        |        |       |       |       |       |       |       |       |       |       |

## STP MAC Address Allocation

A Catalyst 4500 series switch chassis has either 64 or 1024 MAC addresses available to support software features like STP. Enter the **show module** command to view the MAC address range on your chassis.

Release 12.1(12c)EW and later releases 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.

Earlier releases support chassis with 1024 MAC addresses. With earlier releases, STP uses one MAC address per VLAN to make the bridge ID unique for each VLAN.

## Bridge Protocol Data Units

The following elements determine the stable active spanning tree topology of a switched network:

- The unique bridge ID (bridge priority and MAC address) associated with each VLAN on each switch
- The spanning tree path cost (or bridge priority value) to the root bridge
- The port identifier (port priority and MAC address) associated with each Layer 2 interface

Bridge protocol data units (BPDUs) contain information about the transmitting bridge and its ports, including the bridge and MAC addresses, bridge priority, port priority, and path cost. The system computes the spanning tree topology by transmitting BPDUs among connecting switches, and in one direction from the root switch. Each configuration BPDU contains at least the following:

- The unique bridge ID of the switch that the transmitting switch believes to be the root switch
- The spanning tree path cost to the root
- The bridge ID of the transmitting bridge
- The age of the message
- The identifier of the transmitting port
- Values for the *hello*, *forward delay*, and *max-age* protocol timers

When a switch transmits a BPDU frame, all switches connected to the LAN on which the frame is transmitted receive the BPDU. When a switch receives a BPDU, it does not forward the frame but instead uses the information in the frame to calculate a BPDU and, if the topology changes, initiate a BPDU transmission.

A BPDU exchange results in the following:

- One switch is elected as the root bridge.
- The shortest distance to the root bridge is calculated for each switch based on the path cost.
- A designated bridge for each LAN segment is selected. This is the switch closest to the root bridge through which frames are forwarded to the root.
- A root port is selected. This is the port providing the best path from the bridge to the root bridge.
- Ports included in the spanning tree are selected.

## Election of the Root Bridge

For each VLAN, the switch with the highest bridge priority (the lowest numerical priority value) is elected as the root bridge. If all switches are configured with the default priority value (32,768), the switch with the lowest MAC address in the VLAN becomes the root bridge.

The spanning tree root bridge is the logical center of the spanning tree topology in a switched network. All paths that are not required to reach the root bridge from anywhere in the switched network are placed in spanning tree blocking mode.

A spanning tree uses the information provided by BPDUs to elect the root bridge and root port for the switched network, as well as the root port and designated port for each switched segment.

## STP Timers

Table 12-3 describes the STP timers that affect the performance of the entire spanning tree.

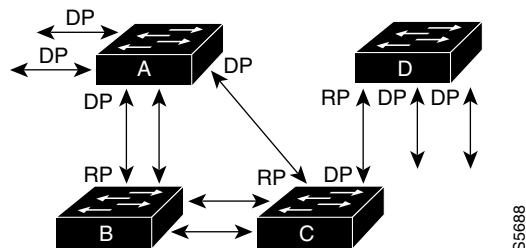
**Table 12-3** *Spanning Tree Protocol Timers*

| Variable            | Description                                                                                                |
|---------------------|------------------------------------------------------------------------------------------------------------|
| <i>hello_time</i>   | Determines how often the switch broadcasts hello messages to other switches.                               |
| <i>forward_time</i> | Determines how long each of the listening and learning states will last before the port begins forwarding. |
| <i>max_age</i>      | Determines the amount of time that protocol information received on a port is stored by the switch.        |

## Creating the STP Topology

The goal of the spanning tree algorithm is to make the most direct link the root port. When the spanning tree topology is calculated based on default parameters, the path between source and destination end stations in a switched network might not be optimal according to link speed. For instance, connecting higher-speed links to a port that has a higher number than the current root port can cause a root-port change.

In Figure 12-1, Switch A is elected as the root bridge. (This could happen if the bridge priority of all the switches is set to the default value [32,768] and Switch A has the lowest MAC address.) However, due to traffic patterns, the number of forwarding ports, or link types, Switch A might not be the ideal root bridge. By increasing the STP port priority (lowering the numerical value) of the ideal switch so that it becomes the root bridge, you force a spanning tree recalculation to form a new spanning tree topology with the ideal switch as the root.

**Figure 12-1 Spanning Tree Topology**

RP = Root Port  
DP = Designated Port

For example, assume that one port on Switch B is a fiber-optic link, and another port on Switch B (an unshielded twisted-pair [UTP] link) is the root port. Network traffic might be more efficient over the high-speed fiber-optic link. By changing the spanning tree port priority on the fiber-optic port to a higher priority (lower numerical value) than the priority set for the root port, the fiber-optic port becomes the new root port.

## STP Port States

Propagation delays can occur when protocol information passes through a switched LAN. As a result, topology changes can take place at different times and at different places in a switched network. When a Layer 2 interface transitions directly from nonparticipation in the spanning tree topology to the forwarding state, it can create temporary data loops. Ports must wait for new topology information to propagate through the switched LAN before starting to forward frames. They must allow the frame lifetime to expire for frames that have been forwarded under the old topology.

Each Layer 2 interface on a switch that uses spanning tree exists in one of the following five states:

- **Blocking**—In this state, the Layer 2 interface does not participate in frame forwarding.
- **Listening**—This state is the first transitional state after the blocking state when spanning tree determines that the Layer 2 interface should participate in frame forwarding.
- **Learning**—In this state, the Layer 2 interface prepares to participate in frame forwarding.
- **Forwarding**—In this state, the Layer 2 interface forwards frames.
- **Disabled**—In this state, the Layer 2 interface does not participate in spanning tree and does not forward frames.

## MAC Address Allocation

The supervisor engine has a pool of 1024 MAC addresses that are used as the bridge IDs for the VLAN spanning trees. You can use the **show module** command to view the MAC address range (allocation range for the supervisor) that the spanning tree uses for the algorithm.

MAC addresses for the Catalyst 4506 switch are allocated sequentially, with the first MAC address in the range assigned to VLAN 1, the second MAC address in the range assigned to VLAN 2, and so forth. For example, if the MAC address range is 00-e0-1e-9b-2e-00 to 00-e0-1e-9b-31-ff, the VLAN 1 bridge ID is 00-e0-1e-9b-2e-00, the VLAN 2 bridge ID is 00-e0-1e-9b-2e-01, the VLAN 3 bridge ID is 00-e0-1e-9b-2e-02, and so on. On other Catalyst 4000 family platforms, all VLANs map to the same MAC address rather than mapping to separate MAC addresses.

## STP and IEEE 802.1Q Trunks

802.1Q VLAN trunks impose some limitations on the spanning tree strategy for a network. In a network of Cisco switches connected through 802.1Q trunks, the switches maintain one instance of spanning tree for each VLAN allowed on the trunks. However, non-Cisco 802.1Q switches maintain only one instance of spanning tree for all VLANs allowed on the trunks.

When you connect a Cisco switch to a non-Cisco device (that supports 802.1Q) through an 802.1Q trunk, the Cisco switch combines the spanning tree instance of the 802.1Q native VLAN of the trunk with the spanning tree instance of the non-Cisco 802.1Q switch. However, all per-VLAN spanning tree information is maintained by Cisco switches separated by a network of non-Cisco 802.1Q switches. The non-Cisco 802.1Q network separating the Cisco switches is treated as a single trunk link between the switches.



### Note

For more information on 802.1Q trunks, see Chapter 6, “Configuring Layer 2 Ethernet Interfaces.”

## Per-VLAN Rapid Spanning Tree

Per-VLAN Rapid Spanning Tree (PVRST+) is the same as PVST+, although PVRST+ utilizes a rapid STP based on IEEE 802.1w rather than 802.1D to provide faster convergence. PVRST+ uses roughly the same configuration as PVST+ and needs only minimal configuration. In PVRST+, dynamic CAM entries are flushed immediately on a per-port basis when any topology change is made. UplinkFast and BackboneFast are enabled but not active in this mode, since the functionality is built into the Rapid STP. PVRST+ provides for rapid recovery of connectivity following the failure of a bridge, bridge port, or LAN.

For enabling information, see “Enabling Per-VLAN Rapid Spanning Tree” on page 20.

## Default STP Configuration

Table 12-4 shows the default spanning tree configuration.

**Table 12-4 Spanning Tree Default Configuration Values**

| Feature                                                                                                                         | Default Value                                                                                                                      |
|---------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| Enable state                                                                                                                    | Spanning tree enabled for all VLANs                                                                                                |
| Bridge priority value                                                                                                           | 32,768                                                                                                                             |
| Spanning tree port priority value (configurable on a per-interface basis—used on interfaces configured as Layer 2 access ports) | 128                                                                                                                                |
| Spanning tree port cost (configurable on a per-interface basis—used on interfaces configured as Layer 2 access ports)           | <ul style="list-style-type: none"> <li>Gigabit Ethernet: 4</li> <li>Fast Ethernet: 19</li> <li>Fast Ethernet 10/100: 19</li> </ul> |
| Spanning tree VLAN port priority value (configurable on a per-VLAN basis—used on interfaces configured as Layer 2 trunk ports)  | 128                                                                                                                                |

**Table 12-4 Spanning Tree Default Configuration Values (continued)**

| Feature                                                                                                              | Default Value                                                                                 |
|----------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| Spanning tree VLAN port cost (configurable on a per-VLAN basis—used on interfaces configured as Layer 2 trunk ports) | <ul style="list-style-type: none"><li>Gigabit Ethernet: 4</li><li>Fast Ethernet: 19</li></ul> |
| Hello time                                                                                                           | 2 sec                                                                                         |
| Forward delay time                                                                                                   | 15 sec                                                                                        |
| Maximum aging time                                                                                                   | 20 sec                                                                                        |

## Configuring STP

The following sections describe how to configure spanning tree on VLANs:

- Enabling STP, page 12-7
- Enabling the Extended System ID, page 12-8
- Configuring the Root Bridge, page 12-9
- Configuring a Secondary Root Switch, page 12-12
- Configuring STP Port Priority, page 12-13
- Configuring STP Port Cost, page 12-15
- Configuring the Bridge Priority of a VLAN, page 12-16
- Configuring the Hello Time, page 12-17
- Configuring the Maximum Aging Time for a VLAN, page 12-18
- Configuring the Forward-Delay Time for a VLAN, page 12-18
- Disabling Spanning Tree Protocol, page 12-19
- Enabling Per-VLAN Rapid Spanning Tree, page 12-20

**Note**

The spanning tree commands described in this chapter can be configured on any interface except those configured with the **no switchport** command.

## Enabling STP

**Note**

By default, spanning tree is enabled on all the VLANs.

You can enable a spanning tree on a per-VLAN basis. The switch maintains a separate instance of spanning tree for each VLAN (except on VLANs on which you have disabled a spanning tree).

To enable a spanning tree on a per-VLAN basis, perform this task:

|        | Command                                                  | Purpose                                                                                            |
|--------|----------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| Step 1 | Switch# <b>configure terminal</b>                        | Enters global configuration mode.                                                                  |
| Step 2 | Switch(config)# <b>spanning-tree vlan <i>vlan_ID</i></b> | Enables spanning tree for VLAN <i>vlan_id</i> . The <i>vlan_ID</i> value can range from 1 to 4094. |
| Step 3 | Switch(config)# <b>end</b>                               | Exits configuration mode.                                                                          |
| Step 4 | Switch# <b>show spanning-tree vlan <i>vlan_ID</i></b>    | Verifies that spanning tree is enabled.                                                            |

This example shows how to enable a spanning tree on VLAN 200:

```
Switch# configure terminal
Switch(config)# spanning-tree vlan 200
Switch(config)# end
Switch#
```



#### Note

Because spanning tree is enabled by default, issuing a **show running** command to view the resulting configuration will not display the command you entered to enable spanning tree.

This example shows how to verify that spanning tree is enabled on VLAN 200:

```
Switch# show spanning-tree vlan 200
```

```
VLAN200 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 264 (FastEthernet5/8), cost of root path is 38
Topology change flag not set, detected flag not set
Number of topology changes 0 last change occurred 01:53:48 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 264 (FastEthernet5/8) of VLAN200 is forwarding
Port path cost 19, Port priority 128, Port Identifier 129.9.
Designated root has priority 16384, address 0060.704c.7000
Designated bridge has priority 32768, address 00e0.4fac.b000
Designated port id is 128.2, designated path cost 19
Timers: message age 3, forward delay 0, hold 0
Number of transitions to forwarding state: 1
BPDU: sent 3, received 3417
```

```
Switch#
```

## Enabling the Extended System ID



#### Note

The extended system ID is enabled permanently on chassis that support 64 MAC addresses.

You can use the **spanning-tree extend system-id** command to enable the extended system ID on chassis that support 1024 MAC addresses. See the “Understanding the Bridge ID” section on page 12-2.



To enable the extended system ID, perform this task:

|        | Command                                               | Purpose                                                                                                                                                                                                                                                          |
|--------|-------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch(config)# <b>spanning-tree extend system-id</b> | Enables the extended system ID.                                                                                                                                                                                                                                  |
|        |                                                       | Disables the extended system ID.<br><br><b>Note</b> You cannot disable the extended system ID on chassis that support 64 MAC addresses or when you have configured extended range VLANs (see “Spanning Tree Default Configuration Values” section on page 12-6). |
| Step 2 | Switch(config)# <b>end</b>                            | Exits configuration mode.                                                                                                                                                                                                                                        |
| Step 3 | Switch# <b>show spanning-tree vlan vlan_ID</b>        | Verifies the configuration.                                                                                                                                                                                                                                      |

**Note**

When you enable or disable the extended system ID, the bridge IDs of all active STP instances are updated, which might change the spanning tree topology.

This example shows how to enable the extended system ID:

```
Switch# configure terminal
Switch(config)# spanning-tree extend system-id
Switch(config)# end
Switch#
```

This example shows how to verify the configuration:

```
Switch# show spanning-tree summary | include extended
Extended system ID is enabled.
```

## Configuring the Root Bridge

A Catalyst 4000 family switch maintains an instance of spanning tree for each active VLAN configured on the switch. A bridge ID, consisting of the bridge priority and the bridge MAC address, is associated with each instance. For each VLAN, the switch with the lowest bridge ID will become the root bridge for that VLAN. Whenever the bridge priority changes, the bridge ID also changes. This results in the recomputation of the root bridge for the VLAN.

To configure a switch to become the root bridge for the specified VLAN, use the **spanning-tree vlan vlan-ID root** command to modify the bridge priority from the default value (32,768) to a significantly lower value. The bridge priority for the specified VLAN is set to 8192 if this value will cause the switch to become the root for the VLAN. If any bridge for the VLAN has a priority lower than 8192, the switch sets the priority to 1 less than the lowest bridge priority.

For example, let's assume that all the switches in the network have the bridge priority for VLAN 100 set to the default value of 32,768. Entering the **spanning-tree vlan 100 root primary** command on a switch will set the bridge priority for VLAN 100 to 8192, causing this switch to become the root bridge for VLAN 100.

**Note**

The root switch for each instance of spanning tree should be a backbone or distribution switch. Do not configure an access switch as the spanning tree primary root.

Use the **diameter** keyword to specify the Layer 2 network diameter (the maximum number of bridge hops between any two end stations in the network). When you specify the network diameter, a switch automatically picks an optimal hello time, forward delay time, and maximum age time for a network of that diameter. This can significantly reduce the spanning tree convergence time.

Use the **hello-time** keyword to override the automatically calculated hello time.

**Note**

We recommend that you avoid manually configuring the hello time, forward delay time, and maximum age time after configuring the switch as the root bridge.

To configure a switch as the root switch, perform this task:

|        | Command                                                                                                  | Purpose                                                                                               |
|--------|----------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| Step 1 | Switch(config)# <b>[no] spanning-tree vlan vlan_ID root primary [diameter hops [hello-time seconds]]</b> | Configures a switch as the root switch.<br>You can use the <b>no</b> keyword to restore the defaults. |
|        | Switch(config)# <b>end</b>                                                                               | Exits configuration mode.                                                                             |

This example shows how to configure a switch as the root bridge for VLAN 10, with a network diameter of 4:

```
Switch# configure terminal
Switch(config)# spanning-tree vlan 10 root primary diameter 4
Switch(config)# end
Switch#
```

This example shows how the configuration changes when a switch becomes a spanning tree root. This is the configuration before the switch becomes the root for VLAN 1:

```
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
Current root has priority 32768, address 0001.6445.4400
Root port is 323 (FastEthernet6/3), cost of root path is 19
Topology change flag not set, detected flag not set
Number of topology changes 2 last change occurred 00:02:19 ago
 from FastEthernet6/1
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 323 (FastEthernet6/3) of VLAN1 is forwarding
Port path cost 19, Port priority 128, Port Identifier 129.67.
Designated root has priority 32768, address 0001.6445.4400
Designated bridge has priority 32768, address 0001.6445.4400
Designated port id is 129.67, designated path cost 0
Timers:message age 2, forward delay 0, hold 0
Number of transitions to forwarding state:1
BPDU:sent 3, received 91
```

```

Port 324 (FastEthernet6/4) of VLAN1 is blocking
 Port path cost 19, Port priority 128, Port Identifier 129.68.
 Designated root has priority 32768, address 0001.6445.4400
 Designated bridge has priority 32768, address 0001.6445.4400
 Designated port id is 129.68, designated path cost 0
 Timers:message age 2, forward delay 0, hold 0
 Number of transitions to forwarding state:0
 BPDU:sent 1, received 89

```

Now, you can set the switch as the root:

```

Switch# configure terminal
Switch(config)# spanning-tree vlan 1 root primary
Switch(config)# spanning-tree vlan 1 root primary
 VLAN 1 bridge priority set to 8192
 VLAN 1 bridge max aging time unchanged at 20
 VLAN 1 bridge hello time unchanged at 2
 VLAN 1 bridge forward delay unchanged at 15
Switch(config)# end

```

This is the configuration after the switch becomes the root:

```

Switch# show spanning-tree vlan 1

VLAN1 is executing the ieee compatible Spanning Tree protocol
 Bridge Identifier has priority 8192, 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 set, detected flag set
 Number of topology changes 3 last change occurred 00:00:09 ago
 Times: hold 1, topology change 35, notification 2
 hello 2, max age 20, forward delay 15
 Timers:hello 0, topology change 25, notification 0, aging 15

Port 323 (FastEthernet6/3) of VLAN1 is forwarding
 Port path cost 19, Port priority 128, Port Identifier 129.67.
 Designated root has priority 8192, address 0030.94fc.0a00
 Designated bridge has priority 8192, address 0030.94fc.0a00
 Designated port id is 129.67, designated path cost 0
 Timers:message age 0, forward delay 0, hold 0
 Number of transitions to forwarding state:1
 BPDU:sent 9, received 105

Port 324 (FastEthernet6/4) of VLAN1 is listening
 Port path cost 19, Port priority 128, Port Identifier 129.68.
 Designated root has priority 8192, address 0030.94fc.0a00
 Designated bridge has priority 8192, address 0030.94fc.0a00
 Designated port id is 129.68, designated path cost 0
 Timers:message age 0, forward delay 5, hold 0
 Number of transitions to forwarding state:0
 BPDU:sent 6, received 102

```

Switch#



#### Note

at the bridge priority is now set at 8192, making this switch the root of the spanning tree.

## Configuring a Secondary Root Switch

When you configure a switch as the secondary root, the spanning tree bridge priority is modified from the default value (32,768) to 16,384. This means that the switch is likely to become the root bridge for the specified VLANs if the primary root bridge fails (assuming the other switches in the network use the default bridge priority of 32,768).

You can run this command on more than one switch to configure multiple backup root switches. Use the same network diameter and hello time values that you used when configuring the primary root switch.



### Note

We recommend that you avoid manually configuring the hello time, forward delay time, and maximum age time after configuring the switch as the root bridge.

To configure a switch as the secondary root switch, perform this task:

|        | Command                                                                                                                         | Purpose                                                                                                         |
|--------|---------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch(config)# <b>[no] spanning-tree vlan <i>vlan_ID</i> root secondary [diameter <i>hops</i> [hello-time <i>seconds</i>]]</b> | Configures a switch as the secondary root switch.<br>You can use the <b>no</b> keyword to restore the defaults. |
| Step 2 | Switch(config)# <b>end</b>                                                                                                      | Exits configuration mode.                                                                                       |

This example shows how to configure the switch as the secondary root switch for VLAN 10, with a network diameter of 4:

```
Switch# configure terminal
Switch(config)# spanning-tree vlan 10 root secondary diameter 4
VLAN 10 bridge priority set to 16384
VLAN 10 bridge max aging time set to 14
VLAN 10 bridge hello time unchanged at 2
VLAN 10 bridge forward delay set to 10
Switch(config)# end
Switch#
```

This example shows how to verify the configuration of VLAN 1:

```
Switch#sh spanning-tree vlan 1

VLAN0001
 Spanning tree enabled protocol ieee
 Root ID Priority 32768
 Address 0003.6b10.e800
 This bridge is the root
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

 Bridge ID Priority 32768
 Address 0003.6b10.e800
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
 Aging Time 300

Interface Role Sts Cost Prio.Nbr Status

Fa3/1 Desg FWD 19 128.129 P2p
Fa3/2 Desg FWD 19 128.130 P2p
Fa3/48 Desg FWD 19 128.176 Edge P2p

Switch#
```

## Configuring STP Port Priority

In the event of a loop, a spanning tree considers port priority when selecting an interface to put into the forwarding state. You can assign higher priority values to interfaces that you want a spanning tree to select first and lower priority values to interfaces that you want a spanning tree to select last. If all interfaces have the same priority value, a spanning tree puts the interface with the lowest interface number in the forwarding state and blocks other interfaces. The possible priority range is 0 through 240, configurable in increments of 16 (the default is 128).



### Note

The Cisco IOS software uses the port priority value when the interface is configured as an access port and uses VLAN port priority values when the interface is configured as a trunk port.

To configure the spanning tree port priority of an interface, perform this task:

|        | Command                                                                                                                                                                 | Purpose                                                                                                                                                                                         |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch(config)# <b>interface</b> {{fastethernet   gigabitethernet} slot/port}   {port-channel port_channel_number}                                                      | Specifies an interface to configure.                                                                                                                                                            |
| Step 2 | Switch(config-if)# [no] <b>spanning-tree port-priority</b> port_priority                                                                                                | Configures the port priority for an interface. The <i>port_priority</i> value can be from 0 to 240, in increments of 16.<br><br>You can use the <b>no</b> keyword to restore the defaults.      |
| Step 3 | Switch(config-if)# [no] <b>spanning-tree vlan</b> vlan_ID <b>port-priority</b> port_priority                                                                            | Configures the VLAN port priority for an interface. The <i>port_priority</i> value can be from 0 to 240, in increments of 16.<br><br>You can use the <b>no</b> keyword to restore the defaults. |
| Step 4 | Switch(config-if)# <b>end</b>                                                                                                                                           | Exits configuration mode.                                                                                                                                                                       |
| Step 5 | Switch# <b>show spanning-tree interface</b> {{fastethernet   gigabitethernet} slot/port}   {port-channel port_channel_number}<br><b>show spanning-tree vlan</b> vlan_ID | Verifies the configuration.                                                                                                                                                                     |

This example shows how to configure the spanning tree port priority of a Fast Ethernet interface:

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/8
Switch(config-if)# spanning-tree port-priority 100
Switch(config-if)# end
Switch#
```

This example shows how to verify the configuration of a Fast Ethernet interface when it is configured as an access port:

```
Switch# show spanning-tree interface fastethernet 3/1
```

```

Vlan Role Sts Cost Prio.Nbr Status

VLAN0001 Desg FWD 19 128.129 P2p
VLAN1002 Desg FWD 19 128.129 P2p
VLAN1003 Desg FWD 19 128.129 P2p
VLAN1004 Desg FWD 19 128.129 P2p
VLAN1005 Desg FWD 19 128.129 P2p
Switch#
```

This example shows how to display the details of the interface configuration when the interface is configured as an access port:

```
Switch# show spanning-tree interface fastethernet 3/1 detail
Port 129 (FastEthernet3/1) of VLAN0001 is forwarding
 Port path cost 19, Port priority 128, Port Identifier 128.129.
 Designated root has priority 32768, address 0003.6b10.e800
 Designated bridge has priority 32768, address 0003.6b10.e800
 Designated port id is 128.129, designated path cost 0
 Timers:message age 0, forward delay 0, hold 0
 Number of transitions to forwarding state:1
 Link type is point-to-point by default
 BPDU:sent 187, received 1

Port 129 (FastEthernet3/1) of VLAN1002 is forwarding
 Port path cost 19, Port priority 128, Port Identifier 128.129.
 Designated root has priority 32768, address 0003.6b10.ebe9
 Designated bridge has priority 32768, address 0003.6b10.ebe9
 Designated port id is 128.129, designated path cost 0
 Timers:message age 0, forward delay 0, hold 0
 Number of transitions to forwarding state:1
 Link type is point-to-point by default
 BPDU:sent 94, received 2

Port 129 (FastEthernet3/1) of VLAN1003 is forwarding
 Port path cost 19, Port priority 128, Port Identifier 128.129.
 Designated root has priority 32768, address 0003.6b10.ebea
 Designated bridge has priority 32768, address 0003.6b10.ebea
 Designated port id is 128.129, designated path cost 0
 Timers:message age 0, forward delay 0, hold 0
 Number of transitions to forwarding state:1
 Link type is point-to-point by default
 BPDU:sent 94, received 2

Port 129 (FastEthernet3/1) of VLAN1004 is forwarding
 Port path cost 19, Port priority 128, Port Identifier 128.129.
 Designated root has priority 32768, address 0003.6b10.ebeb
 Designated bridge has priority 32768, address 0003.6b10.ebeb
 Designated port id is 128.129, designated path cost 0
 Timers:message age 0, forward delay 0, hold 0
 Number of transitions to forwarding state:1
 Link type is point-to-point by default
 BPDU:sent 95, received 2

Port 129 (FastEthernet3/1) of VLAN1005 is forwarding
 Port path cost 19, Port priority 128, Port Identifier 128.129.
 Designated root has priority 32768, address 0003.6b10.ebec
 Designated bridge has priority 32768, address 0003.6b10.ebec
 Designated port id is 128.129, designated path cost 0
 Timers:message age 0, forward delay 0, hold 0
 Number of transitions to forwarding state:1
 Link type is point-to-point by default
 BPDU:sent 95, received 2
Switch#
```

**Note**

The **show spanning-tree port-priority** command displays only information for ports with an active link. If there is no port with an active link, enter a **show running-config interface** command to verify the configuration.

This example shows how to configure the spanning tree VLAN port priority of a Fast Ethernet interface:

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/8
Switch(config-if)# spanning-tree vlan 200 port-priority 64
Switch(config-if)# end
Switch#
```

This example shows how to verify the configuration of VLAN 200 on the interface when it is configured as a trunk port:

```
Switch# show spanning-tree vlan 200
<...output truncated...>

Port 264 (FastEthernet5/8) of VLAN200 is forwarding
Port path cost 19, Port priority 64, Port Identifier 129.8.
 Designated root has priority 32768, address 0010.0d40.34c7
 Designated bridge has priority 32768, address 0010.0d40.34c7
 Designated port id is 128.1, designated path cost 0
 Timers: message age 2, forward delay 0, hold 0
 Number of transitions to forwarding state: 1
 BPDU: sent 0, received 13513

<...output truncated...>
Switch#
```

## Configuring STP Port Cost

The default value for spanning tree port path cost is derived from the interface media speed. In the event of a loop, spanning tree considers port cost when selecting an interface to put into the forwarding state. You can assign lower cost values to interfaces that you want spanning tree to select first, and higher cost values to interfaces that you want spanning tree to select last. If all interfaces have the same cost value, spanning tree puts the interface with the lowest interface number in the forwarding state and blocks other interfaces. The possible cost range is 1 through 200,000,000 (the default is media-specific).

Spanning tree uses the port cost value when the interface is configured as an access port and uses VLAN port cost values when the interface is configured as a trunk port.

To configure the spanning tree port cost of an interface, perform this task:

|        | Command                                                                                                                                                                 | Purpose                                                                                                                                                                    |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch(config)# <b>interface</b> {{fastethernet   gigabitethernet} slot/port}   {port-channel port_channel_number}                                                      | Specifies an interface to configure.                                                                                                                                       |
| Step 2 | Switch(config-if)# [no] <b>spanning-tree cost</b> port_cost                                                                                                             | Configures the port cost for an interface. The <i>port_cost</i> value can be from 1 to 200,000,000.<br><br>You can use the <b>no</b> keyword to restore the defaults.      |
| Step 3 | Switch(config-if)# [no] <b>spanning-tree vlan</b> vlan_ID <b>cost</b> port_cost                                                                                         | Configures the VLAN port cost for an interface. The <i>port_cost</i> value can be from 1 to 200,000,000.<br><br>You can use the <b>no</b> keyword to restore the defaults. |
| Step 4 | Switch(config-if)# <b>end</b>                                                                                                                                           | Exits configuration mode.                                                                                                                                                  |
| Step 5 | Switch# <b>show spanning-tree interface</b> {{fastethernet   gigabitethernet} slot/port}   {port-channel port_channel_number}<br><b>show spanning-tree vlan</b> vlan_ID | Verifies the configuration.                                                                                                                                                |

This example shows how to change the spanning tree port cost of a Fast Ethernet interface:

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/8
Switch(config-if)# spanning-tree cost 18
Switch(config-if)# end
Switch#
```

This example shows how to verify the configuration of the interface when it is configured as an access port:

```
Switch# show spanning-tree interface fastethernet 5/8
Port 264 (FastEthernet5/8) of VLAN200 is forwarding
 Port path cost 18, Port priority 100, Port Identifier 129.8.
 Designated root has priority 32768, address 0010.0d40.34c7
 Designated bridge has priority 32768, address 0010.0d40.34c7
 Designated port id is 128.1, designated path cost 0
 Timers: message age 2, forward delay 0, hold 0
 Number of transitions to forwarding state: 1
 BPDU: sent 0, received 13513
Switch#
```

This example shows how to configure the spanning tree VLAN port cost of a Fast Ethernet interface:

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/8
Switch(config-if)# spanning-tree vlan 200 cost 17
Switch(config-if)# end
Switch#
```

This example shows how to verify the configuration of VLAN 200 on the interface when it is configured as a trunk port:

```
Switch# show spanning-tree vlan 200
<...output truncated...>
Port 264 (FastEthernet5/8) of VLAN200 is forwarding
Port path cost 17, Port priority 64, Port Identifier 129.8.
 Designated root has priority 32768, address 0010.0d40.34c7
 Designated bridge has priority 32768, address 0010.0d40.34c7
 Designated port id is 128.1, designated path cost 0
 Timers: message age 2, forward delay 0, hold 0
 Number of transitions to forwarding state: 1
 BPDU: sent 0, received 13513

<...output truncated...>
Switch#
```



#### Note

The **show spanning-tree** command displays only information for ports with an active link (green light is on). If there is no port with an active link, you can issue a **show running-config** command to confirm the configuration.

## Configuring the Bridge Priority of a VLAN



#### Note

Exercise care when configuring the bridge priority of a VLAN. In most cases, we recommend that you enter the **spanning-tree vlan *vlan\_ID* root primary** and the **spanning-tree vlan *vlan\_ID* root secondary** commands to modify the bridge priority.



To configure the spanning tree bridge priority of a VLAN, perform this task:

|        | Command                                                                                       | Purpose                                                                                                                                                               |
|--------|-----------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch(config)# [no] <b>spanning-tree vlan <i>vlan_ID</i> priority <i>bridge_priority</i></b> | Configures the bridge priority of a VLAN. The <i>bridge_priority</i> value can be from 1 to 65,535.<br><br>You can use the <b>no</b> keyword to restore the defaults. |
| Step 2 | Switch(config)# <b>end</b>                                                                    | Exits configuration mode.                                                                                                                                             |
| Step 3 | Switch# <b>show spanning-tree vlan <i>vlan_ID</i> bridge [brief]</b>                          | Verifies the configuration.                                                                                                                                           |

This example shows how to configure the bridge priority of VLAN 200 to 33,792:

```
Switch# configure terminal
Switch(config)# spanning-tree vlan 200 priority 33792
Switch(config)# end
Switch#
```

This example shows how to verify the configuration:

```
Switch# show spanning-tree vlan 200 bridge brief

Vlan Bridge ID Hello Time Max Age Fwd Delay Protocol

VLAN200 33792 0050.3e8d.64c8 2 20 15 ieee
Switch#
```

## Configuring the Hello Time



### Note

Exercise care when configuring the hello time. In most cases, we recommend that you use the **spanning-tree vlan *vlan\_ID* root primary** and the **spanning-tree vlan *vlan\_ID* root secondary** commands to modify the hello time.

To configure the spanning tree hello time of a VLAN, perform this task:

|        | Command                                                                                    | Purpose                                                                                                                                                         |
|--------|--------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch(config)# [no] <b>spanning-tree vlan <i>vlan_ID</i> hello-time <i>hello_time</i></b> | Configures the hello time of a VLAN. The <i>hello_time</i> value can be from 1 to 10 seconds.<br><br>You can use the <b>no</b> keyword to restore the defaults. |
| Step 2 | Switch(config)# <b>end</b>                                                                 | Exits configuration mode.                                                                                                                                       |
| Step 3 | Switch# <b>show spanning-tree vlan <i>vlan_ID</i> bridge [brief]</b>                       | Verifies the configuration.                                                                                                                                     |

This example shows how to configure the hello time for VLAN 200 to 7 seconds:

```
Switch# configure terminal
Switch(config)# spanning-tree vlan 200 hello-time 7
Switch(config)# end
Switch#
```

This example shows how to verify the configuration:

```
Switch# show spanning-tree vlan 200 bridge brief
Vlan Bridge ID Hello Time Max Age Fwd Delay Protocol

VLAN200 49152 0050.3e8d.64c8 7 20 15 ieee
Switch#
```

## Configuring the Maximum Aging Time for a VLAN



### Note

Exercise care when configuring aging time. In most cases, we recommend that you use the **spanning-tree vlan *vlan\_ID* root primary** and the **spanning-tree vlan *vlan\_ID* root secondary** commands to modify the maximum aging time.

To configure the spanning tree maximum aging time for a VLAN, perform this task:

|        | Command                                                                              | Purpose                                                                                                                                                              |
|--------|--------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch(config)# <b>[no] spanning-tree vlan <i>vlan_ID</i> max-age <i>max_age</i></b> | Configures the maximum aging time of a VLAN. The <i>max_age</i> value can be from 6 to 40 seconds.<br><br>You can use the <b>no</b> keyword to restore the defaults. |
| Step 2 | Switch(config)# <b>end</b>                                                           | Exits configuration mode.                                                                                                                                            |
| Step 3 | Switch# <b>show spanning-tree vlan <i>vlan_ID</i> bridge [brief]</b>                 | Verifies the configuration.                                                                                                                                          |

This example shows how to configure the maximum aging time for VLAN 200 to 36 seconds:

```
Switch# configure terminal
Switch(config)# spanning-tree vlan 200 max-age 36
Switch(config)# end
Switch#
```

This example shows how to verify the configuration:

```
Switch# show spanning-tree vlan 200 bridge brief
Vlan Bridge ID Hello Time Max Age Fwd Delay Protocol

VLAN200 49152 0050.3e8d.64c8 2 36 15 ieee
Switch#
```

## Configuring the Forward-Delay Time for a VLAN



### Note

Exercise care when configuring forward-delay time. In most cases, we recommend that you use the **spanning-tree vlan *vlan\_ID* root primary** and the **spanning-tree vlan *vlan\_ID* root secondary** commands to modify the forward delay time.

To configure the spanning tree forward delay time for a VLAN, perform this task:

|        | Command                                                                                               | Purpose                                                                                                                                                             |
|--------|-------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch(config)# [no] <b>spanning-tree vlan</b> <i>vlan_ID</i> <b>forward-time</b> <i>forward_time</i> | Configures the forward time of a VLAN. The <i>forward_time</i> value can be from 4 to 30 seconds.<br><br>You can use the <b>no</b> keyword to restore the defaults. |
| Step 2 | Switch(config)# <b>end</b>                                                                            | Exits configuration mode.                                                                                                                                           |
| Step 3 | Switch# <b>show spanning-tree vlan</b> <i>vlan_ID</i> <b>bridge</b> [brief]                           | Verifies the configuration.                                                                                                                                         |

This example shows how to configure the forward delay time for VLAN 200 to 21 seconds:

```
Switch# configure terminal
Switch(config)# spanning-tree vlan 200 forward-time 21
Switch(config)# end
Switch#
```

This example shows how to verify the configuration:

```
Switch# show spanning-tree vlan 200 bridge brief

Vlan Bridge ID Hello Time Max Age Fwd Delay Protocol

VLAN200 49152 0050.3e8d.64c8 2 20 21 ieee
Switch#
```

This example shows how to display spanning tree information for the bridge:

```
Switch# show spanning-tree bridge

Vlan Bridge ID Hello Time Max Age Fwd Dly Protocol

VLAN200 49152 0050.3e8d.64c8 2 20 15 ieee
VLAN202 49152 0050.3e8d.64c9 2 20 15 ieee
VLAN203 49152 0050.3e8d.64ca 2 20 15 ieee
VLAN204 49152 0050.3e8d.64cb 2 20 15 ieee
VLAN205 49152 0050.3e8d.64cc 2 20 15 ieee
VLAN206 49152 0050.3e8d.64cd 2 20 15 ieee
Switch#
```

## Disabling Spanning Tree Protocol

To disable spanning tree on a per-VLAN basis, perform this task:

|        | Command                                                     | Purpose                                     |
|--------|-------------------------------------------------------------|---------------------------------------------|
| Step 1 | Switch(config)# <b>no spanning-tree vlan</b> <i>vlan_ID</i> | Disables spanning tree on a per-VLAN basis. |
| Step 2 | Switch(config)# <b>end</b>                                  | Exits configuration mode.                   |
| Step 3 | Switch# <b>show spanning-tree vlan</b> <i>vlan_ID</i>       | Verifies that spanning tree is disabled.    |

This example shows how to disable spanning tree on VLAN 200:

```
Switch# configure terminal
Switch(config)# no spanning-tree vlan 200
Switch(config)# end
Switch#
```

This example shows how to verify the configuration:

```
Switch# show spanning-tree vlan 200
Spanning tree instance for VLAN 200 does not exist.
Switch#
```

## Enabling Per-VLAN Rapid Spanning Tree

Per-VLAN Rapid Spanning Tree (PVRST+) uses the existing PVST+ framework for configuration purposes and for interaction with other features. It also supports some of the PVST+ extensions.

To configure PVRST+, perform this task:

|        | Command                                                                     | Purpose                                                 |
|--------|-----------------------------------------------------------------------------|---------------------------------------------------------|
| Step 1 | Switch(config)# <b>[no] spantree mode rapid-pvst</b>                        | Enables rapid-PVST+.                                    |
| Step 2 | Switch(config)# <b>interface</b> <i>interface/port</i>                      | Switches to interface configuration mode.               |
| Step 3 | Switch(config)#<br><b>spanning-tree link-type point-to-point</b>            | Sets the link-type to point-to-point mode for the port. |
| Step 4 | Switch(config-if)# <b>exit</b>                                              | Exits interface mode.                                   |
| Step 5 | Switch(config)# <b>exit</b>                                                 | Exits configuration mode.                               |
| Step 6 | Switch(config-if)# <b>clear spantree detected-protocols</b> <i>mod/port</i> | Detects any legacy bridges on the port                  |
| Step 7 | Switch# <b>show summary total</b>                                           | Verifies the rapid-PVST+ configuration.                 |

The following example shows how to configure Rapid-PVST+:

```
Switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# spanning-tree mode rapid-pvst
Switch(config)# int fa 6/4
Switch(config-if)# spanning-tree link-type point-to-point
Switch(config-if)# end
Switch(config)# end
Switch#
23:55:32:%SYS-5-CONFIG_I:Configured from console by console
Switch# clear spanning-tree detected-protocols
```

The following example shows how to verify the configuration:

```
Switch# show spanning-tree summary totals
Switch is in rapid-pvst mode
Root bridge for:VLAN0001
Extended system ID is disabled
Portfast Default is disabled
PortFast BPDU Guard Default is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default is disabled
EtherChannel misconfig guard is enabled
UplinkFast is disabled
BackboneFast is disabled
Pathcost method used is short
Name Blocking Listening Learning Forwarding STP Active

1 vlan 0 0 0 2 2
Switch#
```

## Specifying the Link Type

Rapid connectivity is established only on point-to-point links. Spanning tree views a point-to-point link as a segment connecting only two switches running the spanning tree algorithm. Because the switch assumes that all full-duplex links are point-to-point links and that half-duplex links are shared links, you can avoid explicitly configuring the link type. To configure a specific link type, use the **spanning-tree linktype** command.

## Restarting Protocol Migration

A switch running both MSTP and RSTP supports a built-in protocol migration process that enables the switch to interoperate with legacy 802.1D switches. If this switch receives a legacy 802.1D configuration BPDU (a BPDU with the protocol version set to 0), it sends only 802.1D BPDUs on that port. Furthermore, when an MSTP switch receives a legacy BPDU, it can also detect the following:

- that a port is at the boundary of a region
- an MST BPDU (version 3) associated with a different region, or
- an RST BPDU (version 2).

The switch, however, does not automatically revert to the MSTP mode if it no longer receives 802.1D BPDUs because it cannot determine whether or not the legacy switch has been removed from the link unless the legacy switch is the designated switch. A switch also might continue to assign a boundary role to a port when the switch to which it is connected has joined the region.

To restart the protocol migration process on the entire switch (that is, to force renegotiation with neighboring switches), use the **clear spanning-tree detected-protocols** commands in privileged EXEC mode. To restart the protocol migration process on a specific interface, enter the **clear spanning-tree detected-protocols interface** command *in interface-id* privileged EXEC mode.





## Configuring STP Features

---

This chapter describes the Spanning Tree Protocol (STP) features supported on the Catalyst 4500 series switches. It also provides guidelines, procedures, and configuration examples.

This chapter includes the following major sections:

- Overview of Root Guard, page 13-2
- Overview of Loop Guard, page 13-2
- Overview of PortFast, page 13-3
- Overview of BPDU Guard, page 13-4
- Overview of PortFast BPDU Filtering, page 13-4
- Overview of UplinkFast, page 13-5
- Overview of BackboneFast, page 13-6
- Enabling Root Guard, page 13-8
- Enabling Loop Guard, page 13-9
- Enabling PortFast, page 13-11
- Enabling BPDU Guard, page 13-12
- Enabling PortFast BPDU Filtering, page 13-12
- Enabling UplinkFast, page 13-14
- Enabling BackboneFast, page 13-15



### Note

---

For information on configuring STP, see Chapter 12, “Understanding and Configuring STP.”

---



### Note

---

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference* and related publications at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/index.htm>

---

## Overview of Root Guard

Spanning Tree root guard forces an interface to become a designated port, to protect the current root status and prevent surrounding switches from becoming the root switch.

When you enable root guard on a per-port basis, it is automatically applied to all of the active VLANs to which that port belongs. When you disable root guard, it is disabled for the specified port and the port automatically goes into the listening state.

When a switch that has ports with root guard enabled detects a new root, the ports will go into root-inconsistent state. Then, when the switch no longer detects a new root, its ports will automatically go into the listening state.

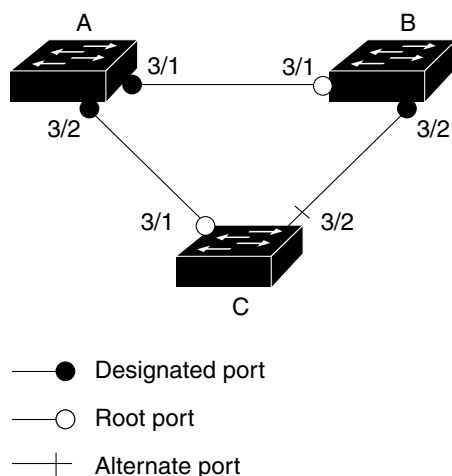
## Overview of Loop Guard

Loop guard helps prevent bridging loops that could occur because of a unidirectional link failure on a point-to-point link. When enabled globally, loop guard applies to all point-to-point ports on the system. Loop guard detects root ports and blocked ports and ensures that they keep receiving BPDUs from their designated port on the segment. If a loop-guard-enabled root or blocked port stop receiving BPDUs from its designated port, it transitions to the blocking state, assuming there is a physical link error on this port. The port recovers from this state as soon as it receives a BPDU.

You can enable loop guard on a per-port basis. When you enable loop guard, it is automatically applied to all of the active instances or VLANs to which that port belongs. When you disable loop guard, it is disabled for the specified ports. Disabling loop guard moves all loop-inconsistent ports to the listening state.

If you enable loop guard on a channel and the first link becomes unidirectional, loop guard blocks the entire channel until the affected port is removed from the channel. Figure 13-1 shows loop guard in a triangular switch configuration.

**Figure 13-1 Triangular Switch Configuration with Loop Guard**



55772



Figure 13-1 illustrates the following configuration:

- Switches A and B are distribution switches.
- Switch C is an access switch.
- Loop guard is enabled on ports 3/1 and 3/2 on Switches A, B, and C.

Enabling loop guard on a root switch has no effect but provides protection when a root switch becomes a nonroot switch.

Follow these guidelines when using loop guard:

- Do not enable loop guard on PortFast-enabled or dynamic VLAN ports.
- Do not enable loop guard if root guard is enabled.

Loop guard interacts with other features as follows:

- Loop guard does not affect the functionality of UplinkFast or BackboneFast.
- Enabling loop guard on ports that are not connected to a point-to-point link will not work.
- Root guard forces a port to always be the root port. Loop guard is effective only if the port is a root port or an alternate port. You cannot enable loop guard and root guard on a port at the same time.
- Loop guard uses the ports known to spanning tree. Loop guard can take advantage of logical ports provided by the Port Aggregation Protocol (PAgP). However, to form a channel, all the physical ports grouped in the channel must have compatible configurations. PAgP enforces uniform configurations of root guard or loop guard on all the physical ports to form a channel.

These caveats apply to loop guard:

- Spanning tree always chooses the first operational port in the channel to send the BPDUs. If that link becomes unidirectional, loop guard blocks the channel, even if other links in the channel are functioning properly.
- If a set of ports that are already blocked by loop guard are grouped together to form a channel, spanning tree loses all the state information for those ports and the new channel port may obtain the forwarding state with a designated role.
- If a channel is blocked by loop guard and the channel breaks, spanning tree loses all the state information. The individual physical ports may obtain the forwarding state with the designated role, even if one or more of the links that formed the channel are unidirectional.

**Note**

You can enable UniDirectional Link Detection (UDLD) to help isolate the link failure. A loop may occur until UDLD detects the failure, but loop guard will not be able to detect it.

- Loop guard has no effect on a disabled spanning tree instance or a VLAN.

## Overview of PortFast

Spanning Tree PortFast causes an interface configured as a Layer 2 access port to enter the forwarding state immediately, bypassing the listening and learning states. You can use PortFast on Layer 2 access ports connected to a single workstation or server to allow those devices to connect to the network immediately, rather than waiting for spanning tree to converge. If the interface receives a bridge protocol data unit (BPDU), which should not happen if the interface is connected to a single workstation or server, spanning tree puts the port into the blocking state.

**Note**

Because the purpose of PortFast is to minimize the time that access ports must wait for spanning tree to converge, it is most effective when used on access ports. If you enable PortFast on a port connecting to another switch, you risk creating a spanning tree loop.

## Overview of BPDU Guard

Spanning Tree BPDU guard shuts down PortFast-configured interfaces that receive BPDUs, rather than putting them into the spanning tree blocking state. In a valid configuration, PortFast-configured interfaces do not receive BPDUs. Reception of a BPDU by a PortFast-configured interface signals an invalid configuration, such as connection of an unauthorized device. BPDU guard provides a secure response to invalid configurations, because the administrator must manually put the interface back in service.

**Note**

When the BPDU guard feature is enabled, spanning tree applies the BPDU guard feature to all PortFast-configured interfaces.

## Overview of PortFast BPDU Filtering

Cisco IOS Release 12.1(11)EW and later support PortFast BPDU filtering, which allows the administrator to prevent the system from sending or even receiving BPDUs on specified ports.

When configured globally, PortFast BPDU filtering applies to all operational PortFast ports. Ports in an operational PortFast state are supposed to be connected to hosts that typically drop BPDUs. If an operational PortFast port receives a BPDU, it immediately loses its operational PortFast status. In that case, PortFast BPDU filtering is disabled on this port and STP resumes sending BPDUs on this port.

PortFast BPDU filtering can also be configured on a per-port basis. When PortFast BPDU filtering is explicitly configured on a port, it does not send any BPDUs and drops all BPDUs it receives.

**Caution**

Explicitly configuring PortFast BPDU filtering on a port that is not connected to a host can result in bridging loops, because the port will ignore any BPDU it receives and go to the forwarding state.

When you enable PortFast BPDU filtering globally and set the port configuration as the default for PortFast BPDU filtering (see the “Enabling PortFast BPDU Filtering” section on page 13-12), PortFast enables or disables PortFast BPDU filtering.

If the port configuration is not set to default, then the PortFast configuration will not affect PortFast BPDU filtering. Table 13-1 lists all the possible PortFast BPDU filtering combinations. PortFast BPDU filtering allows access ports to move directly to the forwarding state as soon as the end hosts are connected.

**Table 13-1 PortFast BPDU Filtering Port Configurations**

| Per-Port Configuration | Global Configuration | PortFast State | PortFast BPDU Filtering State |
|------------------------|----------------------|----------------|-------------------------------|
| Default                | Enable               | Enable         | Enable <sup>1</sup>           |
| Default                | Enable               | Disable        | Disable                       |

**Table 13-1 PortFast BPDU Filtering Port Configurations (continued)**

| Per-Port Configuration | Global Configuration | PortFast State | PortFast BPDU Filtering State |
|------------------------|----------------------|----------------|-------------------------------|
| Default                | Disable              | Not applicable | Disable                       |
| Disable                | Not applicable       | Not applicable | Disable                       |
| Enable                 | Not applicable       | Not applicable | Enable                        |

1. The port transmits at least 10 BPDUs. If this port receives any BPDUs, then PortFast and PortFast BPDU filtering are disabled.

## Overview of UplinkFast

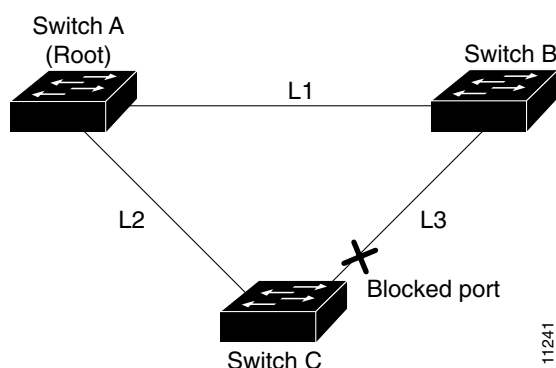


### Note

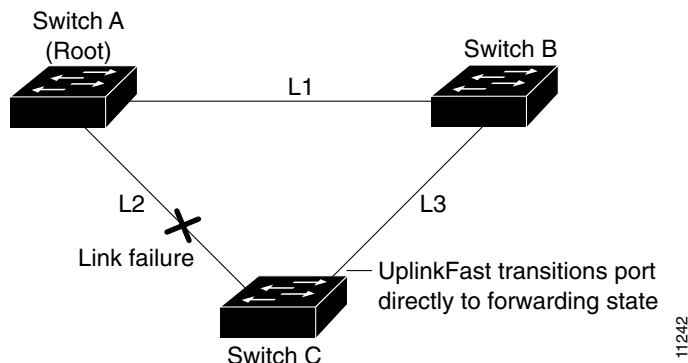
UplinkFast is most useful in wiring-closet switches. This feature might not be useful for other types of applications.

Spanning Tree UplinkFast provides fast convergence after a direct link failure and uses uplink groups to achieve load balancing between redundant Layer 2 links. Convergence is the speed and ability of a group of internetworking devices running a specific routing protocol to agree on the topology of an internetwork after a change in that topology. An uplink group is a set of Layer 2 interfaces (per VLAN), only one of which is forwarding at any given time. Specifically, an uplink group consists of the root port (which is forwarding) and a set of blocked ports, except for self-looping ports. The uplink group provides an alternate path in case the currently forwarding link fails.

Figure 13-2 shows an example of a topology with no link failures. Switch A, the root switch, is connected directly to Switch B over link L1 and to Switch C over link L2. The Layer 2 interface on Switch C that is connected directly to Switch B is in the blocking state.

**Figure 13-2 UplinkFast Before Direct Link Failure**

If Switch C detects a link failure on the currently active link L2 on the root port (a direct link failure), UplinkFast unblocks the blocked port on Switch C and transitions it to the forwarding state without going through the listening and learning states, as shown in Figure 13-3. This switchover takes approximately one to five seconds.

**Figure 13-3 UplinkFast After Direct Link Failure**

## Overview of BackboneFast

BackboneFast is a complementary technology to UplinkFast. Whereas UplinkFast is designed to quickly respond to failures on links directly connected to leaf-node switches, it does not help with indirect failures in the backbone core. BackboneFast optimizes based on the Max Age setting. It allows the default convergence time for indirect failures to be reduced from 50 seconds to 30 seconds. However, it never eliminates forward delays and offers no assistance for direct failures.



### Note

BackboneFast should be enabled on every switch in your network.

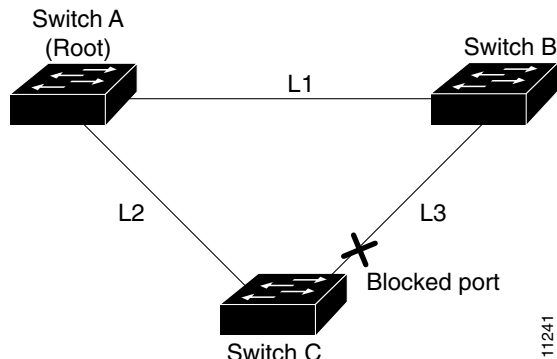
Sometimes a switch receives a BPDU from a designated switch that identifies the root bridge and the designated bridge as the same switch. Because this shouldn't happen, the BPDU is considered inferior. BPDUs are considered inferior when a link from the designated switch has lost its link to the root bridge. The designated switch transmits the BPDUs with the information that it is now the root bridge as well as the designated bridge. The receiving switch will ignore the inferior BPDU for the time defined by the Max Age setting.

After receiving inferior BPDUs, the receiving switch will try to determine if there is an alternate path to the root bridge.

- If the port that the inferior BPDUs are received on is already in blocking mode, then the root port and other blocked ports on the switch become alternate paths to the root bridge.
- If the inferior BPDUs are received on a root port, then all presently blocking ports become the alternate paths to the root bridge. Also, if the inferior BPDUs are received on a root port and there are no other blocking ports on the switch, the receiving switch assumes that the link to the root bridge is down and the time defined by the Max Age setting expires, which turns the switch into the root switch.

If the switch finds an alternate path to the root bridge, it will use this new alternate path. This new path, and any other alternate paths, will be used to send a Root Link Query (RLQ) BPDU. When BackboneFast is enabled, the RLQ BPDUs are sent out as soon as an inferior BPDU is received. This process can enable faster convergence in the event of a backbone link failure.

Figure 13-4 shows an example of a topology with no link failures. Switch A, the root switch, connects directly to Switch B over link L1 and to Switch C over link L2. In this example, because switch B has a lower priority than A but higher than C, switch B becomes the designated bridge for L3. Consequently, the Layer 2 interface on Switch C that connects directly to Switch B must be in the blocking state.

**Figure 13-4 BackboneFast Before Indirect Link Failure**

Next, assume that L1 fails. Switch A and Switch B, the switches directly connected to this segment, instantly know that the link is down. The blocking interface on Switch C must enter the forwarding state for the network to recover by itself. However, because L1 is not directly connected to Switch C, Switch C does not start sending any BPDUs on L3 under the normal rules of STP until the time defined by the Max Age setting has expired.

In an STP environment without BackboneFast, if L1 should fail, Switch C cannot detect this failure because it is not connected directly to link L1. However, because Switch B is directly connected to the root switch over L1, Switch B detects the failure and elects itself the root. Then Switch B begins sending configuration BPDUs to Switch C, listing itself as the root.

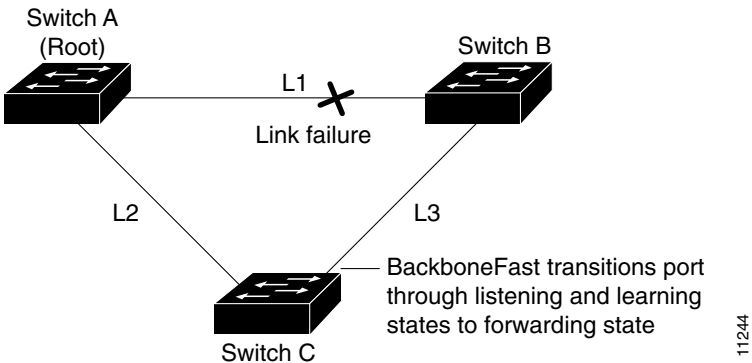
Here is what happens additionally when you use BackboneFast to eliminate the time defined by the Max Age setting (20-second) delay:

1. When Switch C receives the inferior configuration BPDUs from Switch B, Switch C infers that an indirect failure has occurred.
2. Switch C then sends out an RLQ.
3. Switch A receives the RLQ. Because Switch A is the root bridge, it replies with an RLQ response, listing itself as the root bridge.
4. When Switch C receives the RLQ response on its existing root port, it knows that it still has a stable connection to the root bridge. Because Switch C originated the RLQ request, it does not need to forward the RLQ response on to other switches.
5. BackboneFast allows the blocked port on Switch C to move immediately to the listening state without waiting for the time defined by the Max Age setting for the port to expire.
6. BackboneFast transitions the Layer 2 interface on Switch C to the forwarding state, providing a path from Switch B to Switch A.

This switchover takes approximately 30 seconds, twice the Forward Delay time if the default forward delay time of 15 seconds is set.

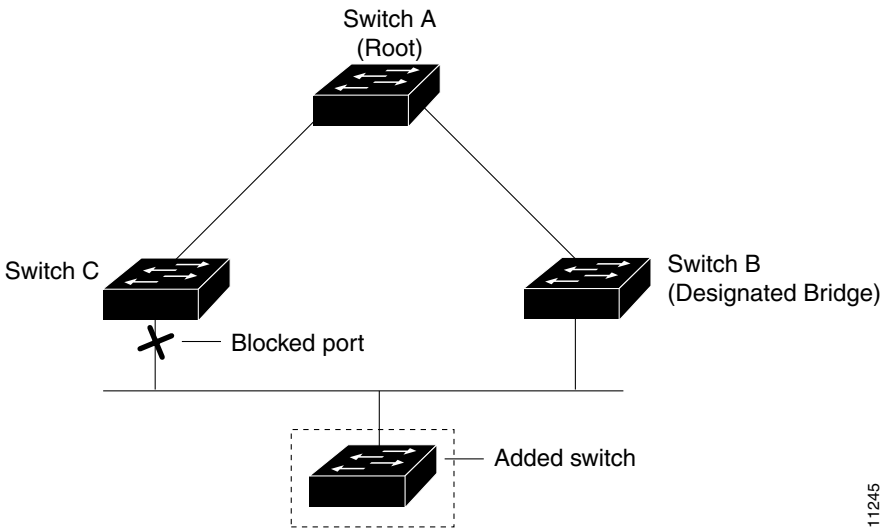
Figure 13-5 shows how BackboneFast reconfigures the topology to account for the failure of link L1.

Figure 13-5 BackboneFast after Indirect Link Failure



If a new switch is introduced into a shared-medium topology as shown in Figure 13-6, BackboneFast is not activated, because the inferior BPDUs did not come from the recognized designated bridge (Switch B). The new switch begins sending inferior BPDUs that say it is the root switch. However, the other switches ignore these inferior BPDUs, and the new switch learns that Switch B is the designated bridge to Switch A, the root switch.

Figure 13-6 Adding a Switch in a Shared-Medium Topology



# Enabling Root Guard

To enable root guard on a Layer 2 access port (to force it to become a designated port), perform this task:

|        | Command                                                                       | Purpose                                                                         |
|--------|-------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| Step 1 | Switch(config)# <b>interface</b> {{fastethernet   gigabitethernet} slot/port} | Specifies an interface to configure.                                            |
| Step 2 | Switch(config-if)# [ <b>no</b> ] <b>spanning-tree guard root</b>              | Enables root guard.<br>You can use the <b>no</b> keyword to disable Root Guard. |

|        | Command                           | Purpose                     |
|--------|-----------------------------------|-----------------------------|
| Step 3 | Switch(config-if)# <b>end</b>     | Exits configuration mode.   |
| Step 4 | Switch# <b>show spanning-tree</b> | Verifies the configuration. |

This example shows how to enable root guard on Fast Ethernet interface 5/8:

```
Switch(config)# interface fastethernet 5/8
Switch(config-if)# spanning-tree guard root
Switch(config-if)# end
Switch#
```

This example shows how to verify the configuration:

```
Switch# show running-config interface fastethernet 5/8
Building configuration...
```

```
Current configuration: 67 bytes
```

```
!
interface FastEthernet5/8
 switchport mode access
 spanning-tree guard root
end
```

```
Switch#
```

This example shows how to determine whether any ports are in root inconsistent state:

```
Switch# show spanning-tree inconsistentports
```

| Name     | Interface       | Inconsistency          |
|----------|-----------------|------------------------|
| -----    | -----           | -----                  |
| VLAN0001 | FastEthernet3/1 | Port Type Inconsistent |
| VLAN0001 | FastEthernet3/2 | Port Type Inconsistent |
| VLAN1002 | FastEthernet3/1 | Port Type Inconsistent |
| VLAN1002 | FastEthernet3/2 | Port Type Inconsistent |
| VLAN1003 | FastEthernet3/1 | Port Type Inconsistent |
| VLAN1003 | FastEthernet3/2 | Port Type Inconsistent |
| VLAN1004 | FastEthernet3/1 | Port Type Inconsistent |
| VLAN1004 | FastEthernet3/2 | Port Type Inconsistent |
| VLAN1005 | FastEthernet3/1 | Port Type Inconsistent |
| VLAN1005 | FastEthernet3/2 | Port Type Inconsistent |

```
Number of inconsistent ports (segments) in the system :10
```

## Enabling Loop Guard

You can enable loop guard globally or per port.

To enable loop guard globally on the switch, perform this task:

|        | Command                                                | Purpose                                      |
|--------|--------------------------------------------------------|----------------------------------------------|
| Step 1 | Switch(config)# <b>spanning-tree loopguard default</b> | Enables loop guard globally on the switch.   |
| Step 2 | Switch(config)# <b>end</b>                             | Exits configuration mode.                    |
| Step 3 | Switch# <b>show spanning tree interface 4/4 detail</b> | Verifies the configuration impact on a port. |

This example shows how to enable loop guard globally:

```
Switch(config)# spanning-tree loopguard default
Switch(config)# Ctrl-Z
```

This example shows how to verify the previous configuration of port 4/4:

```
Switch# show spanning-tree interface fastEthernet 4/4 detail
Port 196 (FastEthernet4/4) of VLAN0010 is forwarding
 Port path cost 1000, Port priority 160, Port Identifier 160.196.
 Designated root has priority 32768, address 00d0.00b8.140a
 Designated bridge has priority 32768, address 00d0.00b8.140a
 Designated port id is 160.196, designated path cost 0
 Timers:message age 0, forward delay 0, hold 0
 Number of transitions to forwarding state:1
 The port is in the portfast mode by portfast trunk configuration
 Link type is point-to-point by default
 Bpdu filter is enabled
 Loop guard is enabled by default on the port
 BPDU:sent 0, received 0
```

To enable loop guard on an interface, perform this task:

|        | Command                                                                         | Purpose                                         |
|--------|---------------------------------------------------------------------------------|-------------------------------------------------|
| Step 1 | Switch(config)# interface {type slot/port}   {port-channel port_channel_number} | Selects an interface to configure.              |
| Step 2 | Switch(config-if)# spanning-tree guard loop                                     | Configures loop guard.                          |
| Step 3 | Switch(config)# end                                                             | Exits configuration mode.                       |
| Step 4 | Switch# show spanning tree interface 4/4 detail                                 | Verifies the configuration impact on that port. |

This example shows how to enable loop guard on port 4/4:

```
Switch(config)# interface fastEthernet 4/4
Switch(config-if)# spanning-tree guard loop
Switch(config-if)# ^Z
```

This example shows how to verify the configuration impact on port 4/4:

```
Switch# show spanning-tree interface fastEthernet 4/4 detail
Port 196 (FastEthernet4/4) of VLAN0010 is forwarding
 Port path cost 1000, Port priority 160, Port Identifier 160.196.
 Designated root has priority 32768, address 00d0.00b8.140a
 Designated bridge has priority 32768, address 00d0.00b8.140a
 Designated port id is 160.196, designated path cost 0
 Timers:message age 0, forward delay 0, hold 0
 Number of transitions to forwarding state:1
 The port is in the portfast mode by portfast trunk configuration
 Link type is point-to-point by default
 Bpdu filter is enabled
 Loop guard is enabled on the port
 BPDU:sent 0, received 0
Switch#
```



# Enabling PortFast



## Caution

Use PortFast *only* when connecting a single end station to a Layer 2 access port. Otherwise, you might create a network loop.

To enable PortFast on a Layer 2 access port to force it to enter the forwarding state immediately, perform this task:

|        | Command                                                                                                                 | Purpose                                                                                                                                              |
|--------|-------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch(config)# <b>interface</b> {{fastethernet   gigabitethernet} slot/port}   {port-channel port_channel_number}      | Specifies an interface to configure.                                                                                                                 |
| Step 2 | Switch(config-if)# [no] <b>spanning-tree portfast</b>                                                                   | Enables PortFast on a Layer 2 access port connected to a single workstation or server.<br><br>You can use the <b>no</b> keyword to disable PortFast. |
| Step 3 | Switch(config-if)# <b>end</b>                                                                                           | Exits configuration mode.                                                                                                                            |
| Step 4 | Switch# <b>show running interface</b> {{fastethernet   gigabitethernet} slot/port}   {port-channel port_channel_number} | Verifies the configuration.                                                                                                                          |

This example shows how to enable PortFast on Fast Ethernet interface 5/8:

```
Switch(config)# interface fastethernet 5/8
Switch(config-if)# spanning-tree portfast
Switch(config-if)# end
Switch#
```

This example shows how to verify the configuration:

```
Switch# show running-config interface fastethernet 5/8
Building configuration...

Current configuration:
!
interface FastEthernet5/8
 no ip address
 switchport
 switchport access vlan 200
 switchport mode access
 spanning-tree portfast
end

Switch#
```

# Enabling BPDU Guard

To enable BPDU guard to shut down PortFast-configured interfaces that receive BPDUs, perform this task:

|        | Command                                               | Purpose                                                                                                                                |
|--------|-------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch(config)# [no] spanning-tree portfast bpduguard | Enables BPDU guard on all the switch's PortFast-configured interfaces.<br><br>You can use the <b>no</b> keyword to disable BPDU guard. |
| Step 2 | Switch(config)# end                                   | Exits configuration mode.                                                                                                              |
| Step 3 | Switch# show spanning-tree summary totals             | Verifies the BPDU configuration.                                                                                                       |

This example shows how to enable BPDU guard:

```
Switch(config)# spanning-tree portfast bpduguard
Switch(config)# end
Switch#
```

This example shows how to verify the BPDU configuration:

```
Switch# show spanning-tree summary totals

Root bridge for: none.
PortFast BPDU Guard is enabled
Etherchannel misconfiguration guard is enabled
UplinkFast is disabled
BackboneFast is disabled
Default pathcost method used is short

Name Blocking Listening Learning Forwarding STP Active

Switch# 34 VLANs 0 0 0 36 36
```

# Enabling PortFast BPDU Filtering

To enable PortFast BPDU filtering globally, perform this task:

|        | Command                                                   | Purpose                                        |
|--------|-----------------------------------------------------------|------------------------------------------------|
| Step 1 | Switch(config)# spanning-tree portfast bpdufilter default | Enables BPDU filtering globally on the switch. |
| Step 2 | Switch# show spanning-tree summary totals                 | Verifies the BPDU configuration.               |

This example shows how to enable PortFast BPDU filtering on a port:

```
Switch(config)# spanning-tree portfast bpdufilter default
Switch(config)# Ctrl-Z
```

This example shows how to verify the BPDU configuration in PVST+ mode:

```
Switch# show spanning-tree summary totals
Root bridge for:VLAN0010
EtherChannel misconfiguration guard is enabled
Extended system ID is disabled
Portfast is enabled by default
PortFast BPDU Guard is disabled by default
Portfast BPDU Filter is enabled by default
Loopguard is disabled by default
UplinkFast is disabled
BackboneFast is disabled
Pathcost method used is long

Name Blocking Listening Learning Forwarding STP Active

2 vlans 0 0 0 3 3

Switch#
```



#### Note

For PVST+ information, see Chapter 14, “Understanding and Configuring Multiple Spanning Trees.”

To enable PortFast BPDU filtering, perform this task:

|        | Command                                                      | Purpose                             |
|--------|--------------------------------------------------------------|-------------------------------------|
| Step 1 | Switch(config)# <b>interface fastEthernet 4/4</b>            | Selects the interface to configure. |
| Step 2 | Switch(config-if)# <b>spanning-tree bpduguard enable</b>     | Enables BPDU filtering.             |
| Step 3 | Switch# <b>show spanning-tree interface fastethernet 4/4</b> | Verifies the configuration.         |

This example shows how to enable PortFast BPDU filtering on port 4/4:

```
Switch(config)# interface fastethernet 4/4
Switch(config-if)# spanning-tree bpduguard enable
Switch(config-if)# ^Z
```

This example shows how to verify that PortFast BPDU filtering is enabled:

```
Switch# show spanning-tree interface fastethernet 4/4

Vlan Role Sts Cost Prio.Nbr Status

VLAN0010 Desg FWD 1000 160.196 Edge P2p
```

This example shows more detail on the port:

```
Switch# show spanning-tree interface fastEthernet 4/4 detail
Port 196 (FastEthernet4/4) of VLAN0010 is forwarding
Port path cost 1000, Port priority 160, Port Identifier 160.196.
Designated root has priority 32768, address 00d0.00b8.140a
Designated bridge has priority 32768, address 00d0.00b8.140a
Designated port id is 160.196, designated path cost 0
Timers:message age 0, forward delay 0, hold 0
Number of transitions to forwarding state:1
The port is in the portfast mode by portfast trunk configuration
Link type is point-to-point by default
Bpdu filter is enabled
BPDU:sent 0, received 0
Switch#
```

# Enabling UplinkFast

UplinkFast increases the bridge priority to 49,152 and adds 3000 to the spanning tree port cost of all interfaces on the switch, making it unlikely that the switch will become the root switch. The *max\_update\_rate* value represents the number of multicast packets transmitted per second (the default is 150 packets per second [pps]).

UplinkFast cannot be enabled on VLANs that have been configured for bridge priority. To enable UplinkFast on a VLAN with bridge priority configured, restore the bridge priority on the VLAN to the default value by entering a **no spanning-tree vlan *vlan\_ID* priority** command in global configuration mode.



**Note**

When you enable UplinkFast, it affects all VLANs on the switch. You cannot configure UplinkFast on an individual VLAN.

To enable UplinkFast, perform this task:

|        | Command                                                                                                   | Purpose                                                                                                                          |
|--------|-----------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch(config)# [no] <b>spanning-tree uplinkfast</b><br>[ <b>max-update-rate</b> <i>max_update_rate</i> ] | Enables UplinkFast.<br><br>You can use the <b>no</b> keyword to disable UplinkFast and restore the default rate, use the command |
| Step 2 | Switch(config)# <b>end</b>                                                                                | Exits configuration mode.                                                                                                        |
| Step 3 | Switch# <b>show spanning-tree vlan <i>vlan_ID</i></b>                                                     | Verifies that UplinkFast is enabled on that VLAN.                                                                                |

This example shows how to enable UplinkFast with a maximum update rate of 400 pps:

```
Switch(config)# spanning-tree uplinkfast max-update-rate 400
Switch(config)# exit
Switch#
```

This example shows how to verify which VLANS have UplinkFast enabled:

```
Switch# show spanning-tree uplinkfast
UplinkFast is enabled

Station update rate set to 150 packets/sec.

UplinkFast statistics

Number of transitions via uplinkFast (all VLANs) :14
Number of proxy multicast addresses transmitted (all VLANs) :5308

Name Interface List

VLAN1 Fa6/9 (fwd) , Gi5/7
VLAN2 Gi5/7 (fwd)
VLAN3 Gi5/7 (fwd)
VLAN4
VLAN5
VLAN6
VLAN7
VLAN8
VLAN10
VLAN15
VLAN1002 Gi5/7 (fwd)
VLAN1003 Gi5/7 (fwd)
VLAN1004 Gi5/7 (fwd)
VLAN1005 Gi5/7 (fwd)
Switch#
```

# Enabling BackboneFast



## Note

For BackboneFast to work, you must enable it on all switches in the network. BackboneFast is supported for use with third-party switches but it is not supported on Token Ring VLANs.

To enable BackboneFast, perform this task:

|        | Command                                                | Purpose                                                                                 |
|--------|--------------------------------------------------------|-----------------------------------------------------------------------------------------|
| Step 1 | Switch(config)# <b>[no] spanning-tree backbonefast</b> | Enables BackboneFast.<br><br>You can use the <b>no</b> keyword to disable BackboneFast. |
| Step 2 | Switch(config)# <b>end</b>                             | Exits configuration mode.                                                               |
| Step 3 | Switch# <b>show spanning-tree backbonefast</b>         | Verifies that BackboneFast is enabled.                                                  |

This example shows how to enable BackboneFast:

```
Switch(config)# spanning-tree backbonefast
Switch(config)# end
Switch#
```

This example shows how to verify that BackboneFast is enabled:

```
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 a summary of port states:

```
Switch#show spanning-tree summary
Root bridge for:VLAN0001, VLAN1002-VLAN1005
Extended system ID is disabled
Portfast is enabled by default
PortFast BPDU Guard is disabled by default
Portfast BPDU Filter is enabled by default
Loopguard is disabled by default
EtherChannel misconfiguration guard is enabled
UplinkFast is enabled
BackboneFast is enabled
Pathcost method used is short
```

| Name     | Blocking | Listening | Learning | Forwarding | STP Active |
|----------|----------|-----------|----------|------------|------------|
| VLAN0001 | 0        | 0         | 0        | 3          | 3          |
| VLAN1002 | 0        | 0         | 0        | 2          | 2          |
| VLAN1003 | 0        | 0         | 0        | 2          | 2          |
| VLAN1004 | 0        | 0         | 0        | 2          | 2          |
| VLAN1005 | 0        | 0         | 0        | 2          | 2          |
| 5 vlans  | 0        | 0         | 0        | 11         | 11         |

#### 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 the total lines of the spanning tree state section:

```

Switch#show spanning-tree summary totals
Root bridge for:VLAN0001, VLAN1002-VLAN1005
Extended system ID is disabled
Portfast is enabled by default
PortFast BPDU Guard is disabled by default
Portfast BPDU Filter is enabled by default
Loopguard is disabled by default
EtherChannel misconfiguration guard is enabled
UplinkFast is enabled
BackboneFast is enabled
Pathcost method used is short

```

| Name    | Blocking | Listening | Learning | Forwarding | STP Active |
|---------|----------|-----------|----------|------------|------------|
| 5 vlans | 0        | 0         | 0        | 11         | 11         |

#### 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#

```



# Understanding and Configuring Multiple Spanning Trees

This chapter describes how to configure the IEEE 802.1s Multiple Spanning Tree (MST) protocol on the Catalyst 4500 series switch. MST is a new IEEE standard derived from Cisco's proprietary Multi-Instance Spanning-Tree Protocol (MISTP) implementation. With MST, you can map a single spanning-tree instance to several VLANs.

This chapter includes the following major sections:

- Overview of MST, page 14-1
- MST Configuration Restrictions and Guidelines, page 14-8
- Configuring MST, page 14-9



## Note

For complete syntax and usage information for the switch commands used in this chapter, refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference* and related publications at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/index.htm>

## Overview of MST

The following sections describe how MST works on a Catalyst 4500 series switch:

- IEEE 802.1s MST, page 14-2
- IEEE 802.1w RSTP, page 14-3
- MST-to-SST Interoperability, page 14-4
- Common Spanning Tree, page 14-5
- MST Instances, page 14-5
- MST Configuration Parameters, page 14-5
- MST Regions, page 14-6
- Message Age and Hop Count, page 14-7
- MST-to-PVST+ Interoperability, page 14-8

## IEEE 802.1s MST

MST extends the IEEE 802.1w rapid spanning tree (RST) algorithm to multiple spanning trees. This extension provides both rapid convergence and load balancing in a VLAN environment. MST converges faster than Per VLAN Spanning Tree Plus (PVST+) and is backward compatible with 802.1D STP, 802.1w (Rapid Spanning Tree Protocol [RSTP]), and the Cisco PVST+ architecture.

MST allows you to build multiple spanning trees over trunks. You can group and associate VLANs to spanning tree instances. Each instance can have a topology independent of other spanning tree instances. This architecture provides multiple forwarding paths for data traffic and enables load balancing. Network fault tolerance is improved because a failure in one instance (forwarding path) does not affect other instances.

In large networks, you can more easily administer the network and use redundant paths by locating different VLAN and spanning tree instance assignments in different parts of the network. A spanning tree instance can exist only on bridges that have compatible VLAN instance assignments. You must configure a set of bridges with the same MST configuration information, which allows them to participate in a specific set of spanning tree instances. Interconnected bridges that have the same MST configuration are referred to as an MST region.

MST uses the modified RSTP, MSTP. MST has the following characteristics:

- MST runs a variant of spanning tree called Internal Spanning Tree (IST). IST augments Common Spanning Tree (CST) information with internal information about the MST region. The MST region appears as a single bridge to adjacent single spanning tree (SST) and MST regions.
- A bridge running MST provides interoperability with SST bridges as follows:
  - MST bridges run IST, which augments CST information with internal information about the MST region.
  - IST connects all the MST bridges in the region and appears as a subtree in the CST that includes the whole bridged domain. The MST region appears as a virtual bridge to adjacent SST bridges and MST regions.
  - The Common and Internal Spanning Tree (CIST) is the collection of the following: ISTs in each MST region, the CST that interconnects the MST regions, and the SST bridges. CIST is identical to an IST inside an MST region and identical to a CST outside an MST region. The STP, RSTP, and MSTP together elect a single bridge as the root of the CIST.
- MST establishes and maintains additional spanning trees within each MST region. These spanning trees are termed MST instances (MSTIs). The IST is numbered 0, and the MSTIs are numbered 1, 2, 3, and so on. Any MSTI is local to the MST region and is independent of MSTIs in another region, even if the MST regions are interconnected.

MST instances combine with the IST at the boundary of MST regions to become the CST as follows:

- Spanning tree information for an MSTI is contained in an MSTP record (M-record).  
M-records are always encapsulated within MST bridge protocol data units (BPDUs). The original spanning trees computed by MSTP are called M-trees, which are active only within the MST region. M-trees merge with the IST at the boundary of the MST region and form the CST.
- MST provides interoperability with PVST+ by generating PVST+ BPDUs for the non-CST VLANs.
- MST supports some of the PVST+ extensions in MSTP as follows:
  - UplinkFast and BackboneFast are not available in MST mode; they are part of RSTP.
  - PortFast is supported.
  - BPDU filter and BPDU guard are supported in MST mode.
  - Loop guard and root guard are supported in MST. MST preserves the VLAN 1 disabled functionality except that BPDUs are still transmitted in VLAN 1.



- MST switches operate as if MAC reduction is enabled.
- For private VLANs (PVLANS), you must map a secondary VLAN to the same instance as the primary.

## IEEE 802.1w RSTP

RSTP, specified in 802.1w, supersedes STP specified in 802.1D, but remains compatible with STP. You configure RSTP when you configure the MST feature. For more information, see the “Configuring MST” section on page 14-9.

RSTP provides the structure on which the MST operates, significantly reducing the time to reconfigure the active topology of a network when its physical topology or configuration parameters change. RSTP selects one switch as the root of a spanning-tree-connected active topology and assigns port roles to individual ports of the switch, depending on whether that port is part of the active topology.

RSTP provides rapid connectivity following the failure of a switch, switch port, or a LAN. A new root port and the designated port on the other side of the bridge transition to the forwarding state through an explicit handshake between them. RSTP allows switch port configuration so the ports can transition to forwarding directly when the switch reinitializes.

RSTP provides backward compatibility with 802.1D bridges as follows:

- RSTP selectively sends 802.1D-configured BPDUs and Topology Change Notification (TCN) BPDUs on a per-port basis.
- When a port initializes, the migration delay timer starts and RSTP BPDUs are transmitted. While the migration delay timer is active, the bridge processes all BPDUs received on that port.
- If the bridge receives an 802.1D BPDU after a port’s migration delay timer expires, the bridge assumes it is connected to an 802.1D bridge and starts using only 802.1D BPDUs.
- When RSTP uses 802.1D BPDUs on a port and receives an RSTP BPDU after the migration delay expires, RSTP restarts the migration delay timer and begins using RSTP BPDUs on that port.

## RSTP Port Roles

In RSTP, the port roles are defined as follows:

- Root—A forwarding port elected for the spanning tree topology.
- Designated—A forwarding port elected for every switched LAN segment.
- Alternate—An alternate path to the root bridge to that provided by the current root port.
- Backup—A backup for the path provided by a designated port toward the leaves of the spanning tree. Backup ports can exist only where two ports are connected together in a loopback mode or bridge with two or more connections to a shared LAN segment.
- Disabled—A port that has no role within the operation of spanning tree.

The system assigns port roles as follows:

- A root port or designated port role includes the port in the active topology.
- An alternate port or backup port role excludes the port from the active topology.

## RSTP Port States

The port state controls the forwarding and learning processes and provides the values of discarding, learning, and forwarding. Table 14-1 shows the STP port states and RSTP port states.

**Table 14-1 Comparison Between STP and RSTP Port States**

| Operational Status | STP Port State        | RSTP Port State         | Port Included in Active Topology |
|--------------------|-----------------------|-------------------------|----------------------------------|
| Enabled            | Blocking <sup>1</sup> | Discarding <sup>2</sup> | No                               |
| Enabled            | Listening             | Discarding              | No                               |
| Enabled            | Learning              | Learning                | Yes                              |
| Enabled            | Forwarding            | Forwarding              | Yes                              |
| Disabled           | Disabled              | Discarding              | No                               |

1. IEEE 802.1D port state designation.

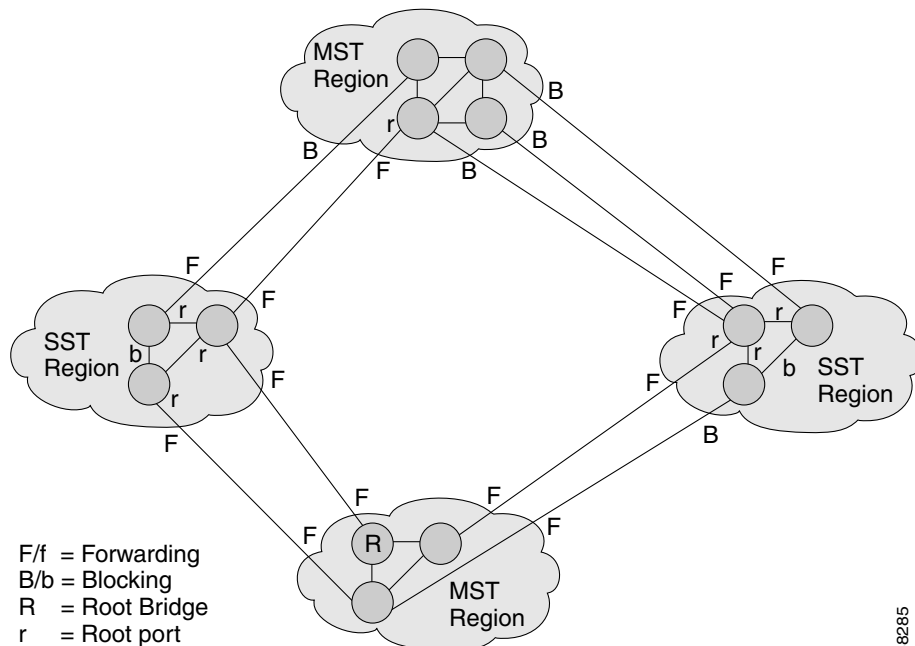
2. IEEE 802.1w port state designation. Discarding is the same as blocking in MST.

In a stable topology, RSTP ensures that every root port and designated port transitions to the forwarding state while all alternate ports and backup ports are always in the discarding state.

## MST-to-SST Interoperability

A virtual bridged LAN may contain interconnected regions of SST and MST bridges. Figure 14-1 shows this relationship.

**Figure 14-1 Network with Interconnected SST and MST Regions**



To STP running in the SST region, an MST region appears as a single SST or pseudobridge, which operates as follows:

- Although the values for root identifiers and root path costs match for all BPDUs in all pseudobridges, a pseudobridge differs from a single SST bridge as follows:
  - The pseudobridge BPDUs have different bridge identifiers. This difference does not affect STP operation in the neighboring SST regions because the root identifier and root cost are the same.
  - BPDUs sent from the pseudobridge ports may have significantly different message ages. Because the message age increases by one second for each hop, the difference in the message age is measured in seconds.
- Data traffic from one port of a pseudobridge (a port at the edge of a region) to another port follows a path entirely contained within the pseudobridge or MST region. Data traffic belonging to different VLANs might follow different paths within the MST regions established by MST.
- The system prevents looping by doing either of the following:
  - Blocking the appropriate pseudobridge ports by allowing one forwarding port on the boundary and blocking all other ports.
  - Setting the CST partitions to block the ports of the SST regions.

## Common Spanning Tree

CST (802.1Q) is a single spanning tree for all the VLANs. In a Catalyst 4000 family switch running PVST+, the VLAN 1 spanning tree corresponds to CST. In a Catalyst 4000 family switch running MST, IST (instance 0) corresponds to CST.

## MST Instances

This release supports up to 16 instances; each spanning tree instance is identified by an instance ID that ranges from 0 to 15. Instance 0 is mandatory and is always present. Instances 1 through 15 are optional.

## MST Configuration Parameters

MST configuration has three parts, as follows:

- Name—A 32-character string (null padded) that identifies the MST region.
- Revision number—An unsigned 16-bit number that identifies the revision of the current MST configuration.

**Note**

You must set the revision number when required as part of the MST configuration. The revision number is not incremented automatically each time you commit the MST configuration.

- MST configuration table—An array of 4096 bytes. Each byte, interpreted as an unsigned integer, corresponds to a VLAN. The value is the instance number to which the VLAN is mapped. The first byte that corresponds to VLAN 0 and the 4096th byte that corresponds to VLAN 4095 are unused and always set to zero.

You must configure each byte manually. You can use SNMP or the CLI to perform the configuration.

MST BPDUs contain the MST configuration ID and the checksum. An MST bridge accepts an MST BPDUs only if the MST BPDUs configuration ID and the checksum match its own MST region configuration ID and checksum. If either value is different, the MST BPDUs is considered to be an SST BPDUs.

## MST Regions

These sections describe MST regions:

- MST Region Overview, page 14-6
- Boundary Ports, page 14-6
- IST Master, page 14-7
- Edge Ports, page 14-7
- Link Type, page 14-7

### MST Region Overview

Interconnected bridges that have the same MST configuration are referred to as an MST region. There is no limit on the number of MST regions in the network.

To form an MST region, bridges can be either of the following:

- An MST bridge that is the only member of the MST region.
- An MST bridge interconnected by a LAN. A LAN's designated bridge has the same MST configuration as an MST bridge. All the bridges on the LAN can process MST BPDUs.

If you connect two MST regions with different MST configurations, the MST regions do the following:

- Load balance across redundant paths in the network. If two MST regions are redundantly connected, all traffic flows on a single connection with the MST regions in a network.
- Provide an RSTP handshake to enable rapid connectivity between regions. However, the handshaking is not as fast as between two bridges. To prevent loops, all the bridges inside the region must agree upon the connections to other regions. This situation introduces a delay. We do not recommend partitioning the network into a large number of regions.

### Boundary Ports

A boundary port is a port that connects to a LAN, the designated bridge of which is either an SST bridge or a bridge with a different MST configuration. A designated port knows that it is on the boundary if it detects an STP bridge or receives an agreement message from an RST or MST bridge with a different configuration.

At the boundary, the role of MST ports do not matter; their state is forced to be the same as the IST port state. If the boundary flag is set for the port, the MSTP Port Role selection mechanism assigns a port role to the boundary and the same state as that of the IST port. The IST port at the boundary can take up any port role except a backup port role.

## IST Master

The IST master of an MST region is the bridge with the lowest bridge identifier and the least path cost to the CST root. If an MST bridge is the root bridge for CST, then it is the IST master of that MST region. If the CST root is outside the MST region, then one of the MST bridges at the boundary is selected as the IST master. Other bridges on the boundary that belong to the same region eventually block the boundary ports that lead to the root.

If two or more bridges at the boundary of a region have an identical path to the root, you can set a slightly lower bridge priority to make a specific bridge the IST master.

The root path cost and message age inside a region stay constant, but the IST path cost is incremented and the IST remaining hops are decremented at each hop. Enter the **show spanning-tree mst** command to display the information about the IST master, path cost, and remaining hops for the bridge.

## Edge Ports

A port that is connected to a nonbridging device (for example, a host or a switch) is an edge port. A port that connects to a hub is also an edge port if the hub or any LAN that is connected to it does not have a bridge. An edge port can start forwarding as soon as the link is up.

MST requires that you configure each port connected to a host. To establish rapid connectivity after a failure, you need to block the non-edge designated ports of an intermediate bridge. If the port connects to another bridge that can send back an agreement, then the port starts forwarding immediately. Otherwise, the port needs twice the forward delay time to start forwarding again. You must explicitly configure the ports that are connected to the hosts and switches as edge ports while using MST.

To prevent a misconfiguration, the PortFast operation is turned off if the port receives a BPDU. You can display the configured and operational status of PortFast by using the **show spanning-tree mst interface** command.

## Link Type

Rapid connectivity is established only on point-to-point links. You must configure ports explicitly to a host or switch. However, cabling in most networks meets this requirement, and you can avoid explicit configuration by treating all full-duplex links as point-to-point links by entering the **spanning-tree linktype** command.

## Message Age and Hop Count

IST and MST instances do not use the message age and maximum age timer settings in the BPDU. IST and MST use a separate hop count mechanism that is very similar to the IP time-to live (TTL) mechanism. You can configure each MST bridge with a maximum hop count. The root bridge of the instance sends a BPDU (or M-record) with the remaining hop count that is equal to the maximum hop count. When a bridge receives a BPDU (or M-record), it decrements the received remaining hop count by one. The bridge discards the BPDU (M-record) and ages out the information held for the port if the count reaches zero after decrementing. The nonroot bridges propagate the decremented count as the remaining hop count in the BPDUs (M-records) they generate.

The message age and maximum age timer settings in the RST portion of the BPDU remain the same throughout the region, and the same values are propagated by the region's designated ports at the boundary.

## MST-to-PVST+ Interoperability

Keep these guidelines in mind when you configure MST switches (in the same region) to interact with PVST+ switches:

- Configure the root for all VLANs inside the MST region as shown in this example:

```
Switch# show spanning-tree mst interface gigabitethernet 1/1

GigabitEthernet1/1 of MST00 is root forwarding
Edge port: no (trunk) port guard : none (default)
Link type: point-to-point (auto) bpdu filter: disable (default)
Boundary : boundary (PVST) bpdu guard : disable (default)
Bpdus sent 10, received 310

Instance Role Sts Cost Prio.Nbr Vlan mapped

0 Root FWD 20000 128.1 1-2,4-2999,4000-4094
3 Boun FWD 20000 128.1 3,3000-3999
```

The ports that belong to the MST switch at the boundary simulate PVST+ and send PVST+ BPDUs for all the VLANs.

If you enable loop guard on the PVST+ switches, the ports might change to a loop-inconsistent state when the MST switches change their configuration. To correct the loop-inconsistent state, you must disable and renewable loop guard on that PVST+ switch.

- Do not locate the root for some or all of the VLANs inside the PVST+ side of the MST switch because when the MST switch at the boundary receives PVST+ BPDUs for all or some of the VLANs on its designated ports, root guard sets the port to the blocking state.

When you connect a PVST+ switch to two different MST regions, the topology change from the PVST+ switch does not pass beyond the first MST region. In such a case, the topology changes are propagated only in the instance to which the VLAN is mapped. The topology change stays local to the first MST region, and the Cisco Access Manager (CAM) entries in the other region are not flushed. To make the topology change visible throughout other MST regions, you can map that VLAN to IST or connect the PVST+ switch to the two regions through access links.

## MST Configuration Restrictions and Guidelines

Follow these restrictions and guidelines to avoid configuration problems:

- Do not disable spanning tree on any VLAN in any of the PVST bridges.
- Do not use PVST bridges as the root of CST.
- Do not connect switches with access links, because access links may partition a VLAN.
- Ensure that all PVST root bridges have lower (numerically higher) priority than the CST root bridge.
- Ensure that trunks carry all of the VLANs mapped to an instance or do not carry any VLANs at all for this instance.
- Complete any MST configuration that incorporates a large number of either existing or new logical VLAN ports during a maintenance window because the complete MST database gets reinitialized for any incremental change (such as adding new VLANs to instances or moving VLANs across instances).

# Configuring MST

The following sections describe how to configure MST:

- Enabling MST, page 14-9
- Configuring MST Instance Parameters, page 14-10
- Configuring MST Instance Port Parameters, page 14-11
- Displaying MST Configurations, page 14-13
- Restarting Protocol Migration, page 14-12

## Enabling MST

To enable and configure MST on a Catalyst 4500 series switch, perform this task:

|        | Command                                                             | Purpose                                                                                                                                                                                                                                                                                                                 |
|--------|---------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch(config)# <b>spanning-tree mode mst</b>                       | Enters MST mode.                                                                                                                                                                                                                                                                                                        |
| Step 2 | Switch(config)# <b>spanning-tree mst configuration</b>              | Enters MST configuration submenu.<br><br>You can use the <b>no</b> keyword to clear the MST configuration.                                                                                                                                                                                                              |
| Step 3 | Switch(config-mst)# <b>show current</b>                             | Displays the current MST configuration.                                                                                                                                                                                                                                                                                 |
| Step 4 | Switch(config-mst)# <b>name name</b>                                | Sets the MST region name.                                                                                                                                                                                                                                                                                               |
| Step 5 | Switch(config-mst)# <b>revision revision_number</b>                 | Sets the MST configuration revision number.                                                                                                                                                                                                                                                                             |
| Step 6 | Switch(config-mst)# <b>instance instance_number vlan vlan_range</b> | Maps the VLANs to an MST instance.<br><br>If you do not specify the <b>vlan</b> keyword, you can use the <b>no</b> keyword to unmap all the VLANs that were mapped to an MST instance.<br><br>If you specify the <b>vlan</b> keyword, you can use the <b>no</b> keyword to unmap a specified VLAN from an MST instance. |
| Step 7 | Switch(config-mst)# <b>show pending</b>                             | Displays the new MST configuration to be applied.                                                                                                                                                                                                                                                                       |
| Step 8 | Switch(config-mst)# <b>end</b>                                      | Applies the configuration and exit MST configuration submenu.                                                                                                                                                                                                                                                           |
| Step 9 | Switch# <b>show spanning-tree mst configuration</b>                 | Displays the current MST configuration.                                                                                                                                                                                                                                                                                 |

This example show how to enable MST:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# spanning-tree mode mst

Switch(config)# spanning-tree mst configuration

Switch(config-mst)# show current
Current MST configuration
Name []
Revision 0
Instance Vlans mapped
```

```

0 1-4094

Switch(config-mst)# name cisco
Switch(config-mst)# revision 2
Switch(config-mst)# instance 1 vlan 1
Switch(config-mst)# instance 2 vlan 1-1000
Switch(config-mst)# show pending
Pending MST configuration
Name [cisco]
Revision 2
Instance Vlans mapped

0 1001-4094
2 1-1000

Switch(config-mst)# no instance 2
Switch(config-mst)# show pending
Pending MST configuration
Name [cisco]
Revision 2
Instance Vlans mapped

0 1-4094

Switch(config-mst)# instance 1 vlan 2000-3000
Switch(config-mst)# no instance 1 vlan 1500
Switch(config-mst)# show pending
Pending MST configuration
Name [cisco]
Revision 2
Instance Vlans mapped

0 1-1999,2500,3001-4094
1 2000-2499,2501-3000

Switch(config-mst)# end
Switch(config)# no spanning-tree mst configuration
Switch(config)# end
Switch# show spanning-tree mst configuration
Name []
Revision 0
Instance Vlans mapped

0 1-4094

```

## Configuring MST Instance Parameters

To configure MST instance parameters, perform this task:

|        | Command                                                               | Purpose                                            |
|--------|-----------------------------------------------------------------------|----------------------------------------------------|
| Step 1 | Switch(config)# <b>spanning-tree mst X priority Y</b>                 | Configures the priority for an MST instance.       |
| Step 2 | Switch(config)# <b>spanning-tree mst X root [primary   secondary]</b> | Configures the bridge as root for an MST instance. |
| Step 3 | Switch(config)# <b>Ctrl-Z</b>                                         | Exits configuration mode.                          |
| Step 4 | Switch# <b>show spanning-tree mst</b>                                 | Verifies the configuration.                        |



This example shows how to configure MST instance parameters:

```
Switch(config)# spanning-tree mst 1 priority ?
<0-61440> bridge priority in increments of 4096

Switch(config)# spanning-tree mst 1 priority 1
% Bridge Priority must be in increments of 4096.
% Allowed values are:
 0 4096 8192 12288 16384 20480 24576 28672
 32768 36864 40960 45056 49152 53248 57344 61440

Switch(config)# spanning-tree mst 1 priority 49152
Switch(config)#

Switch(config)# spanning-tree mst 0 root primary
mst 0 bridge priority set to 24576
mst bridge max aging time unchanged at 20
mst bridge hello time unchanged at 2
mst bridge forward delay unchanged at 15
Switch(config)# ^Z
Switch#

Switch# show spanning-tree mst

MST00 vlans mapped: 11-4094
Bridge address 00d0.00b8.1400 priority 24576 (24576 sysid 0)
Root this switch for CST and IST
Configured hello time 2, forward delay 15, max age 20, max hops 20

Interface Role Sts Cost Prio.Nbr Status

Fa4/4 Back BLK 1000 240.196 P2p
Fa4/5 Desg FWD 200000 128.197 P2p
Fa4/48 Desg FWD 200000 128.240 P2p Bound(STP)

MST01 vlans mapped: 1-10
Bridge address 00d0.00b8.1400 priority 49153 (49152 sysid 1)
Root this switch for MST01

Interface Role Sts Cost Prio.Nbr Status

Fa4/4 Back BLK 1000 160.196 P2p
Fa4/5 Desg FWD 200000 128.197 P2p
Fa4/48 Boun FWD 200000 128.240 P2p Bound(STP)

Switch#
```

## Configuring MST Instance Port Parameters

To configure MST instance port parameters, perform this task:

|        | Command                                                       | Purpose                                    |
|--------|---------------------------------------------------------------|--------------------------------------------|
| Step 1 | Switch(config-if)# <b>spanning-tree mst x cost y</b>          | Configures the MST instance port cost.     |
| Step 2 | Switch(config-if)# <b>spanning-tree mst x port-priority y</b> | Configures the MST instance port priority. |
| Step 3 | Switch(config-if)# <b>Ctrl-Z</b>                              | Exits configuration mode.                  |
| Step 4 | Switch# <b>show spanning-tree mst x interface y</b>           | Verifies the configuration.                |

This example shows how to configure MST instance port parameters:

```
Switch(config)# interface fastethernet 4/4
Switch(config-if)# spanning-tree mst 1 ?
 cost Change the interface spanning tree path cost for an instance
 port-priority Change the spanning tree port priority for an instance

Switch(config-if)# spanning-tree mst 1 cost 1234567

Switch(config-if)# spanning-tree mst 1 port-priority 240
Switch(config-if)# ^Z

Switch# show spanning-tree mst 1 interface fastethernet 4/4

FastEthernet4/4 of MST01 is backup blocking
Edge port:no (default) port guard :none (default)
Link type:point-to-point (auto) bpdu filter:disable (default)
Boundary :internal bpdu guard :disable (default)
Bpdus (MRecords) sent 125, received 1782

Instance Role Sts Cost Prio.Nbr Vlans mapped

1 Back BLK 1234567 240.196 1-10

Switch#
```

## Restarting Protocol Migration

RSTP and MST have built-in compatibility mechanisms that allow them to interact properly with other regions or other versions of IEEE spanning-tree. For example, an RSTP bridge connected to a legacy bridge can send 802.1D BPDUs on one of its ports. Similarly, when an MST bridge receives a legacy BPDU or an MST BPDU associated with a different region, it is also to detect that a port is at the boundary of a region.

Unfortunately, these mechanisms cannot always revert to the most efficient mode. For example, an RSTP bridge designated for a legacy 802.1D will stay in 802.1D mode even after the legacy bridge has been removed from the link. Similarly, an MST port still assumes that it is a boundary port when the bridge(s) to which it is connected have joined the same region. To force a Catalyst 4000 family switch to renegotiate with the neighbors (that is, to restart protocol migration), you must enter the **clear spanning-tree detected-protocols** command, as follows:

```
Switch# clear spanning-tree detected-protocols fastethernet 4/4
Switch#
```

## Displaying MST Configurations

To display MST configurations, perform this task:

|               | Command                                                                        | Purpose                                                         |
|---------------|--------------------------------------------------------------------------------|-----------------------------------------------------------------|
| <b>Step 1</b> | Switch# <b>show spanning-tree mst configuration</b>                            | Displays the active region configuration information.           |
| <b>Step 2</b> | Switch# <b>show spanning-tree mst [detail]</b>                                 | Displays detailed MST protocol information.                     |
| <b>Step 3</b> | Switch# <b>show spanning-tree mst instance-id [detail]</b>                     | Displays information about a specific MST instance.             |
| <b>Step 4</b> | Switch# <b>show spanning-tree mst interface interface [detail]</b>             | Displays information for a given port.                          |
| <b>Step 5</b> | Switch# <b>show spanning-tree mst instance-id interface interface [detail]</b> | Displays MST information for a given port and a given instance. |
| <b>Step 6</b> | Switch# <b>show spanning-tree vlan vlan_ID</b>                                 | Displays VLAN information in MST mode.                          |

The following examples show how to display spanning tree VLAN configurations in MST mode:

```
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# instance 1 vlan 1-10
Switch(config-mst)# name cisco
Switch(config-mst)# revision 1
Switch(config-mst)# Ctrl-D

Switch# show spanning-tree mst configuration
Name [cisco]
Revision 1
Instance Vlan mapped

0 11-4094
1 1-10

Switch# show spanning-tree mst

MST00 vlans mapped: 11-4094
Bridge address 00d0.00b8.1400 priority 32768 (32768 sysid 0)
Root address 00d0.004a.3c1c priority 32768 (32768 sysid 0)
 port Fa4/48 path cost 203100
IST master this switch
Operational hello time 2, forward delay 15, max age 20, max hops 20
Configured hello time 2, forward delay 15, max age 20, max hops 20

Interface Role Sts Cost Prio.Nbr Status

Fa4/4 Back BLK 1000 240.196 P2p
Fa4/5 Desg FWD 200000 128.197 P2p
Fa4/48 Root FWD 200000 128.240 P2p Bound(STP)

MST01 vlans mapped: 1-10
Bridge address 00d0.00b8.1400 priority 32769 (32768 sysid 1)
Root this switch for MST01

Interface Role Sts Cost Prio.Nbr Status

Fa4/4 Back BLK 1000 240.196 P2p
Fa4/5 Desg FWD 200000 128.197 P2p
Fa4/48 Boun FWD 200000 128.240 P2p Bound(STP)
```

```
Switch# show spanning-tree mst 1
```

```
MST01 vlans mapped: 1-10
Bridge address 00d0.00b8.1400 priority 32769 (32768 sysid 1)
Root this switch for MST01
```

| Interface | Role | Sts | Cost   | Prio.Nbr | Status         |
|-----------|------|-----|--------|----------|----------------|
| Fa4/4     | Back | BLK | 1000   | 240.196  | P2p            |
| Fa4/5     | Desg | FWD | 200000 | 128.197  | P2p            |
| Fa4/48    | Boun | FWD | 200000 | 128.240  | P2p Bound(STP) |

```
Switch# show spanning-tree mst interface fastethernet 4/4
```

```
FastEthernet4/4 of MST00 is backup blocking
Edge port:no (default) port guard :none (default)
Link type:point-to-point (auto) bpdu filter:disable (default)
Boundary :internal bpdu guard :disable (default)
Bpdus sent 2, received 368
```

| Instance | Role | Sts | Cost | Prio.Nbr | Vlans mapped |
|----------|------|-----|------|----------|--------------|
| 0        | Back | BLK | 1000 | 240.196  | 11-4094      |
| 1        | Back | BLK | 1000 | 240.196  | 1-10         |

```
Switch# show spanning-tree mst 1 interface fastethernet 4/4
```

```
FastEthernet4/4 of MST01 is backup blocking
Edge port:no (default) port guard :none (default)
Link type:point-to-point (auto) bpdu filter:disable (default)
Boundary :internal bpdu guard :disable (default)
Bpdus (MRecords) sent 2, received 364
```

| Instance | Role | Sts | Cost | Prio.Nbr | Vlans mapped |
|----------|------|-----|------|----------|--------------|
| 1        | Back | BLK | 1000 | 240.196  | 1-10         |

```
Switch# show spanning-tree mst 1 detail
```

```
MST01 vlans mapped: 1-10
Bridge address 00d0.00b8.1400 priority 32769 (32768 sysid 1)
Root this switch for MST01
```

```
FastEthernet4/4 of MST01 is backup blocking
Port info port id 240.196 priority 240 cost 1000
Designated root address 00d0.00b8.1400 priority 32769 cost 0
Designated bridge address 00d0.00b8.1400 priority 32769 port id 128.197
Timers:message expires in 5 sec, forward delay 0, forward transitions 0
Bpdus (MRecords) sent 123, received 1188
```

```
FastEthernet4/5 of MST01 is designated forwarding
Port info port id 128.197 priority 128 cost 200000
Designated root address 00d0.00b8.1400 priority 32769 cost 0
Designated bridge address 00d0.00b8.1400 priority 32769 port id 128.197
Timers:message expires in 0 sec, forward delay 0, forward transitions 1
Bpdus (MRecords) sent 1188, received 123
```

```
FastEthernet4/48 of MST01 is boundary forwarding
Port info port id 128.240 priority 128 cost 200000
Designated root address 00d0.00b8.1400 priority 32769 cost 0
Designated bridge address 00d0.00b8.1400 priority 32769 port id 128.240
Timers:message expires in 0 sec, forward delay 0, forward transitions 1
Bpdus (MRecords) sent 78, received 0
```

```
Switch# show spanning-tree vlan 10
```

```
MST01
```

```
Spanning tree enabled protocol mstp
Root ID Priority 32769
 Address 00d0.00b8.1400
 This bridge is the root
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
 Address 00d0.00b8.1400
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

| Interface | Role | Sts | Cost   | Prio.Nbr | Status |
|-----------|------|-----|--------|----------|--------|
| Fa4/4     | Back | BLK | 1000   | 240.196  | P2p    |
| Fa4/5     | Desg | FWD | 200000 | 128.197  | P2p    |

```
Switch# show spanning-tree summary
```

```
Root bridge for:MST01
EtherChannel misconfiguration guard is enabled
Extended system ID is enabled
Portfast is disabled by default
PortFast BPDU Guard is disabled by default
Portfast BPDU Filter is disabled by default
Loopguard is disabled by default
UplinkFast is disabled
BackboneFast is disabled
Pathcost method used is long
```

| Name   | Blocking | Listening | Learning | Forwarding | STP Active |
|--------|----------|-----------|----------|------------|------------|
| MST00  | 1        | 0         | 0        | 2          | 3          |
| MST01  | 1        | 0         | 0        | 2          | 3          |
| 2 msts | 2        | 0         | 0        | 4          | 6          |

```
Switch#
```





## Configuring IGMP Snooping and Filtering

This chapter describes how to configure Internet Group Management Protocol (IGMP) snooping on the Catalyst 4500 series switch. It provides guidelines, procedures, and configuration examples.

This chapter consists of the following major sections:

- Overview of IGMP Snooping, page 15-1
- Configuring IGMP Snooping, page 15-3
- Displaying IGMP Snooping Information, page 15-10
- Configuring IGMP Filtering, page 15-12
- Displaying IGMP Filtering Configuration, page 15-16



### Note

To support Cisco Group Management Protocol (CGMP) client devices, configure the switch as a CGMP server. For more information, see the chapters “IP Multicast” and “Configuring IP Multicast Routing” in the *Cisco IOS IP and IP Routing Configuration Guide*, Release 12.1 at: [http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip\\_c/ipcprt3/1cdmulti.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_c/ipcprt3/1cdmulti.htm)



### Note

For complete syntax and usage information for commands used in this chapter, refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference* and the additional publications at this URL: <http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/index.htm>

## Overview of IGMP Snooping



### Note

Quality of service does not apply to IGMP packets when IGMP snooping is enabled.

IGMP snooping allows a switch to *snoop* or capture information from IGMP packets being sent back and forth between hosts and a router. Based on this information, a switch will add/delete multicast addresses from its address table, thereby enabling/disabling multicast traffic from flowing to individual host ports.

In subnets where you have configured IGMP, IGMP snooping manages multicast traffic at Layer 2. You can configure interfaces using the **switchport** keyword to dynamically forward multicast traffic only to those interfaces that want to receive it.

IGMP snooping restricts traffic in MAC multicast groups 0100.5e00.0001 to 01-00-5e-ff-ff-ff. IGMP snooping does not restrict Layer 2 multicast packets generated by routing protocols.

**Note**

For more information on IP multicast and IGMP, refer to RFC 1112 and RFC 2236.

IGMP (on a router) periodically sends out IGMP general queries. When you enable IGMP snooping, the switch responds to the IGMP queries with only one IGMP join request per multicast group. The switch creates one entry per subnet in the Layer 2 forwarding table for each Layer 2 multicast group from which it receives an IGMP join request. All hosts interested in this multicast traffic send IGMP join requests and are added to the forwarding table entry.

Layer 2 multicast groups learned through IGMP snooping are dynamic. However, you can statically configure Layer 2 multicast groups using the **ip igmp snooping static** command. If you specify group membership for a multicast group address statically, your static setting supersedes any automatic manipulation by IGMP snooping. Multicast group membership lists can consist of both user-defined settings and IGMP snooping.

Groups with IP addresses in the 224.0.0—255 range are reserved for routing control packets and are flooded to all forwarding ports of the VLAN. These addresses map to the multicast MAC address range 0100.5E00.0001 to 0100.5E00.00FF.

**Note**

If a spanning-tree topology change occurs in a VLAN, IP multicast traffic floods on all VLAN ports where PortFast is not enabled, as well as on ports with “tcn flooding” disabled for two general query intervals.

For a host connected to a Layer 2 interface to join an IP multicast group, the host sends an IGMP join request specifying the IP multicast group. For a host to leave a multicast group, it can either ignore the periodic IGMP general queries or it can send an IGMP leave message. When the switch receives an IGMP leave message from a host, it sends out IGMP group-specific query to determine whether any devices connected to that interface are interested in traffic for the specific multicast group. The switch then updates the table entry for that Layer 2 multicast group so that only those hosts interested in receiving multicast traffic for the group are listed.

## Immediate-Leave Processing

IGMP snooping immediate-leave processing allows the switch to remove an interface from the forwarding-table entry without first sending out immediate-leave IGMP group-specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original IGMP leave message. Immediate-leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are being used simultaneously.

When a switch with IGMP snooping enabled receives an IGMPv2 leave message or an IGMPv3 Block/Exclude, it sends an IGMP group-specific query from the interface where the leave message was received to determine when there are other hosts attached to that interface that are interested in joining the MAC multicast group. If the switch does not receive an IGMP join message within the query response interval, the interface is removed from the port list of the (MAC-group, VLAN) entry in the Layer 2 forwarding table.

**Note**

By default all IGMP joins are forwarded to all multicast router ports.

With immediate-leave processing enabled on the VLAN, an interface can be removed immediately from the port list of the Layer 2 entry when the IGMP leave message is received, unless a multicast router was learned on the port.



**Note**

Use immediate-leave processing only on VLANs where only one host is connected to each interface. If immediate-leave is enabled in VLANs where more than one host is connected to an interface, some hosts might be dropped inadvertently. Immediate-leave processing is supported only with IGMP version 2 hosts.

## IGMPv3 Snooping

IGMPv3 extends IGMPv1 and IGMPv2 functionality to include new membership report messages.

IGMPv3 snooping provides Basic IGMPv3 Snooping Support (BISS) on Catalyst 4500 switches. BISS provides constrained flooding of multicast traffic in the presence of IGMPv3 hosts. This support constrains traffic to approximately the same set of ports as regular IGMPv2 snooping does with IGMPv2 hosts. The constrained flooding only considers the destination multicast address.

**Note**

IGMPv3 is interoperable with older versions of IGMP.

Use the **show ip igmp snooping querier vlan** command to display the IGMP version on a particular VLAN.

## Configuring IGMP Snooping

**Note**

When configuring IGMP, configure the VLAN in the VLAN database mode. (See Chapter 8, “Understanding and Configuring VLANs”.)

IGMP snooping allows switches to examine IGMP packets and make forwarding decisions based on their content.

These sections describe how to configure IGMP snooping:

- Default IGMP Snooping Configuration, page 15-3
- Enabling IGMP Snooping, page 15-4
- Configuring Learning Methods, page 15-5
- Configuring a Multicast Router Port Statically, page 15-6
- Enabling IGMP Immediate-Leave Processing, page 15-6
- Configuring a Host Statically, page 15-7
- Suppressing Multicast Flooding, page 15-7

## Default IGMP Snooping Configuration

Table 15-1 shows the IGMP snooping default configuration values.

**Table 15-1 IGMP Snooping Default Configuration Values**

| Feature                       | Default Value          |
|-------------------------------|------------------------|
| IGMP snooping                 | Enabled                |
| Multicast routers             | None configured        |
| IGMP snooping learning method | PIM/DVMRP <sup>1</sup> |

1. PIM/DVMRP = Protocol Independent Multicast/Distance Vector Multicast Routing Protocol

## Enabling IGMP Snooping

To enable IGMP snooping globally, perform this task:

|               | Command                                 | Purpose                                                                       |
|---------------|-----------------------------------------|-------------------------------------------------------------------------------|
| <b>Step 1</b> | Switch(config)# [no] ip igmp snooping   | Enables IGMP snooping.<br>Use the <b>no</b> keyword to disable IGMP snooping. |
| <b>Step 2</b> | Switch(config)# end                     | Exits configuration mode.                                                     |
| <b>Step 3</b> | Switch# show ip igmp snooping   include | Verifies the configuration.                                                   |

This example shows how to enable IGMP snooping globally and verify the configuration:

```
Switch(config)# ip igmp snooping
Switch(config)# end
Switch# show ip igmp snooping
Global IGMP Snooping configuration:

IGMP snooping : Enabled
IGMPv3 snooping support : Basic
Report suppression : Enabled
TCN solicit query : Disabled
TCN flood query count : 2

Vlan 1:

IGMP snooping : Enabled
Immediate leave : Disabled
Multicast router learning mode : pim-dvmrp
CGMP interoperability mode : IGMP_ONLY

Vlan 5:

IGMP snooping : Enabled
Immediate leave : Disabled
Multicast router learning mode : pim-dvmrp
CGMP interoperability mode : IGMP_ONLY
```

To enable IGMP snooping in a VLAN, perform this task:

|        | Command                                                   | Purpose                                                                       |
|--------|-----------------------------------------------------------|-------------------------------------------------------------------------------|
| Step 1 | Switch(config)# [no] ip igmp snooping vlan <i>vlan_ID</i> | Enables IGMP snooping.<br>Use the <b>no</b> keyword to disable IGMP snooping. |
| Step 2 | Switch(config)# end                                       | Exits configuration mode.                                                     |
| Step 3 | Switch# show ip igmp snooping vlan <i>vlan_ID</i>         | Verifies the configuration.                                                   |

This example shows how to enable IGMP snooping on VLAN 200 and verify the configuration:

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 200
Switch(config)# end
Switch# show ip igmp snooping vlan 200
Global IGMP Snooping configuration:

IGMP snooping :Enabled
IGMPv3 snooping support :Basic
Report suppression :Enabled
TCN solicit query :Disabled
TCN flood query count :2

Vlan 200:

IGMP snooping :Enabled
Immediate leave :Disabled
Multicast router learning mode :pim-dvmrp
CGMP interoperability mode :IGMP_ONLY
```

## Configuring Learning Methods

The following sections describe IGMP snooping learning methods:

- Configuring PIM/DVMRP Learning, page 15-5
- Configuring CGMP Learning, page 15-6

## Configuring PIM/DVMRP Learning

To configure IGMP snooping to learn from PIM/DVMRP packets, perform this task:

| Command                                                                                               | Purpose                                     |
|-------------------------------------------------------------------------------------------------------|---------------------------------------------|
| Switch(config)# ip igmp snooping vlan <i>vlan_ID</i> mrouter learn [ <i>cgmp</i>   <i>pim-dvmrp</i> ] | Specifies the learning method for the VLAN. |

This example shows how to configure IP IGMP snooping to learn from PIM/DVMRP packets:

```
Switch(config)# ip igmp snooping vlan 1 mrouter learn pim-dvmrp
Switch(config)# end
Switch#
```

### Configuring CGMP Learning

To configure IGMP snooping to learn from CGMP self-join packets, perform this task:

| Command                                                                               | Purpose                                     |
|---------------------------------------------------------------------------------------|---------------------------------------------|
| Switch(config)# ip igmp snooping vlan <i>vlan_ID</i> mrouter learn [cgmp   pim-dvmrp] | Specifies the learning method for the VLAN. |

This example shows how to configure IP IGMP snooping to use CGMP self-join packets as the learning method:

```
Switch(config)# ip igmp snooping vlan 1 mrouter learn cgmp
Switch(config)# end
Switch#
```

### Configuring a Multicast Router Port Statically

To configure a static connection to a multicast router, enter the **ip igmp snooping mrouter** command on the switch.

To configure a static connection to a multicast router, perform this task:

|        | Command                                                                                     | Purpose                                                                                                                                                                                                                                            |
|--------|---------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch(config)# ip igmp snooping vlan <i>vlan_ID</i> mrouter interface <i>interface_num</i> | Specifies a static connection to a multicast router for the VLAN.<br><br><b>Note</b> The interface to the router must be in the VLAN where you are entering the command. The router must be administratively up, and the line protocol must be up. |
| Step 2 | Switch(config)# end                                                                         | Exits configuration mode.                                                                                                                                                                                                                          |
| Step 3 | Switch# show ip igmp snooping mrouter vlan <i>vlan_ID</i>                                   | Verifies the configuration.                                                                                                                                                                                                                        |

This example shows how to configure a static connection to a multicast router:

```
Switch(config)# ip igmp snooping vlan 200 mrouter interface fastethernet 2/10
Switch# show ip igmp snooping mrouter vlan 200
vlan ports
-----+-----
 200 Fa2/10
Switch#
```

### Enabling IGMP Immediate-Leave Processing

When you enable IGMP immediate-leave processing in a VLAN, the switch will remove an interface from the multicast group as soon as it detects an IGMP version 2 leave message on that interface.

To enable IGMP immediate-leave processing on an interface, perform this task:

| Command                                                                     | Purpose                                              |
|-----------------------------------------------------------------------------|------------------------------------------------------|
| Switch(config)# <b>ip igmp snooping vlan <i>vlan_ID</i> immediate-leave</b> | Enables IGMP immediate-leave processing in the VLAN. |

This example shows how to enable IGMP immediate-leave processing on interface VLAN 200 and verify the configuration:

```
Switch(config)# ip igmp snooping vlan 200 immediate-leave
Configuring immediate leave on vlan 200
Switch(config)# end
Switch# show ip igmp interface vlan 200 | include immediate-leave
IGMP snooping immediate-leave is enabled on this vlan
Switch(config)#
```

## Configuring a Host Statically

Hosts normally join multicast groups dynamically, but you can also configure a host statically on an interface.

To configure a host statically on an interface, perform this task:

| Command                                                                                                                 | Purpose                                   |
|-------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|
| Switch(config-if)# <b>ip igmp snooping vlan <i>vlan_ID</i> static <i>mac_address</i> interface <i>interface_num</i></b> | Configures a host statically in the VLAN. |

This example shows how to configure a host statically in VLAN 200 on interface FastEthernet 2/11:

```
Switch(config)# ip igmp snooping vlan 200 static 0100.5e02.0203 interface fastethernet 2/11
Configuring port FastEthernet2/11 on group 0100.5e02.0203 vlan 200
Switch(config)#
```

## Suppressing Multicast Flooding

An IGMP snooping-enabled switch will flood multicast traffic to all ports in a VLAN when a spanning-tree Topology Change Notification (TCN) is received. Multicast flooding suppression enables a switch to stop sending such traffic. To support flooding suppression, a new interface command and two new global commands are introduced in release 12.1(11b)EW.

The new interface command is as follows:

**[no | default] ip igmp snooping tcn flood**

These are the new global commands:

**[no | default] ip igmp snooping tcn flood query count [1 - 10]**

**[no | default] ip igmp snooping tcn query solicit**

Prior to release 12.1(11b)EW, when a spanning tree topology change notification (TCN) was received by a switch, the multicast traffic was flooded to all the ports in a VLAN for a period of three IGMP query intervals. This was necessary for redundant configurations. In release 12.1(11b)EW, the default time period the switch will wait before multicast flooding will stop was changed to two IGMP query intervals.

This flooding behavior is undesirable if the switch that does the flooding has many ports that are subscribed to different groups. The traffic could exceed the capacity of the link between the switch and the end host, resulting in packet loss.

With the **no ip igmp snooping tcn flood** command, you can disable multicast flooding on a switch interface following a topology change. Only the multicast groups that have been joined by a port are sent to that port, even during a topology change.

With the **ip igmp snooping tcn flood query count** command, you can enable multicast flooding on a switch interface for a short period of time following a topology change by configuring an IGMP query threshold.

Typically, if a topology change occurs, the spanning tree root switch issues a global IGMP leave message (referred to as a “query solicitation”) with the group multicast address 0.0.0.0. When a switch receives this solicitation, it floods this solicitation on all ports in the VLAN where the spanning tree change occurred. When the upstream router receives this solicitation, it immediately issues an IGMP general query.

With the **ip igmp snooping tcn query solicit** command, you can now direct a non-spanning tree root switch to issue the same query solicitation.

The following sections provide additional details on the new commands and illustrate how you can use them.

## IGMP Snooping Interface Configuration

A topology change in a VLAN may invalidate previously learned IGMP snooping information. A host that was on one port before the topology change may move to another port after the topology change. When the topology changes, the Catalyst 4500 series switch takes special actions to ensure that multicast traffic is delivered to all multicast receivers in that VLAN.

When the spanning tree protocol is running in a VLAN, a spanning tree topology change notification (TCN) is issued by the root switch in the VLAN. A Catalyst 4500 series switch that receives a TCN in a VLAN for which IGMP snooping has been enabled immediately enters into “multicast flooding mode” for a period of time until the topology restabilizes and the new locations of all multicast receivers are learned.

While in “multicast flooding mode,” IP multicast traffic is delivered to all ports in the VLAN, and not restricted to those ports on which multicast group members have been detected.

Starting with 12.1(11b)EW, you can manually prevent IP multicast traffic from being flooded to a switchport by using the **no ip igmp snooping tcn flood** command on that port.

For trunk ports, the configuration will apply to all VLANs.

By default, multicast flooding is enabled. Use the **no** keyword to disable flooding, and use **default** to restore the default behavior (flooding is enabled).

To disable multicast flooding on an interface, perform this task:

|        | Command                                                                                                 | Purpose                                                                                                                                                                                                   |
|--------|---------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch(config)# <b>interface</b> { <b>fastethernet</b>   <b>gigabitethernet</b> } <i>slot/port</i>      | Selects the interface to configure.                                                                                                                                                                       |
| Step 2 | Switch(config-if)# <b>no ip igmp snooping tcn flood</b>                                                 | Disables multicast flooding on the interface when TCNs are received by the switch.<br><br>To enable multicast flooding on the interface, enter this command:<br><b>default ip igmp snooping tcn flood</b> |
| Step 3 | Switch(config)# <b>end</b>                                                                              | Exits configuration mode.                                                                                                                                                                                 |
| Step 4 | Switch# <b>show running interface</b> { <b>fastethernet</b>   <b>gigabitethernet</b> } <i>slot/port</i> | Verifies the configuration.                                                                                                                                                                               |

This example shows how to disable multicast flooding on interface FastEthernet 2/11:

```
Switch(config)# interface fastethernet 2/11
Switch(config-if)# no ip igmp snooping tcn flood
Switch(config-if)# end
Switch#
```

## IGMP Snooping Switch Configuration

By default, “flooding mode” persists until the switch receives two IGMP general queries. You can change this period of time by using the

**ip igmp snooping tcn flood query count** <*n*> command, where *n* is a number between 1 and 10.

This command operates at the global configuration level.

The default number of queries is 2. The **no** and **default** keywords restore the default.

To establish an IGMP query threshold, perform this task:

|        | Command                                                                       | Purpose                                                                                                                                                                                                                                                    |
|--------|-------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch(config)#<br><b>ip igmp snooping tcn flood query count</b> < <i>n</i> > | Modifies the number of IGMP queries the switch will wait for before it stops flooding multicast traffic.<br><br>To return the switch to the default number of IGMP queries, enter this command:<br><b>default ip igmp snooping tcn flood query count .</b> |
| Step 2 | Switch(config)# <b>end</b>                                                    | Exits configuration mode.                                                                                                                                                                                                                                  |

This example shows how to modify the switch to stop flooding multicast traffic after four queries:

```
Switch(config)# ip igmp snooping tcn flood query count 4
Switch(config)# end
Switch#
```

When a spanning tree root switch receives a topology change in an IGMP snooping-enabled VLAN, the switch issues a query solicitation that causes an IOS router to send out one or more general queries. The new command **ip igmp snooping tcn query solicit** causes the switch to send the query solicitation whenever it notices a topology change, even if that switch is not the spanning tree root.

This command operates at the global configuration level.

By default, query solicitation is disabled unless the switch is the spanning tree root. The **default** keyword restores the default behavior.

To direct a switch to send a query solicitation, perform this task:

|        | Command                                                      | Purpose                                                                                                                                                             |
|--------|--------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch(config)#<br><b>ip igmp snooping tcn query solicit</b> | Configures the switch to send a query solicitation when a TCN is detected.                                                                                          |
|        |                                                              | To stop the switch from sending a query solicitation (if it's not a spanning tree root switch), enter this command:<br><b>no ip igmp snooping tcn query solicit</b> |
| Step 2 | Switch(config)# <b>end</b>                                   | Exits configuration mode.                                                                                                                                           |

This example shows how to configure the switch to send a query solicitation upon detecting a TCN:

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

## Displaying IGMP Snooping Information

The following sections tell you how to display IGMP snooping information:

- Displaying Multicast Router Interfaces, page 15-10
- Displaying MAC Address Multicast Entries, page 15-11
- Displaying IGMP Snooping Information for a VLAN Interface, page 15-11

## Displaying Multicast Router Interfaces

When you enable IGMP snooping, the switch automatically learns to which interface the multicast routers are connected.

To display multicast router interfaces, perform this task:

| Command                                                             | Purpose                               |
|---------------------------------------------------------------------|---------------------------------------|
| Switch# <b>show ip igmp snooping mrouter vlan</b><br><i>vlan_ID</i> | Displays multicast router interfaces. |

This example shows how to display the multicast router interfaces in VLAN 1:

```
Switch# show ip igmp snooping mrouter vlan 1
vlan ports
-----+-----
1 Gi1/1,Gi2/1,Fa3/48,Router
Switch#
```



## Displaying MAC Address Multicast Entries

To display MAC address multicast entries for a VLAN, perform this task:

| Command                                                                                        | Purpose                                            |
|------------------------------------------------------------------------------------------------|----------------------------------------------------|
| Switch# <b>show mac-address-table multicast</b><br><b>vlan</b> <i>vlan_ID</i> [ <i>count</i> ] | Displays MAC address multicast entries for a VLAN. |

This example shows how to display MAC address multicast entries for VLAN 1:

```
Switch# show mac-address-table multicast vlan 1
```

Multicast Entries

| vlan | mac address    | type | ports        |
|------|----------------|------|--------------|
| 1    | 0100.5e01.0101 | igmp | Switch,Gi6/1 |
| 1    | 0100.5e01.0102 | igmp | Switch,Gi6/1 |
| 1    | 0100.5e01.0103 | igmp | Switch,Gi6/1 |
| 1    | 0100.5e01.0104 | igmp | Switch,Gi6/1 |
| 1    | 0100.5e01.0105 | igmp | Switch,Gi6/1 |
| 1    | 0100.5e01.0106 | igmp | Switch,Gi6/1 |

Switch#

This example shows how to display a total count of MAC address entries for a VLAN:

```
Switch# show mac-address-table multicast vlan 1 count
```

Multicast MAC Entries for vlan 1: 4

Switch#

## Displaying IGMP Snooping Information for a VLAN Interface

To display IGMP snooping information for a VLAN interface, perform this task:

| Command                                                         | Purpose                                                 |
|-----------------------------------------------------------------|---------------------------------------------------------|
| Switch# <b>show ip igmp snooping</b> <b>vlan</b> <i>vlan_ID</i> | Displays IGMP snooping information on a VLAN interface. |

This example shows how to display IGMP snooping information on interface VLAN 200:

```
Switch#show ip igmp snooping vlan 5
```

Global IGMP Snooping configuration:

```

IGMP snooping : Enabled
IGMPv3 snooping support : Basic
Report suppression : Enabled
TCN solicit query : Disabled
TCN flood query count : 2
```

Vlan 5:

```

IGMP snooping : Enabled
Immediate leave : Disabled
Multicast router learning mode : pim-dvmrp
CGMP interoperability mode : IGMP_ONLY
```

## Configuring IGMP Filtering

In some environments, for example metropolitan or multiple-dwelling unit (MDU) installations, an administrator might want to control the multicast groups to which a user on a switch port can belong. This allows the administrator to control the distribution of multicast services, such as IP/TV, based on some type of subscription or service plan.

With the IGMP filtering feature, an administrator can exert this type of control. With this feature, you can filter multicast joins on a per-port basis by configuring IP multicast profiles and associating them with individual switch ports. An IGMP profile can contain one or more multicast groups and specifies whether access to the group is permitted or denied. If an IGMP profile denying access to a multicast group is applied to a switch port, the IGMP join report requesting the stream of IP multicast traffic is dropped, and the port is not allowed to receive IP multicast traffic from that group. If the filtering action permits access to the multicast group, the IGMP report from the port is forwarded for normal processing.

IGMP filtering controls only IGMP membership join reports and has no relationship to the function that directs the forwarding of IP multicast traffic.

You can also set the maximum number of IGMP groups that a Layer 2 interface can join with the **ip igmp max-groups <n>** command.

## Default IGMP Filtering Configuration

Table 15-2 shows the default IGMP filtering configuration.

**Table 15-2** Default IGMP Filtering Settings

| Feature                            | Default Setting |
|------------------------------------|-----------------|
| IGMP filters                       | No filtering    |
| IGMP maximum number of IGMP groups | No limit        |
| IGMP profiles                      | None defined    |

## Configuring IGMP Profiles

To configure an IGMP profile and to enter IGMP profile configuration mode, use the **ip igmp profile** global configuration command. From the IGMP profile configuration mode, you can specify the parameters of the IGMP profile to be used for filtering IGMP join requests from a port. When you are in IGMP profile configuration mode, you can create the profile using these commands:

- **deny**: Specifies that matching addresses are denied; this is the default condition.
- **exit**: Exits from igmp-profile configuration mode.
- **no**: Negates a command or sets its defaults.
- **permit**: Specifies that matching addresses are permitted.
- **range**: Specifies a range of IP addresses for the profile. You can enter a single IP address or a range with starting and ending addresses.

By default, no IGMP profiles are configured. When a profile is configured with neither the **permit** nor the **deny** keyword, the default is to deny access to the range of IP addresses.

To create an IGMP profile for a port, perform this task:

|        | Command                                                               | Purpose                                                                                                                                                                                                                                                                                                                     |
|--------|-----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch# <b>configure terminal</b>                                     | Enters global configuration mode.                                                                                                                                                                                                                                                                                           |
| Step 2 | Switch(config)# <b>ip igmp profile</b> <i>profile number</i>          | Enters IGMP profile configuration mode, and assigns a number to the profile you are configuring. The range is from 1 to 4,294,967,295.                                                                                                                                                                                      |
| Step 3 | Switch(config-igmp-profile)# <b>permit   deny</b>                     | (Optional) Sets the action to permit or deny access to the IP multicast address. If no action is configured, the default for the profile is to deny access.                                                                                                                                                                 |
| Step 4 | Switch(config-igmp-profile)# <b>range</b> <i>ip multicast address</i> | Enters the IP multicast address or range of IP multicast addresses to which access is being controlled. If entering a range, enter the low IP multicast address, a space, and the high IP multicast address.<br><br>You can use the <b>range</b> command multiple times to enter multiple addresses or ranges of addresses. |
| Step 5 | Switch(config-igmp-profile)# <b>end</b>                               | Returns to privileged EXEC mode.                                                                                                                                                                                                                                                                                            |
| Step 6 | Switch# <b>show ip igmp profile</b> <i>profile number</i>             | Verifies the profile configuration.                                                                                                                                                                                                                                                                                         |
| Step 7 | Switch# <b>copy running-config startup-config</b>                     | (Optional) Saves your entries in the configuration file.                                                                                                                                                                                                                                                                    |

To delete a profile, use the **no ip igmp profile** *profile number* global configuration command.

To delete an IP multicast address or range of IP multicast addresses, use the **no range** *ip multicast address* IGMP profile configuration command.

This example shows how to create IGMP profile 4 (allowing access to the single IP multicast address) and how to verify the configuration. If the action were to deny (the default), it would not appear in the **show ip igmp profile** command output.

```
Switch# config t
Switch(config)# ip igmp profile 4
Switch(config-igmp-profile)# permit
Switch(config-igmp-profile)# range 229.9.9.0
Switch(config-igmp-profile)# end
Switch# show ip igmp profile 4
IGMP Profile 4
 permit
 range 229.9.9.0 229.9.9.0
```

## Applying IGMP Profiles

To control access as defined in an IGMP profile, use the **ip igmp filter** interface configuration command to apply the profile to the appropriate interfaces. You can apply a profile to multiple interfaces, but each interface can only have one profile applied to it.



### Note

You can apply IGMP profiles to Layer 2 ports only. You cannot apply IGMP profiles to routed ports (or SVIs) or to ports that belong to an EtherChannel port group.

To apply an IGMP profile to a switch port, perform this task:

|        | Command                                                                 | Purpose                                                                                                                                                                                                           |
|--------|-------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch# <b>configure terminal</b>                                       | Enters global configuration mode.                                                                                                                                                                                 |
| Step 2 | Switch(config)# <b>interface</b> <i>interface-id</i>                    | Enters interface configuration mode, and enter the physical interface to configure, for example <b>fastethernet2/3</b> . The interface must be a Layer 2 port that does not belong to an EtherChannel port group. |
| Step 3 | Switch(config-if)# <b>ip igmp filter</b> <i>profile number</i>          | Applies the specified IGMP profile to the interface. The profile number can be from 1 to 4,294,967,295.                                                                                                           |
| Step 4 | Switch(config-if)# <b>end</b>                                           | Returns to privileged EXEC mode.                                                                                                                                                                                  |
| Step 5 | Switch# <b>show running configuration interface</b> <i>interface-id</i> | Verifies the configuration.                                                                                                                                                                                       |
| Step 6 | Switch# <b>copy running-config startup-config</b>                       | (Optional) Saves your entries in the configuration file.                                                                                                                                                          |

To remove a profile from an interface, use the **no ip igmp filter** command.

This example shows how to apply IGMP profile 4 to an interface and verify the configuration.

```
Switch# config t
Switch(config)# interface fastethernet2/12
Switch(config-if)# ip igmp filter 4
Switch(config-if)# end
Switch# show running-config interface fastethernet2/12
Building configuration...

Current configuration : 123 bytes
!
interface FastEthernet2/12
 no ip address
 shutdown
 snmp trap link-status
 ip igmp max-groups 25
 ip igmp filter 4
end
```

## Setting the Maximum Number of IGMP Groups

You can set the maximum number of IGMP groups that a Layer 2 interface can join by using the **ip igmp max-groups** interface configuration command. Use the **no** form of this command to set the maximum back to the default, which is no limit.



### Note

This restriction can be applied to Layer 2 ports only. You cannot set a maximum number of IGMP groups on routed ports (or SVIs) or on ports that belong to an EtherChannel port group.

To apply an IGMP profile on a switch port, perform this task:

|        | Command                                                                        | Purpose                                                                                                                                                                                                         |
|--------|--------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch# <b>configure terminal</b>                                              | Enters global configuration mode.                                                                                                                                                                               |
| Step 2 | Switch(config)# <b>interface</b> <i>interface-id</i>                           | Enters interface configuration mode, and enter the physical interface to configure, for example <b>gigabitethernet1/1</b> . The interface must be a Layer 2 port that does not belong to an EtherChannel group. |
| Step 3 | Switch(config-if)# <b>ip igmp max-groups</b> <i>number</i>                     | Sets the maximum number of IGMP groups that the interface can join. The range is from 0 to 4,294,967,294. By default, no maximum is set.                                                                        |
| Step 4 | Switch(config-if)# <b>end</b>                                                  | Returns to privileged EXEC mode.                                                                                                                                                                                |
| Step 5 | Switch# <b>show running-configuration</b> <b>interface</b> <i>interface-id</i> | Verifies the configuration.                                                                                                                                                                                     |
| Step 6 | Switch# <b>copy running-config startup-config</b>                              | (Optional) Saves your entries in the configuration file.                                                                                                                                                        |

To remove the maximum group limitation and return to the default of no maximum, use the **no ip igmp max-groups** command.

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

```
Switch# config t
Switch(config)# interface fastethernet2/12
Switch(config-if)# ip igmp max-groups 25
Switch(config-if)# end
Switch# show running-config interface fastethernet2/12
Building configuration...

Current configuration : 123 bytes
!
interface FastEthernet2/12
 no ip address
 shutdown
 snmp trap link-status
 ip igmp max-groups 25
 ip igmp filter 4
end
```

## Displaying IGMP Filtering Configuration

You can display IGMP profile and maximum group configuration for all interfaces on the switch or for a specified interface.

To display IGMP filtering configuration, use one of the following commands:

**Table 15-3** Commands to Display IGMP Filtering Configuration

| Command                                                                     | Purpose                                                                                                                                                                                                                            |
|-----------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Switch# <b>show ip igmp profile</b> [ <i>profile number</i> ]               | Displays the specified IGMP profile or all IGMP profiles defined on the switch.                                                                                                                                                    |
| Switch# <b>show running-configuration</b> [ <i>interface interface-id</i> ] | Displays the configuration of the specified interface or all interfaces on the switch, including (if configured) the maximum number of IGMP groups to which an interface can belong and the IGMP profile applied to the interface. |

This is an example of the **show ip igmp profile** privileged EXEC command when no profile number is entered. All profiles defined on the switch are displayed.

```
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
```

This is an example of the **show running-config** privileged EXEC command when an interface is specified with IGMP maximum groups configured and IGMP profile 4 has been applied to the interface.

```
Switch# show running-config interface fastethernet2/12
Building configuration...
Current configuration : 123 bytes
!
interface FastEthernet2/12
 no ip address
 shutdown
 snmp trap link-status
 ip igmp max-groups 25
 ip igmp filter 4
end
```



## Understanding and Configuring CDP

This chapter describes how to configure Cisco Discovery Protocol (CDP) on the Catalyst 4500 series switch. It also provides guidelines, procedures, and configuration examples.

This chapter includes the following major sections:

- Overview of CDP, page 16-1
- Configuring CDP, page 16-1



### Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.1; *Cisco IOS System Management; Configuring Cisco Discovery Protocol (CDP)* at: [http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/fun\\_c/fcprt3/fcd301c.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/fun_c/fcprt3/fcd301c.htm) and to the *Cisco IOS Configuration Fundamentals Command Reference*, Release 12.1; *Cisco IOS System Management Commands*; and *CDP Commands* publication at the following URL: [http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/fun\\_r/frprt3/frd3001b.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/fun_r/frprt3/frd3001b.htm)

## Overview of CDP

CDP is a protocol that runs over Layer 2 (the data link layer) on all Cisco routers, bridges, access servers, and switches. CDP allows network management applications to discover Cisco devices that are neighbors of already known devices, in particular, neighbors running lower-layer, transparent protocols. With CDP, network management applications can learn the device type and the SNMP agent address of neighboring devices. CDP enables applications to send SNMP queries to neighboring devices.

CDP runs on all LAN and WAN media that support Subnetwork Access Protocol (SNAP).

Each CDP-configured device sends periodic messages to a multicast address. Each device advertises at least one address at which it can receive SNMP messages. The advertisements also contain the time-to-live, or holdtime information, which indicates the length of time a receiving device should hold CDP information before discarding it.

## Configuring CDP

The following sections describe how to configure CDP:

- Enabling CDP Globally, page 16-2
- Displaying the CDP Global Configuration, page 16-2

- Enabling CDP on an Interface, page 16-2
- Displaying the CDP Interface Configuration, page 16-3
- Monitoring and Maintaining CDP, page 16-3

## Enabling CDP Globally

To enable CDP globally, perform this task:

| Command                             | Purpose                                                                     |
|-------------------------------------|-----------------------------------------------------------------------------|
| Switch(config)# <b>[no] cdp run</b> | Enables CDP globally.<br>Use the <b>no</b> keyword to disable CDP globally. |

This example shows how to enable CDP globally:

```
Switch(config)# cdp run
```

## Displaying the CDP Global Configuration

To display the CDP configuration, perform this task:

| Command                 | Purpose                          |
|-------------------------|----------------------------------|
| Switch# <b>show cdp</b> | Displays global CDP information. |

This example shows how to display the CDP configuration:

```
Switch# show cdp
Global CDP information:
 Sending CDP packets every 120 seconds
 Sending a holdtime value of 180 seconds
 Sending CDPv2 advertisements is enabled
Switch#
```

For additional CDP **show** commands, see the “Monitoring and Maintaining CDP” section on page 16-3.

## Enabling CDP on an Interface

To enable CDP on an interface, perform this task:

| Command                                   | Purpose                                                                                   |
|-------------------------------------------|-------------------------------------------------------------------------------------------|
| Switch(config-if)# <b>[no] cdp enable</b> | Enables CDP on an interface.<br>Use the <b>no</b> keyword to disable CDP on an interface. |



This example shows how to enable CDP on Fast Ethernet interface 5/1:

```
Switch(config)# interface fastethernet 5/1
Switch(config-if)# cdp enable
```

This example shows how to disable CDP on Fast Ethernet interface 5/1:

```
Switch(config)# interface fastethernet 5/1
Switch(config-if)# no cdp enable
```

## Displaying the CDP Interface Configuration

To display the CDP configuration for an interface, perform this task:

| Command                                                | Purpose                                                     |
|--------------------------------------------------------|-------------------------------------------------------------|
| Switch# <b>show cdp interface</b> <i>[type/number]</i> | Displays information about interfaces where CDP is enabled. |

This example shows how to display the CDP configuration of Fast Ethernet interface 5/1:

```
Switch# show cdp interface fastethernet 5/1
FastEthernet5/1 is up, line protocol is up
 Encapsulation ARPA
 Sending CDP packets every 120 seconds
 Holdtime is 180 seconds
Switch#
```

## Monitoring and Maintaining CDP

To monitor and maintain CDP on your device, perform one or more of these tasks:

| Command                                                                        | Purpose                                                                                                                                                              |
|--------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Switch# <b>clear cdp counters</b>                                              | Resets the traffic counters to zero.                                                                                                                                 |
| Switch# <b>clear cdp table</b>                                                 | Deletes the CDP table of information about neighbors.                                                                                                                |
| Switch# <b>show cdp</b>                                                        | Displays global information such as frequency of transmissions and the holdtime for packets being transmitted.                                                       |
| Switch# <b>show cdp entry</b> <i>entry_name</i><br><i>[protocol   version]</i> | Displays information about a specific neighbor. The display can be limited to protocol or version information.                                                       |
| Switch# <b>show cdp interface</b><br><i>[type/number]</i>                      | Displays information about interfaces on which CDP is enabled.                                                                                                       |
| Switch# <b>show cdp neighbors</b><br><i>[type/number] [detail]</i>             | Displays information about neighboring equipment. The display can be limited to neighbors on a specific interface and expanded to provide more detailed information. |

| Command                         | Purpose                                                                                       |
|---------------------------------|-----------------------------------------------------------------------------------------------|
| Switch# <b>show cdp traffic</b> | Displays CDP counters, including the number of packets sent and received and checksum errors. |
| Switch# <b>show debugging</b>   | Displays information about the types of debugging that are enabled for your switch.           |

This example shows how to clear the CDP counter configuration on your switch:

```
Switch# clear cdp counters
```

This example shows how to display information about the neighboring equipment:

```
Switch# show cdp neighbors
```

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge  
S - Switch, H - Host, I - IGMP, r - Repeater

| Device ID   | Local Intrfce | Holdtme | Capability | Platform | Port ID |
|-------------|---------------|---------|------------|----------|---------|
| JAB023807H1 | Fas 5/3       | 127     | T S        | WS-C2948 | 2/46    |
| JAB023807H1 | Fas 5/2       | 127     | T S        | WS-C2948 | 2/45    |
| JAB023807H1 | Fas 5/1       | 127     | T S        | WS-C2948 | 2/44    |
| JAB023807H1 | Gig 1/2       | 122     | T S        | WS-C2948 | 2/50    |
| JAB023807H1 | Gig 1/1       | 122     | T S        | WS-C2948 | 2/49    |
| JAB03130104 | Fas 5/8       | 167     | T S        | WS-C4003 | 2/47    |
| JAB03130104 | Fas 5/9       | 152     | T S        | WS-C4003 | 2/48    |



# Understanding and Configuring EtherChannel

This chapter describes how to use the command-line interface (CLI) to configure EtherChannel on the Catalyst 4500 series switch Layer 2 or Layer 3 interfaces. It also provides guidelines, procedures, and configuration examples.

This chapter includes the following major sections:

- Overview of EtherChannel, page 17-1
- EtherChannel Configuration Guidelines and Restrictions, page 17-5
- Configuring EtherChannel, page 17-6



## Note

The commands in the following sections can be used on all Ethernet interfaces on a Catalyst 4500 series switch, including the uplink ports on the supervisor engine.



## Note

For complete syntax and usage information for the switch commands used in this chapter, refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference* and the publications at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/index.htm>

## Overview of EtherChannel

EtherChannel bundles individual Ethernet links into a single logical link that provides bandwidth up to 1600 Mbps (Fast EtherChannel full duplex) or 16 Gbps (Gigabit EtherChannel) between a Catalyst 4500 series switch and another switch or host.

A Catalyst 4500 series switch supports a maximum of 64 EtherChannels. You can form an EtherChannel with up to eight compatibly configured Ethernet interfaces across modules in a Catalyst 4500 series switch. All interfaces in each EtherChannel must be the same speed and must be configured as either Layer 2 or Layer 3 interfaces.



## Note

The network device to which a Catalyst 4500 series switch is connected may impose its own limits on the number of interfaces in an EtherChannel.

If a segment within an EtherChannel fails, traffic previously carried over the failed link switches to the remaining segments within the EtherChannel. Once the segment fails, an SNMP trap is sent, identifying the switch, the EtherChannel, and the failed link. Inbound broadcast and multicast packets on one segment in an EtherChannel are blocked from returning on any other segment of the EtherChannel.

These subsections describe how EtherChannel works:

- Understanding Port-Channel Interfaces, page 17-2
- Understanding How EtherChannels Are Configured, page 17-2
- Understanding Load Balancing, page 17-5

## Understanding Port-Channel Interfaces

Each EtherChannel has a numbered port-channel interface. A configuration applied to the port-channel interface affects all physical interfaces assigned to that interface.

**Note**

QoS does not propagate to members. The defaults, QoS cos = 0 and QoS dscp = 0, apply on the port-channel. Input or output policies applied on individual interfaces will be ignored.

After you configure an EtherChannel, the configuration that you apply to the port-channel interface affects the EtherChannel; the configuration that you apply to the physical interfaces affects only the interface where you apply the configuration. To change the parameters of all ports in an EtherChannel, apply configuration commands to the port-channel interface (such commands can be STP commands or commands to configure a Layer 2 EtherChannel as a trunk).

## Understanding How EtherChannels Are Configured

These subsections describe how EtherChannels are configured:

- EtherChannel Configuration Overview, page 17-2
- Understanding Manual EtherChannel Configuration, page 17-3
- Understanding PAgP EtherChannel Configuration, page 17-3
- Understanding IEEE 802.3ad LACP EtherChannel Configuration, page 17-3

### EtherChannel Configuration Overview

You can configure EtherChannels manually or you can use the Port Aggregation Control Protocol (PAgP) or, with Release Cisco IOS Release 12.1(11)EW and later, the Link Aggregation Control Protocol (LACP) to form EtherChannels. The EtherChannel protocols allow ports with similar characteristics to form an EtherChannel through dynamic negotiation with connected network devices. PAgP is a Cisco-proprietary protocol and LACP is defined in IEEE 802.3ad.

PAgP and LACP do not interoperate with each other. Ports configured to use PAgP cannot form EtherChannels with ports configured to use LACP and vice versa.

Table 17-1 lists the user-configurable EtherChannel modes.

Table 17-1 EtherChannel Modes

| Mode             | Description                                                                                                                                                                                                                                                                                                                                      |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>on</b>        | Mode that forces the LAN port to channel unconditionally. In the <b>on</b> mode, a usable EtherChannel exists only when a LAN port group in the <b>on</b> mode is connected to another LAN port group in the <b>on</b> mode. Because ports configured in the <b>on</b> mode do not negotiate, there is no negotiation traffic between the ports. |
| <b>auto</b>      | PAgP mode that places a LAN port into a passive negotiating state, in which the port responds to PAgP packets it receives but does not initiate PAgP negotiation.                                                                                                                                                                                |
| <b>desirable</b> | PAgP mode that places a LAN port into an active negotiating state, in which the port initiates negotiations with other LAN ports by sending PAgP packets.                                                                                                                                                                                        |
| <b>passive</b>   | LACP mode that places a port into a passive negotiating state, in which the port responds to LACP packets it receives but does not initiate LACP negotiation.                                                                                                                                                                                    |
| <b>active</b>    | LACP mode that places a port into an active negotiating state, in which the port initiates negotiations with other ports by sending LACP packets.                                                                                                                                                                                                |

## Understanding Manual EtherChannel Configuration

Manually configured EtherChannel ports do not exchange EtherChannel protocol packets. A manually configured EtherChannel forms only when you enter configure all ports in the EtherChannel compatibly.

## Understanding PAgP EtherChannel Configuration

PAgP supports the automatic creation of EtherChannels by exchanging PAgP packets between LAN ports. PAgP packets are exchanged only between ports in **auto** and **desirable** modes.

The protocol learns the capabilities of LAN port groups dynamically and informs the other LAN ports. Once PAgP identifies correctly matched Ethernet links, it facilitates grouping the links into an EtherChannel. The EtherChannel is then added to the spanning tree as a single bridge port.

Both the **auto** and **desirable** modes allow PAgP to negotiate between LAN ports to determine if they can form an EtherChannel, based on criteria such as port speed and trunking state. Layer 2 EtherChannels also use VLAN numbers.

LAN ports can form an EtherChannel when they are in different PAgP modes if the modes are compatible. For example:

- A LAN port in **desirable** mode can form an EtherChannel successfully with another LAN port that is in **desirable** mode.
- A LAN port in **desirable** mode can form an EtherChannel with another LAN port in **auto** mode.
- A LAN port in **auto** mode cannot form an EtherChannel with another LAN port that is also in **auto** mode, because neither port will initiate negotiation.

## Understanding IEEE 802.3ad LACP EtherChannel Configuration

Release Cisco IOS Release 12.1(11)EW and later releases support IEEE 802.3ad LACP EtherChannels. LACP supports the automatic creation of EtherChannels by exchanging LACP packets between LAN ports. LACP packets are exchanged only between ports in **passive** and **active** modes.

The protocol learns the capabilities of LAN port groups dynamically and informs the other LAN ports. Once LACP identifies correctly matched Ethernet links, it facilitates grouping the links into an EtherChannel. The EtherChannel is then added to the spanning tree as a single bridge port.

Both the **passive** and **active** modes allow LACP to negotiate between LAN ports to determine if they can form an EtherChannel, based on criteria such as port speed and trunking state. Layer 2 EtherChannels also use VLAN numbers.

LAN ports can form an EtherChannel when they are in different LACP modes as long as the modes are compatible. For example:

- A LAN port in **active** mode can form an EtherChannel successfully with another LAN port that is in **active** mode.
- A LAN port in **active** mode can form an EtherChannel with another LAN port in **passive** mode.
- A LAN port in **passive** mode cannot form an EtherChannel with another LAN port that is also in **passive** mode, because neither port will initiate negotiation.

LACP uses the following parameters:

- LACP system priority—You may configure an LACP system priority on each switch running LACP. The system priority can be configured automatically or through the CLI. See the “Configuring the LACP System Priority and System ID” section on page 17-11. LACP uses the system priority with the switch MAC address to form the system ID and also during negotiation with other systems.




---

**Note** The LACP system ID is the combination of the LACP system priority value and the MAC address of the switch.

---

- LACP port priority—You must configure an LACP port priority on each port configured to use LACP. The port priority can be configured automatically or through the CLI. See the “Configuring Layer 2 EtherChannel” section on page 17-9. LACP uses the port priority with the port number to form the port identifier.




---

**Note** Standby and “sub-channeling” are not supported in LACP and PagP.

---

- LACP administrative key—LACP automatically configures an administrative key value equal to the channel group identification number on each port configured to use LACP. The administrative key defines the ability of a port to aggregate with other ports. A port’s ability to aggregate with other ports is determined by these factors:
  - Port physical characteristics, such as data rate, duplex capability, and point-to-point or shared medium
  - Configuration restrictions that you establish

LACP tries to configure the maximum number of compatible ports in an EtherChannel, up to the maximum allowed by the hardware (eight ports). If a port can not be actively included in a channel, it will not be included automatically if a channelled port fails.

## Understanding Load Balancing

EtherChannel can balance the traffic load across the links in the channel. It does this by reducing part of the binary pattern formed from the addresses or ports in the frame to a numerical value that selects one of the links in the channel. To balance the load, EtherChannel uses MAC addresses, IP addresses, or Layer 4 port numbers, and either the message source or message destination, or both.

Use the option that provides the greatest variety in your configuration. For example, if the traffic on a channel is going only to a single MAC address, using the destination MAC address always chooses the same link in the channel; using source addresses or IP addresses might result in better load balancing.

**Note**

Load balancing can only be configured globally. As a result, all channels (manually configured, PagP, or LACP) will use the same load balancing method.

For additional information on load balancing, see the “Configuring EtherChannel Load Balancing” section on page 17-12.

## EtherChannel Configuration Guidelines and Restrictions

If improperly configured, some EtherChannel interfaces are disabled automatically to avoid network loops and other problems. Follow these guidelines and restrictions to avoid configuration problems:

- All Ethernet interfaces on all modules support EtherChannel (maximum of eight interfaces) with no requirement that interfaces be physically contiguous or on the same module.
- Configure all interfaces in an EtherChannel to operate at the same speed and duplex mode.
- Enable all interfaces in an EtherChannel. If you shut down an interface in an EtherChannel, it is treated as a link failure and its traffic is transferred to one of the remaining interfaces in the EtherChannel.
- An EtherChannel will not form if one of the interfaces is a Switched Port Analyzer (SPAN) destination port.
- For Layer 3 EtherChannels:
  - Assign Layer 3 addresses to the port-channel logical interface, not to the physical interfaces in the channel.
- For Layer 2 EtherChannels:
  - Assign all interfaces in the EtherChannel to the same VLAN, or configure them as trunks.
  - If you configure an EtherChannel from trunk interfaces, verify that the trunking mode is the same on all the trunks. Interfaces in an EtherChannel with different trunk modes can have unexpected results.
  - An EtherChannel supports the same allowed range of VLANs on all the interfaces in a trunking Layer 2 EtherChannel. If the allowed range of VLANs is not the same, the interfaces do not form an EtherChannel.
  - Interfaces with different Spanning Tree Protocol (STP) port path costs can form an EtherChannel as long they are otherwise compatibly configured. Setting different STP port path costs does not, by itself, make interfaces incompatible for the formation of an EtherChannel.

- After you configure an EtherChannel, any configuration that you apply to the port-channel interface affects the EtherChannel; any configuration that you apply to the physical interfaces affects only the interface where you apply the configuration.
- You cannot configure a 802.1x port in an EtherChannel.

# Configuring EtherChannel

These sections describe how to configure EtherChannel:

- Configuring Layer 3 EtherChannels, page 17-6
- Configuring Layer 2 EtherChannel, page 17-9
- Configuring the LACP System Priority and System ID, page 17-11
- Configuring EtherChannel Load Balancing, page 17-12
- Removing an Interface from an EtherChannel, page 17-13
- Removing an EtherChannel, page 17-13



**Note**

Ensure that the interfaces are configured correctly (see the “EtherChannel Configuration Guidelines and Restrictions” section on page 17-5).

## Configuring Layer 3 EtherChannels

To configure Layer 3 EtherChannels, create the port-channel logical interface and then put the Ethernet interfaces into the port-channel.

These sections describe Layer 3 EtherChannel configuration:

- Creating Port-Channel Logical Interfaces, page 17-6
- Configuring Physical Interfaces as Layer 3 EtherChannels, page 17-7

### Creating Port-Channel Logical Interfaces



**Note**

To move an IP address from a physical interface to an EtherChannel, you must delete the IP address from the physical interface before configuring it on the port-channel interface.

To create a port-channel interface for a Layer 3 EtherChannel, perform this task:

|        | Command                                                              | Purpose                                                                                             |
|--------|----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| Step 1 | Switch(config)# <b>interface</b> port-channel<br>port_channel_number | Creates the port-channel interface. The value for <i>port_channel_number</i> can range from 1 to 64 |
| Step 2 | Switch(config-if)# <b>ip address</b> ip_address mask                 | Assigns an IP address and subnet mask to the EtherChannel.                                          |



|        | Command                                                                       | Purpose                     |
|--------|-------------------------------------------------------------------------------|-----------------------------|
| Step 3 | Switch(config-if)# <b>end</b>                                                 | Exits configuration mode.   |
| Step 4 | Switch# <b>show running-config interface port-channel port_channel_number</b> | Verifies the configuration. |

This example shows how to create port-channel interface 1:

```
Switch# configure terminal
Switch(config)# interface port-channel 1
Switch(config-if)# ip address 172.32.52.10 255.255.255.0
Switch(config-if)# end
```

This example shows how to verify the configuration of port-channel interface 1:

```
Switch# show running-config interface port-channel 1
Building configuration...
```

```
Current configuration:
!
interface Port-channel1
 ip address 172.32.52.10 255.255.255.0
 no ip directed-broadcast
end
```

```
Switch#
```

## Configuring Physical Interfaces as Layer 3 EtherChannels

To configure physical interfaces as Layer 3 EtherChannels, perform this task for each interface:

|        | Command                                                                                                                                                                                                                                                                                                                           | Purpose                                                                                                                                                                                                                                       |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch(config)# <b>interface {fastethernet   gigabitethernet} slot/port</b>                                                                                                                                                                                                                                                       | Selects a physical interface to configure.                                                                                                                                                                                                    |
| Step 2 | Switch(config-if)# <b>no switchport</b>                                                                                                                                                                                                                                                                                           | Makes this a Layer 3 routed port.                                                                                                                                                                                                             |
| Step 3 | Switch(config-if)# <b>no ip address</b>                                                                                                                                                                                                                                                                                           | Ensures that there is no IP address assigned to the physical interface.                                                                                                                                                                       |
| Step 4 | Switch(config-if)# <b>channel-group port_channel_number mode {active   on   auto}   {passive   desirable}</b>                                                                                                                                                                                                                     | Configures the interface in a port-channel and specify the PAgP or LACP mode.<br><br>If you use PAgP, select the keywords <b>active</b> and <b>desirable</b> .<br><br>If you use LACP, select the keywords <b>active</b> and <b>passive</b> . |
| Step 5 | Switch(config-if)# <b>end</b>                                                                                                                                                                                                                                                                                                     | Exits configuration mode.                                                                                                                                                                                                                     |
| Step 6 | Switch# <b>show running-config interface port-channel port_channel_number</b><br><br>Switch# <b>show running-config interface {fastethernet   gigabitethernet} slot/port</b><br><br>Switch# <b>show interfaces {fastethernet   gigabitethernet} slot/port etherchannel</b><br><br>Switch# <b>show etherchannel 1 port-channel</b> | Verifies the configuration.                                                                                                                                                                                                                   |

This example shows how to configure Fast Ethernet interfaces 5/4 and 5/5 into port-channel 1 with PAgP mode **desirable**:

```
Switch# configure terminal
Switch(config)# interface range fastethernet 5/4 - 5 (Note: Space is mandatory.)
Switch(config-if)# no switchport
Switch(config-if)# no ip address
Switch(config-if)# channel-group 1 mode desirable
Switch(config-if)# end
```

**Note**

See the “Configuring a Range of Interfaces” section on page 4-4 for information about the **range** keyword.

The following two examples shows how to verify the configuration of Fast Ethernet interface 5/4:

```
Switch# show running-config interface fastethernet 5/4
Building configuration...
```

```
Current configuration:
!
interface FastEthernet5/4
 no ip address
 no switchport
 no ip directed-broadcast
 channel-group 1 mode desirable
end
```

```
Switch# show interfaces fastethernet 5/4 etherchannel
Port state = EC-Enbld Up In-Bndl Usr-Config
Channel group = 1 Mode = Desirable Gcchange = 0
Port-channel = Po1 GC = 0x00010001 Pseudo-port-channel = Po1
Port indx = 0 Load = 0x55
```

```
Flags: S - Device is sending Slow hello. C - Device is in Consistent state.
 A - Device is in Auto mode. P - Device learns on physical port.
Timers: H - Hello timer is running. Q - Quit timer is running.
 S - Switching timer is running. I - Interface timer is running.
```

Local information:

| Port  | Flags | State | Timers | Hello Interval | Partner Count | PAgP Priority | Learning Method | Group Ifindex |
|-------|-------|-------|--------|----------------|---------------|---------------|-----------------|---------------|
| Fa5/4 | SC    | U6/S7 |        | 30s            | 1             | 128           | Any             | 55            |

Partner's information:

| Port  | Partner Name | Partner Device ID | Partner Port | Partner Age | Partner Flags | Partner Group Cap. |
|-------|--------------|-------------------|--------------|-------------|---------------|--------------------|
| Fa5/4 | JAB031301    | 0050.0f10.230c    | 2/45         | 1s          | SAC           | 2D                 |

Age of the port in the current state: 00h:54m:52s

Switch#

This example shows how to verify the configuration of port-channel interface 1 after the interfaces have been configured:

```
Switch# show etherchannel 1 port-channel

Channel-group listing:

Group: 1

Port-channels in the group:

Port-channel: Po1

Age of the Port-channel = 01h:56m:20s
Logical slot/port = 10/1 Number of ports = 2
GC = 0x00010001 HotStandBy port = null
Port state = Port-channel L3-Ag Ag-Inuse

Ports in the Port-channel:

Index Load Port

 1 00 Fa5/6
 0 00 Fa5/7

Time since last port bundled: 00h:23m:33s Fa5/6

Switch#
```

## Configuring Layer 2 EtherChannel

To configure Layer 2 EtherChannels, configure the Ethernet interfaces with the **channel-group** command. This creates the port-channel logical interface.



### Note

IOS creates port-channel interfaces for Layer 2 EtherChannels when you configure Layer 2 Ethernet interfaces with the **channel-group** command.

To configure Layer 2 Ethernet interfaces as Layer 2 EtherChannels, perform this task for each interface:

|        | Command                                                                                                                                                            | Purpose                                                                                                                                                                                                                                       |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch(config)# <b>interface</b> { <i>fastethernet</i>   <i>gigabitethernet</i> } <i>slot/port</i>                                                                 | Selects a physical interface to configure.                                                                                                                                                                                                    |
| Step 2 | Switch(config-if)# <b>channel-group</b> <i>port_channel_number</i> <b>mode</b> { <i>active</i>   <i>on</i>   <i>auto</i> }   { <i>passive</i>   <i>desirable</i> } | Configures the interface in a port-channel and specify the PAgP or LACP mode.<br><br>If you use PAgP, select the keywords <b>active</b> and <b>desirable</b> .<br><br>If you use LACP, select the keywords <b>active</b> and <b>passive</b> . |

|        | Command                                                                                                                                                                                     | Purpose                     |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|
| Step 3 | Switch(config-if)# <b>end</b>                                                                                                                                                               | Exits configuration mode.   |
| Step 4 | Switch# <b>show running-config interface</b> {fastethernet   gigabitethernet} slot/port<br><br>Switch# <b>show interface</b> {fastethernet   gigabitethernet} slot/port <b>etherchannel</b> | Verifies the configuration. |

This example shows how to configure Fast Ethernet interfaces 5/6 and 5/7 into port-channel 2 with PAgP mode **desirable**:

```
Switch# configure terminal
Switch(config)# interface range fastethernet 5/6 - 7 (Note: Space is mandatory.)
Switch(config-if-range)# channel-group 2 mode desirable
Switch(config-if-range)# end
```

**Note**

See the “Configuring a Range of Interfaces” section on page 4-4 for information about the **range** keyword.

This example shows how to verify the configuration of port-channel interface 2:

```
Switch# show running-config interface port-channel 2
Building configuration...
```

```
Current configuration:
!
interface Port-channel2
 switchport access vlan 10
 switchport mode access
end
```

```
Switch#
```

The following two examples show how to verify the configuration of Fast Ethernet interface 5/6:

```
Switch# show running-config interface fastethernet 5/6
Building configuration...
```

```
Current configuration:
!
interface FastEthernet5/6
 switchport access vlan 10
 switchport mode access
 channel-group 2 mode desirable
end
```

```
Switch# show interfaces fastethernet 5/6 etherchannel
Port state = EC-Enbld Up In-Bndl Usr-Config
Channel group = 1 Mode = Desirable Gcchange = 0
Port-channel = Po1 GC = 0x00010001
Port indx = 0 Load = 0x55
```

```
Flags: S - Device is sending Slow hello. C - Device is in Consistent state.
 A - Device is in Auto mode. P - Device learns on physical port.
Timers: H - Hello timer is running. Q - Quit timer is running.
 S - Switching timer is running. I - Interface timer is running.
```

Local information:

| Port  | Flags | State | Timers | Hello Interval | Partner Count | PAGP Priority | Learning Method | Group Ifindex |
|-------|-------|-------|--------|----------------|---------------|---------------|-----------------|---------------|
| Fa5/6 | SC    | U6/S7 |        | 30s            | 1             | 128           | Any             | 56            |

Partner's information:

| Port  | Partner Name | Partner Device ID | Partner Port | Partner Age | Partner Flags | Partner Group |
|-------|--------------|-------------------|--------------|-------------|---------------|---------------|
| Fa5/6 | JAB031301    | 0050.0f10.230c    | 2/47         | 18s         | SAC           | 2F            |

Age of the port in the current state: 00h:10m:57s

This example shows how to verify the configuration of port-channel interface 2 after the interfaces have been configured:

```
Switch# show etherchannel 2 port-channel
Port-channels in the group:

Port-channel: Po2

Age of the Port-channel = 00h:23m:33s
Logical slot/port = 10/2 Number of ports in agport = 2
GC = 0x00020001 HotStandBy port = null
Port state = Port-channel Ag-Inuse

Ports in the Port-channel:

Index Load Port

 1 00 Fa5/6
 0 00 Fa5/7

Time since last port bundled: 00h:23m:33s Fa5/6

Switch#
```

## Configuring the LACP System Priority and System ID

The LACP system ID is the combination of the LACP system priority value and the MAC address of the switch.

To configure the LACP system priority and system ID, perform this task:

|        | Command                                                           | Purpose                                                                                                         |
|--------|-------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| Step 1 | Router(config)# <b>lacp system-priority</b> <i>priority_value</i> | (Optional for LACP) Valid values are 1 through 65535. Higher numbers have lower priority. The default is 32768. |
|        | Router(config)# <b>no system port-priority</b>                    | Reverts to the default.                                                                                         |
| Step 2 | Router(config)# <b>end</b>                                        | Exits configuration mode.                                                                                       |
| Step 3 | Router# <b>show lacp sys-id</b>                                   | Verifies the configuration.                                                                                     |

This example shows how to configure the LACP system priority:

```
Switch# configure terminal
Switch(config)# lacp system-priority 23456
Switch(config)# end
Switch(config)#
Switch# show module
```

| Mod | Ports | Card Type                           | Model          | Serial No.  |
|-----|-------|-------------------------------------|----------------|-------------|
| 1   | 2     | 1000BaseX (GBIC) Supervisor(active) | WS-X4014       | JAB063808YZ |
| 2   | 48    | 10/100BaseTX (RJ45)                 | WS-X4148-RJ    | JAB0447072W |
| 3   | 48    | 10/100BaseTX (RJ45)V                | WS-X4148-RJ45V | JAE061704J6 |
| 4   | 48    | 10/100BaseTX (RJ45)V                | WS-X4148-RJ45V | JAE061704ML |

| M | MAC addresses                    | Hw  | Fw          | Sw               | Status |
|---|----------------------------------|-----|-------------|------------------|--------|
| 1 | 0005.9a39.7a80 to 0005.9a39.7a81 | 2.1 | 12.1(12r)EW | 12.1(13)EW(0.26) | Ok     |
| 2 | 0002.fd80.f530 to 0002.fd80.f55f | 0.1 |             |                  | Ok     |
| 3 | 0009.7c45.67c0 to 0009.7c45.67ef | 1.6 |             |                  | Ok     |
| 4 | 0009.7c45.4a80 to 0009.7c45.4aaf | 1.6 |             |                  | Ok     |

This example shows how to verify the configuration:

```
Switch# show lacp sys-id
23456,0050.3e8d.6400
Switch#
```

The system priority is displayed first, followed by the MAC address of the switch.

# Configuring EtherChannel Load Balancing



Note

Load balancing can only be configured globally. As a result, all channels (manually configured, PagP, or LACP) will use the same load balancing method.

To configure EtherChannel load balancing, perform this task:

|        | Command                                                                                                                                              | Purpose                                                                                                                                      |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch(config)# [no] port-channel load-balance {src-mac   dst-mac   src-dst-mac   src-ip   dst-ip   src-dst-ip   src-port   dst-port   src-dst-port} | Configures EtherChannel load balancing.<br><br>Use the <b>no</b> keyword to return EtherChannel load balancing to the default configuration. |
| Step 2 | Switch(config)# end                                                                                                                                  | Exits configuration mode.                                                                                                                    |
| Step 3 | Switch# show etherchannel load-balance                                                                                                               | Verifies the configuration.                                                                                                                  |

The load-balancing keywords are:

- **src-mac**—Source MAC addresses
- **dst-mac**—Destination MAC addresses
- **src-dst-mac**—Source and destination MAC addresses
- **src-ip**—Source IP addresses
- **dst-ip**—Destination IP addresses

- **src-dst-ip**—Source and destination IP addresses (Default)
- **src-port**—Source Layer 4 port
- **dst-port**—Destination Layer 4 port
- **src-dst-port**—Source and destination Layer 4 port

This example shows how to configure EtherChannel to use source and destination IP addresses:

```
Switch# configure terminal
Switch(config)# port-channel load-balance dst-mac
Switch(config)# end
Switch(config)#
```

This example shows how to verify the configuration:

```
Switch# show etherchannel load-balance
Source XOR Destination IP address
Switch#
```

## Removing an Interface from an EtherChannel

To remove an Ethernet interface from an EtherChannel, perform this task:

|        | Command                                                                                                                                                                          | Purpose                                                |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|
| Step 1 | Switch(config)# <b>interface</b> {fastethernet   gigabitethernet} slot/port                                                                                                      | Selects a physical interface to configure.             |
| Step 2 | Switch(config-if)# <b>no channel-group</b>                                                                                                                                       | Removes the interface from the port-channel interface. |
| Step 3 | Switch(config-if)# <b>end</b>                                                                                                                                                    | Exits configuration mode.                              |
| Step 4 | Switch# <b>show running-config interface</b> {fastethernet   gigabitethernet} slot/port<br>Switch# <b>show interface</b> {fastethernet   gigabitethernet} slot/port etherchannel | Verifies the configuration.                            |

This example shows how to remove Fast Ethernet interfaces 5/4 and 5/5 from port-channel 1:

```
Switch# configure terminal
Switch(config)# interface range fastethernet 5/4 - 5 (Note: Space is mandatory.)
Switch(config-if)# no channel-group 1
Switch(config-if)# end
```

## Removing an EtherChannel

If you remove an EtherChannel, the member ports are shut down and removed from the Channel group.



### Note

You must remove an EtherChannel before changing a port from Layer 2 to Layer 3, or Layer 3 to Layer 2.

To remove an EtherChannel, perform this task:

|        | Command                                                                        | Purpose                             |
|--------|--------------------------------------------------------------------------------|-------------------------------------|
| Step 1 | Switch(config)# <b>no interface port-channel</b><br><i>port_channel_number</i> | Removes the port-channel interface. |
| Step 2 | Switch(config)# <b>end</b>                                                     | Exits configuration mode.           |
| Step 3 | Switch# <b>show etherchannel summary</b>                                       | Verifies the configuration.         |

This example shows how to remove port-channel 1:

```
Switch# configure terminal
Switch(config)# no interface port-channel 1
Switch(config)# end
```





## Configuring UDLD

This chapter describes how to configure the UniDirectional Link Detection (UDLD) and Unidirectional Ethernet on the Catalyst 4500 series switch. It also provides guidelines, procedures, and configuration examples.

This chapter includes the following major sections:

- Overview of UDLD, page 18-1
- Default UDLD Configuration, page 18-2
- Configuring UDLD on the Switch, page 18-2



### Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference* and the publications at this URL: <http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/index.htm>

## Overview of UDLD

UDLD allows devices connected through fiber-optic or copper Ethernet cables (for example, Category 5 cabling) to monitor the physical configuration of the cables and detect when a unidirectional link exists. A unidirectional link occurs whenever traffic transmitted by the local device over a link is received by the neighbor but traffic transmitted from the neighbor is not received by the local device. When a unidirectional link is detected, UDLD shuts down the affected interface and alerts the user.

Unidirectional links can cause a variety of problems, including spanning tree topology loops.

UDLD is a Layer 2 protocol that works with the Layer 1 mechanisms to determine the physical status of a link. At Layer 1, autonegotiation takes care of physical signaling and fault detection. UDLD performs tasks that autonegotiation cannot perform, such as detecting the identities of neighbors and shutting down misconnected interfaces. When you enable both autonegotiation and UDLD, Layer 1 and Layer 2 detections work together to prevent physical and logical unidirectional connections and the malfunctioning of other protocols.

If one of the fiber strands in a pair is disconnected, as long as autonegotiation is active, the link does not stay up. In this case, the logical link is undetermined, and UDLD does not take any action. If both fibers are working normally from a Layer 1 perspective, then UDLD at Layer 2 determines whether or not those fibers are connected correctly and whether or not traffic is flowing bidirectionally between the right neighbors. This check cannot be performed by autonegotiation because autonegotiation operates at Layer 1.

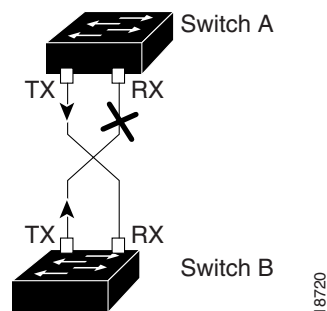
The switch periodically transmits UDLD packets to neighbor devices on interfaces with UDLD enabled. If the packets are echoed back within a specific time frame and they are lacking a specific acknowledgment (echo), the link is flagged as unidirectional and the interface is shut down. Devices on both ends of the link must support UDLD in order for the protocol to successfully identify and disable unidirectional links.

**Note**

By default, UDLD is locally disabled on copper interfaces to avoid sending unnecessary control traffic on this type of media, since it is often used for access interfaces.

Figure 18-1 shows an example of a unidirectional link condition. Switch B successfully receives traffic from Switch A on the interface. However, Switch A does not receive traffic from Switch B on the same interface. UDLD detects the problem and disables the interface.

**Figure 18-1 Unidirectional Link**



## Default UDLD Configuration

Table 18-1 shows the UDLD default configuration.

**Table 18-1 UDLD Default Configuration**

| Feature                                                         | Default Status                                            |
|-----------------------------------------------------------------|-----------------------------------------------------------|
| UDLD global enable state                                        | Globally disabled                                         |
| UDLD per-interface enable state for fiber-optic media           | Enabled on all Ethernet fiber-optic interfaces            |
| UDLD per-interface enable state for twisted-pair (copper) media | Disabled on all Ethernet 10/100 and 1000BaseTX interfaces |

## Configuring UDLD on the Switch

The following sections describe how to configure UDLD:

- Enabling UDLD Globally, page 18-3
- Enabling UDLD on Individual Interfaces, page 18-3
- Disabling UDLD on Nonfiber-Optic Interfaces, page 18-3
- Disabling UDLD on Fiber-Optic Interfaces, page 18-4
- Resetting Disabled Interfaces, page 18-4

## Enabling UDLD Globally

To enable UDLD globally on all fiber-optic interfaces on the switch, perform this task:

| Command                                 | Purpose                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Switch(config)# <b>[no] udld enable</b> | <p>Enables UDLD globally on fiber-optic interfaces on the switch.</p> <p>Use the <b>no</b> keyword to globally disable UDLD on fiber-optic interfaces.</p> <p><b>Note</b> This command configures only fiber-optic interfaces. An individual interface configuration overrides the setting of this command.</p> |

## Enabling UDLD on Individual Interfaces

To enable UDLD on individual interfaces, perform this task:

|        | Command                               | Purpose                                                                                                                                               |
|--------|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch(config-if)# <b>udld enable</b> | Enables UDLD on a specific interface. On a fiber-optic interface, this command overrides the <b>udld enable</b> global configuration command setting. |
| Step 2 | Switch# <b>show udld interface</b>    | Verifies the configuration.                                                                                                                           |

## Disabling UDLD on Nonfiber-Optic Interfaces

To disable UDLD on individual nonfiber-optic interfaces, perform this task:

|        | Command                                  | Purpose                                                                                                                                                                                                                                 |
|--------|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch(config-if)# <b>no udld enable</b> | <p>Disables UDLD on a nonfiber-optic interface.</p> <p><b>Note</b> On fiber-optic interfaces, the <b>no udld enable</b> command reverts the interface configuration to the <b>udld enable</b> global configuration command setting.</p> |
| Step 2 | Switch# <b>show udld interface</b>       | Verifies the configuration.                                                                                                                                                                                                             |

## Disabling UDLD on Fiber-Optic Interfaces

To disable UDLD on individual fiber-optic interfaces, perform this task:

|        | Command                                | Purpose                                                                                                                                                                                                                             |
|--------|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch(config-if)# <b>udld disable</b> | Disables UDLD on a fiber-optic interface.<br><br><b>Note</b> This command is not supported on nonfiber-optic interfaces.<br><br>Use the <b>no</b> keyword to revert to the <b>udld enable</b> global configuration command setting. |
| Step 2 | Switch# <b>show udld interface</b>     | Verifies the configuration.                                                                                                                                                                                                         |

## Resetting Disabled Interfaces

To reset all interfaces that have been shut down by UDLD, perform this task:

| Command                   | Purpose                                                 |
|---------------------------|---------------------------------------------------------|
| Switch# <b>udld reset</b> | Resets all interfaces that have been shut down by UDLD. |



# Configuring DHCP Snooping and IP Source Guard

This chapter describes how to configure Dynamic Host Configuration Protocol (DHCP) snooping and IP Source Guard on Catalyst 4500 series switches. It provides guidelines, procedures, and configuration examples.

This chapter consists of the following major sections:

- Overview of DHCP Snooping, page 19-1
- Configuring DHCP Snooping on the Switch, page 19-3
- Displaying DHCP Snooping Information, page 19-9
- Overview of IP Source Guard, page 19-10
- Configuring IP Source Guard on the Switch, page 19-11
- Displaying IP Source Guard Information, page 19-12



**Note**

For complete syntax and usage information for the switch commands used in this chapter, refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference* and related publications at [http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/12\\_1\\_12/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/12_1_12/index.htm)

## Overview of DHCP Snooping

DHCP snooping is a DHCP security feature that provides security by filtering untrusted DHCP messages and by building and maintaining a DHCP snooping binding table. An untrusted message is a message that is received from outside the network or firewall and that can cause traffic attacks within your network.

The DHCP snooping binding table contains the MAC address, IP address, lease time, binding type, VLAN number, and interface information that corresponds to the local untrusted interfaces of a switch; it does not contain information regarding hosts interconnected with a trusted interface. An untrusted interface is an interface that is configured to receive messages from outside the network or firewall. A trusted interface is an interface that is configured to receive only messages from within the network.

DHCP snooping acts like a firewall between untrusted hosts and DHCP servers. It also gives you a way to differentiate between untrusted interfaces connected to the end-user and trusted interfaces connected to the DHCP server or another switch.



**Note**

In order to enable DHCP snooping on a VLAN, you must enable DHCP snooping on the switch.

You can configure DHCP snooping for switches and VLANs. When you enable DHCP snooping on a switch, the interface acts as a Layer 2 bridge, intercepting and safeguarding DHCP messages going to a Layer 2 VLAN. When you enable DHCP snooping on a VLAN, the switch acts as a Layer 2 bridge within a VLAN domain.

## Overview of the DHCP Snooping Database Agent

To retain the bindings across switch reloads, you must use the DHCP snooping database agent. Without this agent, the bindings established by DHCP snooping are lost upon switch reload. Connectivity is lost as well.

The mechanism for the database agent stores the bindings in a file at a configured location. Upon reload, the switch reads the file to build the database for the bindings. The switch keeps the file current by writing to the file as the database changes.

The format of the file that contains the bindings is as follows:

```
<initial-checksum>
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
<entry-1> <checksum-1>
<entry-2> <checksum-1-2>
...
...
<entry-n> <checksum-1-2-...-n>
END
```

Each entry in the file is tagged with a checksum that is used to validate the entries whenever the file is read. The <initial-checksum> entry on the first line helps distinguish entries associated with the latest write from entries that are associated with a previous write.

This is a sample bindings file:

```
3ebe1518
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
1.1.1.1 512 0001.0001.0005 3EBE2881 Gi1/1 e5e1e733
1.1.1.1 512 0001.0001.0002 3EBE2881 Gi1/1 4b3486ec
1.1.1.1 1536 0001.0001.0004 3EBE2881 Gi1/1 f0e02872
1.1.1.1 1024 0001.0001.0003 3EBE2881 Gi1/1 ac41adf9
1.1.1.1 1 0001.0001.0001 3EBE2881 Gi1/1 34b3273e
END
```

Each entry holds an IP address, VLAN, MAC address, lease time (in hex), and the interface associated with a binding. At the end of each entry is a checksum that accounts for all the bytes from the start of the file through all the bytes associated with the entry. Each entry consists of 72 bytes of data, followed by a space, followed by a checksum.

Upon bootup, when the calculated checksum equals the stored checksum, a switch reads entries from the file and adds the bindings to the DHCP snooping database. When the calculated checksum does not equal the stored checksum, the entry read from the file is ignored and so are all the entries following the failed entry. The switch also ignores all those entries from the file whose lease time has expired. (This is possible because the lease time might indicate an expired time.) An entry from the file is also ignored if the interface referred to in the entry, no longer exists on the system or if it is a router port or a DHCP snooping-trusted interface.

When a switch learns of new bindings or when it loses some bindings, the switch writes the modified set of entries from the snooping database to the file. The writes are performed with a configurable delay to batch as many changes as possible before the actual write happens. Associated with each transfer is a timeout after which a transfer is aborted if it is not completed. These timers are referred to as the write delay and abort timeout.

## Configuring DHCP Snooping on the Switch

When you configure DHCP snooping on your switch, you are enabling the switch to differentiate untrusted interfaces from trusted interfaces. You must enable DHCP snooping globally before you can use DHCP snooping on a VLAN. You can enable DHCP snooping independently from other DHCP features.

Once you have enabled DHCP snooping, all the DHCP relay information option configuration commands are disabled; this includes the following commands:

- **ip dhcp relay information check**
- **ip dhcp relay information policy**
- **ip dhcp relay information trusted**
- **ip dhcp relay information trust-all**

These sections describe how to configure DHCP snooping:

- Default Configuration for DHCP Snooping, page 19-3
- Enabling DHCP Snooping, page 19-4
- Enabling DHCP Snooping on Private VLAN, page 19-5
- Enabling the DHCP Snooping Database Agent, page 19-5
- Configuration Examples for the Database Agent, page 19-6



### Note

For DHCP server configuration information, refer to “Configuring DHCP” in the *Cisco IOS IP and IP Routing Configuration Guide* at:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip\\_c/ipcp1/1cddhcp.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_c/ipcp1/1cddhcp.htm)

## Default Configuration for DHCP Snooping

DHCP snooping is disabled by default. Table 19-1 shows all the default configuration values for each DHCP snooping option.

**Table 19-1 Default Configuration Values for DHCP Snooping**

| Option                           | Default Value/State                                    |
|----------------------------------|--------------------------------------------------------|
| DHCP snooping                    | Disabled                                               |
| DHCP snooping information option | Enabled                                                |
| DHCP snooping limit rate         | Infinite (functions as if rate limiting were disabled) |
| DHCP snooping trust              | Untrusted                                              |
| DHCP snooping vlan               | Disabled                                               |

If you want to change the default configuration values, see the “Enabling DHCP Snooping” section.

# Enabling DHCP Snooping



**Note**

When DHCP snooping is enabled globally, DHCP requests are dropped until the ports are configured. Consequently, you should probably this feature during a maintenance window and not during production.

To enable DHCP snooping, perform this task:

|        | Command                                                                                                             | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------|---------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch(config)# <b>ip dhcp snooping</b>                                                                             | Enables DHCP snooping globally.<br>You can use the <b>no</b> keyword to disable DHCP snooping.                                                                                                                                                                                                                                                                                                                                                                 |
| Step 2 | Switch(config)# <b>ip dhcp snooping</b> <i>vlan number</i><br>[ <i>number</i> ]   <b>vlan</b> { <i>vlan range</i> } | Enables DHCP snooping on your VLAN or VLAN range                                                                                                                                                                                                                                                                                                                                                                                                               |
| Step 3 | Switch(config)# <b>ip dhcp snooping information option</b>                                                          | Enables DHCP Option 82 data insertion.                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Step 4 | Switch(config-if)# <b>ip dhcp snooping trust</b>                                                                    | Configures the interface as trusted or untrusted.<br>You can use the <b>no</b> keyword to configure an interface to receive messages from an untrusted client.                                                                                                                                                                                                                                                                                                 |
| Step 5 | Switch(config-if)# <b>ip dhcp snooping limit rate</b><br><i>rate</i>                                                | Configures the number of DHCP packets per second (pps) that an interface can receive.<br><br><b>Note</b> You may not want to configure untrusted rate limiting to more than 100 pps.<br><br>Normally, the rate limit applies to untrusted interfaces. If you want to set up rate limiting for trusted interfaces, keep in mind that trusted interfaces aggregate all DHCP traffic in the switch, and you will need to adjust the rate limit to a higher value. |
| Step 6 | Switch(config)# <b>end</b>                                                                                          | Exits configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Step 7 | Switch# <b>show ip dhcp snooping</b>                                                                                | Verifies the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                    |

You can configure DHCP snooping for a single VLAN or a range of VLANs. To configure a single VLAN, enter a single VLAN number. To configure a range of VLANs, enter a beginning and an ending VLAN number.

This example shows how to enable DHCP snooping on VLANs 10 through 100:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10 100
Switch(config)# ip dhcp snooping information option
Switch(config-if)# ip dhcp snooping trust
Switch(config-if)# ip dhcp snooping limit rate 100
Switch(config)# end
```



```

Switch# show ip dhcp snooping
Switch DHCP snooping is enabled.
DHCP Snooping is configured on the following VLANs:
 10-100
Insertion of option 82 information is enabled.
Interface Trusted Rate limit (pps)

FastEthernet2/1 yes 100
FastEthernet2/2 yes none
FastEthernet3/1 no 20
Switch#

```

## Enabling DHCP Snooping on Private VLAN

DHCP snooping can be enabled on private VLANs, which provide isolation between Layer 2 ports within the same VLAN. If DHCP snooping is enabled (or disabled), the configuration is propagated to both the primary VLAN and its associated secondary VLANs. You cannot enable (or disable) DHCP snooping on a primary VLAN without reflecting this configuration change on the secondary VLANs.

Configuring DHCP snooping on a secondary VLAN is still allowed, but it will not take effect if the associated primary VLAN is already configured. If the associated primary VLAN is configured, the effective DHCP snooping mode on the secondary VLAN is derived from the corresponding primary VLAN. Manually configuring DHCP snooping on a secondary VLAN will cause the switch to issue this warning message:

```
DHCP Snooping configuration may not take effect on secondary vlan XXX
```

The **show ip dhcp snooping** command will display all VLANs (both primary and secondary) that have DHCP snooping enabled.

## Enabling the DHCP Snooping Database Agent

To configure the database agent, perform one or more of the following tasks:

| Command                                                                                                    | Purpose                                                                                                             |
|------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Switch(config)# <b>ip dhcp snooping database</b> { url   write-delay seconds   timeout seconds }           | (Required) Configures a URL for the database agent (or file) and the related timeout values.                        |
| Switch(config)# <b>no ip dhcp snooping database</b> [write-delay   timeout]                                |                                                                                                                     |
| Switch# <b>show ip dhcp snooping database</b> [detail]                                                     | (Optional) Displays the current operating state of the database agent and statistics associated with the transfers. |
| Switch# <b>clear ip dhcp snooping database statistics</b>                                                  | (Optional) Clears the statistics associated with the database agent.                                                |
| Switch# <b>renew ip dhcp snooping database</b> [validation none] [url]                                     | (Optional) Requests the read entries from a file at the given URL.                                                  |
| Switch# <b>ip dhcp snooping binding</b> mac-addr vlan vlan ipaddr interface ifname expiry lease-in-seconds | (Optional) Adds/deletes bindings to the snooping database.                                                          |
| Switch# <b>no ip dhcp snooping binding</b> mac-addr vlan vlan ipaddr interface ifname                      |                                                                                                                     |

**Note**

Because both NVRAM and bootflash have limited storage capacity, storing a file on an TFTP server is preferred. Moreover, when a file is stored in a remote location accessible through TFTP, an RPR standby supervisor engine can take over the binding list when a switchover occurs.

**Note**

Network-based URLs (such as TFTP and FTP) require that you create an empty file at the configured URL before the switch can write the set of bindings for the first time.

## Configuration Examples for the Database Agent

The following examples show how to use the above commands.

### Example 1: Enabling the Database Agent

The following example shows how to configure the DHCP snooping database agent to store the bindings at a given location and to view the configuration and operating state:

```
Switch# configure terminal
Switch(config)# ip dhcp snooping database tftp://10.1.1.1/directory/file
Switch(config)# end
Switch# show ip dhcp snooping database detail
Agent URL : tftp://10.1.1.1/directory/file
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : 7 (00:00:07)
Abort Timer Expiry : Not Running

Last Succeeded Time : None
Last Failed Time : 17:14:25 UTC Sat Jul 7 2001
Last Failed Reason : Unable to access URL.

Total Attempts : 21 Startup Failures : 0
Successful Transfers : 0 Failed Transfers : 21
Successful Reads : 0 Failed Reads : 0
Successful Writes : 0 Failed Writes : 21
Media Failures : 0

First successful access: Read

Last ignored bindings counters :
Binding Collisions : 0 Expired leases : 0
Invalid interfaces : 0 Unsupported vlans : 0
Parse failures : 0

Last Ignored Time : None

Total ignored bindings counters:
Binding Collisions : 0 Expired leases : 0
Invalid interfaces : 0 Unsupported vlans : 0
Parse failures : 0

Switch#
```

The first three lines of output show the configured URL and related timer configuration values. The next three lines show the operating state and the amount of time left for expiry of write delay and abort timers.

Among the statistics shown in the output, startup failures indicate the number of attempts the read or create of the file has failed upon bootstrap.



#### Note

Because the location is based off in the network, you must create a temporary file on the TFTP server. You can create a temporary file on a typical UNIX workstation by creating a 0 byte file “file” in the directory “directory” that can be referenced by the TFTP server daemon. With some server implementations on UNIX workstations, the file should be provided with full (777) permissions for write access to the file.

DHCP snooping bindings are keyed on the MAC address and VLAN combination. Therefore, if an entry in the remote file has an entry for a given MAC address and VLAN set, for which the switch already has a binding, the entry from the remote file is ignored when the file is read. This condition is referred to as the binding collision.

An entry in a file may no longer be valid because the lease indicated by the entry may have expired by the time it is read. The expired leases counter indicates the number of bindings ignored because of this condition. The Invalid interfaces counter refers to the number of bindings that have been ignored when the interface referred by the entry either does not exist on the system or is a router or DHCP snooping trusted interface if it exists, when the read happened. Unsupported VLANs refers to the number of entries that have been ignored because the indicated VLAN is not supported on the system. The Parse failures counter provides the number of entries that have been ignored when the switch is unable to interpret the meaning of the entries from the file.

The switch maintains two sets of counters for these ignored bindings. One provides the counters for a read that has at least one binding ignored by at least one of these conditions. These counters are shown as the “Last ignored bindings counters.” The total ignored bindings counters provides a sum of the number of bindings that have been ignored because of all the reads since the switch bootstrap. These two set of counters are cleared by the **clear** command. Therefore, the total counter set may indicate the number of bindings that have been ignored since the last clear.

## Example 2: Reading Binding Entries from a TFTP File

To manually read the entries from a tftp file, perform this task:

|        | Command                                     | Purpose                                               |
|--------|---------------------------------------------|-------------------------------------------------------|
| Step 1 | Switch# <b>sh ip dhcp snooping database</b> | Displays the DHCP snooping database agent statistics. |
| Step 2 | Switch# <b>renew ip dhcp snoop data url</b> | Directs the switch to read the file from given URL.   |
| Step 3 | Switch# <b>sh ip dhcp snoop data</b>        | Displays the read status.                             |
| Step 4 | Switch# <b>sh ip dhcp snoop bind</b>        | Verifies whether the bindings were read successfully. |

This is an example of how to manually read entries from the tftp://10.1.1.1/directory/file:

```
Switch# sh ip dhcp snooping database
Agent URL :
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : Not Running
```

Abort Timer Expiry : Not Running

Last Succeeded Time : None

Last Failed Time : None

Last Failed Reason : No failure recorded.

```
Total Attempts : 0 Startup Failures : 0
Successful Transfers : 0 Failed Transfers : 0
Successful Reads : 0 Failed Reads : 0
Successful Writes : 0 Failed Writes : 0
Media Failures : 0
```

Switch#

Switch# **renew ip dhcp snoop data tftp://10.1.1.1/directory/file**

Loading directory/file from 10.1.1.1 (via GigabitEthernet1/1): !

[OK - 457 bytes]

Database downloaded successfully.

Switch#

00:01:29: %DHCP\_SNOOPING-6-AGENT\_OPERATION\_SUCCEEDED: DHCP snooping database Read succeeded.

Switch#

Switch# **sh ip dhcp snoop data**

Agent URL :

Write delay Timer : 300 seconds

Abort Timer : 300 seconds

Agent Running : No

Delay Timer Expiry : Not Running

Abort Timer Expiry : Not Running

Last Succeeded Time : 15:24:34 UTC Sun Jul 8 2001

Last Failed Time : None

Last Failed Reason : No failure recorded.

```
Total Attempts : 1 Startup Failures : 0
Successful Transfers : 1 Failed Transfers : 0
Successful Reads : 1 Failed Reads : 0
Successful Writes : 0 Failed Writes : 0
Media Failures : 0
```

Switch#

Switch# **sh ip dhcp snoop bind**

| MacAddress        | IpAddress | Lease(sec) | Type          | VLAN | Interface          |
|-------------------|-----------|------------|---------------|------|--------------------|
| 00:01:00:01:00:05 | 1.1.1.1   | 49810      | dhcp-snooping | 512  | GigabitEthernet1/1 |
| 00:01:00:01:00:02 | 1.1.1.1   | 49810      | dhcp-snooping | 512  | GigabitEthernet1/1 |
| 00:01:00:01:00:04 | 1.1.1.1   | 49810      | dhcp-snooping | 1536 | GigabitEthernet1/1 |
| 00:01:00:01:00:03 | 1.1.1.1   | 49810      | dhcp-snooping | 1024 | GigabitEthernet1/1 |
| 00:01:00:01:00:01 | 1.1.1.1   | 49810      | dhcp-snooping | 1    | GigabitEthernet1/1 |

Switch#

Switch# **clear ip dhcp snoop bind**

Switch# **sh ip dhcp snoop bind**

| MacAddress | IpAddress | Lease(sec) | Type | VLAN | Interface |
|------------|-----------|------------|------|------|-----------|
|------------|-----------|------------|------|------|-----------|

Switch#

### Example 3: Adding Information to the DHCP Snooping Database

To manually add a binding to the DHCP snooping database, perform the following task:

|        | Command                                                                                                     | Purpose                                                    |
|--------|-------------------------------------------------------------------------------------------------------------|------------------------------------------------------------|
| Step 1 | Switch# <code>show ip dhcp snooping binding</code>                                                          | Views the DHCP snooping database                           |
| Step 2 | Switch# <code>ip dhcp snooping binding binding-id vlan vlan-id interface interface expiry lease-time</code> | Adds the binding using the 'ip dhcp snooping' exec command |
| Step 3 | Switch# <code>show ip dhcp snooping binding</code>                                                          | Checks the DHCP snooping database                          |

This example shows how to manually add a binding to the DHCP snooping database:

```
Switch# show ip dhcp snooping binding
MacAddress IpAddress Lease(sec) Type VLAN Interface

Switch#
Switch# ip dhcp snooping binding 1.1.1 vlan 1 1.1.1.1 interface gil1/1 expiry 1000

Switch# show ip dhcp snooping binding
MacAddress IpAddress Lease(sec) Type VLAN Interface

00:01:00:01:00:01 1.1.1.1 992 dhcp-snooping 1 GigabitEthernet1/1
Switch#
```

## Displaying DHCP Snooping Information

You can display a DHCP snooping binding table and configuration information for all interfaces on a switch.

### Displaying a Binding Table

The DHCP snooping binding table for each switch contains binding entries that correspond to untrusted ports. The table does not contain information about hosts interconnected with a trusted port because each interconnected switch will have its own DHCP snooping binding table.

This example shows how to display the DHCP snooping binding information for a switch:

```
Switch# sh ip dhcp snooping binding
MacAddress IpAddress Lease(sec) Type VLAN Interface

00:02:B3:3F:3B:99 55.5.5.2 6943 dhcp-snooping 10 FastEthernet6/10
Switch#
```

Table 19-2 describes the fields in the `show ip dhcp snooping binding` command output.

**Table 19-2** *show ip dhcp snooping binding Command Output*

| Field       | Description                                     |
|-------------|-------------------------------------------------|
| MAC Address | Client hardware MAC address                     |
| IP Address  | Client IP address assigned from the DHCP server |

**Table 19-2** *show ip dhcp snooping binding Command Output (continued)*

| Field           | Description                                                                              |
|-----------------|------------------------------------------------------------------------------------------|
| Lease (seconds) | IP address lease time                                                                    |
| Type            | Binding type; dynamic binding learned by dhcp-snooping or statically-configured binding. |
| VLAN            | VLAN number of the client interface                                                      |
| Interface       | Interface that connects to the DHCP client host                                          |

## Displaying the DHCP Snooping Configuration

This example shows how to display the DHCP snooping configuration for a switch.

```
Switch# show ip dhcp snooping
Switch DHCP snooping is enabled.
DHCP Snooping is configured on the following VLANs:
 10 30-40 100 200-220
Insertion of option 82 information is enabled.
Interface Trusted Rate limit (pps)

FastEthernet2/1 yes 10
FastEthernet3/1 yes none
GigabitEthernet1/1 no 20
Switch#
```

## Overview of IP Source Guard

Similar to DHCP snooping, this feature is enabled on a DHCP snooping untrusted Layer 2 port. Initially, all IP traffic on the port is blocked except for DHCP packets that are captured by the DHCP snooping process. When a client receives a valid IP address from the DHCP server, or when a static IP source binding is configured by the user, a per-port and VLAN Access Control List (PACL) is installed on the port. This process restricts the client IP traffic to those source IP addresses configured in the binding; any IP traffic with a source IP address other than that in the IP source binding will be filtered out. This filtering limits a host's ability to attack the network by claiming neighbor host's IP address.



### Note

If IP Source Guard is enabled on a trunk port with a large number of VLANs that have DHCP snooping enabled, you might run out of ACL hardware resources and some packets might be switched in software.

IP Source Guard supports only the Layer 2 port, including both access and trunk. For each untrusted Layer 2 port, there are two levels of IP traffic security filtering:

- Source IP address filter

IP traffic is filtered based on its source IP address. Only IP traffic with a source IP address that matches the IP source binding entry is permitted.

An IP source address filter is changed when a new IP source entry binding is created or deleted on the port. The port PACL will be recalculated and reapplied in the hardware to reflect the IP source binding change. By default, if the IP filter is enabled without any IP source binding on the port, a default PACL that denies all IP traffic is installed on the port. Similarly, when the IP filter is disabled, any IP source filter PACL will be removed from the interface.

- Source IP and MAC address filter

IP traffic is filtered based on its source IP address as well as its MAC address; only IP traffic with source IP and MAC addresses matching the IP source binding entry are permitted.

**Note**

When IP source guard is enabled in IP and MAC filtering mode, the DHCP snooping option 82 must be enabled to ensure that the DHCP protocol works properly. Without option 82 data, the switch cannot locate the client host port to forward the DHCP server reply. Instead, the DHCP server reply is dropped and the client cannot obtain an IP address.

## Configuring IP Source Guard on the Switch

To enable IP Source Guard, perform this task:

|        | Command                                                                             | Purpose                                                                                                                                                                              |
|--------|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch(config)# <b>ip dhcp snooping</b>                                             | Enables DHCP snooping globally.<br>You can use the <b>no</b> keyword to disable DHCP snooping.                                                                                       |
| Step 2 | Switch(config)# <b>ip dhcp snooping vlan</b> <i>number</i> [ <i>number</i> ]        | Enables DHCP snooping on your VLANs.                                                                                                                                                 |
| Step 3 | Switch(config-if)# <b>no ip dhcp snooping trust</b>                                 | Configures the interface as trusted or untrusted.<br>You can use the <b>no</b> keyword of to configure an interface to receive only messages from within the network.                |
| Step 4 | Switch(config-if)# <b>ip verify source vlan dhcp-snooping port-security</b>         | Enables 12 port IP source guard on DHCP snooping to filter both source IP and MAC addresses.                                                                                         |
| Step 5 | Switch(config-if)# <b>switchport port-security limit rate invalid-source-mac N</b>  | Enables a per-12-port DHCP snooping security rate limit.<br><b>Note</b> This limit only applies to the port where IP Source Guard is enabled as filtering both IP and MAC addresses. |
| Step 6 | Switch(config)# <b>ip source binding ip-addr ip vlan number interface interface</b> | Configures a static IP binding on the port.                                                                                                                                          |
| Step 7 | Switch(config)# <b>end</b>                                                          | Exits configuration mode.                                                                                                                                                            |
| Step 8 | Switch# <b>show ip verify source interface interface-name</b>                       | Verifies the configuration.                                                                                                                                                          |

**Note**

The static IP source binding can only be configured on switch port. If you issue the **ip source binding vlan interface** command on a Layer 3 port, you will receive this error message: Static IP source binding can only be configured on switch port.

This example shows how to enable per-12-port IP source guard on VLANs 10 through 20:

```
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 fa6/1
```

```

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# sh 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 -----
Fa6/1 ip-mac active deny-all -----
Switch#

```

The output shows that there is one valid DHCP binding to VLAN 10.

## Configuring IP Source Guard on Private VLANs

For private VLAN ports, you must enable DHCP snooping on primary VLANs in order for IP source guard to be effective. IP source guard on a primary VLAN will automatically propagate to a secondary VLAN. Configuring a static IP source binding on a secondary VLAN is allowed, but it will not take effect. When manually configuring a static IP source binding on a secondary VLAN, you will receive the following warning:



### Warning

**IP source filter may not take effect on secondary vlan where IP source binding is configured. If private vlan feature is enabled, IP source filter on primary vlan will automatically propagate to all secondary vlans.**

## Displaying IP Source Guard Information

You can display IP Source Guard PACL information for all interfaces on a switch using the **show ip verify source** command.

- Displayed PACLs if DHCP snooping is enabled on VLAN 10 through 20, interface fa6/1 is configured for IP filtering, and there is an existing IP address binding 10.0.01 on VLAN 10:

| Interface | Filter-type | Filter-mode | IP-address | Mac-address | Vlan  |
|-----------|-------------|-------------|------------|-------------|-------|
| fa6/1     | ip          | active      | 10.0.0.1   |             | 10    |
| fa6/1     | ip          | active      | deny-all   |             | 11-20 |



### Note

The second entry shows that a default PACL (deny all IP traffic) is installed on the port for those snooping-enabled VLANs that do not have a valid IP source binding.

- Displayed PACL for a trusted port:

| Interface | Filter-type | Filter-mode         | IP-address | Mac-address | Vlan |
|-----------|-------------|---------------------|------------|-------------|------|
| fa6/2     | ip          | inactive-trust-port |            |             |      |

- Displayed PACL for a port in a VLAN not configured for DHCP snooping:

| Interface | Filter-type | Filter-mode               | IP-address | Mac-address | Vlan |
|-----------|-------------|---------------------------|------------|-------------|------|
| fa6/3     | ip          | inactive-no-snooping-vlan |            |             |      |



- Displayed PACLs for a port with multiple bindings configured for an IP/MAC filtering:

| Interface | Filter-type | Filter-mode | IP-address | Mac-address    | Vlan  |
|-----------|-------------|-------------|------------|----------------|-------|
| fa6/4     | ip-mac      | active      | 10.0.0.2   | aaaa.bbbb.cccc | 10    |
| fa6/4     | ip-mac      | active      | 11.0.0.1   | aaaa.bbbb.cccd | 11    |
| fa6/4     | ip-mac      | active      | deny-all   | deny-all       | 12-20 |

- Displayed PACLs for a port configured for IP/MAC filtering but not for port security:

| Interface | Filter-type | Filter-mode | IP-address | Mac-address | Vlan  |
|-----------|-------------|-------------|------------|-------------|-------|
| fa6/5     | ip-mac      | active      | 10.0.0.3   | permit-all  | 10    |
| fa6/5     | ip-mac      | active      | deny-all   | permit-all  | 11-20 |



**Note** The MAC filter shows permit-all because port security is not enabled, so the MAC filter cannot apply to the port/VLAN and is effectively disabled. Always enable port security first.

- Displayed error message when issuing the **show ip verify source** command on a port that does not have an IP source filter mode configured:

IP Source Guard is not configured on the interface fa6/6.

You can also use the **show ip verify source** command to display all interfaces on the switch that have IP source guard enabled:

| Interface | Filter-type | Filter-mode               | IP-address | Mac-address    | Vlan  |
|-----------|-------------|---------------------------|------------|----------------|-------|
| fa6/1     | ip          | active                    | 10.0.0.1   |                | 10    |
| fa6/1     | ip          | active                    | deny-all   |                | 11-20 |
| fa6/2     | ip          | inactive-trust-port       |            |                |       |
| fa6/3     | ip          | inactive-no-snooping-vlan |            |                |       |
| fa6/4     | ip-mac      | active                    | 10.0.0.2   | aaaa.bbbb.cccc | 10    |
| fa6/4     | ip-mac      | active                    | 11.0.0.1   | aaaa.bbbb.cccd | 11    |
| fa6/4     | ip-mac      | active                    | deny-all   | deny-all       | 12-20 |
| fa6/5     | ip-mac      | active                    | 10.0.0.3   | permit-all     | 10    |
| fa6/5     | ip-mac      | active                    | deny-all   | permit-all     | 11-20 |

## Displaying IP Source Binding Information

You can display all IP source bindings configured on all interfaces on a switch using the **show ip source binding** command.

```
Switch# sh ip source binding
MacAddress IpAddress Lease(sec) Type VLAN Interface

00:02:B3:3F:3B:99 55.5.5.2 6522 dhcp-snooping 10 FastEthernet6/10
00:00:00:0A:00:0B 11.0.0.1 infinite static 10 FastEthernet6/10
Switch#
```

Table 19-3 describes the fields in the **show ip source binding** command output.

**Table 19-3** *show ip dhcp snooping binding Command Output*

| Field       | Description                                     |
|-------------|-------------------------------------------------|
| Mac Address | Client hardware MAC address                     |
| IP Address  | Client IP address assigned from the DHCP server |

**Table 19-3** *show ip dhcp snooping binding Command Output (continued)*

| Field           | Description                                                                                     |
|-----------------|-------------------------------------------------------------------------------------------------|
| Lease (seconds) | IP address lease time                                                                           |
| Type            | Binding type; static bindings configured from CLI to dynamic binding learned from DHCP Snooping |
| VLAN            | VLAN number of the client interface                                                             |
| Interface       | Interface that connects to the DHCP client host                                                 |



## Configuring Layer 3 Interfaces

---

This chapter describes the Layer 3 interfaces on a Catalyst 4500 series switch. It also provides guidelines, procedures, and configuration examples.

This chapter includes the following major sections:

- Overview of Layer 3 Interfaces, page 20-1
- Configuration Guidelines, page 20-3
- Configuring Logical Layer 3 VLAN Interfaces, page 20-3
- Configuring Physical Layer 3 Interfaces, page 20-4



**Note**

For complete syntax and usage information for the switch commands used in this chapter, refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference* and the publications at: <http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/index.htm>

---

## Overview of Layer 3 Interfaces

The Catalyst 4500 series switch supports Layer 3 interfaces with the Cisco IOS IP and IP routing protocols. Layer 3, the *network* layer, is primarily responsible for the routing of data in packets across logical internetwork paths.

Layer 2, the *data link* layer, contains the protocols that control the *physical* layer (Layer 1) and how data is framed before being transmitted on the medium. The Layer 2 function of filtering and forwarding data in frames between two segments on a LAN is known as *bridging*.

The Catalyst 4500 series switch supports two types of Layer 3 interfaces. The logical Layer 3 VLAN interfaces integrate the functions of routing and bridging. The physical Layer 3 interfaces allow the Catalyst 4500 series switch to be configured like a traditional router.

This section contains the following subsections:

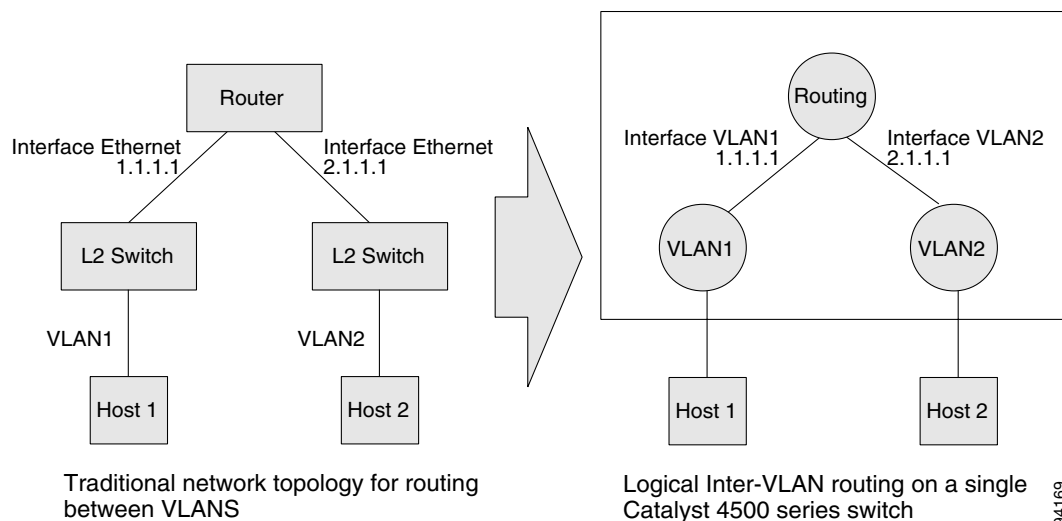
- Logical Layer 3 VLAN Interfaces, page 20-2
- Physical Layer 3 Interfaces, page 20-2

## Logical Layer 3 VLAN Interfaces

The logical Layer 3 VLAN interfaces provide logical routing interfaces to VLANs on Layer 2 switches. A traditional network requires a physical interface from a router to a switch to perform inter-VLAN routing. The Catalyst 4500 series switch supports inter-VLAN routing by integrating the routing and bridging functions on a single Catalyst 4500 series switch.

Figure 20-1 shows how the routing and bridging functions in the three physical devices of the traditional network are performed logically on one Catalyst 4500 series switch.

**Figure 20-1 Logical Layer 3 VLAN Interfaces for the Catalyst 4500 Series Switch**

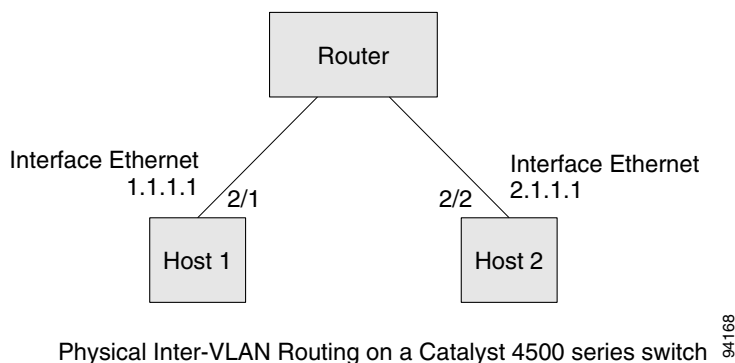


## Physical Layer 3 Interfaces

The physical Layer 3 interfaces support capabilities equivalent to a traditional router. These Layer 3 interfaces provide hosts with physical routing interfaces to a Catalyst 4500 series switch.

Figure 20-2 shows how the Catalyst 4500 series switch functions as a traditional router.

**Figure 20-2 Physical Layer 3 Interfaces for the Catalyst 4500 Series Switch**



# Configuration Guidelines

A Catalyst 4500 series switch supports AppleTalk routing and IPX routing. For AppleTalk routing and IPX routing information, refer to “Configuring AppleTalk” and “Configuring Novell IPX” in the Cisco IOS AppleTalk and Novell IPX Configuration Guide at the following URL:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/atipx\\_c/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/atipx_c/index.htm)

A Catalyst 4500 series switch does not support subinterfaces or the **encapsulation** keyword on Layer 3 Fast Ethernet or Gigabit Ethernet interfaces.

## Configuring Logical Layer 3 VLAN Interfaces



### Note

Before you can configure logical Layer 3 VLAN interfaces, you must create and configure the VLANs on the switch, assign VLAN membership to the Layer 2 interfaces, enable IP routing if IP routing is disabled, and specify an IP routing protocol.

To configure logical Layer 3 VLAN interfaces, perform this task:

|        | Command                                                                                                                                                                                                                                                                                       | Purpose                                    |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------|
| Step 1 | Switch(config)# <b>vlan</b> <i>vlan_ID</i>                                                                                                                                                                                                                                                    | Creates the VLAN.                          |
| Step 1 | Switch(config)# <b>interface</b> <i>vlan</i> <i>vlan_ID</i>                                                                                                                                                                                                                                   | Selects an interface to configure.         |
| Step 2 | Switch(config-if)# <b>ip address</b> <i>ip_address</i> <i>subnet_mask</i>                                                                                                                                                                                                                     | Configures the IP address and IP subnet.   |
| Step 3 | Switch(config-if)# <b>no shutdown</b>                                                                                                                                                                                                                                                         | Enables the interface.                     |
| Step 4 | Switch(config-if)# <b>end</b>                                                                                                                                                                                                                                                                 | Exits configuration mode.                  |
| Step 5 | Switch# <b>copy running-config startup-config</b>                                                                                                                                                                                                                                             | Saves your configuration changes to NVRAM. |
| Step 6 | Switch# <b>show interfaces</b> [ <i>type slot/interface</i> ]<br>Switch# <b>show ip interfaces</b> [ <i>type slot/interface</i> ]<br>Switch# <b>show running-config interfaces</b> [ <i>type slot/interface</i> ]<br>Switch# <b>show running-config interfaces</b> <i>vlan</i> <i>vlan_ID</i> | Verifies the configuration.                |

This example shows how to configure the logical Layer 3 VLAN interface *vlan 2* and assign an IP address:

```
Switch> enable
Switch# config term
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# vlan 2
Switch(config)# interface vlan 2
Switch(config-if)# ip address 10.1.1.1 255.255.255.248
Switch(config-if)# no shutdown
Switch(config-if)# end
```

This example uses the **show interfaces** command to display the interface IP address configuration and status of Layer 3 VLAN interface vlan 2:

```
Switch# show interfaces vlan 2
Vlan2 is up, line protocol is down
 Hardware is Ethernet SVI, address is 00D.588F.B604 (bia 00D.588F.B604)
 Internet address is 172.20.52.106/29
 MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
 reliability 255/255, txload 1/255, rxload 1/255
 Encapsulation ARPA, loopback not set
 ARP type: ARPA, ARP Timeout 04:00:00
 Last input never, output never, output hang never
 Last clearing of "show interface" counters never
 Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
 Queueing strategy: fifo
 Output queue: 0/40 (size/max)
 5 minute input rate 0 bits/sec, 0 packets/sec
 5 minute output rate 0 bits/sec, 0 packets/sec
 0 packets input, 0 bytes, 0 no buffer
 Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
 0 packets output, 0 bytes, 0 underruns
 0 output errors, 0 interface resets
 0 output buffer failures, 0 output buffers swapped out
Switch#
```

This example uses the **show running-config** command to display the interface IP address configuration of Layer 3 VLAN interface vlan 2:

```
Switch# show running-config
Building configuration...

Current configuration : !
interface Vlan2
 ip address 10.1.1.1 255.255.255.248
 !
 ip classless
 no ip http server
 !
 !
 line con 0
 line aux 0
 line vty 0 4
 !
end
```

## Configuring Physical Layer 3 Interfaces



### Note

Before you can configure physical Layer 3 interfaces, you must enable IP routing if IP routing is disabled, and specify an IP routing protocol.

To configure physical Layer 3 interfaces, perform this task:

|               | Command                                                                                                                                                                                                           | Purpose                                                                 |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| <b>Step 1</b> | Switch(config)# <b>ip routing</b>                                                                                                                                                                                 | Enables IP routing (Required only if disabled.)                         |
| <b>Step 1</b> | Switch(config)# <b>interface</b> { <b>fastethernet</b>   <b>gigabitethernet</b> } <i>slot/port</i>   { <b>port-channel</b> <i>port_channel_number</i> }                                                           | Selects an interface to configure.                                      |
| <b>Step 2</b> | Switch(config-if)# <b>no switchport</b>                                                                                                                                                                           | Converts this port from physical Layer 2 port to physical Layer 3 port. |
| <b>Step 3</b> | Switch(config-if)# <b>ip address</b> <i>ip_address subnet_mask</i>                                                                                                                                                | Configures the IP address and IP subnet.                                |
| <b>Step 4</b> | Switch(config-if)# <b>no shutdown</b>                                                                                                                                                                             | Enables the interface.                                                  |
| <b>Step 5</b> | Switch(config-if)# <b>end</b>                                                                                                                                                                                     | Exits configuration mode.                                               |
| <b>Step 6</b> | Switch# <b>copy running-config startup-config</b>                                                                                                                                                                 | Saves your configuration changes to NVRAM.                              |
| <b>Step 7</b> | Switch# <b>show interfaces</b> [ <i>type slot/interface</i> ]<br>Switch# <b>show ip interfaces</b> [ <i>type slot/interface</i> ]<br>Switch# <b>show running-config interfaces</b> [ <i>type slot/interface</i> ] | Verifies the configuration.                                             |

This example shows how to configure an IP address on Fast Ethernet interface 2/1:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip routing
Switch(config)# interface fastethernet 2/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.1.1.1 255.255.255.248
Switch(config-if)# no shutdown
Switch(config-if)# end
Switch#
```

This example uses the **show running-config** command to display the interface IP address configuration of Fast Ethernet interface 2/1:

```
Switch# show running-config
Building configuration...
!
interface FastEthernet2/1
 no switchport
 ip address 10.1.1.1 255.255.255.248
!
...
ip classless
no ip http server
!
!
line con 0
line aux 0
line vty 0 4
!
end
```







# Configuring Cisco Express Forwarding

This chapter describes Cisco Express Forwarding (CEF) on the Catalyst 4500 series switch. It also provides guidelines, procedures, and examples to configure this feature.

This chapter includes the following major sections:

- Overview of CEF, page 21-1
- Catalyst 4500 Series Switch Implementation of CEF, page 21-3
- CEF Configuration Restrictions, page 21-6
- Configuring CEF, page 21-6
- Monitoring and Maintaining CEF, page 21-8



## Note

For complete syntax and usage information for the switch commands used in this chapter, refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference* and the publications at: <http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/index.htm>

## Overview of CEF

This section contains information on the two primary components that comprise the CEF operation:

- Benefits of CEF, page 21-1
- Forwarding Information Base, page 21-2
- Adjacency Tables, page 21-2

## Benefits of CEF

CEF is advanced Layer 3 IP switching technology that optimizes performance and scalability for large networks with dynamic traffic patterns or networks with intensive web-based applications and interactive sessions.

CEF provides the following benefits:

- Improves performance over the caching schemes of multilayer switches, which often flush the entire cache when information changes in the routing tables.

- Provides load balancing that distributes packets across multiple links based on Layer 3 routing information. If a network device discovers multiple paths to a destination, the routing table is updated with multiple entries for that destination. Traffic to that destination is then distributed among the various paths.

CEF stores information in several data structures rather than the route cache of multilayer switches. The data structures optimize lookup for efficient packet forwarding.

## Forwarding Information Base

The Forwarding Information Base (FIB) is a table that contains a copy of the forwarding information in the IP routing table. When routing or topology changes occur in the network, the route processor updates the IP routing table and CEF updates the FIB. Because there is a one-to-one correlation between FIB entries and routing table entries, the FIB contains all known routes and eliminates the need for route cache maintenance that is associated with switching paths, such as fast switching and optimum switching. CEF uses the FIB to make IP destination-based switching decisions and maintain next-hop address information based on the information in the IP routing table.

On the Catalyst 4500 series switches, CEF loads the FIB in to the Integrated Switching Engine hardware to increase the performance of forwarding. The Integrated Switching Engine has a finite number of forwarding slots for storing routing information. If this limit is exceeded, CEF is automatically disabled and all packets are forwarded in software. In this situation, you should reduce the number of routes on the switch and then reenable hardware switching with the **ip cef** command.

## Adjacency Tables

In addition to the FIB, CEF uses adjacency tables to prepend Layer 2 addressing information. Nodes in the network are said to be *adjacent* if they are within a single hop from each other. The adjacency table maintains Layer 2 next-hop addresses for all FIB entries.

## Adjacency Discovery

The adjacency table is populated as new adjacent nodes are discovered. Each time an adjacency entry is created (such as through the Address Resolution Protocol (ARP), a link-layer header for that adjacent node is stored in the adjacency table. Once a route is determined, the link-layer header points to a next hop and corresponding adjacency entry. The link-layer header is subsequently used for encapsulation during CEF switching of packets.

## Adjacency Resolution

A route might have several paths to a destination prefix, such as when a router is configured for simultaneous load balancing and redundancy. For each resolved path, a pointer is added for the adjacency corresponding to the next-hop interface for that path. This mechanism is used for load balancing across several paths.

## Adjacency Types That Require Special Handling

In addition to adjacencies for next-hop interfaces (host-route adjacencies), other types of adjacencies are used to expedite switching when certain exception conditions exist. When the prefix is defined, prefixes requiring exception processing are cached with one of the special adjacencies listed in Table 21-1.

**Table 21-1 Adjacency Types for Exception Processing**

| This adjacency type... | Receives this processing...                                                                                                                                                                                                                                                                                               |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Null adjacency         | Packets destined for a Null0 interface are dropped. A Null0 interface can be used as an effective form of access filtering.                                                                                                                                                                                               |
| Glean adjacency        | When a router is connected directly to several hosts, the FIB table on the router maintains a prefix for the subnet rather than for each individual host. The subnet prefix points to a glean adjacency. When packets need to be forwarded to a specific host, the adjacency database is gleaned for the specific prefix. |
| Punt adjacency         | Features that require special handling or features that are not yet supported by CEF switching are sent (punted) to the next higher switching level.                                                                                                                                                                      |
| Discard adjacency      | Packets are discarded.                                                                                                                                                                                                                                                                                                    |
| Drop adjacency         | Packets are dropped.                                                                                                                                                                                                                                                                                                      |

## Unresolved Adjacency

When a link-layer header is prepended to packets, FIB requires the prepend to point to an adjacency corresponding to the next hop. If an adjacency was created by FIB and was not discovered through a mechanism such as ARP, the Layer 2 addressing information is not known and the adjacency is considered incomplete. When the Layer 2 information is known, the packet is forwarded to the route processor, and the adjacency is determined through ARP.

# Catalyst 4500 Series Switch Implementation of CEF

This section contains the following subsections:

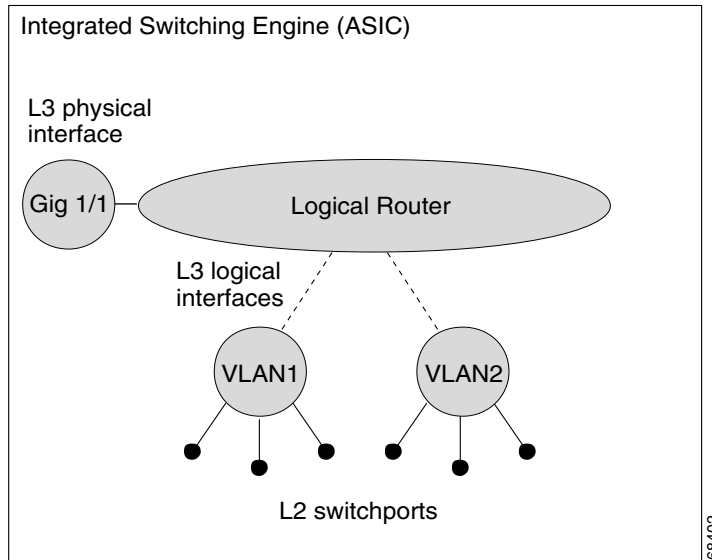
- Hardware and Software Switching, page 21-4
- Load Balancing, page 21-6
- Software Interfaces, page 21-6

The Catalyst 4500 series switches support an ASIC-based Integrated Switching Engine that provides these features:

- Ethernet bridging at Layer 2
- IP routing at Layer 3

Because the ASIC is specifically designed to forward packets, the Integrated Switching Engine hardware can run this process much faster than CPU subsystem software.

Figure 21-1 shows a high-level view of the ASIC-based Layer 2 and Layer 3 switching process on the Integrated Switching Engine.

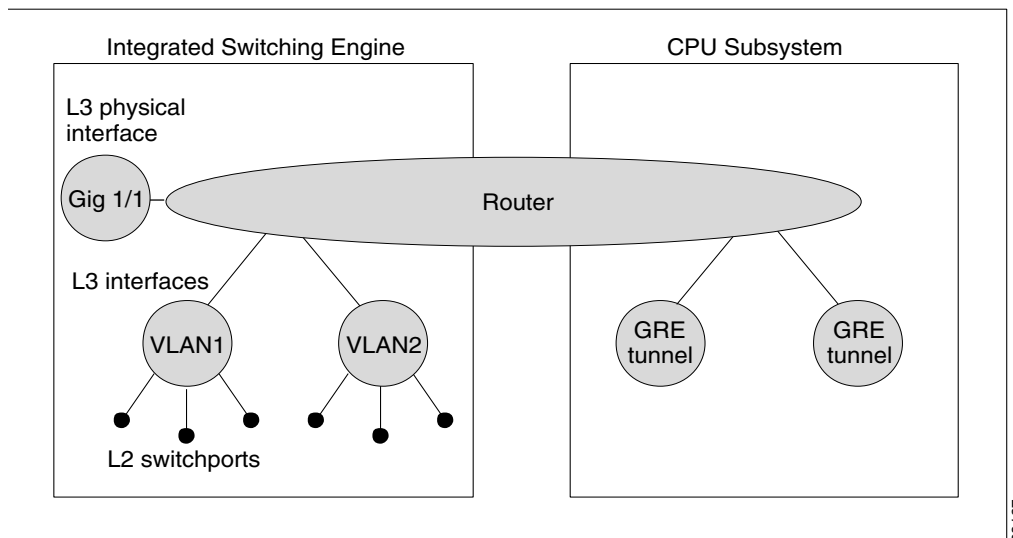
**Figure 21-1 Logical L2/L3 Switch Components**

The Integrated Switching Engine performs inter-VLAN routing on logical Layer 3 interfaces with the ASIC hardware. The ASIC hardware also supports a physical Layer 3 interface that can be configured to connect with a host, a switch, or a router.

## Hardware and Software Switching

For the majority of packets, the Integrated Switching Engine performs the packet forwarding function in hardware. These packets are hardware-switched at very high rates. Exception packets are forwarded by the CPU subsystem software. Statistic reports should show that the Integrated Switching Engine is forwarding the vast majority of packets in hardware. Software forwarding is significantly slower than hardware forwarding, but packets forwarded by the CPU subsystem do not reduce hardware forwarding speed.

Figure 21-2 shows a logical view of the Integrated Switching Engine and the CPU subsystem switching components.

**Figure 21-2 Hardware and Software Switching Components**

The Integrated Switching Engine performs inter-VLAN routing in hardware. The CPU subsystem software supports Layer 3 interfaces to VLANs that use Subnetwork Access Protocol (SNAP) encapsulation. The CPU subsystem software also supports generic routing encapsulation (GRE) tunnel.

## Hardware Switching

Hardware switching is the normal operation for the Supervisor Engine III and Supervisor Engine IV.

## Software Switching

Software switching occurs when traffic cannot be processed in hardware. The following types of exception packets are processed in software at a much slower rate:

- Packets that use IP header options



### Note

Packets that use TCP header options are switched in hardware because they do not affect the forwarding decision.

- Packets that have an expiring IP time-to-live (TTL) counter
- Packets that are forwarded to a tunnel interface
- Packets that arrive with non-supported encapsulation types
- Packets that are routed to an interface with non-supported encapsulation types
- Packets that exceed the MTU of an output interface and must be fragmented
- Packets that require an IGMP redirect to be routed
- 802.3 Ethernet packets

## Load Balancing

The Catalyst 4500 series switch supports load balancing for routing packets in the Integrated Switching Engine hardware. Load balancing is always enabled. It works when multiple routes for the same network with different next-hop addresses are configured. These routes can be configured either statically or through a routing protocol such as OSPF or EIGRP.

The hardware makes a forwarding decision by using a hardware load sharing hash function to compute a value, based on the source and destination IP addresses and the source and destination TCP port numbers (if available). This load sharing hash value is then used to select which route to use to forward the packet. All hardware switching within a particular flow (such as a TCP connection) will be routed to the same next hop, thereby reducing the chance that packet reordering will occur. Up to eight different routes for a particular network are supported.

## Software Interfaces

Cisco IOS for the Catalyst 4500 series switch supports GRE and IP tunnel interfaces that are not part of the hardware forwarding engine. All packets that flow to or from these interfaces must be processed in software and will have a significantly lower forwarding rate than that of hardware-switched interfaces. Also, Layer 2 features are not supported on these interfaces.

## CEF Configuration Restrictions

The Integrated Switching Engine supports only ARPA and ISL/802.1q encapsulation types for Layer 3 switching in hardware. The CPU subsystem supports a number of encapsulations such as SNAP for Layer 2 switching that you can use for Layer 3 switching in software.

## Configuring CEF

These sections describe how to configure CEF:

- Enabling CEF, page 21-6
- Configuring Load Balancing for CEF, page 21-7

**Note**

---

The **ip mtu** command is not supported in this release.

---

## Enabling CEF

**Note**

By default, CEF is enabled globally on the Catalyst 4500 series switch. No configuration is required.

---

When you disable CEF, Cisco IOS software forwards packets using the CPU subsystem software. Do not disable CEF for normal operation.

---

To disable CEF, perform this task:

| Command                          | Purpose                 |
|----------------------------------|-------------------------|
| Switch(config)# <b>no ip cef</b> | Disables CEF operation. |

To reenable CEF, perform this task:

| Command                       | Purpose                         |
|-------------------------------|---------------------------------|
| Switch(config)# <b>ip cef</b> | Enables standard CEF operation. |

## Configuring Load Balancing for CEF

CEF load balancing is based on a combination of source and destination packet information; it allows you to optimize resources by distributing traffic over multiple paths for transferring data to a destination. You can configure load balancing on a per-destination basis. Load-balancing decisions are made on the outbound interface. You can configure per-destination load balancing for CEF on outbound interfaces.

The following topics are discussed:

- Configuring Per-Destination Load Balancing, page 21-7
- Configuring Load Sharing Hash Function, page 21-8
- Viewing CEF Information, page 21-8

## Configuring Per-Destination Load Balancing

Per-destination load balancing is enabled by default when you enable CEF. To use per-destination load balancing, you do not perform any additional tasks once you enable CEF.

Per-destination load balancing allows the router to use multiple paths to achieve load sharing. Packets for a given source-destination host pair are guaranteed to take the same path, even if multiple paths are available. Traffic destined for different pairs tend to take different paths. Per-destination load balancing is enabled by default when you enable CEF; it is the load balancing method of choice in most situations.

Because per-destination load balancing depends on the statistical distribution of traffic, load sharing becomes more effective as the number of source-destination pairs increases.

You can use per-destination load balancing to ensure that packets for a given host pair arrive in order. All packets for a certain host pair are routed over the same link or links.

### Disabling Per-Destination Load Balancing

To disable per-destination load balancing, perform this task:

| Command                                                       | Purpose                                  |
|---------------------------------------------------------------|------------------------------------------|
| Switch (config-if)# <b>no ip load-sharing per-destination</b> | Disables per-destination load balancing. |

## Configuring Load Sharing Hash Function

When multiple unicast routes exist to a particular destination IP prefix, the hardware will send packets matching that prefix across all possible routes, thereby sharing the load across all next hop routers. By default, the route used is chosen by computing a hash of the source and destination IP addresses and using the resulting value to select the route. This preserves packet ordering for packets within a flow by ensuring that all packets within a single IP source/destination flow are sent on the same route, but it provides a near-random distribution of flows to routes.

The load-sharing hash function can be changed, so that in addition to the source and destination IP addresses, the source TCP/UDP port, the destination TCP/UDP port, or both can also be included in the hash.

To the configure load sharing hash function to use the source and/or destination ports, perform this task:

| Command                                                                               | Purpose                                                                                                                                                                   |
|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Switch (config)# [no] ip cef load-sharing algorithm include-ports source destination] | Enables load sharing hash function to use source and destination ports.<br><br>Use the <b>no</b> keyword to set the switch to use the default IOS load-sharing algorithm. |

For more information on load sharing, refer to the *Configuring Cisco Express Forwarding* module of the Cisco IOS documentation at:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgr/switch\\_c/xcprt2/xcdcefc.htm#xtocid0](http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgr/switch_c/xcprt2/xcdcefc.htm#xtocid0)



### Note

The **include-ports** option does not apply to software-switched traffic on the Catalyst 4500 series switches.

## Viewing CEF Information

You can view the collected CEF information. To do so, perform this task:

| Command             | Purpose                                 |
|---------------------|-----------------------------------------|
| Switch# show ip cef | Displays the collected CEF information. |

## Monitoring and Maintaining CEF

To display information about IP traffic, perform this task:

| Command                                               | Purpose                                   |
|-------------------------------------------------------|-------------------------------------------|
| Switch# show interface type slot/interface   begin L3 | Displays a summary of IP unicast traffic. |

This example shows how to display information about IP unicast traffic on interface Fast Ethernet 3/3:

```
Switch# show interface fastethernet 3/3 | begin L3
```



```

L3 in Switched: ucast: 0 pkt, 0 bytes - mcast: 12 pkt, 778 bytes mcast
L3 out Switched: ucast: 0 pkt, 0 bytes - mcast: 0 pkt, 0 bytes
4046399 packets input, 349370039 bytes, 0 no buffer
Received 3795255 broadcasts, 2 runts, 0 giants, 0 throttles
<...output truncated...>
Switch#

```

**Note**

The IP unicast packet count is updated approximately every five seconds.

## Displaying IP Statistics

IP unicast statistics are gathered on a per-interface basis. To display IP statistics, perform this task:

| Command                                                   | Purpose                 |
|-----------------------------------------------------------|-------------------------|
| Switch# <b>show interface type number counters detail</b> | Displays IP statistics. |

This example shows how to display IP unicast statistics for Part 3/1:

```
Switch# show interface fastethernet 3/1 counters detail
```

|       |                  |                   |                  |                   |
|-------|------------------|-------------------|------------------|-------------------|
| Port  | InBytes          | InUcastPkts       | InMcastPkts      | InBcastPkts       |
| Fa3/1 | 7263539133       | 5998222           | 6412307          | 156               |
| Port  | OutBytes         | OutUcastPkts      | OutMcastPkts     | OutBcastPkts      |
| Fa3/1 | 7560137031       | 5079852           | 12140475         | 38                |
| Port  | InPkts 64        | OutPkts 64        | InPkts 65-127    | OutPkts 65-127    |
| Fa3/1 | 11274            | 168536            | 7650482          | 12395769          |
| Port  | InPkts 128-255   | OutPkts 128-255   | InPkts 256-511   | OutPkts 256-511   |
| Fa3/1 | 31191            | 55269             | 26923            | 65017             |
| Port  | InPkts 512-1023  | OutPkts 512-1023  |                  |                   |
| Fa3/1 | 133807           | 151582            |                  |                   |
| Port  | InPkts 1024-1518 | OutPkts 1024-1518 | InPkts 1519-1548 | OutPkts 1519-1548 |
| Fa3/1 | N/A              | N/A               | N/A              | N/A               |
| Port  | InPkts 1024-1522 | OutPkts 1024-1522 | InPkts 1523-1548 | OutPkts 1523-1548 |
| Fa3/1 | 4557008          | 4384192           | 0                | 0                 |
| Port  | Tx-Bytes-Queue-1 | Tx-Bytes-Queue-2  | Tx-Bytes-Queue-3 | Tx-Bytes-Queue-4  |
| Fa3/1 | 64               | 0                 | 91007            | 7666686162        |
| Port  | Tx-Drops-Queue-1 | Tx-Drops-Queue-2  | Tx-Drops-Queue-3 | Tx-Drops-Queue-4  |
| Fa3/1 | 0                | 0                 | 0                | 0                 |
| Port  | Rx-No-Pkt-Buff   | RxPauseFrames     | TxPauseFrames    | PauseFramesDrop   |
| Fa3/1 | 0                | 0                 | 0                | N/A               |
| Port  | UnsupOpcodePause |                   |                  |                   |
| Fa3/1 | 0                |                   |                  |                   |

Switch#

To display CEF (software switched) and hardware IP unicast adjacency table information, perform this task:

| Command                                                                                                 | Purpose                                                                                                                  |
|---------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| Switch# <b>show adjacency</b> [ <i>interface</i> ] [ <b>detail</b>   <b>internal</b>   <b>summary</b> ] | Displays detailed adjacency information, including Layer 2 information, when the optional <b>detail</b> keyword is used. |

This example shows how to display adjacency statistics:

```
Switch# show adjacency gigabitethernet 3/5 detail
Protocol Interface Address
IP GigabitEthernet9/5 172.20.53.206 (11)
504 packets, 6110 bytes
00605C865B82
000164F83FA50800
ARP 03:49:31
```



**Note**

Adjacency statistics are updated approximately every 10 seconds.



## Configuring Policy-Based Routing

This chapter describes the tasks for configuring policy-based routing (PBR) on a router and includes these major sections:

- Overview of Policy-Based Routing, page 22-1
- Policy-Based Routing Configuration Task List, page 22-2
- Policy-Based Routing Configuration Examples, page 22-4



### Note

For a complete description of the PBR commands in this chapter, refer to the *Cisco IOS Quality of Service Solutions Command Reference*.



### Note

To identify the hardware platform or software image information associated with a feature, use the Feature Navigator on Cisco.com to search for information about the feature or refer to the software release notes for a specific release.

## Overview of Policy-Based Routing

PBR gives you a flexible means of routing packets by allowing you to configure a defined policy for traffic flows, lessening reliance on routes derived from routing protocols. To this end, PBR gives you more control over routing by extending and complementing the existing mechanisms provided by routing protocols. PBR allows you to specify a path for certain traffic, such as priority traffic over a high-cost link.

You can set up PBR as a way to route packets based on configured policies. For example, you can implement routing policies to allow or deny paths based on the identity of a particular end system, an application protocol, or the size of packets.

PBR allows you to perform the following tasks:

- Classify traffic based on extended access list criteria. Access lists, then establish the match criteria.
- Route packets to specific traffic-engineered paths.

Policies can be based on IP address, port numbers, or protocols. For a simple policy, you can use any one of these descriptors; for a complicated policy, you can use all of them.

## Understanding PBR

All packets received on an interface with PBR enabled are passed through enhanced packet filters known as route maps. The route maps used by PBR dictate the policy, determining to where the packets are forwarded.

Route maps are composed of statements. The route map statements can be marked as permit or deny, and they are interpreted in the following ways:

- If a statement is marked as deny, the packets meeting the match criteria are sent back through the normal forwarding channels and destination-based routing is performed.
- If the statement is marked as permit and a packet matches the access-lists, then the first valid set clause is applied to that packet.

You specify PBR on the incoming interface (the interface on which packets are received), not outgoing interface.

## Using Policy-Based Routing

You might enable PBR if you want certain packets to be routed some way other than the obvious shortest path. For example, PBR can be used to provide the following functionality:

- equal access
- protocol-sensitive routing
- source-sensitive routing
- routing based on interactive versus batch traffic
- routing based on dedicated links

Some applications or traffic can benefit from source-specific routing; for example, you could transfer stock records to a corporate office on a higher-bandwidth, higher-cost link for a short time while sending routine application data such as e-mail over a lower-bandwidth, lower-cost link.

## Policy-Based Routing Configuration Task List

To configure PBR, perform the tasks described in the following sections. The task in the first section is required; the tasks in the remaining sections are optional.

- Enabling PBR (Required)
- Enabling Local PBR (Optional)

See the end of this chapter for the section “Policy-Based Routing Configuration Examples.”

## Enabling PBR

To enable PBR, you must create a route map that specifies the match criteria and the resulting action if all of the match clauses are met. Then, you must enable PBR for that route map on a particular interface. All packets arriving on the specified interface matching the match clauses will be subject to PBR.

To enable PBR on an interface, perform this task:

|        | Command                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch(config)# <b>route-map</b> <i>map-tag</i> [ <b>permit</b>   <b>deny</b> ] [ <i>sequence-number</i> ]                                                                                                                                                                                                                                                                                                                                                                                   | Defines a route map to control where packets are output. This command puts the router into route-map configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Step 2 | Switch(config-route-map)# <b>match ip address</b> { <i>access-list-number</i>   <i>name</i> }<br>[... <i>access-list-number</i>   <i>name</i> ]                                                                                                                                                                                                                                                                                                                                              | Specifies the match criteria. Matches the source and destination IP address that is permitted by one or more standard or extended access lists.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Step 3 | Switch(config-route-map)# <b>set ip next-hop</b> <i>ip-address</i> [... <i>ip-address</i> ]<br><br>Switch(config-route-map)# <b>set interface</b> <i>interface-type</i> <i>interface-number</i> [... <i>type</i> <i>number</i> ]<br><br>Switch(config-route-map)# <b>set ip default next-hop</b> <i>ip-address</i> [... <i>ip-address</i> ]<br><br>Switch(config-route-map)# <b>set default interface</b> <i>interface-type</i> <i>interface-number</i> [... <i>type</i> ... <i>number</i> ] | Specifies the action or actions to take on the packets that match the criteria. You can specify any or all of the following: <ul style="list-style-type: none"> <li>Specifies the next hop for which to route the packet (the next hop must be adjacent). This behavior is identical to a next hop specified in the normal routing table.</li> <li>Sets output interface for the packet. This action specifies that the packet is forwarded out of the local interface. The interface must be a Layer 3 interface (no switchports), and the destination address in the packet must lie within the IP network assigned to that interface. If the destination address for the packet does not lie within that network, the packet is dropped.</li> <li>Sets next hop to which to route the packet if there is no explicit route for this destination. Before forwarding the packet to the next hop, the switch looks up the packet's destination address in the unicast routing table. If a match is found, the packet is forwarded by way of the routing table. If no match is found, the packet is forwarded to the specified next hop.</li> <li>Sets output interface for the packet if there is no explicit route for this destination. Before forwarding the packet to the next hop, the switch looks up the packet's destination address in the unicast routing table. If a match is found, the packet is forwarded via the routing table. If no match is found, the packet is forwarded to the specified output interface. If the destination address for the packet does not lie within that network, the packet is dropped.</li> </ul> |
| Step 4 | Switch(config-route-map)# <b>interface</b> <i>interface-type</i> <i>interface-number</i>                                                                                                                                                                                                                                                                                                                                                                                                     | Specifies the interface. This command puts the router into interface configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Step 5 | Switch(config-if)# <b>ip policy route-map</b> <i>map-tag</i>                                                                                                                                                                                                                                                                                                                                                                                                                                 | Identifies the route map to use for PBR. One interface can only have one route map tag, but you can have multiple route map entries with different sequence numbers. These entries are evaluated in sequence number order until the first match. If there is no match, packets will be routed as usual.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

The **set** commands can be used in conjunction with each other. These commands are evaluated in the order shown in Step 3 in the previous task table. A usable next hop implies an interface. Once the local router finds a next hop and a usable interface, it routes the packet.

## Enabling Local PBR

Packets that are generated by the router are not normally policy-routed. To enable local PBR for such packets, indicate which route map the router should use by performing this task:

| Command                                                         | Purpose                                        |
|-----------------------------------------------------------------|------------------------------------------------|
| Switch(config)# <b>ip local policy route-map</b> <i>map-tag</i> | Identifies the route map to use for local PBR. |

All packets originating on the router will then be subject to local PBR.

Use the **show ip local policy** command to display the route map used for local PBR, if one exists.

## Unsupported Commands

The following PBR commands in config-route-map mode are in the CLI but not supported in Cisco IOS for the Catalyst 4500 series switches. If you attempt to use these commands, an error message displays.

- **match-length**
- **set ip qos**
- **set ip tos**
- **set ip precedence**

## Policy-Based Routing Configuration Examples

The following sections provide PBR configuration examples:

- Equal Access Example
- Differing Next Hops Example
- Deny ACE Example

For information on how to configure policy-based routing, see the section “Policy-Based Routing Configuration Task List” in this chapter.

### Equal Access Example

The following example provides two sources with equal access to two different service providers. Packets arriving on fastethernet interface 1 from the source 1.1.1.1 are sent to the router at 6.6.6.6 if the router has no explicit route for the destination of the packet. Packets arriving from the source 2.2.2.2 are sent to the router at 7.7.7.7 if the router has no explicit route for the destination of the packet. All other packets for which the router has no explicit route to the destination are discarded.

```
Switch (config)# access-list 1 permit ip 1.1.1.1
access-list 2 permit ip 2.2.2.2
!
interface fastethernet 1
 ip policy route-map equal-access
!
route-map equal-access permit 10
 match ip address 1
```

```
set ip default next-hop 6.6.6.6
route-map equal-access permit 20
match ip address 2
set ip default next-hop 7.7.7.7
route-map equal-access permit 30
set default interface null0
```

**Note**

If the packets you want dropped do not match either of the first two route-map clauses, then change **set default interface null0** to **set interface null0**.

## Differing Next Hops Example

The following example illustrates how to route traffic from different sources to different places (next hops). Packets arriving from source 1.1.1.1 are sent to the next hop at 3.3.3.3; packets arriving from source 2.2.2.2 are sent to the next hop at 3.3.3.5.

```
access-list 1 permit ip 1.1.1.1
access-list 2 permit ip 2.2.2.2
!
interface ethernet 1
 ip policy route-map Texas
!
route-map Texas permit 10
 match ip address 1
 set ip next-hop 3.3.3.3
!
route-map Texas permit 20
 match ip address 2
 set ip next-hop 3.3.3.5
```

## Deny ACE Example

The following example illustrates how to stop processing a given route map sequence, and to jump to the next sequence. Packets arriving from source 1.1.1.1 will skip sequence 10 and jump to sequence 20. All other packets from subnet 1.1.1.0 will follow the set statement in sequence 10.

```
access-list 1 deny ip 1.1.1.1
access-list 1 permit ip 1.1.1.0 0.0.0.255
access-list 2 permit ip 1.1.1.1
access-list 2 permit ip 2.2.2.2
!
interface ethernet 1
 ip policy route-map Texas
!
route-map Texas permit 10
 match ip address 1
 set ip next-hop 3.3.3.3
!
route-map Texas permit 20
 match ip address 2
 set ip next-hop 3.3.3.5
```







## Understanding and Configuring IP Multicast

This chapter describes IP multicast routing on the Catalyst 4500 series switch. It also provides procedures and examples to configure IP multicast routing.



**Note**

For complete syntax and usage information for the switch commands used in this chapter, refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference* and the publications at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/index.htm>



**Note**

For more detailed information on IP multicast, refer to the discussion at: [http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr\\_c/ipcpt3/](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcpt3/)

This chapter includes the following major sections:

- Overview of IP Multicast, page 23-1
- Configuring IP Multicast Routing, page 23-12
- Monitoring and Maintaining IP Multicast Routing, page 23-15
- Configuration Examples, page 23-21

## Overview of IP Multicast

This section includes these subsections:

- IP Multicast Protocols, page 23-2
- IP Multicast on the Catalyst 4500 Series Switch, page 23-4
- Unsupported Features, page 23-12

At one end of the IP communication spectrum is IP unicast, where a source IP host sends packets to a specific destination IP host. In IP unicast, the destination address in the IP packet is the address of a single, unique host in the IP network. These IP packets are forwarded across the network from the source to the destination host by routers. At each point on the path between source and destination, a router uses a unicast routing table to make unicast forwarding decisions, based on the IP destination address in the packet.

At the other end of the IP communication spectrum is an IP broadcast, where a source host sends packets to all hosts on a network segment. The destination address of an IP broadcast packet has the host portion of the destination IP address set to all ones and the network portion set to the address of the subnet. IP hosts, including routers, understand that packets, which contain an IP broadcast address as the destination address, are addressed to all IP hosts on the subnet. Unless specifically configured otherwise, routers do not forward IP broadcast packets, so IP broadcast communication is normally limited to a local subnet.

IP multicasting falls between IP unicast and IP broadcast communication. IP multicast communication enables a host to send IP packets to a *group* of hosts anywhere within the IP network. To send information to a specific group, IP multicast communication uses a special form of IP destination address called an *IP multicast group address*. The IP multicast group address is specified in the IP destination address field of the packet.

To multicast IP information, Layer 3 switches and routers must forward an incoming IP packet to all output interfaces that lead to *members* of the IP multicast group. In the multicasting process on the Catalyst 4500 series switch, a packet is replicated in the Integrated Switching Engine, forwarded to the appropriate output interfaces, and sent to each member of the multicast group.

It is not uncommon for people to think of IP multicasting and video conferencing as almost the same thing. Although the first application in a network to use IP multicast is often video conferencing, video is only one of many IP multicast applications that can add value to a company's business model. Other IP multicast applications that have potential for improving productivity include multimedia conferencing, data replication, real-time data multicasts, and simulation applications.

This section contains the following subsections:

- IP Multicast Protocols, page 23-2
- IP Multicast on the Catalyst 4500 Series Switch, page 23-4
- Unsupported Features, page 23-12

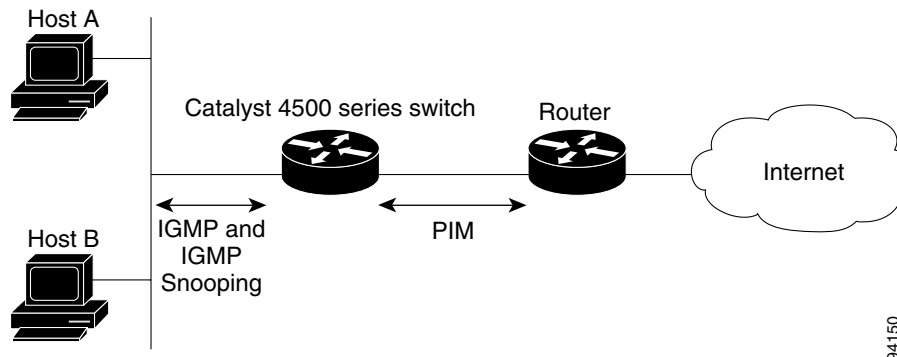
## IP Multicast Protocols

The Catalyst 4500 series switch primarily uses these protocols to implement IP multicast routing:

- Internet Group Management Protocol (IGMP)
- Protocol Independent Multicast (PIM)
- IGMP snooping and Cisco Group Management Protocol

Figure 23-1 shows where these protocols operate within the IP multicast environment.

Figure 23-1 IP Multicast Routing Protocols



## Internet Group Management Protocol

IGMP messages are used by IP multicast hosts to send their local Layer 3 switch or router a request to join a specific multicast group and begin receiving multicast traffic. With some extensions in IGMPv2, IP hosts can also send a request to a Layer 3 switch or router to leave an IP multicast group and not receive the multicast group traffic.

Using the information obtained via IGMP, a Layer 3 switch or router maintains a list of multicast group memberships on a per-interface basis. A multicast group membership is active on an interface if at least one host on the interface sends an IGMP request to receive multicast group traffic.

## Protocol-Independent Multicast

PIM is *protocol independent* because it can leverage whichever unicast routing protocol is used to populate the unicast routing table, including EIGRP, OSPF, BGP, or static route, to support IP multicast. PIM also uses a unicast routing table to perform the reverse path forwarding (RPF) check function instead of building a completely independent multicast routing table. PIM does not send and receive multicast routing updates between routers like other routing protocols do.

### PIM Dense Mode

PIM Dense Mode (PIM-DM) uses a *push* model to flood multicast traffic to every corner of the network. PIM-DM is intended for networks in which most LANs need to receive the multicast, such as LAN TV and corporate or financial information broadcasts. It can be an efficient delivery mechanism if there are active receivers on every subnet in the network.

### PIM Sparse Mode

PIM Sparse Mode (PIM-SM) uses a *pull* model to deliver multicast traffic. Only networks with active receivers that have explicitly requested the data will be forwarded the traffic. PIM-SM is intended for networks with several different multicasts, such as desktop video conferencing and collaborative computing, that go to a small number of receivers and are typically in progress simultaneously.

For more detailed information on PIM Dense and Sparse Mode, refer to this URL:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr\\_c/ipcpt3](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcpt3).

## IGMP Snooping and CGMP

IGMP snooping is used for multicasting in a Layer 2 switching environment. With IGMP snooping, a Layer 3 switch or router examines Layer 3 information in the IGMP packets in transit between hosts and a router. When the switch receives the IGMP Host Report from a host for a particular multicast group, the switch adds the host's port number to the associated multicast table entry. When the switch receives the IGMP Leave Group message from a host, it removes the host's port from the table entry.

Because IGMP control messages are transmitted as multicast packets, they are indistinguishable from multicast data if only the Layer 2 header is examined. A switch running IGMP snooping examines every multicast data packet to determine whether it contains any pertinent IGMP control information. If IGMP snooping is implemented on a low end switch with a slow CPU, performance could be severely impacted when data is transmitted at high rates. On the Catalyst 4500 series switches, IGMP snooping is implemented in the forwarding ASIC, so it does not impact the forwarding rate.

**Note**

A Catalyst 4500 series switch can act as a CGMP server for switches that do not support IGMP snooping, such as Catalyst 4500 family switches with Supervisor Engine I and Supervisor Engine II. You cannot configure the switch as a CGMP client. To configure a Catalyst 4500 series switch as a client, use IGMP snooping.

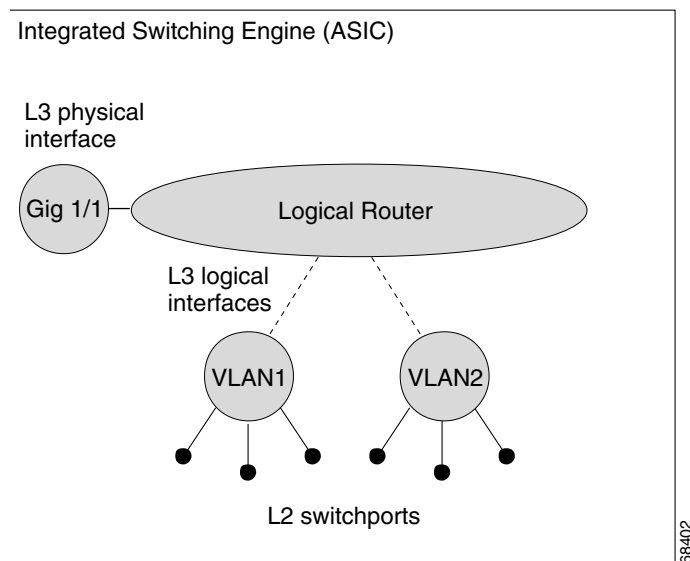
CGMP is a Cisco protocol that allows Catalyst switches to leverage IGMP information on Cisco routers to make Layer 2 forwarding decisions. CGMP is configured on the multicast routers and the Layer 2 switches. As a result, IP multicast traffic is delivered only to those Catalyst switchports with hosts that have requested the traffic. Switchports that have not explicitly requested the traffic will not receive it.

## IP Multicast on the Catalyst 4500 Series Switch

The Catalyst 4500 series switch supports an ASIC-based Integrated Switching Engine that provides Ethernet bridging at Layer 2 and IP routing at Layer 3. Because the ASIC is specifically designed to forward packets, the Integrated Switching Engine hardware provides very high performance with ACLs and QoS enabled. At wire-speed, forwarding in hardware is significantly faster than the CPU subsystem software, which is designed to handle exception packets.

The Integrated Switching Engine hardware supports interfaces for inter-VLAN routing and switchports for Layer 2 bridging. It also provides a physical Layer 3 interface that can be configured to connect with a host, a switch, or a router.

Figure 23-2 shows a logical view of Layer 2 and Layer 3 forwarding in the Integrated Switching Engine hardware.

**Figure 23-2 Logical View of Layer 2 and Layer 3 Forwarding in Hardware**

This section contains the following subsections:

- CEF, MFIB, and Layer 2 Forwarding, page 23-5
- IP Multicast Tables, page 23-7
- Hardware and Software Forwarding, page 23-8
- Non-Reverse Path Forwarding Traffic, page 23-9
- Multicast Fast Drop, page 23-10
- Multicast Forwarding Information Base, page 23-11
- S/M, 224/4, page 23-12

## CEF, MFIB, and Layer 2 Forwarding

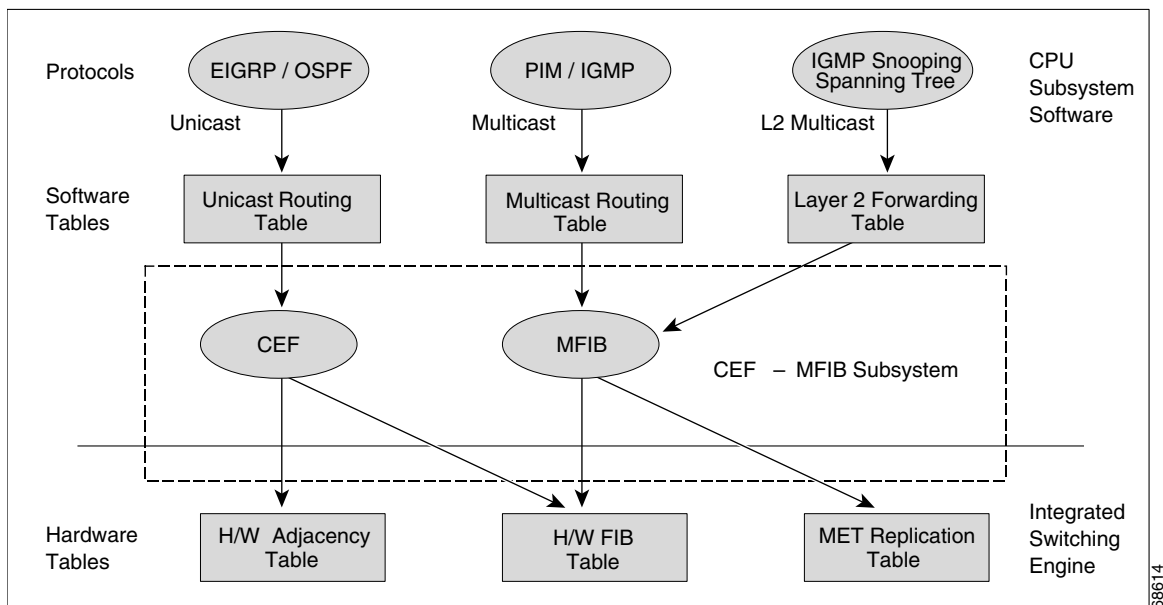
The implementation of IP multicast on the Catalyst 4500 series switch is an extension of centralized Cisco Express Forwarding (CEF). CEF extracts information from the unicast routing table, which is created by unicast routing protocols, such as BGP, OSPF, and EIGR and loads it into the hardware Forwarding Information Base (FIB). With the unicast routes in the FIB, when a route is changed in the upper-layer routing table, only one route needs to be changed in the hardware routing state. To forward unicast packets in hardware, the Integrated Switching Engine looks up source and destination routes in ternary content addressable memory (TCAM), takes the adjacency index from the hardware FIB, and gets the Layer 2 rewrite information and next-hop address from the hardware adjacency table.

The new Multicast Forwarding Information Base (MFIB) subsystem is the multicast analog of the unicast CEF. The MFIB subsystem extracts the multicast routes that PIM and IGMP create and refines them into a protocol-independent format for forwarding in hardware. The MFIB subsystem removes the protocol-specific information and leaves only the essential forwarding information. Each entry in the MFIB table consists of an (S,G) or (\*,G) route, an input RPF VLAN, and a list of Layer 3 output interfaces. The MFIB subsystem, together with platform-dependent management software, loads this multicast routing information into the hardware FIB and hardware multicast expansion table (MET).

The Catalyst 4500 series switch performs Layer 3 routing and Layer 2 bridging at the same time. There can be multiple Layer 2 switchports on any VLAN interface. To determine the set of output switchports on which to forward a multicast packet, the Supervisor Engine III combines Layer 3 MFIB information with Layer 2 forwarding information and stores it in the hardware MET for packet replication.

Figure 23-3 shows a functional overview of how the Catalyst 4500 series switch combines unicast routing, multicast routing, and Layer 2 bridging information to forward in hardware.

**Figure 23-3 Combining CEF, MFIB, and Layer 2 Forwarding Information in Hardware**



Like the CEF unicast routes, the MFIB routes are Layer 3 and must be merged with the appropriate Layer 2 information. The following example shows an MFIB route:

```
(* ,224.1.2.3)
RPF interface is Vlan3
Output Interfaces are:
Vlan 1
Vlan 2
```

The route (\*,224.1.2.3) is loaded in the hardware FIB table and the list of output interfaces is loaded into the MET. A pointer to the list of output interfaces, the MET index, and the RPF interface are also loaded in the hardware FIB with the (\*,224.1.2.3) route. With this information loaded in hardware, merging of the Layer 2 information can begin. For the output interfaces on VLAN1, the Integrated Switching Engine must send the packet to all switchports in VLAN1 that are in the spanning tree forwarding state. The same process applies to VLAN 2. To determine the set of switchports in VLAN 2, the Layer 2 Forwarding Table is used.

When the hardware routes a packet, in addition to sending it to all of the switchports on all output interfaces, the hardware also sends the packet to all switchports (other than the one it arrived on) in the input VLAN. For example, assume that VLAN 3 has two switchports in it, Gig 3/1 and Gig 3/2. If a host on Gig 3/1 sends a multicast packet, the host on Gig 3/2 might also need to receive the packet. To send a multicast packet to the host on Gig 3/2, all of the switchports in the ingress VLAN must be added to the portset that is loaded in the MET.

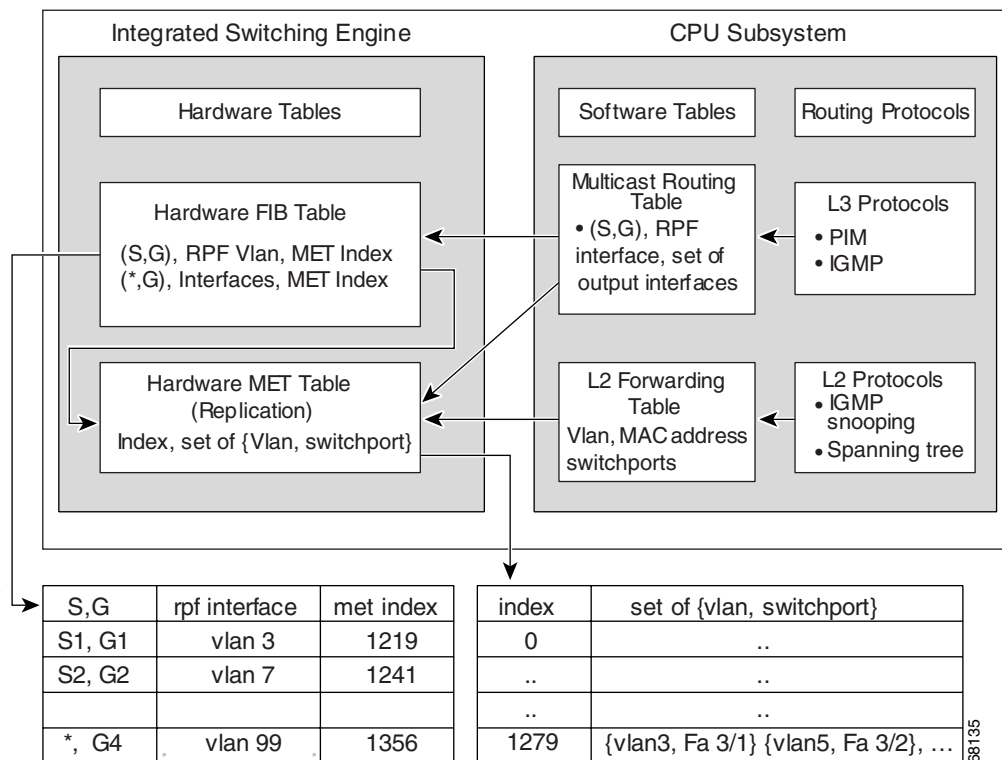
If VLAN 1 contains 1/1 and 1/2, VLAN 2 contains 2/1 and 2/2, and VLAN 3 contains 3/1 and 3/2, the MET chain for this route would contain these switchports: (1/1,1/2,2/1,2/2,3/1, and 3/2).

If IGMP snooping is on, the packet should not be forwarded to all output switchports on VLAN 2. The packet should be forwarded only to switchports where IGMP snooping has determined that there is either a group member or router. For example, if VLAN 1 had IGMP snooping enabled, and IGMP snooping determined that only port 1/2 had a group member on it, then the MET chain would contain these switchports: (1/1,1/2, 2/1, 2/2, 3/1, and 3/2).

## IP Multicast Tables

Figure 23-4 shows some key data structures that the Catalyst 4500 series switch uses to forward IP multicast packets in hardware.

**Figure 23-4 IP Multicast Tables and Protocols**



The Integrated Switching Engine maintains the hardware FIB table to identify individual IP multicast routes. Each entry consists of a destination group IP address and an optional source IP address. Multicast traffic flows on primarily two types of routes: (S,G) and (\*,G). The (S,G) routes flow from a source to a group based on the IP address of the multicast source and the IP address of the multicast group destination. Traffic on a (\*,G) route flows from the PIM RP to all receivers of group G. Only sparse-mode groups use (\*,G) routes. The Integrated Switching Engine hardware contains space for a total of 128,000 routes, which are shared by unicast routes, multicast routes, and multicast fast-drop entries.

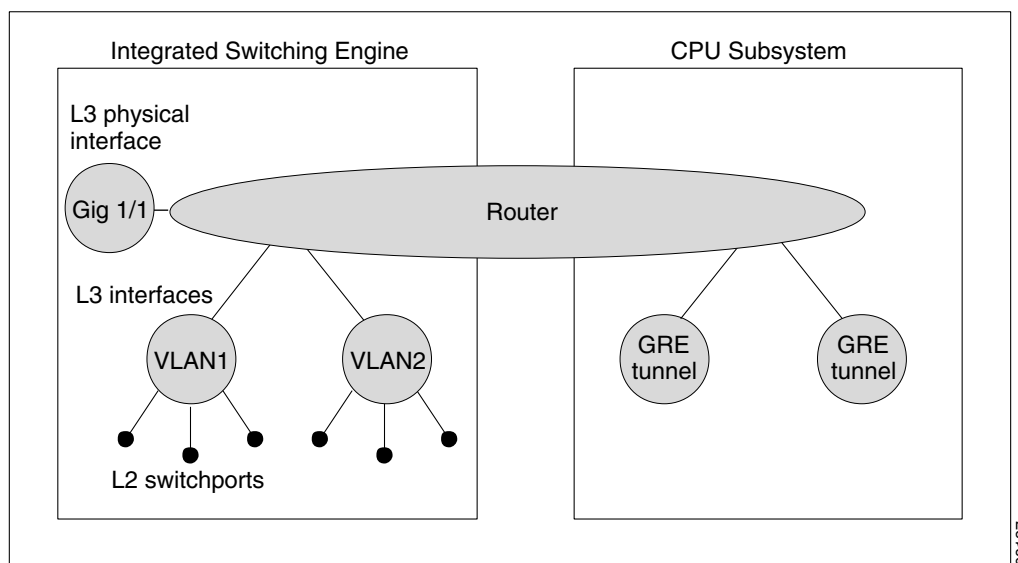
Output interface lists are stored in the multicast expansion table (MET). The MET has room for up to 32,000 output interface lists. The MET resources are shared by both Layer 3 multicast routes and by Layer 2 multicast entries. The actual number of output interface lists available in hardware depends on the specific configuration. If the total number of multicast routes exceed 32,000, multicast packets might not be switched by the Integrated Switching Engine. They would be forwarded by the CPU subsystem at much slower speeds.

## Hardware and Software Forwarding

The Integrated Switching Engine forwards the majority of packets in hardware at very high rates of speed. The CPU subsystem forwards exception packets in software. Statistical reports should show that the Integrated Switching Engine is forwarding the vast majority of packets in hardware.

Figure 23-5 shows a logical view of the hardware and software forwarding components.

**Figure 23-5 Hardware and Software Forwarding Components**



In the normal mode of operation, the Integrated Switching Engine performs inter-VLAN routing in hardware. The CPU subsystem supports generic routing encapsulation (GRE) tunnels for forwarding in software.

Replication is a particular type of forwarding where, instead of sending out one copy of the packet, the packet is replicated and multiple copies of the packet are sent out. At Layer 3, replication occurs only for multicast packets; unicast packets are never replicated to multiple Layer 3 interfaces. In IP multicasting, for each incoming IP multicast packet that is received, many replicas of the packet are sent out.

IP multicast packets can be transmitted on the following types of routes:

- Hardware routes
- Software routes
- Partial routes



Hardware routes occur when the Integrated Switching Engine hardware forwards all replicas of a packet. Software routes occur when the CPU subsystem software forwards all replicas of a packet. Partial routes occur when the Integrated Switching Engine forwards some of the replicas in hardware and the CPU subsystem forwards some of the replicas in software.

## Partial Routes



### Note

The conditions listed below cause the replicas to be forwarded by the CPU subsystem software, but the performance of the replicas that are forwarded in hardware is not affected.

The following conditions cause some replicas of a packet for a route to be forwarded by the CPU subsystem:

- The switch is configured with the **ip igmp join-group** command as a member of the IP multicast group on the RPF interface of the multicast source.
- The switch is the first-hop to the source in PIM sparse mode. In this case, the switch must send PIM-register messages to the RP.

## Software Routes



### Note

If any one of the following conditions is configured on the RPF interface or the output interface, all replication of the output is performed in software.

The following conditions cause all replicas of a packet for a route to be forwarded by the CPU subsystem software:

- The interface is configured with multicast helper.
- The interface is a generic routing encapsulation (GRE) or Distance Vector Multicast Routing Protocol (DVMRP) tunnel.
- The interface uses non-Advanced Research Products Agency (ARPA) encapsulation.

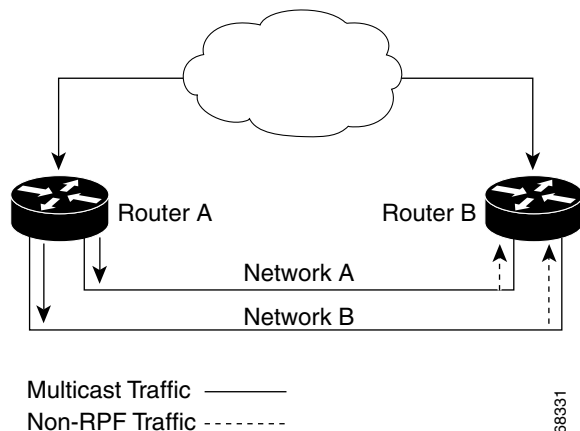
The following packets are always forwarded in software:

- Packets sent to multicast groups that fall into the range 224.0.0.\* (where \* is in the range from 0 to 255). This range is used by routing protocols. Layer 3 switching supports all other multicast group addresses.
- Packets with IP options.

## Non-Reverse Path Forwarding Traffic

Traffic that fails an Reverse Path Forwarding (RPF) check is called non-RPF traffic. Non-RPF traffic is forwarded by the Integrated Switching Engine by filtering (persistently dropping) or rate limiting the non-RPF traffic.

In a redundant configuration where multiple Layer 3 switches or routers connect to the same LAN segment, only one device forwards the multicast traffic from the source to the receivers on the outgoing interfaces. Figure 23-6 shows how Non-RPF traffic can occur in a common network configuration.

**Figure 23-6 Redundant Multicast Router Configuration in a Stub Network**

In this kind of topology, only Router A, the PIM designated router (PIM DR), forwards data to the common VLAN. Router B receives the forwarded multicast traffic, but must drop this traffic because it has arrived on the wrong interface and fails the RPF check. Traffic that fails the RPF check is called non-RPF traffic.

## Multicast Fast Drop

In IP multicast protocols, such as PIM-SM and PIM-DM, every (S,G) or (\*,G) route has an incoming interface associated with it. This interface is referred to as the reverse path forwarding interface. In some cases, when a packet arrives on an interface other than the expected RPF interface, the packet must be forwarded to the CPU subsystem software to allow PIM to perform special protocol processing on the packet. One example of this special protocol processing that PIM performs is the PIM Assert protocol.

By default, the Integrated Switching Engine hardware sends all packets that arrive on a non-RPF interface to the CPU subsystem software. However, processing in software is not necessary in many cases, because these non-RPF packets are often not needed by the multicast routing protocols. The problem is that if no action is taken, the non-RPF packets that are sent to the software can overwhelm the CPU.

Use the **ip mfib fastdrop** command to enable or disable MFIB fast drops.

To prevent this from happening, the CPU subsystem software loads fast-drop entries in the hardware when it receives an RPF failed packet that is not needed by the PIM protocols running on the switch. A fast-drop entry is keyed by (S,G, incoming interface). Any packet matching a fast-drop entry is bridged in the ingress VLAN, but is not sent to the software, so the CPU subsystem software is not overloaded by processing these RPF failures unnecessarily.

Protocol events, such as a link going down or a change in the unicast routing table, can impact the set of packets that can safely be fast dropped. A packet that was correctly fast dropped before might, after a topology change, need to be forwarded to the CPU subsystem software so that PIM can process it. The CPU subsystem software handles flushing fast-drop entries in response to protocol events so that the PIM code in IOS can process all the necessary RPF failures.

The use of fast-drop entries in the hardware is critical in some common topologies because it is possible to have persistent RPF failures. Without the fast-drop entries, the CPU would be exhausted by RPF failed packets that it did not need to process.

## Multicast Forwarding Information Base

The Multicast Forwarding Information Base (MFIB) subsystem supports IP multicast routing in the Integrated Switching Engine hardware on the Catalyst 4500 series switch. The MFIB logically resides between the IP multicast routing protocols in the CPU subsystem software (PIM, IGMP, MSDP, MBGP, and DVMRP) and the platform-specific code that manages IP multicast routing in hardware. The MFIB translates the routing table information created by the multicast routing protocols into a simplified format that can be efficiently processed and used for forwarding by the Integrated Switching Engine hardware.

To display the information in the multicast routing table, use the **show ip mroute** command. To display the MFIB table information, use the **show ip mfib** command. To display the information in the hardware tables, use the **show platform hardware** command.

The MFIB table contains a set of IP multicast routes. There are several types of IP multicast routes, including (S,G) and (\*,G) routes. Each route in the MFIB table can have one or more optional flags associated with it. The route flags indicate how a packet that matches a route should be forwarded. For example, the Internal Copy (IC) flag on an MFIB route indicates that a process on the switch needs to receive a copy of the packet. The following flags can be associated with MFIB routes:

- Internal Copy (IC) flag—set on a route when a process on the router needs to receive a copy of all packets matching the specified route
- Signalling (S) flag—set on a route when a process needs to be notified when a packet matching the route is received; the expected behavior is that the protocol code updates the MFIB state in response to receiving a packet on a signalling interface
- Connected (C) flag—when set on an MFIB route, has the same meaning as the Signalling (S) flag, except that the C flag indicates that only packets sent by directly connected hosts to the route should be signalled to a protocol process

A route can also have a set of optional flags associated with one or more interfaces. For example, an (S,G) route with the flags on VLAN 1 indicates how packets arriving on VLAN 1 should be treated, and they also indicate whether packets matching the route should be forwarded onto VLAN 1. The per-interface flags supported in the MFIB include the following:

- Accepting (A)—set on the interface that is known in multicast routing as the RPF interface. A packet that arrives on an interface that is marked as Accepting (A) is forwarded to all Forwarding (F) interfaces.
- Forwarding (F)—used in conjunction with the Accepting (A) flag as described above. The set of Forwarding interfaces that form what is often referred to as the multicast *olist* or output interface list.
- Signalling (S)—set on an interface when some multicast routing protocol process in IOS needs to be notified of packets arriving on that interface.
- Not platform fast-switched (NP)—used in conjunction with the Forwarding (F) flag. A Forwarding interface is also marked as not platform fast-switched whenever that output interface cannot be fast switched by the platform. The NP flag is typically used when the Forwarding interface cannot be routed in hardware and requires software forwarding. For example, Catalyst 4500 series switch tunnel interfaces are not hardware switched, so they are marked with the NP flag. If there are any NP interfaces associated with a route, then for every packet arriving on an Accepting interface, one copy of that packet is sent to the software forwarding path for software replication to those interfaces that were not switched in hardware.

**Note**

When PIM-SM routing is in use, the MFIB route might include an interface like in this example: PimTunnel [1.2.3.4]. This is a virtual interface that the MFIB subsystem creates to indicate that packets are being tunneled to the specified destination address. A PimTunnel interface cannot be displayed with the normal **show interface** command.

## S/M, 224/4

An (S/M, 224/4) entry is created in the MFIB for every multicast-enabled interface. This entry ensures that all packets sent by directly connected neighbors can be Register-encapsulated to the PIM-SM RP. Typically, only a small number of packets would be forwarded using the (S/M,224/4) route, until the (S,G) route is established by PIM-SM.

For example, on an interface with IP address 10.0.0.1 and netmask 255.0.0.0, a route would be created matching all IP multicast packets in which the source address is anything in the class A network 10. This route can be written in conventional subnet/masklength notation as (10/8,224/4). If an interface has multiple assigned IP addresses, then one route is created for each such IP address.

## Unsupported Features

The following IP multicast features are not supported in this release:

- Controlling the transmission rate to a multicast group
- Load splitting IP multicast traffic across equal-cost paths

## Configuring IP Multicast Routing

The following sections describe IP multicast routing configuration tasks:

- Default Configuration in IP MULTicast Routing, page 23-13
- Enabling IP Multicast Routing, page 23-13
- Enabling PIM on an Interface, page 23-13

For more detailed information on IP multicast routing, such as Auto-RP, PIM Version 2, and IP multicast static routes, refer to the *Cisco IOS IP and IP Routing Configuration Guide, Release 12.1*.

## Default Configuration in IP Multicast Routing

Table 23-1 shows the IP multicast default configuration.

**Table 23-1** Default IP Multicast Configuration

| Feature              | Default Value                                                                                                                                                                                                                                                                                                                                                   |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Rate limiting of RPF | Enabled globally                                                                                                                                                                                                                                                                                                                                                |
| IP multicast routing | Disabled globally<br><br><b>Note</b> When IP multicast routing is disabled, IP multicast traffic data packets are not forwarded by the Catalyst 4500 series switch. However, IP multicast control traffic will continue to be processed and forwarded. Therefore, IP multicast routes can remain in the routing table even if IP multicast routing is disabled. |
| PIM                  | Disabled on all interfaces                                                                                                                                                                                                                                                                                                                                      |
| IGMP snooping        | Enabled on all VLAN interfaces<br><br><b>Note</b> If you disable IGMP snooping on an interface, all output ports are forwarded by the Integrated Switching Engine. When IGMP snooping is disabled on an input VLAN interface, multicast packets related to that interface are sent to all forwarding switchports in the VLAN.                                   |



### Note

Source-specific multicast and IGMP v3 are supported.

For more information about source-specific multicast with IGMPv3 and IGMP, see the following URL:  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dtssm5t.htm>

## Enabling IP Multicast Routing

Enabling IP multicast routing allows the Catalyst 4500 series switch to forward multicast packets. To enable IP multicast routing on the router, perform this task in global configuration mode:

| Command                                     | Purpose                       |
|---------------------------------------------|-------------------------------|
| Switch(config)# <b>ip multicast-routing</b> | Enables IP multicast routing. |

## Enabling PIM on an Interface

Enabling PIM on an interface also enables IGMP operation on that interface. An interface can be configured to be in dense mode, sparse mode, or sparse-dense mode. The mode determines how the Layer 3 switch or router populates its multicast routing table and how the Layer 3 switch or router forwards multicast packets it receives from its directly connected LANs. You must enable PIM in one of these modes for an interface to perform IP multicast routing.

When the switch populates the multicast routing table, dense-mode interfaces are always added to the table. Sparse-mode interfaces are added to the table only when periodic join messages are received from downstream routers, or when there is a directly connected member on the interface. When forwarding from a LAN, sparse-mode operation occurs if there is an RP known for the group. If so, the packets are encapsulated and sent toward the RP. When no RP is known, the packet is flooded in a dense-mode fashion. If the multicast traffic from a specific source is sufficient, the receiver's first-hop router can send join messages toward the source to build a source-based distribution tree.

There is no default mode setting. By default, multicast routing is disabled on an interface.

## Enabling Dense Mode

To configure PIM on an interface to be in dense mode, perform this task:

| Command                                     | Purpose                                  |
|---------------------------------------------|------------------------------------------|
| Switch(config-if)# <b>ip pim dense-mode</b> | Enables dense-mode PIM on the interface. |

See the “PIM Dense Mode Example” section at the end of this chapter for an example of how to configure a PIM interface in dense mode.

## Enabling Sparse Mode

To configure PIM on an interface to be in sparse mode, perform this task:

| Command                                      | Purpose                                   |
|----------------------------------------------|-------------------------------------------|
| Switch(config-if)# <b>ip pim sparse-mode</b> | Enables sparse-mode PIM on the interface. |

See the “PIM Sparse Mode Example” section at the end of this chapter for an example of how to configure a PIM interface in sparse mode.

## Enabling Sparse-Dense Mode

When you enter either the **ip pim sparse-mode** or **ip pim dense-mode** command, sparseness or denseness is applied to the interface as a whole. However, some environments might require PIM to run in a single region in sparse mode for some groups and in dense mode for other groups.

An alternative to enabling only dense mode or only sparse mode is to enable sparse-dense mode. In this case, the interface is treated as dense mode if the group is in dense mode; the interface is treated in sparse mode if the group is in sparse mode. If you want to treat the group as a sparse group, and the interface is in sparse-dense mode, you must have an RP.

If you configure sparse-dense mode, the idea of sparseness or denseness is applied to the group on the switch, and the network manager should apply the same concept throughout the network.

Another benefit of sparse-dense mode is that Auto-RP information can be distributed in a dense-mode manner; yet, multicast groups for user groups can be used in a sparse-mode manner. Thus, there is no need to configure a default RP at the leaf routers.

When an interface is treated in dense mode, it is populated in a multicast routing table's outgoing interface list when either of the following is true:

- When there are members or DVMRP neighbors on the interface
- When there are PIM neighbors and the group has not been pruned

When an interface is treated in sparse mode, it is populated in a multicast routing table's outgoing interface list when either of the following is true:

- When there are members or DVMRP neighbors on the interface
- When an explicit join has been received by a PIM neighbor on the interface

To enable PIM to operate in the same mode as the group, perform this task:

| Command                                            | Purpose                                                                 |
|----------------------------------------------------|-------------------------------------------------------------------------|
| Switch(config-if)# <b>ip pim sparse-dense-mode</b> | Enables PIM to operate in sparse or dense mode, depending on the group. |

## Monitoring and Maintaining IP Multicast Routing

You can remove all contents of a particular cache, table, or database. You also can display specific statistics. The following sections describe how to monitor and maintain IP multicast:

- Displaying System and Network Statistics, page 23-15
- Displaying the Multicast Routing Table, page 23-16
- Displaying IP MFIB, page 23-18
- Displaying IP MFIB Fast Drop, page 23-19
- Displaying PIM Statistics, page 23-20
- Clearing Tables and Databases, page 23-20

### Displaying System and Network Statistics

You can display specific statistics, such as the contents of IP routing tables and databases. Information provided can be used to determine resource utilization and solve network problems. You can also display information about node reachability and discover the routing path your device's packets are taking through the network.

To display various routing statistics, you can perform any of these tasks:

| Command                                                                      | Purpose                                                   |
|------------------------------------------------------------------------------|-----------------------------------------------------------|
| Switch# <b>ping</b> [ <i>group-name</i>   <i>group-address</i> ]             | Sends an ICMP Echo Request to a multicast group address.  |
| Switch# <b>show ip mroute</b> [ <i>hostname</i>   <i>group_number</i> ]      | Displays the contents of the IP multicast routing table.  |
| Switch# <b>show ip pim interface</b> [ <i>type number</i> ] [ <i>count</i> ] | Displays information about interfaces configured for PIM. |
| Switch# <b>show ip interface</b>                                             | Displays PIM information for all interfaces.              |

## Displaying the Multicast Routing Table

The following is sample output from the **show ip mroute** command for a router operating in dense mode. This command displays the contents of the IP multicast FIB table for the multicast group named cbone-audio.

```
Switch# show ip mroute cbone-audio

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Connected, L - Local, P - Pruned
R - RP-bit set, F - Register flag, T - SPT-bit set
Timers: Uptime/Expires
Interface state: Interface, Next-Hop, State/Mode

(*, 224.0.255.1), uptime 0:57:31, expires 0:02:59, RP is 0.0.0.0, flags: DC
 Incoming interface: Null, RPF neighbor 0.0.0.0, Dvmrp
 Outgoing interface list:
 Ethernet0, Forward/Dense, 0:57:31/0:02:52
 Tunnel0, Forward/Dense, 0:56:55/0:01:28

(198.92.37.100/32, 224.0.255.1), uptime 20:20:00, expires 0:02:55, flags: C
 Incoming interface: Tunnel0, RPF neighbor 10.20.37.33, Dvmrp
 Outgoing interface list:
 Ethernet0, Forward/Dense, 20:20:00/0:02:52
```

The following is sample output from the **show ip mroute** command for a router operating in sparse mode:

```
Switch# show ip mroute

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Connected, L - Local, P - Pruned
R - RP-bit set, F - Register flag, T - SPT-bit set
Timers: Uptime/Expires
Interface state: Interface, Next-Hop, State/Mode

(*, 224.0.255.3), uptime 5:29:15, RP is 198.92.37.2, flags: SC
 Incoming interface: Tunnel0, RPF neighbor 10.3.35.1, Dvmrp
 Outgoing interface list:
 Ethernet0, Forward/Sparse, 5:29:15/0:02:57

(198.92.46.0/24, 224.0.255.3), uptime 5:29:15, expires 0:02:59, flags: C
 Incoming interface: Tunnel0, RPF neighbor 10.3.35.1
 Outgoing interface list:
 Ethernet0, Forward/Sparse, 5:29:15/0:02:57
```



### Note

Output interface timers are not updated for hardware-forwarded packets. Entry timers are updated approximately every five seconds.

The following is sample output from the **show ip mroute** command with the **summary** keyword:

```
Switch# show ip mroute summary

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Connected, L - Local, P - Pruned
 R - RP-bit set, F - Register flag, T - SPT-bit set, J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, Next-Hop, State/Mode

(*, 224.255.255.255), 2d16h/00:02:30, RP 171.69.10.13, flags: SJPC
```



```
(*, 224.2.127.253), 00:58:18/00:02:00, RP 171.69.10.13, flags: SJC
(*, 224.1.127.255), 00:58:21/00:02:03, RP 171.69.10.13, flags: SJC
(*, 224.2.127.254), 2d16h/00:00:00, RP 171.69.10.13, flags: SJCL
(128.9.160.67/32, 224.2.127.254), 00:02:46/00:00:12, flags: CLJT
(129.48.244.217/32, 224.2.127.254), 00:02:15/00:00:40, flags: CLJT
(130.207.8.33/32, 224.2.127.254), 00:00:25/00:02:32, flags: CLJT
(131.243.2.62/32, 224.2.127.254), 00:00:51/00:02:03, flags: CLJT
(140.173.8.3/32, 224.2.127.254), 00:00:26/00:02:33, flags: CLJT
(171.69.60.189/32, 224.2.127.254), 00:03:47/00:00:46, flags: CLJT
```

The following is sample output from the **show ip mroute** command with the **active** keyword:

```
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-el.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-el.acm97.interop.net)
 Rate: 3 pps/31 kbps(1sec), 63 kbps(last 19 secs), 65 kbps(life avg)
```

The following is sample output from the **show ip mroute** command with the **count** keyword:

```
Switch# show ip mroute count

IP Multicast Statistics - Group count: 8, Average sources per group: 9.87
Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second

Group: 224.255.255.255, Source count: 0, Group pkt count: 0
 RP-tree: 0/0/0/0

Group: 224.2.127.253, Source count: 0, Group pkt count: 0
 RP-tree: 0/0/0/0

Group: 224.1.127.255, Source count: 0, Group pkt count: 0
 RP-tree: 0/0/0/0

Group: 224.2.127.254, Source count: 9, Group pkt count: 14
 RP-tree: 0/0/0/0
 Source: 128.2.6.9/32, 2/0/796/0
 Source: 128.32.131.87/32, 1/0/616/0
 Source: 128.125.51.58/32, 1/0/412/0
 Source: 130.207.8.33/32, 1/0/936/0
 Source: 131.243.2.62/32, 1/0/750/0
 Source: 140.173.8.3/32, 1/0/660/0
 Source: 146.137.28.69/32, 1/0/584/0
 Source: 171.69.60.189/32, 4/0/447/0
 Source: 204.162.119.8/32, 2/0/834/0

Group: 224.0.1.40, Source count: 1, Group pkt count: 3606
 RP-tree: 0/0/0/0
 Source: 171.69.214.50/32, 3606/0/48/0, RPF Failed: 1203

Group: 224.2.201.241, Source count: 36, Group pkt count: 54152
```

```

RP-tree: 7/0/108/0
Source: 13.242.36.83/32, 99/0/123/0
Source: 36.29.1.3/32, 71/0/110/0
Source: 128.9.160.96/32, 505/1/106/0
Source: 128.32.163.170/32, 661/1/88/0
Source: 128.115.31.26/32, 192/0/118/0
Source: 128.146.111.45/32, 500/0/87/0
Source: 128.183.33.134/32, 248/0/119/0
Source: 128.195.7.62/32, 527/0/118/0
Source: 128.223.32.25/32, 554/0/105/0
Source: 128.223.32.151/32, 551/1/125/0
Source: 128.223.156.117/32, 535/1/114/0
Source: 128.223.225.21/32, 582/0/114/0
Source: 129.89.142.50/32, 78/0/127/0
Source: 129.99.50.14/32, 526/0/118/0
Source: 130.129.0.13/32, 522/0/95/0
Source: 130.129.52.160/32, 40839/16/920/161
Source: 130.129.52.161/32, 476/0/97/0
Source: 130.221.224.10/32, 456/0/113/0
Source: 132.146.32.108/32, 9/1/112/0

```

**Note**

Multicast route byte and packet statistics are supported only for the first 1024 multicast routes. Output interface statistics are not maintained.

## Displaying IP MFIB

You can display all routes in the MFIB, including routes that might not exist directly in the upper-layer routing protocol database but that are used to accelerate fast switching. These routes appear in the MFIB, even if dense-mode forwarding is in use.

To display various MFIB routing routes, perform one of these tasks:

| Command                              | Purpose                                                                                                                                                                                                                  |
|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Switch# <b>show ip mfib</b>          | Displays the (S,G) and (*,G) routes that are used for packet forwarding. Displays counts for fast, slow, and partially-switched packets for every multicast route.                                                       |
| Switch# <b>show ip mfib all</b>      | Displays all routes in the MFIB, including routes that may not exist directly in the upper-layer routing protocol database, but that are used to accelerate fast switching. These routes include the (S/M,224/4) routes. |
| Switch# <b>show ip mfib log [n]</b>  | Displays a log of the most recent n MFIB related events, most recent first.                                                                                                                                              |
| Switch# <b>show ip mfib counters</b> | Displays counts of MFIB related events. Only non-zero counters are shown.                                                                                                                                                |

The following is sample output from the **show ip mfib** command.

```
IP Multicast Forwarding Information Base
Entry Flags: C - Directly Connected, S - Signal,
 IC - Internal Copy
Interface Flags: A - Accept, F - Forward, S - 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)
..
```

The fast-switched packet count represents the number of packets that were switched in hardware on the corresponding route.

The partially switched packet counter represents the number of times that a fast-switched packet was also copied to the CPU for software processing or for forwarding to one or more non-platform switched interfaces (such as a PimTunnel interface).

The slow-switched packet count represents the number of packets that were switched completely in software on the corresponding route.

## Displaying IP MFIB Fast Drop

To display fast-drop entries, perform this task:

| Command                              | Purpose                                                                                           |
|--------------------------------------|---------------------------------------------------------------------------------------------------|
| Switch# <b>show ip mfib fastdrop</b> | Displays all currently active fast-drop entries and indicates whether <b>fastdrop</b> is enabled. |

The following is sample output from the **show ip mfib fastdrop** command.

```
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
```

The full (S,G) flow and the ingress interface on which incoming packets are dropped is shown. The timestamp indicates the age of the entry.

## Displaying PIM Statistics

The following is sample output from the **show ip pim interface** command:

```
Switch# show ip pim interface
```

| Address       | Interface | Mode  | Neighbor Count | Query Interval | DR            |
|---------------|-----------|-------|----------------|----------------|---------------|
| 198.92.37.6   | Ethernet0 | Dense | 2              | 30             | 198.92.37.33  |
| 198.92.36.129 | Ethernet1 | Dense | 2              | 30             | 198.92.36.131 |
| 10.1.37.2     | Tunnel0   | Dense | 1              | 30             | 0.0.0.0       |

The following is sample output from the **show ip pim interface** command with a **count**:

```
Switch# show ip pim interface count
```

| Address       | Interface    | FS | Mpackets In/Out    |
|---------------|--------------|----|--------------------|
| 171.69.121.35 | Ethernet0    | *  | 548305239/13744856 |
| 171.69.121.35 | Serial0.33   | *  | 8256/67052912      |
| 198.92.12.73  | Serial0.1719 | *  | 219444/862191      |

The following is sample output from the **show ip pim interface** command with a **count** when IP multicast is enabled. The example lists the PIM interfaces that are fast-switched and process-switched, and the packet counts for these. The H is added to interfaces where IP multicast is enabled.

```
Switch# show ip pim interface count
```

States: FS - Fast Switched, H - Hardware Switched

| Address    | Interface | FS  | Mpackets In/Out |
|------------|-----------|-----|-----------------|
| 192.1.10.2 | Vlan10    | * H | 40886/0         |
| 192.1.11.2 | Vlan11    | * H | 0/40554         |
| 192.1.12.2 | Vlan12    | * H | 0/40554         |
| 192.1.23.2 | Vlan23    | *   | 0/0             |
| 192.1.24.2 | Vlan24    | *   | 0/0             |

## Clearing Tables and Databases

You can remove all contents of a particular cache, table, or database. Clearing a cache, table, or database might be necessary when the contents of the particular structure have become, or are suspected to be, invalid.

To clear IP multicast caches, tables, and databases, perform one of these tasks:

| Command                               | Purpose                                         |
|---------------------------------------|-------------------------------------------------|
| Switch# <b>clear ip mroute</b>        | Deletes entries from the IP routing table.      |
| Switch# <b>clear ip mfib counters</b> | Deletes all per-route and global MFIB counters. |
| Switch# <b>clear ip mfib fastdrop</b> | Deletes all fast-drop entries.                  |



### Note

IP multicast routes can be regenerated in response to protocol events and as data packets arrive.

# Configuration Examples

The following sections provide IP multicast routing configuration examples:

- PIM Dense Mode Example, page 23-21
- PIM Sparse Mode Example, page 23-21
- BSR Configuration Example, page 23-21

## PIM Dense Mode Example

This example is a configuration of dense-mode PIM on an Ethernet interface:

```
ip multicast-routing
interface ethernet 0
 ip pim dense-mode
```

## PIM Sparse Mode Example

This example is a configuration of sparse-mode PIM. The RP router is the router with the address 10.8.0.20.

```
ip multicast-routing
 ip pim rp-address 10.8.0.20 1
interface ethernet 1
 ip pim sparse-mode
```

## BSR Configuration Example

This example is a configuration of a candidate BSR, which also happens to be a candidate RP:

```
version 11.3
!
ip multicast-routing
!
interface Ethernet0
 ip address 171.69.62.35 255.255.255.240
!
interface Ethernet1
 ip address 172.21.24.18 255.255.255.248
 ip pim sparse-dense-mode
!
interface Ethernet2
 ip address 172.21.24.12 255.255.255.248
 ip pim sparse-dense-mode
!
router ospf 1
 network 172.21.24.8 0.0.0.7 area 1
 network 172.21.24.16 0.0.0.7 area 1
!
ip pim bsr-candidate Ethernet2 30 10
ip pim rp-candidate Ethernet2 group-list 5
access-list 5 permit 239.255.2.0 0.0.0.255
```





## Configuring Network Security with ACLs

This chapter describes how to use access control lists (ACLs) to configure network security on the Catalyst 4500 series switches.



### Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference* and related information at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/index.htm>.

This chapter consists of the following major sections:

- Understanding ACLs, page 24-1
- Hardware and Software ACL Support, page 24-5
- Layer 4 Operators in ACLs, page 24-6
- Configuring Unicast MAC Address Filtering, page 24-9
- Configuring Named MAC Extended ACLs, page 24-9
- Configuring VLAN Maps, page 24-10
- Displaying VLAN Access Map Information, page 24-17
- Using VLAN Maps with Router ACLs, page 24-18
- Configuring PACLs, page 24-20
- Using PACL with VLAN Maps and Router ACLs, page 24-24

## Understanding ACLs

This section contains the following subsections:

- ACL Overview, page 24-2
- Supported Features That Use ACLs, page 24-2
- Router ACLs, page 24-3
- Port ACLs, page 24-4
- VLAN Maps, page 24-5

## ACL Overview

An ACL is a collection of sequential permit and deny conditions that applies to packets. When a packet is received on an interface, the switch compares the fields in the packet against any applied ACLs to verify that the packet has the permissions required to be forwarded, based on the conditions specified in the access lists. It tests the packets against the conditions in an access list one-by-one. The first match determines whether the switch accepts or rejects the packets. Because the switch stops testing conditions after the first match, the order of conditions in the list is critical. If no conditions match, the switch drops the packet. If there are no restrictions, the switch forwards the packet; otherwise, the switch drops the packet.

Switches traditionally operate at Layer 2, switching traffic within a VLAN, whereas routers route traffic between VLANs at Layer 3. The Catalyst 4500 series switch can accelerate packet routing between VLANs by using Layer 3 switching. The Layer 3 switch bridges the packet, and then routes the packet internally without going to an external router. The packet is then bridged again and sent to its destination. During this process, the switch can control all packets, including packets bridged within a VLAN.

You configure access lists on a router or switch to filter traffic and provide basic security for your network. If you do not configure ACLs, all packets passing through the switch could be allowed on all parts of the network. You can use ACLs to control which hosts can access different parts of a network or to decide which types of traffic are forwarded or blocked at router interfaces. For example, you can allow e-mail traffic to be forwarded but not Telnet traffic. ACLs can be configured to block inbound traffic, outbound traffic, or both. However, on Layer 2 interfaces, you can apply ACLs only in the inbound direction.

An ACL contains an ordered list of access control entries (ACEs). Each ACE specifies permit or deny and a set of conditions the packet must satisfy in order to match the ACE. The meaning of permit or deny depends on the context in which the ACL is used.

The Catalyst 4500 series switch supports two types of ACLs:

- IP ACLs, which filter IP traffic, including TCP, the User Datagram Protocol (UDP), Internet Group Management Protocol (IGMP), and Internet Control Message Protocol (ICMP).
- MAC (Ethernet) ACLs, which filter non-IP traffic.

## Supported Features That Use ACLs

The switch supports two applications of ACLs to filter traffic:

- Router ACLs are applied to Layer 3 interfaces. They control the access of routed traffic between VLANs. All Catalyst 4500 series switches can create router ACLs, but you must have a Cisco IOS software image on your switch to apply an ACL to a Layer 3 interface and filter packets routed between VLANs.
- Port ACLs perform access control on traffic entering a Layer 2 interface. If there are not enough hardware CAM entries, the output port ACL is not applied to the port and a warning message is given to user. (This restriction applies to all access group modes for output port ACLs.) When there are enough CAM entries, the output port ACL might be re-applied.

If there is any output port ACL configured on a Layer 2 port, then no VACL or Router ACL can be configured on the VLANs that the Layer 2 port belongs to, and vice-versa. In other words, port ACLs and VLAN-based ACLs (VACL and Router ACL) are mutually exclusive on a Layer 2 port. This restriction applies to all access group mode.

You can apply only one IP access list and one MAC access list to a Layer 2 interface.



- VLAN ACLs or VLAN maps control the access of all packets (bridged and routed). You can use VLAN maps to filter traffic between devices in the same VLAN. You do not need the enhanced image to create or apply VLAN maps. VLAN maps are configured to control access based on Layer 3 addresses for IP. MAC addresses using Ethernet ACEs control the access of unsupported protocols. After you apply a VLAN map to a VLAN, all packets (routed or bridged) entering the VLAN are checked against that map. Packets can either enter the VLAN through a switch port or through a routed port after being routed.

You can use both router ACLs and VLAN maps on the same switch.

## Router ACLs

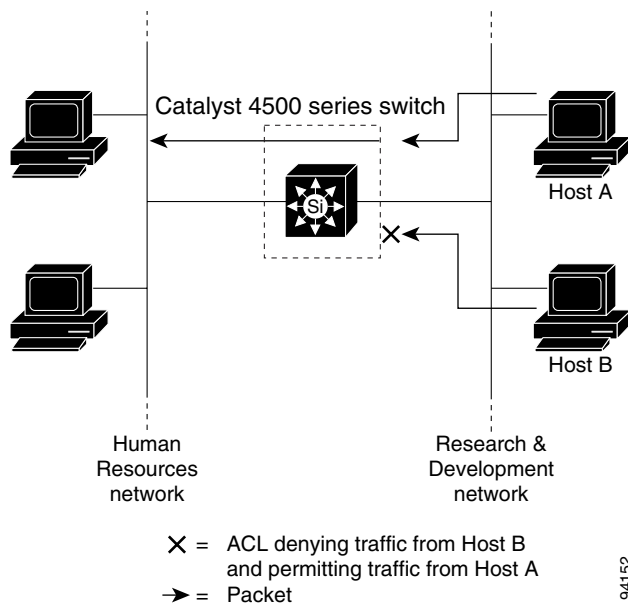
You can apply router ACLs on switch virtual interfaces (SVIs), which are Layer 3 interfaces to VLANs; on physical Layer 3 interfaces; and on Layer 3 EtherChannel interfaces. Router ACLs are applied on interfaces for specific directions (inbound or outbound). You can apply one IP access list in each direction.

Multiple features can use one ACL for a given interface, and one feature can use multiple ACLs. When a single router ACL is used by multiple features, it is examined multiple times. The access list type determines the input to the matching operation:

- Standard IP access lists use source addresses for matching operations.
- Extended IP access lists use source and destination addresses and optional protocol type information for matching operations.

The switch examines ACLs associated with features configured on a given interface and a direction. As packets enter the switch on an interface, ACLs associated with all inbound features configured on that interface are examined. After packets are routed and before they are forwarded to the next hop, all ACLs associated with outbound features configured on the egress interface are examined.

ACLs permit or deny packet forwarding based on how the packet matches the entries in the ACL. For example, you can use access lists to allow one host to access a part of a network, but prevent another host from accessing the same part. In Figure 24-1, ACLs applied at the router input allow Host A to access the Human Resources network, but prevent Host B from accessing the same network.

**Figure 24-1 Using ACLs to Control Traffic to a Network**

## Port ACLs

You can also apply ACLs to Layer 2 interfaces on a switch. Port ACLs are supported on physical interfaces and EtherChannel interfaces.

The following access lists are supported on Layer 2 interfaces:

- Standard IP access lists using source addresses
- Extended IP access lists using source and destination addresses and optional protocol type information
- MAC extended access lists using source and destination MAC addresses and optional protocol type information

As with router ACLs, the switch examines ACLs associated with features configured on a given interface and permits or denies packet forwarding based on how the packet matches the entries in the ACL. In the example in Figure 24-1, if all workstations were in the same VLAN, ACLs applied at the Layer 2 input would allow Host A to access the Human Resources network, but prevent Host B from accessing the same network.

When you apply a port ACL to a trunk port, the ACL filters traffic on all VLANs present on the trunk port. When you apply a port ACL to a port with voice VLAN, the ACL filters traffic on both data and voice VLANs.

With port ACLs, you can filter IP traffic by using IP access lists and non-IP traffic by using MAC addresses. You can filter both IP and non-IP traffic on the same Layer 2 interface by applying both an IP access list and a MAC access list to the interface.



### Note

You cannot apply more than one IP access list and one MAC access list to a Layer 2 interface. If an IP access list or MAC access list is already configured on a Layer 2 interface and you apply a new IP access list or MAC access list to the interface, the new ACL replaces the previously configured one.

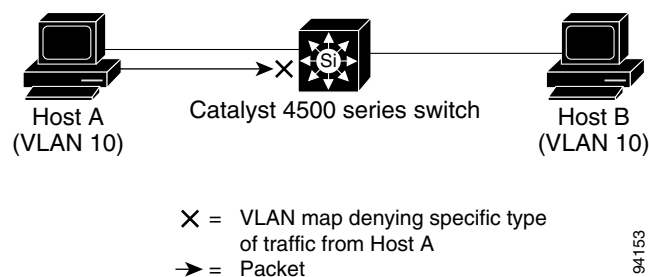
## VLAN Maps

VLAN maps can control the access of all traffic in a VLAN. You can apply VLAN maps on the switch to all packets that are routed into or out of a VLAN or are bridged within a VLAN. Unlike router ACLs, VLAN maps are not defined by direction (input or output).

You can configure VLAN maps to match Layer 3 addresses for IP traffic. Access of all non-IP protocols is controlled with a MAC address and an Ethertype using MAC ACLs in VLAN maps. (IP traffic is not controlled by MAC ACLs in VLAN maps.) You can enforce VLAN maps only on packets going through the switch; you cannot enforce VLAN maps on traffic between hosts on a hub or on another switch connected to this switch.

With VLAN maps, forwarding packets is permitted or denied, based on the action specified in the map. Figure 24-2 illustrates how a VLAN map is applied to deny a specific type of traffic from Host A in VLAN 10 from being forwarded.

**Figure 24-2 Using VLAN Maps to Control Traffic**



## Hardware and Software ACL Support

This section describes how to determine whether ACLs are processed in hardware or in software:

- Flows that match a deny statement in standard and extended ACLs (input only) are dropped in hardware if ICMP unreachable messages are disabled.
- Flows that match a permit statement in standard and extended ACLs (input and output) are processed in hardware.
- The following ACL types are not supported in software:
  - Standard Xerox Network Systems (XNS) Protocol access list
  - Extended XNS access list
  - DECnet access list
  - Protocol type-code access list
  - Standard Internet Packet Exchange (IPX) access list
  - Extended IPX access list

**Note**

Packets that require logging are processed in software. A copy of the packets is sent to the CPU for logging while the actual packets are forwarded in hardware so that non-logged packet processing is not impacted.

By default, the Catalyst 4500 series switch sends ICMP unreachable messages when a packet is denied by an access list; these packets are not dropped in hardware but are forwarded to the switch so that it can generate the ICMP unreachable message.

To drop access-list denied packets in hardware on the input interface, you must disable ICMP unreachable messages using the **no ip unreachable** interface configuration command. The **ip unreachable** command is enabled by default.

Packets denied by an output access list are always forwarded to the CPU.

## Layer 4 Operators in ACLs

The following sections describe guidelines and restrictions for configuring ACLs that include Layer 4 port operations:

- Restrictions for Layer 4 Operations, page 24-6
- Configuration Guidelines for Layer 4 Operations, page 24-6
- How ACL Processing Impacts CPU, page 24-8

## Restrictions for Layer 4 Operations

You can specify these operator types, each of which uses one Layer 4 operation in the hardware:

- gt (greater than)
- lt (less than)
- neq (not equal)
- range (inclusive range)

We recommend that you not specify more than six different operations on the same ACL. If you exceed this number, each new operation might cause the affected ACE (access control entry) to be translated into multiple ACEs in hardware. If you exceed this number, the affected ACE might be processed in software.

## Configuration Guidelines for Layer 4 Operations

Keep the following guidelines in mind when using Layer 4 operators:

- Layer 4 operations are considered different if the operator or operand differ. For example, the following ACL contains three different Layer 4 operations because gt 10 and gt 11 are considered two different Layer 4 operations:

```
... gt 10 permit
... lt 9 deny
... gt 11 deny
```

**Note**

The eq operator can be used an unlimited number of times because eq does not use a Layer 4 operation in hardware.

- Layer 4 operations are considered different if the same operator/operand couple applies once to a source port and once to a destination port, as in the following example:

```
... Src gt 10...
... Dst gt 10
```

A more detailed example follows:

```
access-list 101
... (dst port) gt 10 permit
... (dst port) lt 9 deny
... (dst port) gt 11 deny
... (dst port) neq 6 permit
... (src port) neq 6 deny
... (dst port) gt 10 deny

access-list 102
... (dst port) gt 20 deny
... (src port) lt 9 deny
... (src port) range 11 13 deny
... (dst port) neq 6 permit
```

Access lists 101 and 102 use the following Layer 4 operations:

- Access list 101 Layer 4 operations: 5
  - gt 10 permit and gt 10 deny both use the same operation because they are identical and both operate on the destination port.
- Access list 102 Layer 4 operations: 4
- Total Layer 4 operations: 8 (due to sharing between the two access lists)
  - neg6 permit is shared between the two ACLs because they are identical and both operate on the same destination port.
- A description of the Layer 4 operations usage is as follows:
  - Layer 4 operation 1 stores gt 10 permit and gt 10 deny from ACL 101
  - Layer 4 operation 2 stores lt 9 deny from ACL 101
  - Layer 4 operation 3 stores gt 11 deny from ACL 101
  - Layer 4 operation 4 stores neg 6 permit from ACL 101 and 102
  - Layer 4 operation 5 stores neg 6 deny from ACL 101
  - Layer 4 operation 6 stores gt 20 deny from ACL 102
  - Layer 4 operation 7 stores lt 9 deny from ACL 102
  - Layer 4 operation 8 stores range 11 13 deny from ACL 102

## How ACL Processing Impacts CPU

ACL processing can impact the CPU in two ways:

- For some packets, when the hardware runs out of resources, the software must perform the ACL matches:
  - TCP flag combinations other than rst ack and syn fin rst are processed in software. rst ack is equivalent to the keyword **established**.
  - You can specify up to six Layer 4 operations (lt, gt, neq, and range) in an ACL in order for all operations to be guaranteed to be processed in hardware. More than six Layer 4 operations will trigger an attempt to translate the excess operations into multiple ACEs in hardware. If this attempt fails, packets will be processed in software. The translation process is less likely to succeed on large ACLs with a great number of Layer 4 operations, and on switches with large numbers of ACLs configured. The precise limit depends on how many other ACLs are configured and which specific Layer 4 operations are used by the ACLs being translated. The eq operator does not require any Layer 4 operations and can be used any number of times.
  - If the total number of Layer 4 operations in an ACL is less than six, you can distribute the operations in any way you choose.

Examples:

The following access lists will be processed completely in hardware:

```
access-list 104 permit tcp any any established
access-list 105 permit tcp any any rst ack
access-list 107 permit tcp any synfin rst
```

Access lists 104 and 105 are identical; established is shorthand for rst and ack.

Access list 101, below, will be processed completely in software:

```
access-list 101 permit tcp any any urg
```

Because four source and two destination operations exist, access list 106, below, will be processed in hardware:

```
access-list 106 permit tcp any range 100 120 any range 120 140
access-list 106 permit tcp any range 140 160 any range 180 200
access-list 106 permit tcp any range 200 220
access-list 106 deny tcp any range 220 240
```

In the following code, the Layer 4 operations for the third ACE will trigger an attempt to translate dst lt 1023 into multiple ACEs in hardware, because three source and three destination operations exist. If the translation attempt fails, the third ACE will be processed in software.

```
access-list 102 permit tcp any lt 80 any gt 100
access-list 102 permit tcp any range 100 120 any range 120 1024
access-list 102 permit tcp any gt 1024 any lt 1023
```

Similarly, for access list 103, below, the third ACE will trigger an attempt to translate dst gt 1023 into multiple ACEs in hardware. If the attempt fails, the third ACE will be processed in software. Although the operations for source and destination ports look similar, they are considered different Layer 4 operations.)

```
access-list 103 permit tcp any lt 80 any lt 80
access-list 103 permit tcp any range 100 120 any range 100 120
access-list 103 permit tcp any gt 1024 any gt 1023
```

**Note**

Remember that source port lt 80 and destination port lt 80 are considered different operations.

- Some packets must be sent to the CPU for accounting purposes, but the action is still performed by the hardware. For example, if a packet must be logged, a copy is sent to the CPU for logging, but the forwarding (or dropping) is performed in the hardware. Although logging slows the CPU, it does not affect the forwarding rate. This sequence of events would happen under the following conditions:
  - When a log keyword is used
  - When an output ACL denies a packet
  - When an input ACL denies a packet, and on the interface where the ACL is applied, **ip unreachable** is enabled (**ip unreachable** is enabled by default on all the interfaces)

## Configuring Unicast MAC Address Filtering

To block all unicast traffic to or from a MAC address in a specified VLAN, perform this task:

| Command                                                                                                      | Purpose                                                                                                                                                                                                     |
|--------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Router(config)# <b>mac-address-table static</b> <i>mac_address</i><br><b>vlan</b> <i>vlan_ID</i> <b>drop</b> | Blocks all traffic to or from the configured unicast MAC address in the specified VLAN.<br><br>To clear MAC address-based blocking, use the <b>no</b> form of this command without the <b>drop</b> keyword. |

This example shows how to block all unicast traffic to or from MAC address 0050.3e8d.6400 in VLAN 12:

```
Router# configure terminal
Router(config)# mac-address-table static 0050.3e8d.6400 vlan 12 drop
```

## Configuring Named MAC Extended ACLs

You can filter non-IP traffic on a VLAN and on a physical Layer 2 port by using MAC addresses and named MAC extended ACLs. The procedure is similar to that of configuring other extended named ACLs. You can use a number to name the access list, but MAC access list numbers from 700 to 799 are not supported.

**Note**

Named MAC extended ACLs cannot be applied to Layer 3 interfaces.

For more information about the supported non-IP protocols in the **mac access-list extended** command, refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference*.

To create a named MAC extended ACL, perform this task:

|        | Command                                                                                                                                                                                                                                                                                                                                                                                                                                      | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch# <b>configure terminal</b>                                                                                                                                                                                                                                                                                                                                                                                                            | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Step 2 | Switch(config)# <b>mac access-list extended</b> <i>name</i>                                                                                                                                                                                                                                                                                                                                                                                  | Defines an extended MAC access list using a name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Step 3 | Switch(config-ext-macl)# { <b>deny</b>   <b>permit</b> }<br>{ <b>any</b>   <b>host</b> <i>source MAC address</i> / <i>source MAC address mask</i> } { <b>any</b>   <b>host</b> <i>destination MAC address</i> / <i>destination MAC address mask</i> } [ <b>protocol-family</b> { <b>appletalk</b>   <b>arp-non-ipv4</b>   <b>decnet</b>   <b>ipx</b>   <b>ipv6</b>   <b>rarp-ipv4</b>   <b>rarp-non-ipv4</b>   <b>vines</b>   <b>xns</b> } ] | In extended MAC access-list configuration mode, specify to <b>permit</b> or <b>deny</b> any source MAC address, a source MAC address with a mask, or a specific <b>host</b> source MAC address and <b>any</b> destination MAC address, destination MAC address with a mask, or a specific destination MAC address.<br><br>(Optional)<br><ul style="list-style-type: none"> <li>[ <b>protocol-family</b> {<b>appletalk</b>   <b>arp-non-ipv4</b>   <b>decnet</b>   <b>ipx</b>   <b>ipv6</b>   <b>rarp-ipv4</b>   <b>rarp-non-ipv4</b>   <b>vines</b>   <b>xns</b>} ]</li> </ul> |
| Step 4 | Switch(config-ext-macl)# <b>end</b>                                                                                                                                                                                                                                                                                                                                                                                                          | Returns to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Step 5 | Switch# <b>show access-lists</b> [ <i>number</i>   <i>name</i> ]                                                                                                                                                                                                                                                                                                                                                                             | Shows the access list configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Step 6 | Switch(config)# <b>copy running-config startup-config</b>                                                                                                                                                                                                                                                                                                                                                                                    | (Optional) Saves your entries in the configuration file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

You can use the **no mac access-list extended** *name* global configuration command to delete the entire ACL. You can also delete individual ACEs from named MAC extended ACLs.

This example shows how to create and display an access list named *mac1*, denying only EtherType DECnet Phase IV traffic, but permitting all other types of traffic.

```
Switch(config)# mac access-list extended mac1
Switch(config-ext-macl)# deny any any decnet-iv (old) protocol-family decnet (new)
Switch(config-ext-macl)# permit any any
Switch(config-ext-macl)# end
Switch # show access-lists
Extended MAC access list mac1
 deny any any decnet-iv (old) protocol-family decnet (new)
 permit any any
```

## Configuring VLAN Maps

This section describes how to configure VLAN maps, which is the only way to control filtering within a VLAN. VLAN maps have no direction. To filter traffic in a specific direction by using a VLAN map, you need to include an ACL with specific source or destination addresses. If there is a match clause for that type of packet (IP or MAC) in the VLAN map, the default action is to drop the packet if the packet does not match any of the entries within the map. If there is no match clause for that type of packet, the default is to forward the packet.

To create a VLAN map and apply it to one or more VLANs, perform this task

- |               |                                                                                                        |
|---------------|--------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Create the standard or extended IP ACLs or named MAC extended ACLs that you want to apply to the VLAN. |
| <b>Step 2</b> | Enter the <b>vlan access-map</b> global configuration command to create a VLAN ACL map entry.          |



**Step 3** In access map configuration mode, you have the optional to enter an **action** (**forward** [the default] or **drop**) and enter the **match** command to specify an IP packet or a non-IP packet and to match the packet against one or more ACLs (standard or extended). If a match clause is not specified, the action is applied to all packets. The match clause can be used to match against multiple ACLs. If a packet matches any of the specified ACLs, the action is applied.



**Note** If the VLAN map has a match clause for the type of packet (IP or MAC) and the packet does not match the type, the default is to drop the packet. If there is no match clause in the VLAN map for that type of packet, and no action specified, the packet is forwarded.

**Step 4** Use the **vlan filter** global configuration command to apply a VLAN map to one or more VLANs.



**Note** You cannot apply a VLAN map to a VLAN on a switch that has ACLs applied to Layer 2 interfaces (port ACLs).

## VLAN Map Configuration Guidelines

Keep the following guidelines in mind when configuring VLAN maps:

- VLAN maps do not filter IPv4 ARP packets.
- If there is no router ACL configured to deny traffic on a routed VLAN interface (input or output), and no VLAN map configured, all traffic is permitted.
- Each VLAN map consists of a series of entries. The order of entries in a VLAN map is important. A packet that comes into the switch is tested against the first entry in the VLAN map. If it matches, the action specified for that part of the VLAN map is taken. If there is no match, the packet is tested against the next entry in the map.
- If the VLAN map has at least one match clause for the type of packet (IP or MAC) and the packet does not match any of these match clauses, the default is to drop the packet. If there is no match clause for that type of packet in the VLAN map, the default is to forward the packet.
- The system might take longer to boot if you have configured a very large number of ACLs.

## Creating and Deleting VLAN Maps

Each VLAN map consists of an ordered series of entries. To create, add to, or delete a VLAN map entry, perform this task:

|        | Command                                                                                                                                           | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch# <b>configure terminal</b>                                                                                                                 | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                      |
| Step 2 | Switch(config)# <b>vlan access-map</b> <i>name</i> [ <i>number</i> ]                                                                              | Creates a VLAN map, and give it a name and (optionally) a number. The number is the sequence number of the entry within the map.<br><br>When you create VLAN maps with the same name, numbers are assigned sequentially in increments of 10. When modifying or deleting maps, you can enter the number of the map entry that you want to modify or delete.<br><br>This command enables access-map configuration mode.  |
| Step 3 | Switch(config-access-map)# <b>action</b> { <b>drop</b>   <b>forward</b> }                                                                         | (Optional) Sets the action for the map entry. The default is to forward.                                                                                                                                                                                                                                                                                                                                               |
| Step 4 | Switch(config-access-map)# <b>match</b> { <b>ip</b>   <b>mac</b> } <b>address</b> { <i>name</i>   <i>number</i> } [ <i>name</i>   <i>number</i> ] | Matches the packet (using either the IP or MAC address) against one or more standard or extended access lists. Note that packets are matched only against access lists of the correct protocol type. IP packets are compared with standard or extended IP access lists. Non-IP packets are only compared with named MAC extended access lists. If a match clause is not specified, the action is taken on all packets. |
| Step 5 | Switch(config-access-map)# <b>end</b>                                                                                                             | Returns to global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                  |
| Step 6 | Switch(config)# <b>show running-config</b>                                                                                                        | Displays the access list configuration.                                                                                                                                                                                                                                                                                                                                                                                |
| Step 7 | Switch(config)# <b>copy running-config startup-config</b>                                                                                         | (Optional) Saves your entries in the configuration file.                                                                                                                                                                                                                                                                                                                                                               |

You can use the **no vlan access-map** *name* global configuration command to delete a map. You can use the **no vlan access-map** *name number* global configuration command to delete a single sequence entry from within the map. You can use the **no action** access-map configuration command to enforce the default action, which is to forward.

VLAN maps do not use the specific **permit** or **deny** keywords. To deny a packet by using VLAN maps, create an ACL that would match the packet, and then set the action to drop. A permit in the ACL is the same as a match. A deny in the ACL means no match.

## Examples of ACLs and VLAN Maps

These examples show how to create ACLs and VLAN maps that for specific purposes.

### Example 1

This example shows how to create an ACL and a VLAN map to deny a packet. In the first map, any packets that match the ip1 ACL (TCP packets) would be dropped. You first create the ip1 ACL to permit any TCP packet and no other packets. Because there is a match clause for IP packets in the VLAN map, the default action is to drop any IP packet that does not match any of the match clauses.

```
Switch(config)# ip access-list extended ip1
Switch(config-ext-nacl)# permit tcp any any
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map map_1 10
```

```
Switch(config-access-map)# match ip address ip1
Switch(config-access-map)# action drop
```

This example shows how to create a VLAN map to permit a packet. ACL ip2 permits UDP packets; and any packets that match the ip2 ACL are forwarded.

```
Switch(config)# ip access-list extended ip2
Switch(config-ext-nacl)# permit udp any any
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map map_1 20
Switch(config-access-map)# match ip address ip2
Switch(config-access-map)# action forward
```

In this map, any IP packets that did not match any of the previous ACLs (that is, packets that are not TCP packets or UDP packets) would get dropped.

## Example 2

In this example, the VLAN map is configured to drop IP packets and to forward MAC packets by default. By applying standard ACL 101 and the extended named access lists **igmp-match** and **tcp-match**, the VLAN map is configured to do the following:

- Forward all UDP packets
- Drop all IGMP packets
- Forward all TCP packets
- Drop all other IP packets
- Forward all non-IP packets

```
Switch(config)# access-list 101 permit udp any any
Switch(config)# ip access-list extended igmp-match
Switch(config-ext-nacl)# permit igmp any any
Switch(config)# ip access-list extended tcp-match
Switch(config-ext-nacl)# permit tcp any any
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map drop-ip-default 10
Switch(config-access-map)# match ip address 101
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
Switch(config)# vlan access-map drop-ip-default 20
Switch(config-access-map)# match ip address igmp-match
Switch(config-access-map)# action drop
Switch(config-access-map)# exit
Switch(config)# vlan access-map drop-ip-default 30
Switch(config-access-map)# match ip address tcp-match
Switch(config-access-map)# action forward
```

## Example 3

In this example, the VLAN map is configured to drop MAC packets and forward IP packets by default. By applying MAC extended access lists, **good-hosts** and **good-protocols**, the VLAN map is configured to do the following:

- Forward MAC packets from hosts 0000.0c00.0111 and 0000.0c00.0211
- Forward MAC packets of DECnet or VINES (Virtual Integrated Network Service) protocol-family
- Drop all other non-IP packets
- Forward all IP packets

```
Switch(config)# mac access-list extended good-hosts
Switch(config-ext-macl)# permit host 000.0c00.0111 any
Switch(config-ext-macl)# permit host 000.0c00.0211 any
Switch(config-ext-nacl)# exit
Switch(config)# mac access-list extended good-protocols
Switch(config-ext-macl)# permit any any protocol-family decnet
Switch(config-ext-macl)# permit any any protocol-family vines
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map drop-mac-default 10
Switch(config-access-map)# match mac address good-hosts
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
Switch(config)# vlan access-map drop-mac-default 20
Switch(config-access-map)# match mac address good-protocols
Switch(config-access-map)# action forward
```

Example 4

In this example, the VLAN map is configured to drop all packets (IP and non-IP). By applying access lists **tcp-match** and **good-hosts**, the VLAN map is configured to do the following:

- Forward all TCP packets
- Forward MAC packets from hosts 0000.0c00.0111 and 0000.0c00.0211
- Drop all other IP packets
- Drop all other MAC packets

```
Switch(config)# vlan access-map drop-all-default 10
Switch(config-access-map)# match ip address tcp-match
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
Switch(config)# vlan access-map drop-all-default 20
Switch(config-access-map)# match mac address good-hosts
Switch(config-access-map)# action forward
```

Applying a VLAN Map to a VLAN

To apply a VLAN map to one or more VLANs, perform this task:

|        | Command                                                                    | Purpose                                                                                                                                                                                                    |
|--------|----------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch# <b>configure terminal</b>                                          | Enters global configuration mode.                                                                                                                                                                          |
| Step 2 | Switch(config)# <b>vlan filter</b><br><i>mapname</i> <b>vlan-list list</b> | Applies the VLAN map to one or more VLAN IDs.<br><br>The list can be a single VLAN ID (22), a consecutive list (10-22), or a string of VLAN IDs (12, 22, 30). Spaces around comma, and dash, are optional. |
| Step 3 | Switch(config)# <b>show</b><br><b>running-config</b>                       | Displays the access list configuration.                                                                                                                                                                    |
| Step 4 | cSwitch(config)# <b>copy</b><br><b>running-config startup-config</b>       | (Optional) Saves your entries in the configuration file.                                                                                                                                                   |

**Note**

You cannot apply a VLAN map to a VLAN on a switch that has ACLs applied to Layer 2 interfaces (port ACLs).

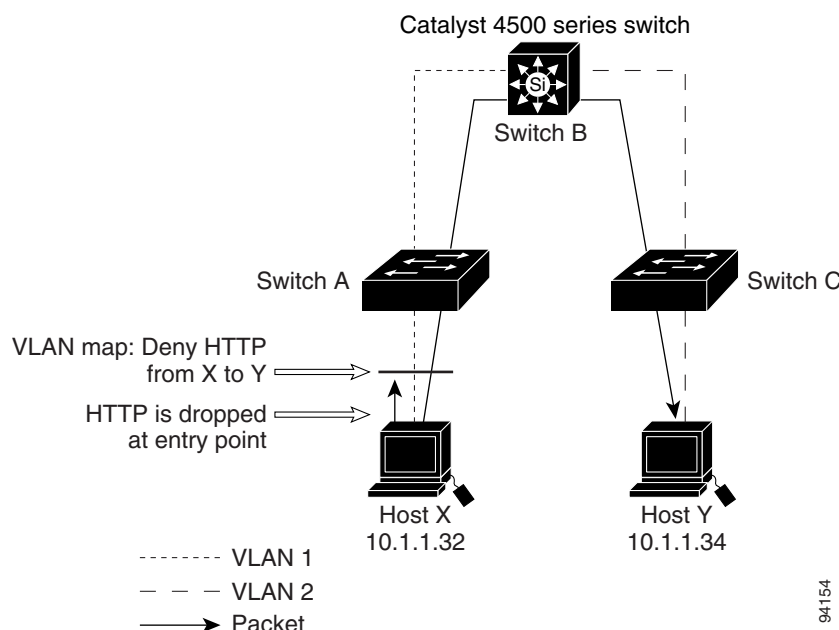
This example shows how to apply VLAN map 1 to VLANs 20 through 22:

```
Switch(config)# vlan filter map 1 vlan-list 20-22
```

## Using VLAN Maps in Your Network

Figure 24-3 shows a typical wiring closet configuration. Host X and Host Y are in different VLANs, connected to wiring closet switches A and C. Traffic moving from Host X to Host Y is routed by Switch B. Access to traffic moving from Host X to Host Y can be controlled at the entry point of Switch A. In the following configuration, the switch can support a VLAN map and a QoS classification ACL.

**Figure 24-3 Wiring Closet Configuration**



For example, if you do not want HTTP traffic to be switched from Host X to Host Y, you could apply a VLAN map on Switch A to drop all HTTP traffic moving from Host X (IP address 10.1.1.32) to Host Y (IP address 10.1.1.34) at Switch A and not bridge the traffic to Switch B. To configure this scenario, you would do the following:

First, define an IP access list http to permit (match) any TCP traffic on the HTTP port, as follows:

```
Switch(config)# ip access-list extended http
Switch(config-ext-nacl)# permit tcp host 10.1.1.32 host 10.1.1.34 eq www
Switch(config-ext-nacl)# exit
```

Next, create a VLAN access map named map2 so that traffic that matches the http access list is dropped and all other IP traffic is forwarded, as follows:

```
Switch(config)# vlan access-map map2 10
Switch(config-access-map)# match ip address http
Switch(config-access-map)# action drop
Switch(config-access-map)# exit
```

```

Switch(config)# ip access-list extended match_all
Switch(config-ext-nacl)# permit ip any any
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map map2 20
Switch(config-access-map)# match ip address match_all
Switch(config-access-map)# action forward

```

Then, apply the VLAN access map named map2 to VLAN 1, as follows:

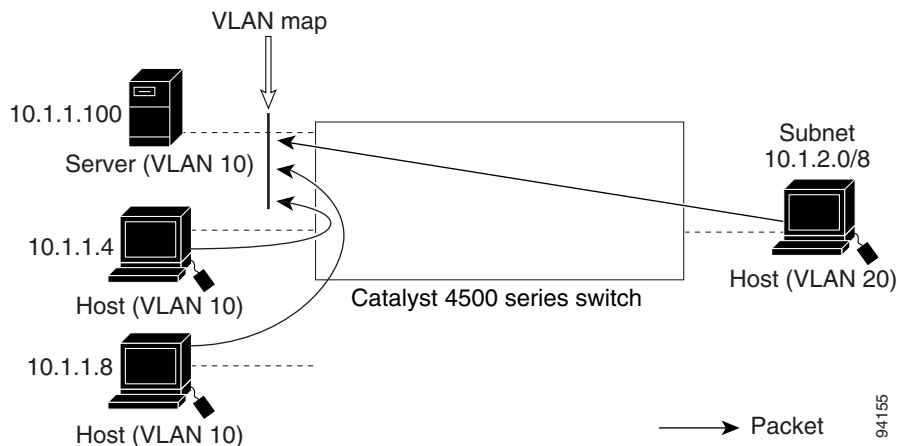
```
Switch(config)# vlan filter map2 vlan 1
```

## Denying Access to a Server on Another VLAN

Figure 24-4 shows how to restrict access to a server on another VLAN. In this example, server 10.1.1.100 in VLAN 10 has the following access restrictions:

- Hosts in subnet 10.1.2.0/8 in VLAN 20 should not have access.
- Hosts 10.1.1.4 and 10.1.1.8 in VLAN 10 should not have access.

**Figure 24-4 Deny Access to a Server on Another VLAN**



This procedure configures ACLs with VLAN maps to deny access to a server on another VLAN. The VLAN map SERVER 1\_ACL denies access to hosts in subnet 10.1.2.0/8, host 10.1.1.4, and host 10.1.1.8. Then it permits all other IP traffic. In Step 3, VLAN map SERVER1 is applied to VLAN 10.

To configure this scenario, you could take the following steps:

### Step 1 Define the IP ACL to match and permit the correct packets.

```

Switch(config)# ip access-list extended SERVER1_ACL
Switch(config-ext-nacl)# permit ip 10.1.2.0 0.0.0.255 host 10.1.1.100
Switch(config-ext-nacl)# permit ip host 10.1.1.4 host 10.1.1.100
Switch(config-ext-nacl)# permit ip host 10.1.1.8 host 10.1.1.100
Switch(config-ext-nacl)# exit

```

- Step 2** Define a VLAN map using the ACL to drop IP packets that match SERVER1\_ACL and forward IP packets that do not match the ACL.

```
Switch(config)# vlan access-map SERVER1_MAP
Switch(config-access-map)# match ip address SERVER1_ACL
Switch(config-access-map)# action drop
Switch(config)# vlan access-map SERVER1_MAP 20
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
```

- Step 3** Apply the VLAN map to VLAN 10.

```
Switch(config)# vlan filter SERVER1_MAP vlan-list 10.
```

## Displaying VLAN Access Map Information

To display information about VLAN access maps or VLAN filters, perform one of these tasks.

| Command                                                                                        | Purpose                                                                               |
|------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| Switch# <b>show vlan access-map</b> [ <i>mapname</i> ]                                         | Show information about all VLAN access-maps or the specified access map.              |
| Switch# <b>show vlan filter</b> [ <b>access-map</b> <i>name</i>   <b>vlan</b> <i>vlan-id</i> ] | Show information about all VLAN filters or about a specified VLAN or VLAN access map. |

This is a sample output of the **show vlan access-map** privileged EXEC command:

```
Switch# show vlan access-map
Vlan access-map "map_1" 10
 Match clauses:
 ip address: ip1
 Action:
 drop
Vlan access-map "map_1" 20
 Match clauses:
 mac address: mac1
 Action:
 forward
Vlan access-map "map_1" 30
 Match clauses:
 Action:
 drop
```



### Note

Sequence 30 does not have a match clause. All packets (IP as well as non-IP) will be matched against it and dropped.

This is a sample output of the **show vlan filter** privileged EXEC command:

```
Switch# show vlan filter
VLAN Map map_1 is filtering VLANs:
 20-22
```

## Using VLAN Maps with Router ACLs

If the VLAN map has a match clause for a packet type (IP or MAC) and the packet does not match the type, the default is to drop the packet. If there is no match clause in the VLAN map, and no action is specified, the packet is forwarded if it does not match any VLAN map entry.

**Note**

You cannot combine VLAN maps or input router ACLs with port ACLs on a switch.

## Guidelines for Using Router ACLs and VLAN Maps

Use these guidelines when you need to use a router ACL and a VLAN map on the same VLAN.

Because the switch hardware performs one lookup for each direction (input and output), you must merge a router ACL and a VLAN map when they are configured on the same VLAN. Merging the router ACL with the VLAN map can significantly increase the number of ACEs.

When possible, try to write the ACL so that all entries have a single action except for the final, default action. You should write the ACL using one of these two forms:

```
permit...
permit...
permit...
deny ip any any
```

or

```
deny...
deny...
deny...
permit ip any any
```

To define multiple permit or deny actions in an ACL, group each action type together to reduce the number of entries.

If you need to specify the full-flow mode and the ACL contains both IP ACEs and TCP/UDP/ICMP ACEs with Layer 4 information, put the Layer 4 ACEs at the end of the list. Doing this gives priority to the filtering of traffic based on IP addresses.

## Examples of Router ACLs and VLAN Maps Applied to VLANs

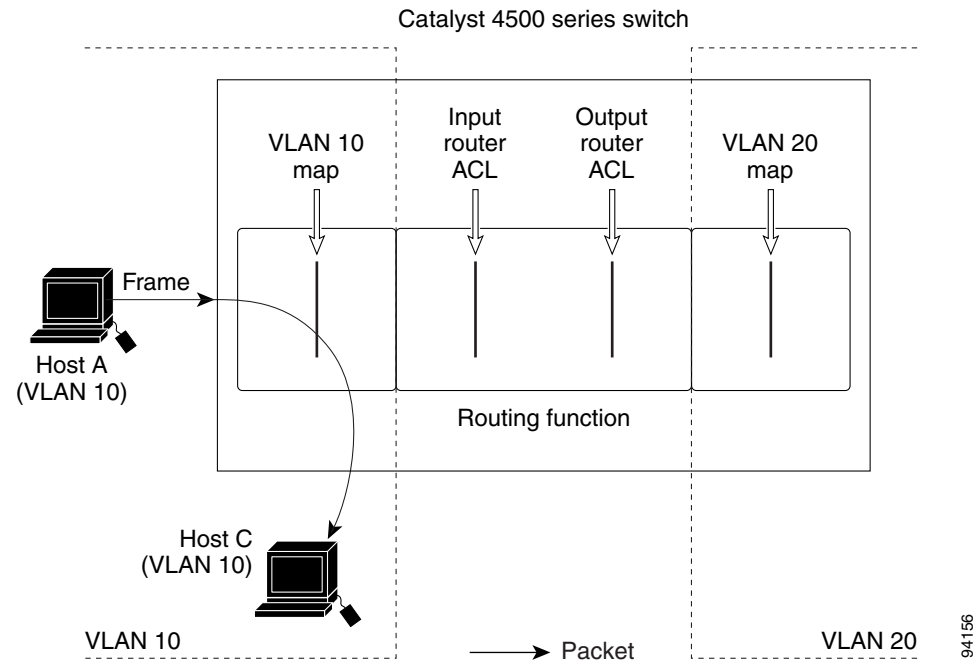
These examples show how router ACLs and VLAN maps are applied on a VLAN to control the access of switched, bridged, routed, and multicast packets. Although the following illustrations show packets being forwarded to their destination, each time a packet crosses a line indicating a VLAN map or an ACL, the packet could be dropped rather than forwarded.



## ACLs and Switched Packets

Figure 24-5 shows how an ACL processes packets that are switched within a VLAN. Packets switched within the VLAN are not processed by router ACLs.

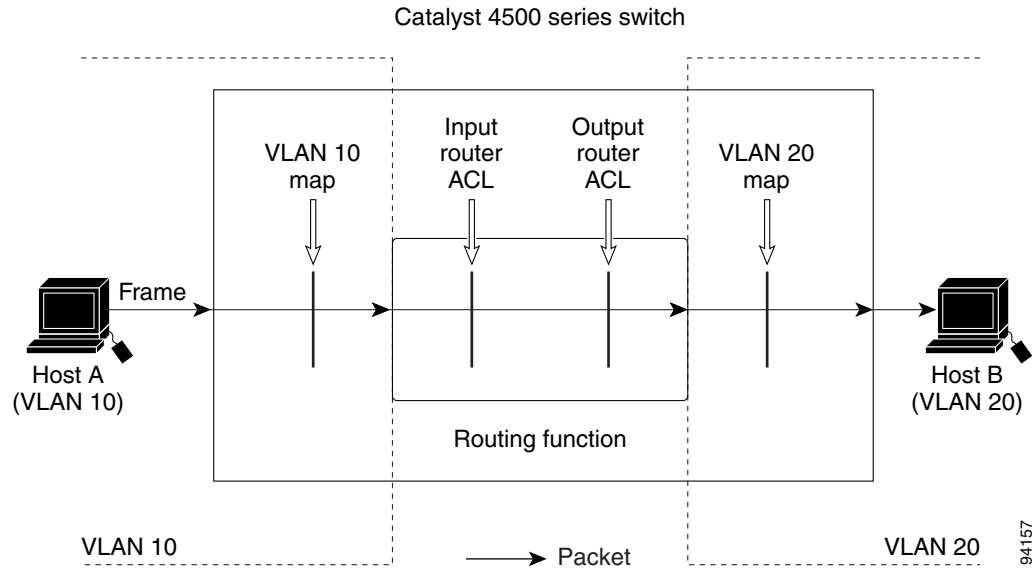
**Figure 24-5 Applying ACLs on Switched Packets**



## ACLs and Routed Packets

Figure 24-6 shows how ACLs are applied on routed packets. For routed packets, the ACLs are applied in this order:

1. VLAN map for input VLAN
2. Input router ACL
3. Output router ACL
4. VLAN map for output VLAN

**Figure 24-6 Applying ACLs on Routed Packets**

94157

## Configuring PACLS

This section describes how to configure PACLS, which are used to control filtering on Layer 2 interfaces. PACLS can filter traffic to or from Layer 2 interfaces based on Layer 3 information, Layer 4 head information or non-IP Layer 2 information.

This section contains the following topics:

- Creating a PACL, page 24-20
- PACL Configuration Guidelines, page 24-21
- Configuring IP and MAC ACLs on a Layer 2 interface, page 24-21
- Using PACL with Access-group Mode, page 24-22
- Configuring Access-group Mode on Layer 2 Interface, page 24-22
- Applying ACLs to a Layer 2 Interface, page 24-23
- Displaying an ACL Configuration on a Layer 2 Interface, page 24-23

## Creating a PACL

To create a PACL and apply it to one or more interfaces, perform this task:

- 
- Step 1** Create the standard or extended IP ACLs or named MAC extended ACLs that you want to apply to the interface.
- Step 2** Use the **ip access-group** or **mac access-group interface** command to apply a IP ACL or MAC ACL to one or more Layer 2 interfaces.
-

## PACL Configuration Guidelines

Consider the following guidelines when configuring PACLS:

- There can be at most one IP access list and MAC access list applied to the same Layer 2 interface per direction.
- The IP access list filters only IP packets, whereas the MAC access list filters only non-IP packets.
- The number of ACLs and ACEs that can be configured as part of a PACL are bounded by the hardware resources on the switch. Those hardware resources are shared by various ACL features (for example, RACL, VACL) that are configured on the system. If there are insufficient hardware resources to program PACL in hardware, the actions for input and output PACLS differ:
  - For input PACLS, some packets are sent to CPU for software forwarding.
  - For output PACLS, the PACL is disabled on the port.
- These restrictions pertain to output PACLS only:
  - If there are insufficient hardware resources to program the PACL, the output PACL is not applied to the port, and you receive a warning message.
  - If an output PACL is configured on a Layer 2 port, then neither a VACL nor a Router ACL can be configured on the VLANs to which the Layer 2 port belongs.  
 If any VACL or Router ACL is configured on the VLANs to which the Layer 2 port belongs, the output PACL cannot be configured on the Layer 2 port. That is, PACLS and VLAN-based ACLs (VACL and Router ACL) are mutually exclusive on Layer 2 ports.
- The input IP ACL logging option is supported, although logging is not supported for output IP ACLs, and MAC ACLs.
- The access group mode can change the way PACLS interact with other ACLs. To maintain consistent behavior across Cisco platforms, use the default access group mode.

## Configuring IP and MAC ACLs on a Layer 2 interface

Only IP or MAC ACLs can be applied to Layer 2 physical interfaces. Standard (numbered, named) and Extended (numbered, named) IP ACLs, and Extended Named MAC ACLs are also supported.

To apply IP or MAC ACLs on a Layer 2 interface, perform this task:

|        | Command                                                                                                 | Purpose                                                                                                                     |
|--------|---------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch# <b>configure t</b>                                                                              | Enters global configuration mode.                                                                                           |
| Step 2 | Switch(config)# <b>interface</b><br><i>interface</i>                                                    | Enters interface config mode.                                                                                               |
| Step 3 | Switch(config-if)# <b>[no] {ip   mac}</b><br><b>} access-group {name   number  </b><br><b>in   out}</b> | Applies numbered or named ACL to the Layer 2 interface. The NO prefix deletes the IP or MAC ACL from the Layer 2 interface. |
| Step 4 | Switch(config)# <b>show</b><br><b>running-config</b>                                                    | Displays the access list configuration.                                                                                     |

The following example shows how to configure the Extended Named IP ACL `simple-ip-acl` to permit all TCP traffic and implicitly deny all other IP traffic:

```
Switch(config)# ip access-list extended simple-ip-acl
Switch(config-ext-nacl)# permit tcp any any
Switch(config-ext-nacl)# end
```

The following example shows how to configure the Extended Named MACL `simple-mac-acl` to permit source host 000.000.011 to any destination host:

```
Switch(config)# mac access-list extended simple-mac-acl
Switch(config-ext-macl)# permit host 000.000.011 any
Switch(config-ext-macl)# end
```

## Using PACL with Access-group Mode

You can use the access group mode to change the way PACLS interact with other ACLs. For example, if a Layer 2 interface belongs to VLAN100, VACL (VLAN filter) V1 is applied on VLAN100, and PACL P1 is applied on the Layer 2 interface. In this situation, you must specify how P1 and V1 impact the traffic with the Layer 2 interface on VLAN100. In a per-interface fashion, the **access-group mode** command can be used to specify one of the desired behaviors that are defined below.

The following modes are defined:

**prefer port mode**—If PACL is configured on a Layer 2 interface, then PACL takes effect and overwrites the effect of other ACLs (Router ACL and VACL). If no PACL feature is configured on the Layer 2 interface, other features applicable to the interface are merged and applied on the interface. This is the default access group mode.

**prefer vlan mode**—VLAN-based ACL features take effect on the port provided they have been applied on the port and no PACLS are in effect. If no VLAN-based ACL features are applicable to the Layer 2 interface, then the PACL feature already on the interface is applied.

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



### Note

Because output PACLS are mutually exclusive with VACL and Router ACLs, the access group mode does not change the behavior of output traffic filtering.

## Configuring Access-group Mode on Layer 2 Interface

To configure an access mode on a Layer 2 interface, perform this task:

|        | Command                                                                                                               | Purpose                                                                                                                     |
|--------|-----------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch# <b>configure t</b>                                                                                            | Enters global configuration mode.                                                                                           |
| Step 2 | Switch(config)# <b>interface</b><br><i>interface</i>                                                                  | Enters interface config mode.                                                                                               |
| Step 3 | Switch(config-if)# [no]<br><b>access-group mode</b><br>{ <b>prefer</b> { <b>port</b>   <b>vlan</b> }   <b>merge</b> } | Applies numbered or named ACL to the Layer 2 interface. The no prefix deletes the IP or MAC ACL from the Layer 2 interface. |
| Step 4 | Switch(config)# <b>show</b><br><b>running-config</b>                                                                  | Displays the access list configuration.                                                                                     |

This example shows how to merge and apply features other than PACL on the interface:

```
Switch# configure t
Switch(config)# interface interface
Switch(config-if)# access-group mode prefer port
```

This example shows how to merge applicable ACL features before they are programmed into hardware:

```
Switch# configure t
Switch(config)# interface interface
Switch(config-if)# access-group mode merge
```

## Applying ACLs to a Layer 2 Interface

To apply IP and MAC ACLs to a Layer 2 interface, perform one of these tasks:

| Command                                                            | Purpose                                     |
|--------------------------------------------------------------------|---------------------------------------------|
| Switch(config-if)# <b>ip access-group</b> <i>ip-acl</i> {in out}   | Applies an IP ACL to the Layer 2 interface  |
| Switch(config-if)# <b>mac access-group</b> <i>mac-acl</i> {in out} | Applies a MAC ACL to the Layer 2 interface. |



### Note

Supervisor Engines III and Supervisor Engine IV running on a Catalyst 4500 series switch support both input and output PACLS on an interface.

This example applies the extended named IP ACL *simple-ip-acl* to interface FastEthernet 6/1 ingress traffic:

```
Switch# configure t
Switch(config)# interface fastEthernet 6/1
Switch(config-if)# ip access-group simple-ip-acl in
```

This example applies the extended named MAC ACL *simple-mac-acl* to interface FastEthernet 6/1 egress traffic:

```
Switch# configure t
Switch(config)# interface fastEthernet 6/1
Switch(config-if)# mac access-group simple-mac-acl out
```

## Displaying an ACL Configuration on a Layer 2 Interface

To display information about an ACL configuration on Layer 2 interfaces, perform one of these tasks:

| Command                                                                   | Purpose                                                     |
|---------------------------------------------------------------------------|-------------------------------------------------------------|
| Switch# <b>show ip interface</b> [ <i>interface-name</i> ]                | Shows the IP access group configuration on the interface.   |
| Switch# <b>show mac access-group interface</b> [ <i>interface-name</i> ]  | Shows the MAC access group configuration on the interface.  |
| Switch# <b>show access-group mode interface</b> [ <i>interface-name</i> ] | Shows the access group mode configuration on the interface. |

This example shows that the IP access group `simple-ip-acl` is configured on the inbound direction of interface `fa6/1`:

```
Switch# show ip interface fast 6/1
FastEthernet6/1 is up, line protocol is up
 Inbound access list is simple-ip-acl
 Outgoing access list is not set
```

This example shows that MAC access group `simple-mac-acl` is configured on the inbound direction of interface `fa6/1`:

```
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
```

This example shows that access group merge is configured on interface `fa6/1`:

```
Switch# show access-group mode interface fast 6/1
Interface FastEthernet6/1:
 Access group mode is: merge
```

## Using PACL with VLAN Maps and Router ACLs

For output PACLs, there is no interaction with VACL or output Router ACLs. (See the restrictions listed in the “PACL Configuration Guidelines” section on page 24-21.) For input PACLs, however, the interaction with Router ACLs and VACLs depends on the interface access group mode as shown in Table 24-1.

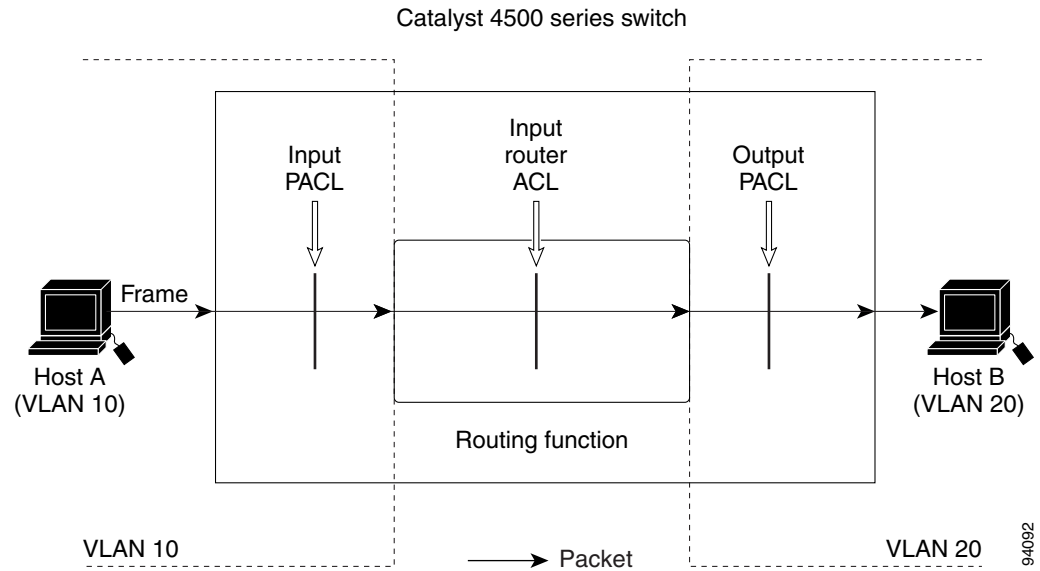
**Table 24-1 Interaction Between PACLs, VACLs and Router ACLs**

| ACL Type(s)                       | Input PACL       |                                 |                                                                  |
|-----------------------------------|------------------|---------------------------------|------------------------------------------------------------------|
|                                   | prefer port mode | prefer vlan mode                | merge mode                                                       |
| <b>1) Input Router ACL</b>        | PACL applied     | Input Router ACL applied        | PACL, Input Router ACL (merged) applied in order (ingress)       |
| <b>2) VACL</b>                    | PACL applied     | VACL applied                    | PACL, VACL (merged) applied in order (ingress)                   |
| <b>3) VACL + Input Router ACL</b> | PACL applied     | VACL + Input Router ACL applied | PACL, VACL, Input Router ACL (merged) applied in order (ingress) |

Each ACL Type listed in Table 24-1 is synonymous with a different scenario, as explained in the following discussion.

Scenario 1: Host A is connected to an interface in VLAN 20, which has an SVI configured. The interface has input PACL configured, and the SVI has input Router ACL configured as shown in Figure 24-7:

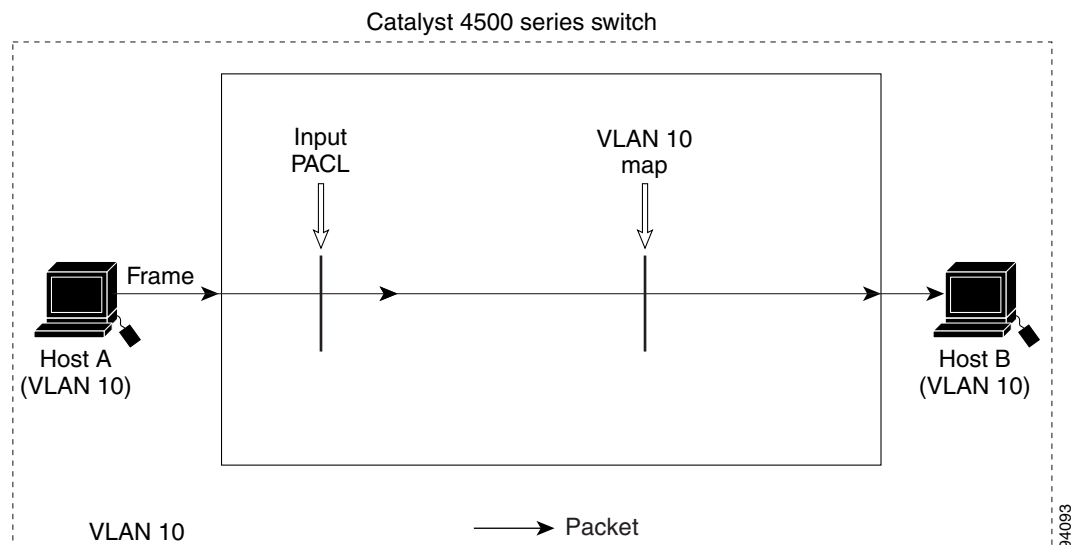
**Figure 24-7 Scenario 1: PACL Interaction with an Input Router ACL**



If the interface access group mode is prefer port, then only the input PACL is applied on the ingress traffic from Host A. If the mode is prefer vlan, then only the input Router ACL is applied to ingress traffic from Host A that requires routing. If the mode is merge, then the input PACL is first applied to the ingress traffic from Host A, and the input Router ACL is applied on the traffic that requires routing.

Scenario 2: Host A is connected to an interface in VLAN 10, which has a VACL (VLAN Map) configured and an input PACL configured as shown in Figure 24-8:

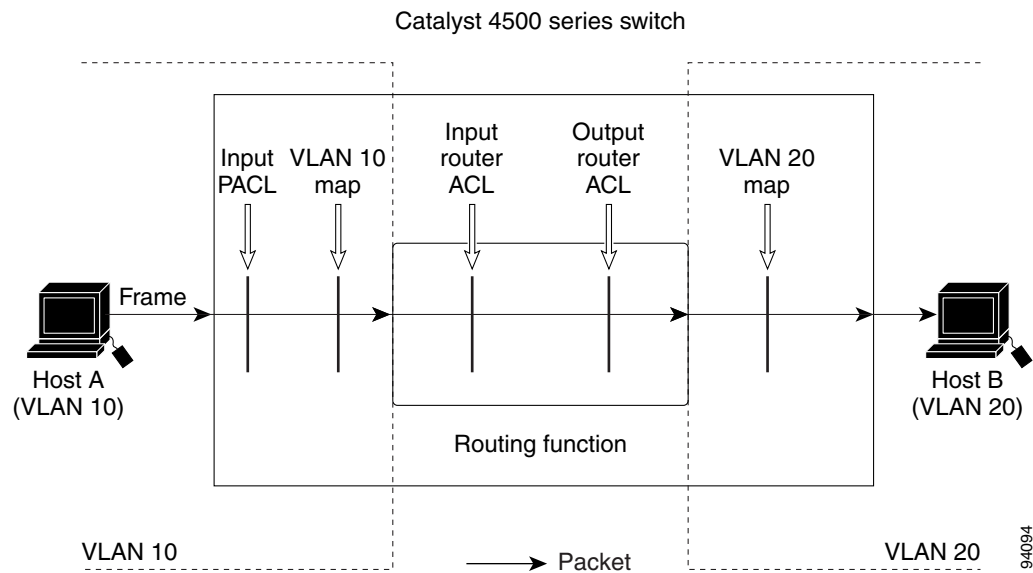
**Figure 24-8 Scenario 2: PACL Interaction with a VACL**



If the interface access group mode is `prefer port`, then only the input PACL is applied on the ingress traffic from Host A. If the mode is `prefer vlan`, then only the VACL is applied to the ingress traffic from Host A. If the mode is `merge`, the input PACL is first applied to the ingress traffic from Host A, and the VACL is applied on the traffic.

Scenario 3: Host A is connected to an interface in VLAN 10, which has a VACL and an SVI configured. The SVI has an input Router ACL configured and the interface has an input PACL configured, as shown in Figure 24-9:

**Figure 24-9 Scenario 3: VACL and Input Router ACL**



If the interface access group mode is `prefer port`, then only the input PACL is applied on the ingress traffic from Host A. If the mode is `prefer vlan`, then the merged results of the VACL and the input Router ACL are applied to the ingress traffic from Host A. If the mode is `merge`, the input PACL is first applied to the ingress traffic from Host A, the VACL is applied on the traffic and finally, and the input Router ACL is applied to the traffic that needs routing. (that is, the merged results of the input PACL, VACL, and input Router ACL are applied to the traffic).





## Configuring Port Security

This chapter describes how to configure the port security feature.



**Note**

For complete syntax and usage information for the switch commands used in this chapter, refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference* and related publications at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/index.htm>

This chapter consists of these sections:

- Understanding Port Security, page 25-1
- Default Port Security Configuration, page 25-2
- Port Security Guidelines and Restrictions, page 25-3
- Configuring Port Security, page 25-3
- Displaying Port Security Settings, page 25-7

## Understanding Port Security

You can use the port security feature to restrict input to an interface by limiting and identifying MAC addresses of the workstations that are allowed to access the port. When you assign secure MAC addresses to a secure port, the port does not forward packets with source addresses outside the group of defined addresses. If you limit the number of secure MAC addresses to one and assign a single secure MAC address, the workstation attached to that port is assured the full bandwidth of the port.

If a port is configured as a secure port and the maximum number of secure MAC addresses is reached, when the MAC address of a workstation attempting to access the port is different from any of the identified secure MAC addresses, a security violation occurs.

After you have set the maximum number of secure MAC addresses on a port, the secure addresses are included in an address table in one of these ways:

- You can configure all secure MAC addresses by using the **switchport port-security mac-address mac\_address** interface configuration command.
- You can allow the port to dynamically configure secure MAC addresses with the MAC addresses of connected devices.
- You can configure a number of addresses and allow the rest to be dynamically configured.

**Note**

If the port shuts down, all dynamically learned addresses are removed.

After the maximum number of secure MAC addresses is configured, they are stored in an address table. To ensure that an attached device has the full bandwidth of the port, configure the MAC address of the attached device and set the maximum number of addresses to one, which is the default.

**Note**

When a Catalyst 4000 switch port is configured to support voice as well as port security, the maximum number of allowable MAC addresses on this port should be changed to three.

A security violation occurs if the maximum number of secure MAC addresses has been added to the address table and a workstation whose MAC address is not in the address table attempts to access the interface.

You can configure the interface for one of these violation modes, based on the action to be taken if a violation occurs:

- **Restrict**—A port security violation restricts data, causes the SecurityViolation counter to increment, and causes an SNMP Notification to be generated. The rate at which SNMP traps are generated can be controlled by the **snmp-server enable traps port-security trap-rate** command. The default value (“0”) causes an SNMP trap to be generated for every security violation.
- **Shutdown**—A port security violation causes the interface to shut down immediately. When a secure port is in the error-disabled state, you can bring it out of this state by entering the **errdisable recovery cause psecure\_violation** global configuration command or you can manually reenale it by entering the **shutdown** and **no shut down** interface configuration commands. This is the default mode.

You can also customize the time to recover from the specified error disable cause (default is 300 seconds) by entering the **errdisable recovery interval interval** command.

## Default Port Security Configuration

Table 25-1 shows the default port security configuration for an interface.

**Table 25-1 Default Port Security Configuration**

| Feature                                | Default Setting                                                                                                                   |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| Port security                          | Disabled on a port                                                                                                                |
| Maximum number of secure MAC addresses | 1                                                                                                                                 |
| Violation mode                         | Shutdown. The port shuts down when the maximum number of secure MAC addresses is exceeded, and an SNMP trap notification is sent. |
| Aging                                  | Disabled                                                                                                                          |
| Aging type                             | Absolute                                                                                                                          |
| Static Aging                           | Disabled                                                                                                                          |

# Port Security Guidelines and Restrictions

Follow these guidelines when configuring port security:

- A secure port cannot be a trunk port.
- A secure port cannot be a destination port for Switch Port Analyzer (SPAN).
- A secure port cannot belong to an EtherChannel port-channel interface.
- A secure port cannot be an 802.1X port. If you try to enable 802.1X on a secure port, an error message appears, and 802.1X is not enabled. If you try to change an 802.1X-enabled port to a secure port, an error message appears, and the security settings are not changed.
- A secure port and static MAC address configuration are mutually exclusive.

## Configuring Port Security

These sections describe how to configure port security:

- Configuring Port Security on an Interface, page 25-3
- Configuring Port Security Aging, page 25-5

### Configuring Port Security on an Interface

To restrict traffic through a port by limiting and identifying MAC addresses of the stations allowed to access the port, perform this task:

|        | Command                                                                    | Purpose                                                                                                                        |
|--------|----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch(config)# <b>interface</b> <i>interface_id</i>                       | Enters interface configuration mode and enters the physical interface to configure, for example <b>gigabitethernet 3/1</b> .   |
| Step 2 | Switch(config-if)# <b>switchport mode access</b>                           | Sets the interface mode as access; an interface in the default mode (dynamic desirable) cannot be configured as a secure port. |
| Step 3 | Switch(config-if)# <b>switchport port-security</b>                         | Enables port security on the interface.                                                                                        |
| Step 4 | Switch(config-if)# <b>switchport port-security</b><br><i>maximum value</i> | (Optional) Sets the maximum number of secure MAC addresses for the interface. The range is 1 to 1024; the default is 1.        |

|        | Command                                                                                                       | Purpose (continued)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------|---------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5 | Switch(config-if)# <b>switchport port-security violation {restrict   shutdown}</b>                            | <p>(Optional) Sets the violation mode, the action to be taken when a security violation is detected, as one of these:</p> <ul style="list-style-type: none"> <li>• <b>restrict</b>—A port security violation restricts data and causes the SecurityViolation counter to increment and send an SNMP trap notification.</li> <li>• <b>shutdown</b>—The interface is error-disabled when a security violation occurs.</li> </ul> <p><b>Note</b> When a secure port is in the error-disabled state, you can bring it out of this state by entering the <b>errdisable recovery cause psecure-violation</b> global configuration command or you can manually reenab it by entering the <b>shutdown</b> and <b>no shut down</b> interface configuration commands.</p> |
| Step 6 | Switch(config-if)# <b>switchport port-security limit rate invalid-source-mac</b>                              | Sets the rate limit for bad packets.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Step 7 | Switch(config-if)# <b>switchport port-security mac-address mac_address</b>                                    | (Optional) Enters a secure MAC address for the interface. You can use this command to enter the maximum number of secure MAC addresses. If you configure fewer secure MAC addresses than the maximum, the remaining MAC addresses are dynamically learned.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Step 8 | Switch(config-if)# <b>end</b>                                                                                 | Returns to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Step 9 | Switch# <b>show port-security address interface interface_id</b><br>Switch# <b>show port-security address</b> | Verifies your entries.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

- To return the interface to the default condition as not a secure port, use the **no switchport port-security** interface configuration command.
- To return the interface to the default number of secure MAC addresses, use the **no switchport port-security maximum value**.
- To delete a MAC address from the address table, use the **no switchport port-security mac-address mac\_address** command.
- To return the violation mode to the default condition (shutdown mode), use the **no switchport port-security violation {restrict | shutdown}** command.

This example shows how to enable port security on Fast Ethernet port 12 and how to set the maximum number of secure addresses to 5. The violation mode is the default, and no secure MAC addresses are configured.

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 3/12
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 5
Switch(config-if)# end
Switch# show port-security interface fastethernet 3/12
Port Security :Enabled
Port Status :Secure-up
Violation Mode :Shutdown
Aging Time :0
Aging Type :Absolute
SecureStatic Address Aging :Enabled
Maximum MAC Addresses :5
Total MAC Addresses :0
Configured MAC Addresses :0
Last Source Address :0000.0000.0401
Security Violation Count :0
```

This example shows how to configure a secure MAC address on Fast Ethernet port 12 and verify the configuration:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 5/12
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address 1000.2000.3000
Switch(config-if)# end
Switch#sh port-security address
 Secure Mac Address Table

Vlan Mac Address Type Ports Remaining Age
 (mins)
---- -
 1 1000.2000.3000 SecureConfigured Fa5/12 15 (I)
```

## Configuring Port Security Aging

You can use port security aging to set the aging time and aging type for all secure addresses on a port.

Use this feature to remove and add PCs on a secure port without manually deleting the existing secure MAC addresses while still limiting the number of secure addresses on a port.

To configure port security aging, perform this task:

|        | Command                                                                                                                                                                         | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch(config)# <b>interface</b> <i>interface_id</i>                                                                                                                            | Enters interface configuration mode for the port on which you want to enable port security aging.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Step 2 | Switch(config-if)# <b>switchport port-security</b><br>[ <b>aging</b> { <b>static</b>   <b>time</b> <i>aging_time</i>   <b>type</b><br>{ <b>absolute</b>   <b>inactivity</b> } ] | Sets the aging time for the secure port.<br><br>The <b>static</b> keyword enables aging for statically configured secure addresses on this port.<br><br>The <b>time</b> <i>aging_time</i> keyword specifies the aging time for this port. Valid range for <i>aging_time</i> is from 0 to 1440 minutes. If the time is equal to 0, aging is disabled for this port.<br><br>The <b>type</b> keyword sets the aging type as <b>absolute</b> or <b>inactive</b> . For 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. For inactive 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. |
| Step 3 | Switch(config-if)# <b>end</b>                                                                                                                                                   | Returns to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Step 4 | Switch# <b>show port security</b> [ <i>interface interface_id</i> ] [ <i>address</i> ]                                                                                          | Verifies your entries.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

To disable port security aging for all secure addresses on a port, use the **no switchport port-security aging time** interface configuration command.

This example shows how to set the aging time as 2 hours for the secure addresses on the Fast Ethernet interface 5/1:

```
Switch(config)# interface fastethernet 5/1
Switch(config-if)# switchport port-security aging time 120
```

This example shows how to set the aging time as 2 minutes:

```
Switch(config-if)# switchport port-security aging time 2
```

You can verify the previous commands by entering the **show port-security interface** *interface\_id* privileged EXEC command.

# Displaying Port Security Settings

Use the **show port-security** command to display port-security settings for an interface or for the switch.

To display traffic control information, perform one or more of these tasks:

| Command                                                                                   | Purpose                                                                                                                                                                                                                                                                                            |
|-------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Switch# <b>show port-security</b> [ <b>interface</b> <i>interface_id</i> ]                | Displays port security settings for the switch or for the specified interface, including the maximum allowed number of secure MAC addresses for each interface, the number of secure MAC addresses on the interface, the number of security violations that have occurred, and the violation mode. |
| Switch# <b>show port-security</b> [ <b>interface</b> <i>interface_id</i> ] <b>address</b> | Displays all secure MAC addresses configured on all switch interfaces or on a specified interface with aging information for each address.                                                                                                                                                         |

This example displays output from the **show port-security** command when you do not enter an interface:

```
Switch# show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
 (Count) (Count) (Count)

 Fa3/1 2 2 0 Restrict
 Fa3/2 2 2 0 Restrict
 Fa3/3 2 2 0 Shutdown
 Fa3/4 2 2 0 Shutdown
 Fa3/5 2 2 0 Shutdown
 Fa3/6 2 2 0 Shutdown
 Fa3/7 2 2 0 Shutdown
 Fa3/8 2 2 0 Shutdown
 Fa3/10 1 0 0 Shutdown
 Fa3/11 1 0 0 Shutdown
 Fa3/12 1 0 0 Restrict
 Fa3/13 1 0 0 Shutdown
 Fa3/14 1 0 0 Shutdown
 Fa3/15 1 0 0 Shutdown
 Fa3/16 1 0 0 Shutdown

Total Addresses in System (excluding one mac per port) :8
Max Addresses limit in System (excluding one mac per port) :1024
Global SNMP trap control for port-security :20 (traps per
second)
```

This example displays output from the **show port-security** command for a specified interface:

```
Switch# show port-security interface fastethernet 5/1
Port Security :Enabled
Port Status :Secure-up
Violation Mode :Restrict
Aging Time :15 mins
Aging Type :Absolute
SecureStatic Address Aging :Enabled
Maximum MAC Addresses :2
Total MAC Addresses :2
Configured MAC Addresses :2
Last Source Address :0000.0000.0401
Security Violation Count :0
```

This example displays output from the **show port-security address** command:

```
Switch#sh port-security address
 Secure Mac Address Table

```

| Vlan | Mac Address    | Type             | Ports | Remaining Age<br>(mins) |
|------|----------------|------------------|-------|-------------------------|
| 1    | 0000.0001.0000 | SecureConfigured | Fa3/1 | 15 (I)                  |
| 1    | 0000.0001.0001 | SecureConfigured | Fa3/1 | 14 (I)                  |
| 1    | 0000.0001.0100 | SecureConfigured | Fa3/2 | -                       |
| 1    | 0000.0001.0101 | SecureConfigured | Fa3/2 | -                       |
| 1    | 0000.0001.0200 | SecureConfigured | Fa3/3 | -                       |
| 1    | 0000.0001.0201 | SecureConfigured | Fa3/3 | -                       |
| 1    | 0000.0001.0300 | SecureConfigured | Fa3/4 | -                       |
| 1    | 0000.0001.0301 | SecureConfigured | Fa3/4 | -                       |
| 1    | 0000.0001.1000 | SecureConfigured | Fa3/5 | -                       |
| 1    | 0000.0001.1001 | SecureConfigured | Fa3/5 | -                       |
| 1    | 0000.0001.1100 | SecureConfigured | Fa3/6 | -                       |
| 1    | 0000.0001.1101 | SecureConfigured | Fa3/6 | -                       |
| 1    | 0000.0001.1200 | SecureConfigured | Fa3/7 | -                       |
| 1    | 0000.0001.1201 | SecureConfigured | Fa3/7 | -                       |
| 1    | 0000.0001.1300 | SecureConfigured | Fa3/8 | -                       |
| 1    | 0000.0001.1301 | SecureConfigured | Fa3/8 | -                       |

```

Total Addresses in System (excluding one mac per port) :8
Max Addresses limit in System (excluding one mac per port) :1024
```





## Configuring 802.1x Port-Based Authentication

This chapter describes how to configure IEEE 802.1x port-based authentication to prevent unauthorized client devices from gaining access to the network.

This chapter consists of the following major sections:

- Understanding 802.1x Port-Based Authentication, page 26-1
- How to Configure 802.1x, page 26-6
- Displaying 802.1x Statistics and Status, page 26-16



**Note**

For complete syntax and usage information for the switch commands used in this chapter, refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference* and related publications at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/index.htm>

## Understanding 802.1x Port-Based Authentication



**Note**

802.1x authentication will not work unless the switch is able to route packets to the configured RADIUS server. You can verify that the switch is able to route packets to the RADIUS server by pinging the server from the switch.

The IEEE 802.1x standard defines 802.1x port-based authentication as a client-server based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. The authentication server validates each client connected to a switch port before making available any services offered by the switch or the LAN.

Until the client is authenticated, 802.1x access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.

To configure 802.1x on this switch, you need to understand the concepts covered in the following sections:

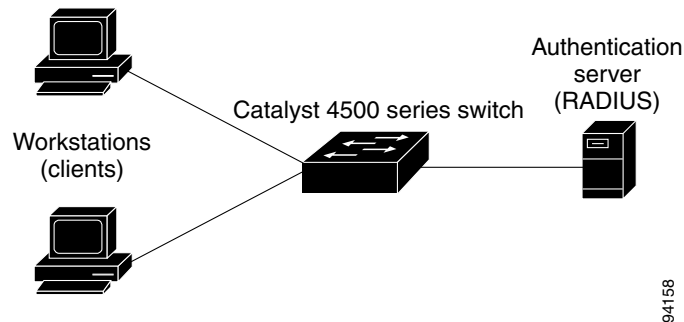
- Device Roles, page 26-2
- Authentication Initiation and Message Exchange, page 26-3
- Ports in Authorized and Unauthorized States, page 26-4
- Using 802.1X with VLAN Assignment, page 26-4

- Using 802.1x Authentication for Guest VLANs, page 26-5
- Supported Topologies, page 26-6

## Device Roles

With 802.1x port-based authentication, network devices have specific roles. Figure 26-1 shows the roles of each device.

**Figure 26-1 802.1x Device Roles**



- **Client**—The workstation that requests access to the LAN, switch services, and responds to requests from the switch. The workstation must be running 802.1x-compliant client software such as that offered with the Microsoft Windows XP operating system.



### Note

For more information on Windows XP network connectivity and 802.1x authentication issues, see the Microsoft Knowledge Base article at this URL:  
<http://support.microsoft.com/support/kb/articles/Q303/5/97.ASP>

- **Authentication server**—Performs the actual authentication of the client. The authentication server validates the identity of the client and notifies the switch whether the client is authorized to access the LAN and switch services. Because the switch acts as the proxy, the authentication service is transparent to the client. The Remote Authentication Dial-In User Service (RADIUS) security system with Extensible Authentication Protocol (EAP) extensions is the only supported authentication server; it is available in Cisco Secure Access Control Server version 3.0. RADIUS operates in a client/server model in which secure authentication information is exchanged between the RADIUS server and one or more RADIUS clients.
- **Switch (edge switch or wireless access point)**—Controls physical access to the network based on the authentication status of the client. The switch acts as an intermediary (proxy) between the client and the authentication server, requesting identity information from the client, verifying that information with the authentication server, and relaying a response to the client. The switch includes the RADIUS client, which is responsible for encapsulating and decapsulating the EAP frames and interacting with the authentication server.

When the switch receives EAPOL frames and relays them to the authentication server, the Ethernet header is stripped and the remaining EAP frame is re-encapsulated in the RADIUS format. The EAP frames are not modified or examined during encapsulation, and the authentication server must support EAP within the native frame format. When the switch receives frames from the authentication server, the server's frame header is removed, leaving the EAP frame, which is then encapsulated for Ethernet and sent to the client.

The devices that can act as intermediaries include other Catalyst 4000 family switches, the Catalyst 3550 multilayer switch, the Catalyst 2950 switch, or a wireless access point. These devices must be running software that supports the RADIUS client and 802.1x.

## Authentication Initiation and Message Exchange

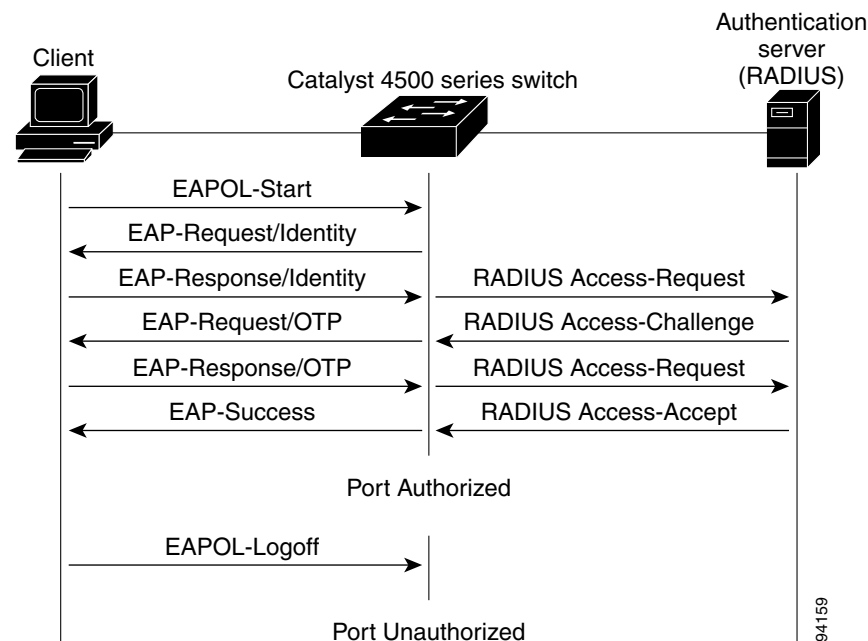
The switch or the client can initiate authentication. If you enable authentication on a port by using the **dot1x port-control auto** interface configuration command, the switch must initiate authentication when it determines that the port link state has changed. It then sends an EAP-request/identity frame to the client to request its identity (typically, the switch sends an initial identity/request frame followed by one or more requests for authentication information). Upon receipt of the frame, the client responds with an EAP-response/identity frame.

However, if during bootup, the client does not receive an EAP-request/identity frame from the switch, the client can initiate authentication by sending an EAPOL-start frame, which prompts the switch to request the client's identity.

If 802.1x is not enabled or supported on the network access device, any EAPOL frames from the client are dropped. If the client does not receive an EAP-request/identity frame after three attempts to start authentication, the client transmits frames as if the port is in the authorized state. A port in the authorized state effectively means that the client has been successfully authenticated. When the client supplies its identity, the switch begins its role as the intermediary, passing EAP frames between the client and the authentication server until authentication succeeds or fails. If the authentication succeeds, the switch port becomes authorized.

The specific exchange of EAP frames depends on the authentication method being used. Figure 26-2 shows a message exchange initiated by the client using the One-Time Password (OTP) authentication method with a RADIUS server.

**Figure 26-2 Message Exchange**



## Ports in Authorized and Unauthorized States

The switch port state determines whether or not the client is granted access to the network. The port starts in the unauthorized state. While in this state, the port disallows all ingress and egress traffic except for 802.1x protocol packets. When a client is successfully authenticated, the port transitions to the authorized state, allowing all traffic for the client to flow normally.

If a client that does not support 802.1x is connected to an unauthorized 802.1x port, the switch requests the client's identity. In this situation, the client does not respond to the request, the port remains in the unauthorized state, and the client is not granted access to the network. If the guest VLAN feature is configured for a port that connects to a 802.1x in-capable client, the port will be placed in the authorized state and assigned the guest VLAN. For more details, see "Using 802.1x Authentication for Guest VLANs" section on page 26-5.

In contrast, when an 802.1x-enabled client connects to a port that is not running the 802.1x protocol, the client initiates the authentication process by sending the EAPOL-start frame. When no response is received, the client sends the request a fixed number of times. Because no response is received, the client begins sending frames as if the port is in the authorized state.

You can control the port authorization state with the **dot1x port-control** interface configuration command and these keywords:

- **force-authorized**—Disables 802.1x authentication 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. This is the default setting.
- **force-unauthorized**—Causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the interface.
- **auto**—Enables 802.1x authentication and causes the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received 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 switch requests the identity of the client and begins relaying authentication messages between the client and the authentication server. Each client attempting to access the network is uniquely identified by the switch by using the client's MAC address.

If the client is successfully authenticated (receives an Accept frame from the authentication server), the port state changes to authorized, and all frames from the authenticated client are allowed through the port. If the authentication fails, the port remains in the unauthorized state, but authentication can be retried. If the authentication server cannot be reached, the switch can retransmit the request. If no response is received from the server after the specified number of attempts, authentication fails and network access is not granted.

When a client logs off, it sends an EAPOL-logoff message, causing the switch port to transition to the unauthorized state.

If the link state of a port transitions from up to down, or if an EAPOL-logoff frame is received, the port returns to the unauthorized state.

## Using 802.1X with VLAN Assignment

You can use the VLAN assignment to limit network access for certain users. With the VLAN assignment, 802.1X-authenticated ports are assigned to a VLAN based on the username of the client connected to that port. The RADIUS server database maintains the username-to-VLAN mappings. After successful 802.1X authentication of the port, the RADIUS server sends the VLAN assignment to the user.

When configured on the switch and the RADIUS server, 802.1X with the VLAN assignment has these characteristics:

- If no VLAN is supplied by the RADIUS server or if AAA authorization is disabled, the port is configured in its access VLAN after successful authentication.
- If authorization is enabled but the VLAN information from the server is not valid, the port remains down in the unauthenticated state. This situation prevents ports from appearing unexpectedly in an inappropriate VLAN because of a configuration error.

Configuration errors could include specifying a VLAN for a routed port, a malformed VLAN ID, a non-existent or internal (routed port) VLAN ID, or attempting an assignment to a voice VLAN ID.

- If authorization is enabled and all information from the server is valid, the port is placed in the specified VLAN after successful authentication.
- If the multiple-hosts mode is enabled, all hosts are in the same VLAN as the first authenticated user.
- If 802.1X is disabled on the port, it is returned to the configured access VLAN.

To configure VLAN assignment you need to:

- Enable AAA
- Enable 802.1X
- Assign vendor-specific tunnel attributes in the RADIUS server. The RADIUS server must return these attributes to the switch:
  - Tunnel-Type = VLAN
  - Tunnel-Medium-Type = 802
  - Tunnel-Private-Group-ID = VLAN NAME

The attribute must contain the value *VLAN* (type 13). The attribute must contain the value *802* (type 6). The attribute specifies the *VLAN name* assigned to the 802.1X-authenticated user.

## Using 802.1x Authentication for Guest VLANs

You can use the guest VLAN feature to enable non-802.1x capable hosts to access networks that use 802.1x authentication. For example, you can use this feature while you are upgrading your system to support 802.1x authentication.

The guest VLAN feature is supported on per-port basis, and you can use any VLAN (except a private VLAN) as a guest VLAN. If a port is already forwarding on the guest VLAN and you enable 802.1x support on the network interface of the host, the port is immediately moved out of the guest VLAN and the authenticator waits for authentication to occur.

Enabling 802.1x authentication on a port starts the 802.1x protocol. If the host fails to respond to the packets from the authenticator within a certain amount of time, the authenticator puts the port in the guest VLAN.

## Usage Guidelines for Using 802.1x Authentication with Guest VLANs on Windows-XP Hosts

The usage guidelines for using 802.1x authentication with guest VLANs on Windows-XP hosts are as follows:

- If the host fails to respond to the authenticator, the port will remain in the connecting state for 90 seconds (default). After this time period, the login / password window will not appear on the host, so you will need to unplug and then reconnect the network interface cable.

- Hosts that respond with an incorrect login / password will fail authentication. Hosts that fail authentication will not be put in the guest VLAN. The first time a host fails authentication, the quiet-period timer starts, and no activity will occur for the duration of the quiet-period timer. When the quiet-period timer expires, the host is presented with the login / password window. If the host fails authentication for the second time, the quiet-period timer starts again, and no activity will occur for the duration of the quiet-period timer. The host is presented with the login / password window a third time. If the host fails authentication the third time, the port is put in the connecting and unauthorized states, so you will need to unplug and then reconnect the network interface cable.

## Supported Topologies

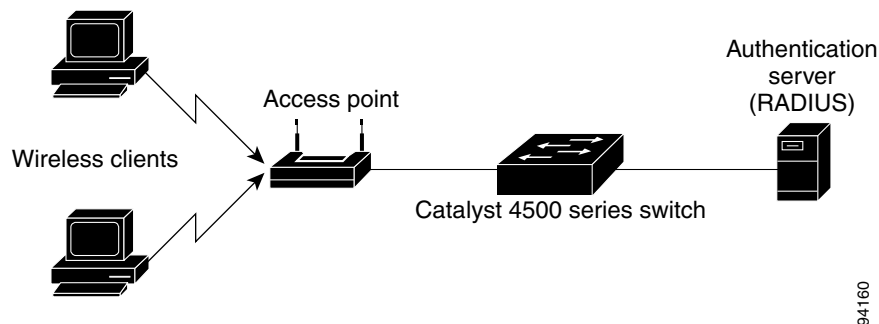
The 802.1x port-based authentication supports two topologies:

- Point-to-point
- Wireless LAN

In a point-to-point configuration (see Figure 26-1 on page 26-2), only one client can be connected to the 802.1x-enabled switch port. The switch detects the client when the port link state changes to the up state. If a client leaves or is replaced with another client, the switch changes the port link state to down, and the port returns to the unauthorized state.

Figure 26-3 shows 802.1x port-based authentication in a wireless LAN. The 802.1x port is configured as a multiple-host port that is authorized as soon as a client is authenticated. When the port is authorized, all other hosts indirectly attached to the port are granted access to the network. If the port becomes unauthorized (re-authentication fails or an EAPOL-logoff message is received), the switch denies access to the network to all attached clients. In this topology, the wireless access point is responsible for authenticating clients attached to it, and the wireless access point acts as a client to the switch.

**Figure 26-3 Wireless LAN Example**



## How to Configure 802.1x

These sections describe how to configure 802.1x:

- Default 802.1x Configuration, page 26-7
- 802.1x Configuration Guidelines, page 26-8
- Enabling 802.1x Authentication, page 26-8 (required)
- Configuring Switch-to-RADIUS-Server Communication, page 26-10 (required)
- Enabling Periodic Re-Authentication, page 26-11 (optional)

- Manually Re-Authenticating a Client Connected to a Port, page 26-12 (optional)
- Changing the Quiet Period, page 26-12 (optional)
- Changing the Switch-to-Client Retransmission Time, page 26-13 (optional)
- Setting the Switch-to-Client Frame-Retransmission Number, page 26-14 (optional)
- Enabling Multiple Hosts, page 26-15 (optional)
- Resetting the 802.1x Configuration to the Default Values, page 26-15 (optional)

## Default 802.1x Configuration

Table 26-1 shows the default 802.1x configuration.

**Table 26-1 Default 802.1x Configuration**

| Feature                                                                                                                        | Default Setting                                                                                                                                            |
|--------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Authentication, authorization, and accounting (AAA)                                                                            | Disabled                                                                                                                                                   |
| RADIUS server <ul style="list-style-type: none"> <li>• IP address</li> <li>• UDP authentication port</li> <li>• Key</li> </ul> | <ul style="list-style-type: none"> <li>• None specified</li> <li>• 1812</li> <li>• None specified</li> </ul>                                               |
| Per-interface 802.1x protocol enable state                                                                                     | Disabled (force-authorized)<br>The port transmits and receives normal traffic without 802.1x-based authentication of the client.                           |
| Periodic re-authentication                                                                                                     | Disabled                                                                                                                                                   |
| Time between re-authentication attempts                                                                                        | 3600 sec                                                                                                                                                   |
| Quiet period                                                                                                                   | 60 sec<br>Number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client.                         |
| Retransmission time                                                                                                            | 30 sec<br>Number of seconds that the switch should wait for a response to an EAP request/identity frame from the client before retransmitting the request. |
| Maximum retransmission number                                                                                                  | 2<br>Number of times that the switch will send an EAP-request/identity frame before restarting the authentication process.                                 |
| Multiple host support                                                                                                          | Disabled                                                                                                                                                   |

Table 26-1 Default 802.1x Configuration (continued)

| Feature                              | Default Setting                                                                                                                                                                                                          |
|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Client timeout period                | 30 sec<br><br>When relaying a request from the authentication server to the client, the amount of time the switch waits for a response before retransmitting the request to the client.                                  |
| Authentication server timeout period | 30 sec<br><br>When relaying a response from the client to the authentication server, the amount of time the switch waits for a reply before retransmitting the response to the server. This setting is not configurable. |

## 802.1x Configuration Guidelines

Keep these guidelines in mind when configuring 802.1x authentication:

- When 802.1x is enabled, ports are authenticated before any other Layer 2 or Layer 3 features are enabled.
- The 802.1x protocol is supported on both Layer 2 static-access ports and Layer 3 routed ports, but it is not supported on these port 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.
  - Default ports—All ports default as dynamic-access ports (auto). Use the **no switchport** command to access a router port.
  - 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 a not-yet active port of an EtherChannel, the port does not join the EtherChannel.
  - Switched 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.

## Enabling 802.1x Authentication

To enable 802.1x port-based authentication, you must enable AAA and specify the authentication method list. A method list describes the sequence and authentication methods to be queried to authenticate a user.



The software uses the first method listed to authenticate users; if that method fails to respond, the software selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this cycle, the authentication process stops, and no other authentication methods are attempted.

To configure 802.1x port-based authentication, perform this task:

|        | Command                                                                        | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------|--------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch # <b>configure terminal</b>                                             | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Step 2 | Switch(config)# <b>aaa new-model</b>                                           | Enables AAA.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Step 3 | Switch(config)# <b>aaa authentication dot1x {default} method1 [method2...]</b> | Creates an 802.1x authentication method list.<br><br>To create a default list that is used when a named list is not specified in the <b>authentication</b> command, use the <b>default</b> keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all interfaces.<br><br>Enter at least one of these keywords: <ul style="list-style-type: none"> <li>• <b>group radius</b>—Use the list of all RADIUS servers for authentication.</li> <li>• <b>none</b>—Use no authentication. The client is automatically authenticated by the switch without using the information supplied by the client.</li> </ul> |
| Step 4 | Switch(config)# <b>interface interface-id</b>                                  | Enters interface configuration mode and specify the interface to be enabled for 802.1x authentication.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Step 5 | Switch(config-if)# <b>dot1x port-control auto</b>                              | Enables 802.1x authentication on the interface.<br><br>For feature interaction information with trunk, dynamic, dynamic-access, EtherChannel, secure, and SPAN ports, see the “802.1x Configuration Guidelines” section on page 26-8.                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Step 6 | Switch(config-if)# <b>end</b>                                                  | Returns to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Step 7 | Switch # <b>show dot1x all</b>                                                 | Verifies your entries.<br><br>Check the Status column in the 802.1x Port Summary section of the display. An enabled status means the port-control value is set either to <b>auto</b> or to <b>force-unauthorized</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Step 8 | Switch # <b>copy running-config startup-config</b>                             | (Optional) Saves your entries in the configuration file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

To disable AAA, use the **no aaa new-model** global configuration command.

To disable 802.1x AAA authentication, use the **no aaa authentication dot1x {default | list-name} method1 [method2...]** global configuration command.

To disable 802.1x authentication, use the **dot1x port-control force-authorized** or the **no dot1x port-control** interface configuration command.

This example shows how to enable AAA and 802.1x on Fast Ethernet port 0/1:

```
Switch# configure terminal
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius
Switch(config)# interface fastethernet0/1
Switch(config-if)# dot1x port-control auto
Switch(config-if)# end
```

## Configuring 802.1x with Guest-VLANs

To configure 802.1x with guest-VLAN, perform this task:

|        | Command                                                               | Purpose                                                                                                                                                                                                                               |
|--------|-----------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch # <b>configure terminal</b>                                    | Enters global configuration mode.                                                                                                                                                                                                     |
| Step 2 | Switch(config-if) # <b>interface</b><br><i>interface-id</i>           | Enters interface configuration mode and specifies the interface to be enabled for 802.1x authentication.                                                                                                                              |
| Step 3 | Switch(config-if) # <b>dot1x</b><br><b>port-control auto]</b>         | Enables 802.1x authentication on the interface.<br><br>For feature interaction information with trunk, dynamic, dynamic-access, EtherChannel, secure, and SPAN ports, see the “802.1x Configuration Guidelines” section on page 26-8. |
| Step 4 | Switch(config-if) # <b>dot1x guest-vlan</b><br><i>&lt;vlan-id&gt;</i> | Enables guest VLAN on a particular interface.                                                                                                                                                                                         |
| Step 5 | Switch(config-if) # <b>end</b>                                        | Returns to configuration mode.                                                                                                                                                                                                        |
| Step 6 | Switch(config) # <b>end</b>                                           | Returns to privileged EXEC mode.                                                                                                                                                                                                      |

To disable the guest VLAN feature on a particular port, use the **no dot1x guest-vlan** interface configuration command.

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

```
Switch# configure terminal
Switch(config)# interface fastethernet4/3
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x guest-vlan <vlan-id>
Switch(config-if)# end
Switch(config)# end
Switch#
```

## Configuring Switch-to-RADIUS-Server Communication

A RADIUS security server is identified by its hostname or IP address, hostname and specific UDP port number, or IP address and specific UDP port numbers. The combination of the IP address and UDP port number creates a unique identifier, which enables RADIUS requests to be sent to multiple UDP ports on a server at the same IP address. If two different host entries on the same RADIUS server are configured for the same service—for example, authentication—the second host entry configured acts as the fail-over backup to the first one. The RADIUS host entries are tried in the order they were configured.

To configure the RADIUS server parameters on the switch, perform this task:

|        | Command                                                                                                          | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------|------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch# <b>configure terminal</b>                                                                                | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Step 2 | Switch(config)# <b>radius-server host</b> {hostname   ip-address} <b>auth-port</b> port-number <b>key</b> string | <p>Configures the RADIUS server parameters on the switch.</p> <p>For <i>hostname</i>   <i>ip-address</i>, specify the hostname or IP address of the remote RADIUS server.</p> <p>For <b>auth-port</b> <i>port-number</i>, specify the UDP destination port for authentication requests. The default is 1812.</p> <p>For <b>key</b> <i>string</i>, specify the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server. The key is a text string that must match the encryption key used on the RADIUS server.</p> <p><b>Note</b> Always configure the key as the last item in the <b>radius-server host</b> command syntax because leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in the key, do not enclose the key in quotation marks unless the quotation marks are part of the key. This key must match the encryption used on the RADIUS daemon.</p> <p>If you want to use multiple RADIUS servers, re-enter this command.</p> |
| Step 3 | Switch(config)# <b>end</b>                                                                                       | Returns to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Step 4 | Switch# <b>show running-config</b>                                                                               | Verifies your entries.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Step 5 | Switch# <b>copy running-config startup-config</b>                                                                | (Optional) Saves your entries in the configuration file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

To delete the specified RADIUS server, use the **no radius-server host** {hostname | ip-address} global configuration command.

This example shows how to specify the server with IP address 172.20.39.46 as the RADIUS server, to use port 1612 as the authorization port, and to set the encryption key to rad123, matching the key on the RADIUS server:

```
Switch(config)# radius-server host 172.120.39.46 auth-port 1612 key rad123
```

You can globally configure the timeout, retransmission, and encryption key values for all RADIUS servers by using the **radius-server host** global configuration command. If you want to configure these options on a per-server basis, use the **radius-server timeout**, **radius-server retransmit**, and the **radius-server key** global configuration commands.

You also need to configure some settings on the RADIUS server. These settings include the IP address of the switch and the key string to be shared by both the server and the switch.

## Enabling Periodic Re-Authentication

You can enable periodic 802.1x client re-authentication and specify how often it occurs. If you do not specify a time value before enabling re-authentication, the time between re-authentication attempts is 3600 sec.

Automatic 802.1x client re-authentication is a per interface setting and can be set for clients connected to individual ports. To manually re-authenticate the client connected to a specific port, see the “Manually Re-Authenticating a Client Connected to a Port” section on page 26-12.

To enable periodic re-authentication of the client and to configure the number of seconds between re-authentication attempts, perform this task:

|        | Command                                                                     | Purpose                                                                                                                                                                                                                            |
|--------|-----------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch# <b>configure terminal</b>                                           | Enters global configuration mode.                                                                                                                                                                                                  |
| Step 1 | Switch(config)# <b>interface</b><br><i>interface-id</i>                     | Enters interface configuration mode and specify the interface to be enabled for periodic re-authentication.                                                                                                                        |
| Step 2 | Switch(config-if)# <b>dot1x</b><br><b>re-authentication</b>                 | Enables periodic re-authentication of the client, which is disabled by default.                                                                                                                                                    |
| Step 3 | Switch(config)# <b>dot1x timeout</b><br><b>reauth-period</b> <i>seconds</i> | Sets the number of seconds between re-authentication attempts.<br><br>The range is 1 to 65,535; the default is 3600 seconds.<br><br>This command affects the behavior of the switch only if periodic re-authentication is enabled. |
| Step 4 | Switch(config)# <b>end</b>                                                  | Returns to privileged EXEC mode.                                                                                                                                                                                                   |
| Step 5 | Switch# <b>show dot1x all</b>                                               | Verifies your entries.                                                                                                                                                                                                             |
| Step 6 | Switch(config)# <b>copy running-config</b><br><b>startup-config</b>         | (Optional) Saves your entries in the configuration file.                                                                                                                                                                           |

To disable periodic re-authentication, use the **no dot1x re-authentication** interface configuration command. To return to the default number of seconds between re-authentication attempts, use the **no dot1x timeout reauth-period** global configuration command.

This example shows how to enable periodic re-authentication and set the number of seconds between re-authentication attempts to 4000:

```
Switch(config)# dot1x re-authentication
Switch(config)# dot1x timeout reauth-period 4000
```

## Manually Re-Authenticating a Client Connected to a Port

You can manually re-authenticate the client connected to a specific port at any time by entering the **dot1x re-authenticate interface** *interface-id* privileged EXEC command. If you want to enable or disable periodic re-authentication, see the “Enabling Periodic Re-Authentication” section on page 26-11.

This example shows how to manually re-authenticate the client connected to Fast Ethernet port 0/1:

```
Switch# dot1x re-authenticate interface fastethernet0/1
Starting reauthentication on FastEthernet0/1
```

## Changing the Quiet Period

When the switch cannot authenticate the client, the switch remains idle for a set period of time, and then tries again. The idle time is determined by the **quiet-period** value. A failed authentication of the client might occur because the client provided an invalid password. You can provide a faster response time to the user by entering a number smaller than the default.

To change the quiet period, perform this task:

|        | Command                                                                    | Purpose                                                                                                                                                                                               |
|--------|----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch# <b>configure terminal</b>                                          | Enters global configuration mode.                                                                                                                                                                     |
| Step 2 | Switch(config)# <b>interface</b><br><i>interface-id</i>                    | Enters interface configuration mode and specify the interface to be enabled for timeout <b>quiet-period</b> .                                                                                         |
| Step 3 | Switch(config)# <b>dot1x timeout</b><br><b>quiet-period</b> <i>seconds</i> | Sets the number of seconds that the switch remains in the <b>quiet-period</b> following a failed authentication exchange with the client.<br><br>The range is 0 to 65,535 seconds; the default is 60. |
| Step 4 | Switch(config)# <b>end</b>                                                 | Returns to privileged EXEC mode.                                                                                                                                                                      |
| Step 5 | Switch# <b>show dot1x all</b>                                              | Verifies your entries.                                                                                                                                                                                |
| Step 6 | Switch# <b>copy running-config</b><br><b>startup-config</b>                | (Optional) Saves your entries in the configuration file.                                                                                                                                              |

To return to the default quiet-period, use the **no dot1x timeout quiet-period** configuration command. This example shows how to set the **quiet-period** on the switch to 30 seconds:

```
Switch(config)# dot1x timeout quiet-period 30
```

## Changing the Switch-to-Client Retransmission Time

The client responds to the EAP-request/identity frame from the switch with an EAP-response/identity frame. If the switch does not receive this response, it waits a set period of time (known as the retransmission time) and then retransmits the frame.



### Note

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.

To change the amount of time that the switch waits for client notification, perform this task:

|        | Command                                                                    | Purpose                                                                                                                                                                                                         |
|--------|----------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch# <b>configure terminal</b>                                          | Enters global configuration mode.                                                                                                                                                                               |
| Step 2 | Switch(config)# <b>interface</b><br><i>interface-id</i>                    | Enters interface configuration mode and specify the interface to be enabled for timeout tx-period.                                                                                                              |
| Step 3 | Switch(config-if)# <b>dot1x timeout</b><br><b>tx-period</b> <i>seconds</i> | Sets the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request.<br><br>The range is 1 to 65,535 seconds; the default is 30. |
| Step 4 | Switch(config)# <b>end</b>                                                 | Returns to privileged EXEC mode.                                                                                                                                                                                |
| Step 5 | Switch# <b>show dot1x all</b>                                              | Verifies your entries.                                                                                                                                                                                          |
| Step 6 | Switch# <b>copy running-config</b><br><b>startup-config</b>                | (Optional) Saves your entries in the configuration file.                                                                                                                                                        |

To return to the default retransmission time, use the **no dot1x timeout tx-period** interface configuration command.

This example shows how to set the retransmission time to 60 seconds:

```
Switch(config)# dot1x timeout tx-period 60
```

## Setting the Switch-to-Client Frame-Retransmission Number

In addition to changing the switch-to-client retransmission times, you can change the number of times that the switch sends EAP-Request/Identity and other EAP-Request frames to the client before restarting the authentication process. The number of EAP-Request/Identity retransmissions is controlled by the **dot1x max-reauth-req** command; the number of retransmissions for other EAP-Request frames is controlled by the **dot1x max-req** command.



### Note

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

To set the switch-to-client frame-retransmission numbers, perform this task:

|        | Command                                                                                                                          | Purpose                                                                                                                                                                                                                                                                                                                                                                                               |
|--------|----------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch# <b>configure terminal</b>                                                                                                | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                     |
| Step 2 | Switch(config)# <b>interface</b><br><i>interface-id</i>                                                                          | Enters interface configuration mode and specifies the interface to be enabled for <b>max-reauth-req</b> and/or <b>max-req</b> .                                                                                                                                                                                                                                                                       |
| Step 3 | Switch(config-if)# <b>dot1x max-req</b><br><i>count</i><br><br>or<br><br>Switch(config-if)# <b>dot1x max-req</b><br><i>count</i> | Sets the number of times that the switch retransmits an EAP-Request frame of a type other than EAP-Request/Identity to the client before restarting the authentication process.<br><br>Sets the number of times that the switch retransmits an EAP-Request/Identity frame to the client before restarting the authentication process.<br><br>The range for <i>count</i> is 1 to 10; the default is 2. |
| Step 4 | Switch(config)# <b>end</b>                                                                                                       | Returns to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                      |
| Step 5 | Switch# <b>show dot1x all</b>                                                                                                    | Verifies your entries.                                                                                                                                                                                                                                                                                                                                                                                |
| Step 6 | Switch# <b>copy running-config</b><br><b>startup-config</b>                                                                      | (Optional) Saves your entries in the configuration file.                                                                                                                                                                                                                                                                                                                                              |

To return to the default retransmission number, use the **no dot1x max-req** and **no dot1x max-reauth-req** global configuration command.

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

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

## Enabling Multiple Hosts

You can attach multiple hosts to a single 802.1x-enabled port as shown in Figure 26-3 on page 26-6. In this mode, only one of the attached hosts must be successfully authorized for all hosts to be granted network access. If the port becomes unauthorized (re-authentication fails or an EAPOL-logoff message is received), all attached clients are denied access to the network.

To allow multiple hosts (clients) on an 802.1x-authorized port that has the **dot1x port-control** interface configuration command set to **auto**, perform this task:

|        | Command                                              | Purpose                                                                                                                                                                                              |
|--------|------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch# <b>configure terminal</b>                    | Enters global configuration mode.                                                                                                                                                                    |
| Step 2 | Switch(config)# <b>interface interface-id</b>        | Enters interface configuration mode and specify the interface to which multiple hosts are indirectly attached.                                                                                       |
| Step 3 | Switch(config-if)# <b>dot1x multiple-hosts</b>       | Allows multiple hosts (clients) on an 802.1x-authorized port.<br>Make sure that the <b>dot1x port-control</b> interface configuration command set is set to <b>auto</b> for the specified interface. |
| Step 4 | Switch(config-if)# <b>end</b>                        | Returns to privileged EXEC mode.                                                                                                                                                                     |
| Step 5 | Switch# <b>show dot1x all interface interface-id</b> | Verifies your entries.                                                                                                                                                                               |
| Step 6 | Switch# <b>copy running-config startup-config</b>    | (Optional) Saves your entries in the configuration file.                                                                                                                                             |

To disable multiple hosts on the port, use the **no dot1x multiple-hosts** interface configuration command.

This example shows how to enable 802.1x on Fast Ethernet interface 0/1 and to allow multiple hosts:

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x multiple-hosts
```

## Resetting the 802.1x Configuration to the Default Values

To reset the 802.1x configuration to the default values, perform this task:

|        | Command                                           | Purpose                                                          |
|--------|---------------------------------------------------|------------------------------------------------------------------|
| Step 1 | Switch# <b>configure terminal</b>                 | Enters global configuration mode.                                |
| Step 2 | Switch(config)# <b>dot1x default</b>              | Resets the configurable 802.1x parameters to the default values. |
| Step 3 | Switch(config)# <b>end</b>                        | Returns to privileged EXEC mode.                                 |
| Step 4 | Switch# <b>show dot1x all</b>                     | Verifies your entries.                                           |
| Step 5 | Switch# <b>copy running-config startup-config</b> | (Optional) Saves your entries in the configuration file.         |

## Displaying 802.1x Statistics and Status

To display 802.1x statistics for all interfaces, use the **show dot1x statistics** privileged EXEC command. To display 802.1x statistics for a specific interface, use the **show dot1x statistics interface *interface-id*** privileged EXEC command.

To display the 802.1x administrative and operational status for the switch, use the **show dot1x all** privileged EXEC command. To display the 802.1x administrative and operational status for a specific interface, use the **show dot1x interface *interface-id*** privileged EXEC command.





## Port Unicast and Multicast Flood Blocking

This chapter describes how to configure multicast and unicast flood blocking on the Catalyst 4500 series switch. This chapter contains these topics:

- Overview of Flood Blocking, page 27-1
- Configuring Port Blocking, page 27-1



### Note

For complete syntax and usage information for the switch commands used in this chapter, refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference* and related publications at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/index.htm>

## Overview of Flood Blocking

Occasionally, unknown unicast or multicast traffic is flooded to a switch port because a MAC address has timed out or has not been learned by the switch. (This condition is especially undesirable for a private VLAN isolated port.) To guarantee that no unicast and multicast traffic is flooded to the port, use the **switchport block unicast** and **switchport block multicast** commands.



### Note

This feature is supported on all switched ports (including PVLAN ports) and is applied to all VLANs on which the port is forwarding.

## Configuring Port Blocking

By default, a switch floods packets with unknown destination MAC addresses to all ports. If unknown unicast and multicast traffic is forwarded to a switch port, there might be security issues. To prevent forwarding such traffic, you can configure a port to block unknown unicast or multicast packets.



### Note

Blocking unicast or multicast traffic is not automatically enabled on a switch port; you must explicitly configure it.

# Blocking Flooded Traffic on an Interface



**Note**

The interface can be a physical interface (for example, GigabitEthernet 1/1) or an EtherChannel group (such as port-channel 5). When you block multicast or unicast traffic for a port channel, it is blocked on all ports in the port channel group.

To disable the flooding of multicast and unicast packets to an interface, perform this task:

|        | Command                                                                | Purpose                                                                                                                           |
|--------|------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch# <b>configure terminal</b>                                      | Enters global configuration mode.                                                                                                 |
| Step 2 | Switch(config)# <b>interface</b> <i>interface-id</i>                   | Enters interface configuration mode and enter the type and number of the switchport interface (for example, GigabitEthernet 1/1). |
| Step 3 | Switch(config-if)# <b>switchport block multicast</b>                   | Blocks unknown multicast forwarding to the port.                                                                                  |
| Step 4 | Switch(config-if)# <b>switchport block unicast</b>                     | Blocks unknown unicast forwarding to the port.                                                                                    |
| Step 5 | Switch(config)# <b>end</b>                                             | Returns to privileged EXEC mode.                                                                                                  |
| Step 6 | Switch#<br><b>show interface</b> <i>interface-id</i> <b>switchport</b> | Verifies your entry.                                                                                                              |
| Step 7 | Switch# <b>copy running-config startup-config</b>                      | (Optional) Saves your entries in the configuration file.                                                                          |

This example shows how to block unicast and multicast flooding on a GigabitEthernet interface 0/1 and how to verify the configuration:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport block multicast
Switch(config-if)# switchport block unicast
Switch(config-if)# end
Switch# show interface gigabitethernet1/1 switchport
Name: Gi1/3
Switchport: Enabled

<output truncated>

Port Protected: On
Unknown Unicast Traffic: Not Allowed
Unknown Multicast Traffic: Not Allowed

Broadcast Suppression Level: 100
Multicast Suppression Level: 100
Unicast Suppression Level: 100
```

## Resuming Normal Forwarding on a Port

To resume normal forwarding on a port, perform this task:

|        | Command                                                                | Purpose                                                                                                                 |
|--------|------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch# <b>configure terminal</b>                                      | Enters global configuration mode.                                                                                       |
| Step 2 | Switch(config)# <b>interface</b><br><i>interface-id</i>                | Enters interface configuration mode and enter the type and number of the switchport interface (ie. GigabitEthernet1/1). |
| Step 3 | Switch(config-if)# <b>no switchport</b><br><b>block multicast</b>      | Enables unknown multicast flooding to the port.                                                                         |
| Step 4 | Switch(config-if)# <b>no switchport</b><br><b>block unicast</b>        | Enables unknown unicast flooding to the port.                                                                           |
| Step 5 | Switch(config)# <b>end</b>                                             | Returns to privileged EXEC mode.                                                                                        |
| Step 6 | Switch# <b>show interface</b> <i>interface-id</i><br><b>switchport</b> | Verifies your entry.                                                                                                    |
| Step 7 | Switch# <b>copy running-config</b><br><b>startup-config</b>            | (Optional) Saves your entries in the configuration file.                                                                |





## Configuring Port-Based Traffic Control

This chapter describes how to configure port-based traffic control on the Catalyst 4500 series switch.



### Note

Storm control is supported in hardware on non-blocking gigabit ports on all supervisor engines (WS-X4014, WS-X4015, WS-X4013+) and in software on all other ports, implying that the counters for these interfaces are approximate and computed.



### Note

For complete syntax and usage information for the switch commands used in this chapter, refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference* and related publications at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/index.htm>

This chapter consists of these sections:

- Overview of Storm Control, page 28-1
- Enabling Storm Control, page 28-3
- Disabling Storm Control, page 28-4
- Displaying Storm Control, page 28-5

## Overview of Storm Control

Storm control prevents LAN interfaces from being disrupted by a broadcast storm. A broadcast storm occurs when broadcast packets flood the subnet, creating excessive traffic and degrading network performance. Errors in the protocol-stack implementation or in the network configuration can cause a broadcast storm.



### Note

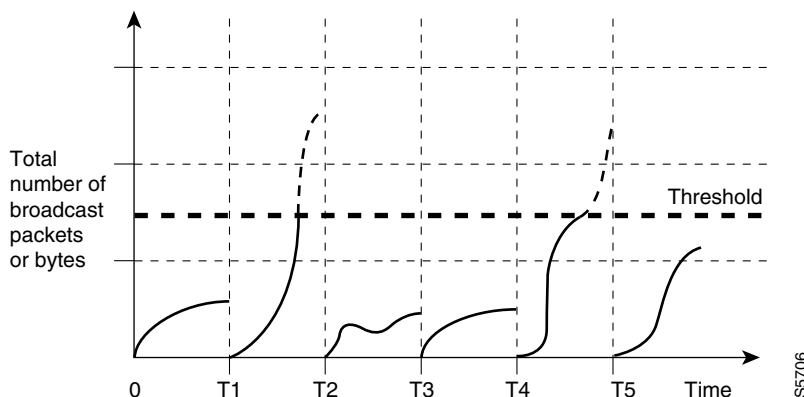
Some ports support hardware-based broadcast suppression, whereas others support software-based broadcast suppression.

## Hardware-based Storm Control Implementation

Broadcast suppression uses filtering that measures broadcast activity in a subnet over a one-second interval and compares the measurement with a predefined threshold. If the threshold is reached, further broadcast activity is suppressed for the duration of the interval. Broadcast suppression is disabled by default.

Figure 28-1 shows the broadcast traffic patterns on a LAN interface over a given interval. In this example, broadcast suppression occurs between times T1 and T2 and between T4 and T5. During those intervals, the amount of broadcast traffic exceeded the configured threshold.

**Figure 28-1 Storm Control Example - Hardware-based Implementation**



The broadcast suppression threshold numbers and the time interval combination make the broadcast suppression algorithm work with different levels of granularity. A higher threshold allows more broadcast packets to pass through.

Broadcast suppression on the Catalyst 4500 series switches is implemented in hardware. The suppression circuitry monitors packets passing from a LAN interface to the switching bus. If the packet destination address is broadcast, then the broadcast suppression circuitry tracks the current count of broadcasts within the one-second interval, and when a threshold is reached, it filters out subsequent broadcast packets.

Because hardware broadcast suppression uses a bandwidth-based method to measure broadcast activity, the most significant implementation factor is setting the percentage of total available bandwidth that can be used by broadcast traffic. Because packets do not arrive at uniform intervals, the one-second interval during which broadcast activity is measured can affect the behavior of broadcast suppression.

## Software-based Storm Control Implementation

When storm control is enabled on an interface, the switch monitors packets received on the interface and determines whether or not the packets are broadcast. The switch monitors the number of broadcast packets received within a one-second time interval. When the interface threshold is met, all incoming data traffic on the interface is dropped. This threshold is specified as a percentage of total available bandwidth that can be used by broadcast traffic. If the lower threshold is specified, all data traffic is forwarded as soon as the incoming traffic falls below that threshold.

# Enabling Storm Control

To enable storm control, perform this task:

|        | Command                                                                                              | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------|------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch# <b>configure terminal</b>                                                                    | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Step 2 | Switch(config)# <b>interface</b> <i>interface-id</i>                                                 | Enters interface configuration mode and enter the port to configure.                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Step 3 | Switch(config-if)# <b>storm-control broadcast level</b> [ <i>high level</i> ] [ <i>lower level</i> ] | Configures broadcast storm control.<br><br>Specifies the upper threshold levels for broadcast traffic. The storm control action occurs when traffic utilization reaches this level.<br><br>(Optional) Specifies the falling threshold level. The normal transmission restarts (if the action is filtering) when traffic drops below this level for interfaces that support software-based suppression.<br><br><b>Note</b> For ports that perform hardware-based suppression, the lower threshold is ignored. |
| Step 4 | Switch(config-if)# <b>storm-control action</b> { <i>shutdown</i>   <i>trap</i> }                     | Specifies the action to be taken when a storm is detected.<br><br>The default is to filter out the broadcast traffic and not to send out traps.<br><br>The <b>shutdown</b> keyword sets the port to error-disable state during a storm. If the recover interval is not set, the port remains in shutdown state.<br><br><b>Note</b> The <b>trap</b> keyword generates an SNMP trap when a storm is detected. This keyword is available but not supported in the 12.1(19) EW release.                          |
| Step 5 | Switch(config-if)# <b>exit</b>                                                                       | Returns to configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Step 6 | Switch(config)# <b>end</b>                                                                           | Returns to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Step 7 | Switch# <b>show storm-control</b> [ <i>interface</i> ] <b>broadcast</b>                              | Displays the number of packets suppressed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Step 8 | Switch# <b>copy running-config startup-config</b>                                                    | (Optional) Saves your entries in the configuration file.                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

The following example shows how to enable storm control on interface.

```
Switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# int fa3/1
Switch(config-if)# storm-control broadcast level 50
Switch(config-if)# end
Switch# wr
Building configuration...

00:11:06: %SYS-5-CONFIG_I: Configured from console by consoleCompressed configuration from
5394 bytes to 1623 bytes[OK]
Switch#sh stor
Switch#sh storm-control
Interface Filter State Upper Lower Current
----- -
Fa3/1 Forwarding 50.00% 50.00% 0.00%
Switch#
```

# Disabling Storm Control

To disable storm control, perform this task:

|        | Command                                                                       | Purpose                                                                           |
|--------|-------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| Step 1 | Switch# <b>configure terminal</b>                                             | Enters global configuration mode.                                                 |
| Step 2 | Switch(config)# <b>interface</b><br><i>interface-id</i>                       | Enters interface configuration mode and enter the port to configure.              |
| Step 3 | Switch(config-if)# <b>no storm-control</b><br><b>broadcast level</b>          | Disables port storm control.                                                      |
| Step 4 | Switch(config-if)# <b>no storm-control</b><br><b>action {shutdown   trap}</b> | Disables the specified storm control action and returns to default filter action. |
| Step 5 | Switch(config-if)# <b>exit</b>                                                | Returns to configuration mode.                                                    |
| Step 6 | Switch(config)# <b>end</b>                                                    | Returns to privileged EXEC mode.                                                  |
| Step 7 | Switch# <b>show storm-control</b><br><b>broadcast</b>                         | Verifies your entries.                                                            |
| Step 8 | Switch# <b>copy running-config</b><br><b>startup-config</b>                   | (Optional) Saves your entries in the configuration file.                          |

The following example shows how to disable storm control on interface.

```
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int fa3/1
Switch(config-if)#no storm-control broadcast level
Switch(config-if)#end
Switch#wr
Building configuration...

00:12:09: %SYS-5-CONFIG_I: Configured from console by consoleCompressed configuration from
5357 bytes to 1594 bytes[OK]
Switch#sh sto
Switch#sh storm-control
Interface Filter State Upper Lower Current
----- -
Switch#
```



# Displaying Storm Control



## Note

Use the **show interface capabilities** command to determine the mode in which storm control is supported on an interface.

The following example shows an interface that supports broadcast suppression in software (sw).

```
Switch# show interfaces g4/4 capabilities
show interfaces g4/4 capabilities
GigabitEthernet4/4
 Model: WS-X4418-Gbic
 Type: 1000BaseSX
 Speed: 1000
 Duplex: full
 Trunk encap. type: 802.1Q
 Trunk mode: on,off,desirable,nonegotiate
 Channel: yes
 Broadcast suppression: percentage(0-100), sw
 Flowcontrol: rx-(off,on,desired),tx-(off,on,desired)
 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, no baby giants
Switch#
```

The following example shows an interface that supports broadcast suppression in hardware (hw).

```
Switch# show interfaces g4/1 capabilities
show interfaces g4/1 capabilities
GigabitEthernet4/1
 Model: WS-X4418-Gbic
 Type: No 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
Link Debounce Time: no
Port Security: yes
Dot1x: yes
MTU Supported: jumbo frames, baby giants
Switch#

```

**Note**

Use the **show interfaces counters storm-control** command to display a count of discarded packets.

```

Switch# show interfaces counters storm-control

Port BcastSuppLevel TotalSuppressedPackets
Gi4/4 2.00% 0
Switch#

```

**Note**

Use the **show storm-control** command to display the configured thresholds and status of storm on an interface.

```

Switch# show storm-control

Interface Filter State Upper Lower Current

Gi4/4 Forwarding 2.00% 2.00% N/A
Switch#

```

**Note**

In the example shown above, “current” represents the percentage of traffic suppressed at a given instant, and the value is N/A for ports that perform suppression in hardware.



## Configuring QoS

This chapter describes how to configure quality of service (QoS) by using automatic QoS (auto-QoS) commands or by using standard QoS commands on a Catalyst 4500 series switch. It also provides guidelines, procedures, and configuration examples.

This chapter consists of these sections:

- Overview of QoS, page 29-1
- Configuring Auto-QoS, page 29-15
- Configuring QoS, page 29-21



### Note

For complete syntax and usage information for the switch commands used in this chapter, refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference* and related publications at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/index.htm>

## Overview of QoS

Typically, networks operate on a *best-effort* delivery basis, which means that all traffic has equal priority and an equal chance of being delivered in a timely manner. When congestion occurs, all traffic has an equal chance of being dropped.

QoS selects network traffic (both unicast and multicast), prioritizes it according to its relative importance, and uses congestion avoidance to provide priority-indexed treatment; QoS can also limit the bandwidth used by network traffic. QoS can make network performance more predictable and bandwidth utilization more effective.

This section contains the following subsections:

- Prioritization, page 29-2
- QoS Terminology, page 29-3
- Basic QoS Model, page 29-5
- Classification, page 29-5
- Policing and Marking, page 29-9
- Mapping Tables, page 29-12
- Queueing and Scheduling, page 29-13
- Packet Modification, page 29-14

## Prioritization

The QoS implementation for this release is based on the DiffServ architecture, an emerging standard from the Internet Engineering Task Force (IETF). This architecture specifies that each packet is classified upon entry into the network. The classification is carried in the IP packet header, using 6 bits from the deprecated IP type of service (TOS) field to carry the classification (*class*) information. Classification can also be carried in the Layer 2 frame. These special bits in the Layer 2 frame or a Layer 3 packet are described here and shown in Figure 29-1:

- Prioritization values in Layer 2 frames:

Layer 2 Inter-Switch Link (ISL) frame headers have a 1-byte User field that carries an IEEE 802.1p class of service (CoS) value in the three least-significant bits. On interfaces configured as Layer 2 ISL trunks, all traffic is in ISL frames.

Layer 2 802.1Q frame headers have a 2-byte Tag Control Information field that carries the CoS value in the three most-significant bits, which are called the User Priority bits. On interfaces configured as Layer 2 802.1Q trunks, all traffic is in 802.1Q frames except for traffic in the native VLAN.

Other frame types cannot carry Layer 2 CoS values.

Layer 2 CoS values range from 0 for low priority to 7 for high priority.

- Prioritization bits in Layer 3 packets:

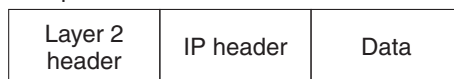
Layer 3 IP packets can carry either an IP precedence value or a Differentiated Services Code Point (DSCP) value. QoS supports the use of either value because DSCP values are backward-compatible with IP precedence values.

IP precedence values range from 0 to 7.

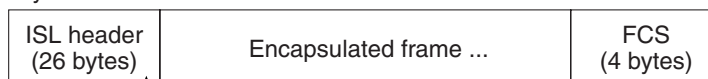
DSCP values range from 0 to 63.

**Figure 29-1 QoS Classification Layers in Frames and Packets**

Encapsulated Packet

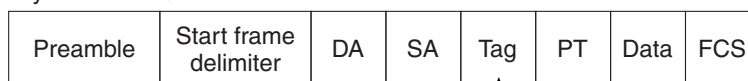


Layer 2 ISL Frame



↑ 3 bits used for CoS

Layer 2 802.1Q/P Frame



↑ 3 bits used for CoS (user priority)

Layer 3 IPv4 Packet



↑ IP precedence or DSCP

68140

All switches and routers across the Internet rely on the class information to provide the same forwarding treatment to packets with the same class information and different treatment to packets with different class information. The class information in the packet can be assigned by end hosts or by switches or routers along the way, based on a configured policy, detailed examination of the packet, or both. Detailed examination of the packet is expected to happen closer to the edge of the network so that the core switches and routers are not overloaded.

Switches and routers along the path can use the class information to limit the amount of resources allocated per traffic class. The behavior of an individual device when handling traffic in the DiffServ architecture is called per-hop behavior. If all devices along a path provide a consistent per-hop behavior, you can construct an end-to-end QoS solution.

Implementing QoS in your network can be a simple or complex task and depends on the QoS features offered by your internetworking devices, the traffic types and patterns in your network, and the granularity of control you need over incoming and outgoing traffic.

## QoS Terminology

The following terms are used when discussing QoS features:

- *Packets* carry traffic at Layer 3.
- *Frames* carry traffic at Layer 2. Layer 2 frames carry Layer 3 packets.
- *Labels* are prioritization values carried in Layer 3 packets and Layer 2 frames:
  - Layer 2 class of service (CoS) values, which range between zero for low priority and seven for high priority:

Layer 2 Inter-Switch Link (ISL) frame headers have a 1-byte User field that carries an IEEE 802.1p CoS value in the three least significant bits.

Layer 2 802.1Q frame headers have a 2-byte Tag Control Information field that carries the CoS value in the three most significant bits, which are called the User Priority bits.

Other frame types cannot carry Layer 2 CoS values.

**Note**

On interfaces configured as Layer 2 ISL trunks, all traffic is in ISL frames. On interfaces configured as Layer 2 802.1Q trunks, all traffic is in 802.1Q frames except for traffic in the native VLAN.

- Layer 3 IP precedence values—The IP version 4 specification defines the three most significant bits of the 1-byte ToS field as IP precedence. IP precedence values range between zero for low priority and seven for high priority.
- Layer 3 differentiated services code point (DSCP) values—The Internet Engineering Task Force (IETF) has defined the six most significant bits of the 1-byte IP ToS field as the DSCP. The per-hop behavior represented by a particular DSCP value is configurable. DSCP values range between 0 and 63. See the “Configuring DSCP Maps” section on page 29-40.

**Note**

Layer 3 IP packets can carry either an IP precedence value or a DSCP value. QoS supports the use of either value, since DSCP values are backwards compatible with IP precedence values. See Table 29-1.

Table 29-1 IP Precedence and DSCP Values

| 3-bit IP<br>Precedence | 6 MSb <sup>1</sup> of ToS |   |   |   |   |   | 6-bit<br>DSCP |  | 3-bit IP<br>Precedence | 6 MSb <sup>1</sup> of ToS |   |   |   |   |   | 6-bit<br>DSCP |
|------------------------|---------------------------|---|---|---|---|---|---------------|--|------------------------|---------------------------|---|---|---|---|---|---------------|
|                        | 8                         | 7 | 6 | 5 | 4 | 3 |               |  |                        | 8                         | 7 | 6 | 5 | 4 | 3 |               |
| 0                      | 0                         | 0 | 0 | 0 | 0 | 0 | 0             |  | 4                      | 1                         | 0 | 0 | 0 | 0 | 0 | 32            |
|                        | 0                         | 0 | 0 | 0 | 0 | 1 | 1             |  |                        | 1                         | 0 | 0 | 0 | 0 | 1 | 33            |
|                        | 0                         | 0 | 0 | 0 | 1 | 0 | 2             |  |                        | 1                         | 0 | 0 | 0 | 1 | 0 | 34            |
|                        | 0                         | 0 | 0 | 0 | 1 | 1 | 3             |  |                        | 1                         | 0 | 0 | 0 | 1 | 1 | 35            |
|                        | 0                         | 0 | 0 | 1 | 0 | 0 | 4             |  |                        | 1                         | 0 | 0 | 1 | 0 | 0 | 36            |
|                        | 0                         | 0 | 0 | 1 | 0 | 1 | 5             |  |                        | 1                         | 0 | 0 | 1 | 0 | 1 | 37            |
|                        | 0                         | 0 | 0 | 1 | 1 | 0 | 6             |  |                        | 1                         | 0 | 0 | 1 | 1 | 0 | 38            |
|                        | 0                         | 0 | 0 | 1 | 1 | 1 | 7             |  |                        | 1                         | 0 | 0 | 1 | 1 | 1 | 39            |
| 1                      | 0                         | 0 | 1 | 0 | 0 | 0 | 8             |  | 5                      | 1                         | 0 | 1 | 0 | 0 | 0 | 40            |
|                        | 0                         | 0 | 1 | 0 | 0 | 1 | 9             |  |                        | 1                         | 0 | 1 | 0 | 0 | 1 | 41            |
|                        | 0                         | 0 | 1 | 0 | 1 | 0 | 10            |  |                        | 1                         | 0 | 1 | 0 | 1 | 0 | 42            |
|                        | 0                         | 0 | 1 | 0 | 1 | 1 | 11            |  |                        | 1                         | 0 | 1 | 0 | 1 | 1 | 43            |
|                        | 0                         | 0 | 1 | 1 | 0 | 0 | 12            |  |                        | 1                         | 0 | 1 | 1 | 0 | 0 | 44            |
|                        | 0                         | 0 | 1 | 1 | 0 | 1 | 13            |  |                        | 1                         | 0 | 1 | 1 | 0 | 1 | 45            |
|                        | 0                         | 0 | 1 | 1 | 1 | 0 | 14            |  |                        | 1                         | 0 | 1 | 1 | 1 | 0 | 46            |
|                        | 0                         | 0 | 1 | 1 | 1 | 1 | 15            |  |                        | 1                         | 0 | 1 | 1 | 1 | 1 | 47            |
| 2                      | 0                         | 1 | 0 | 0 | 0 | 0 | 16            |  | 6                      | 1                         | 1 | 0 | 0 | 0 | 0 | 48            |
|                        | 0                         | 1 | 0 | 0 | 0 | 1 | 17            |  |                        | 1                         | 1 | 0 | 0 | 0 | 1 | 49            |
|                        | 0                         | 1 | 0 | 0 | 1 | 0 | 18            |  |                        | 1                         | 1 | 0 | 0 | 1 | 0 | 50            |
|                        | 0                         | 1 | 0 | 0 | 1 | 1 | 19            |  |                        | 1                         | 1 | 0 | 0 | 1 | 1 | 51            |
|                        | 0                         | 1 | 0 | 1 | 0 | 0 | 20            |  |                        | 1                         | 1 | 0 | 1 | 0 | 0 | 52            |
|                        | 0                         | 1 | 0 | 1 | 0 | 1 | 21            |  |                        | 1                         | 1 | 0 | 1 | 0 | 1 | 53            |
|                        | 0                         | 1 | 0 | 1 | 1 | 0 | 22            |  |                        | 1                         | 1 | 0 | 1 | 1 | 0 | 54            |
|                        | 0                         | 1 | 0 | 1 | 1 | 1 | 23            |  |                        | 1                         | 1 | 0 | 1 | 1 | 1 | 55            |
| 3                      | 0                         | 1 | 1 | 0 | 0 | 0 | 24            |  | 7                      | 1                         | 1 | 1 | 0 | 0 | 0 | 56            |
|                        | 0                         | 1 | 1 | 0 | 0 | 1 | 25            |  |                        | 1                         | 1 | 1 | 0 | 0 | 1 | 57            |
|                        | 0                         | 1 | 1 | 0 | 1 | 0 | 26            |  |                        | 1                         | 1 | 1 | 0 | 1 | 0 | 58            |
|                        | 0                         | 1 | 1 | 0 | 1 | 1 | 27            |  |                        | 1                         | 1 | 1 | 0 | 1 | 1 | 59            |
|                        | 0                         | 1 | 1 | 1 | 0 | 0 | 28            |  |                        | 1                         | 1 | 1 | 1 | 0 | 0 | 60            |
|                        | 0                         | 1 | 1 | 1 | 0 | 1 | 29            |  |                        | 1                         | 1 | 1 | 1 | 0 | 1 | 61            |
|                        | 0                         | 1 | 1 | 1 | 1 | 0 | 30            |  |                        | 1                         | 1 | 1 | 1 | 1 | 0 | 62            |
|                        | 0                         | 1 | 1 | 1 | 1 | 1 | 31            |  |                        | 1                         | 1 | 1 | 1 | 1 | 1 | 63            |

1. MSb = most significant bit

- *Classification* is the selection of traffic to be marked.
- *Marking*, according to RFC 2475, is the process of setting a Layer 3 DSCP value in a packet; in this publication, the definition of marking is extended to include setting Layer 2 CoS values.
- *Scheduling* is the assignment of Layer 2 frames to a queue. QoS assigns frames to a queue based on internal DSCP values as shown in Internal DSCP Values, page 29-12.
- *Policing* is limiting bandwidth used by a flow of traffic. Policing can mark or drop traffic.

## Basic QoS Model

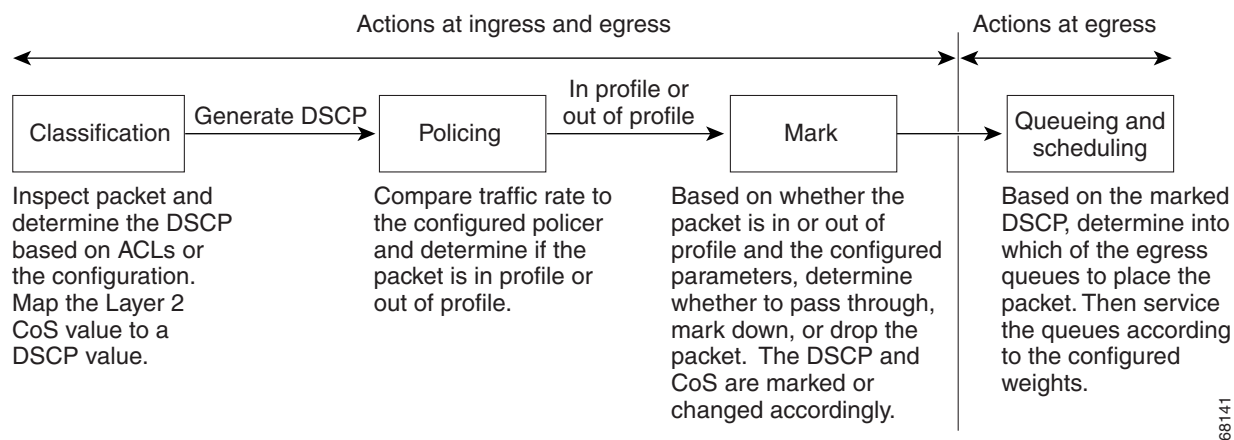
Figure 29-2 shows the basic QoS model. Actions at the ingress and egress interfaces include classifying traffic, policing, and marking:

- Classifying distinguishes one kind of traffic from another. The process generates an internal DSCP for a packet, which identifies all the future QoS actions to be performed on this packet. For more information, see the “Classification” section on page 29-5.
- Policing determines whether a packet is in or out of profile by comparing the traffic rate to the configured policer, which limits the bandwidth consumed by a flow of traffic. The result of this determination is passed to the marker. For more information, see the “Policing and Marking” section on page 29-9.
- Marking evaluates the policer configuration information regarding the action to be taken when a packet is out of profile and decides what to do with the packet (pass through a packet without modification, mark down the DSCP value in the packet, or drop the packet). For more information, see the “Policing and Marking” section on page 29-9.

Actions at the egress interface include queueing and scheduling:

- Queueing evaluates the internal DSCP and determines which of the four egress queues in which to place the packet.
- Scheduling services the four egress (transmit) queues based on the sharing and shaping configuration of the egress (transmit) port. Sharing and shaping configurations are described in the “Queueing and Scheduling” section on page 29-13.

**Figure 29-2 Basic QoS Model**



## Classification

Classification is the process of distinguishing one kind of traffic from another by examining the fields in the packet. Classification is enabled only if QoS is globally enabled on the switch. By default, QoS is globally disabled, so no classification occurs.

You specify which fields in the frame or packet that you want to use to classify incoming traffic.

Classification options are shown in Figure 29-3.

For non-IP traffic, you have the following classification options:

- Use the port default. If the packet is a non-IP packet, assign the default port DSCP value to the incoming packet.
- Trust the CoS value in the incoming frame (configure the port to trust CoS). Then use the configurable CoS-to-DSCP map to generate the internal DSCP value. Layer 2 ISL frame headers carry the CoS value in the three least-significant bits of the 1-byte User field. Layer 2 802.1Q frame headers carry the CoS value in the three most-significant bits of the Tag Control Information field. CoS values range from 0 for low priority to 7 for high priority. If the frame does not contain a CoS value, assign the default port CoS to the incoming frame.

The trust DSCP configuration is meaningless for non-IP traffic. If you configure a port with trust DSCP and non-IP traffic is received, the switch assigns the default port DSCP.

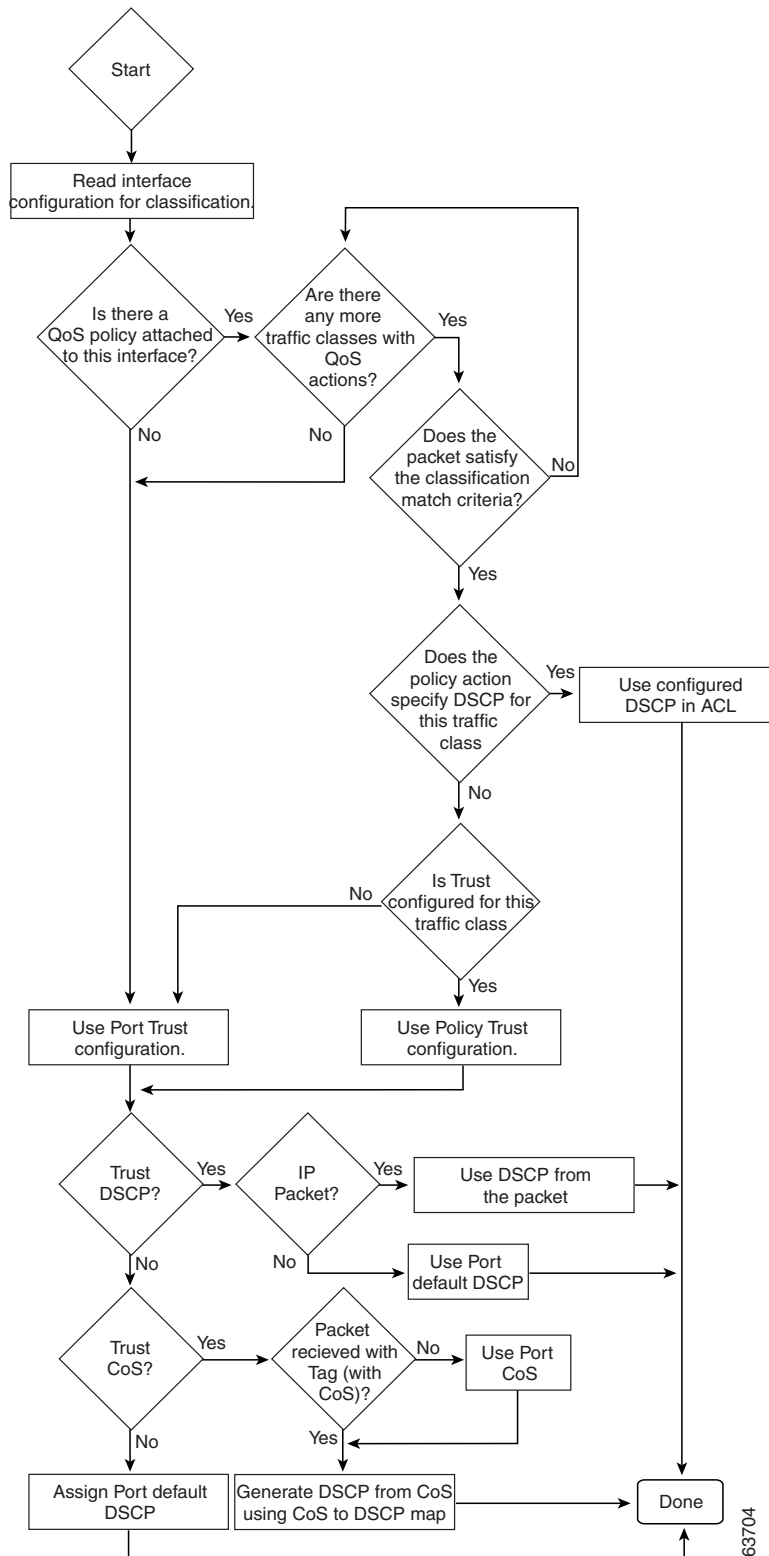
For IP traffic, you have the following classification options:

- Trust the IP DSCP in the incoming packet (configure the port to trust DSCP), and assign the same DSCP to the packet for internal use. The IETF defines the six most-significant bits of the 1-byte Type of Service (ToS) field as the DSCP. The priority represented by a particular DSCP value is configurable. DSCP values range from 0 to 63.
- Trust the CoS value (if present) in the incoming packet, and generate the DSCP by using the CoS-to-DSCP map.
- Perform the classification based on a configured IP standard or extended ACL, which examines various fields in the IP header. If no ACL is configured, the packet is assigned the default DSCP based on the trust state of the ingress port; otherwise, the policy map specifies the DSCP to assign to the incoming frame.

For information on the maps described in this section, see the “Mapping Tables” section on page 29-12. For configuration information on port trust states, see the “Configuring the Trust State of Interfaces” section on page 29-35.



Figure 29-3 Classification Flowchart



63704

## Classification Based on QoS ACLs

A packet can be classified for QoS using multiple match criteria, and the classification can specify whether the packet should match all of the specified match criteria or at least one of the match criteria. To define a QoS classifier, you can provide the match criteria using the 'match' statements in a class-map. In the 'match' statements, you can specify the fields in the packet to match on, or you can use IP standard or IP extended ACLs. For more information, see Classification Based on Class Maps and Policy Maps, page 29-8.

If the class-map is configured to match all the match criteria, then a packet must satisfy all the match statements in the class-map before the QoS action is taken. The QoS action for the packet is not taken if the packet does not match even one match criterion in the class-map.

If the class-map is configured to match at least one match criterion, then a packet must satisfy at least one of the match statements in the class-map before the QoS action is taken. The QoS action for the packet is not taken if the packet does not match any match criteria in the class-map.

**Note**

When you use the IP standard and IP extended ACLs, the permit and deny ACEs in the ACL have a slightly different meaning in the QoS context.

- If a packet encounters (and satisfies) an ACE with a “permit,” then the packet “matches” the match criterion in the QoS classification.
- If a packet encounters (and satisfies) an ACE with a “deny,” then the packet “does not match” the match criterion in the QoS classification.
- If no match with a permit action is encountered and all the ACEs have been examined, then the packet “does not match” the criterion in the QoS classification.

**Note**

When creating an access list, remember that, by default, the end of the access list contains an implicit deny statement for everything if it did not find a match before reaching the end.

After a traffic class has been defined with the class map, you can create a policy that defines the QoS actions for a traffic class. A policy might contain multiple classes with actions specified for each one of them. A policy might include commands to classify the class as a particular aggregate (for example, assign a DSCP) or rate limit the class. This policy is then attached to a particular port on which it becomes effective.

You implement IP ACLs to classify IP traffic by using the **access-list** global configuration command. For configuration information, see the “Configuring a QoS Policy” section on page 29-27.

## Classification Based on Class Maps and Policy Maps

A class map is a mechanism that you use to isolate and name a specific traffic flow (or class) from all other traffic. The class map defines the criterion used to match against a specific traffic flow to further classify it; the criteria can include matching the access group defined by the ACL or matching a specific list of DSCP or IP precedence values. If you have more than one type of traffic that you want to classify, you can create another class map and use a different name. After a packet is matched against the class-map criteria, you can specify the QoS actions via a policy map.

A policy map specifies the QoS actions for the traffic classes. Actions can include trusting the CoS or DSCP values in the traffic class; setting a specific DSCP or IP precedence value in the traffic class; or specifying the traffic bandwidth limitations and the action to take when the traffic is out of profile. Before a policy map can be effective, you must attach it to an interface.

You create a class map by using the **class-map** global configuration command. When you enter the **class-map** command, the switch enters the class-map configuration mode. In this mode, you define the match criteria for the traffic by using the **match** class-map configuration command.

You create and name a policy map by using the **policy-map** global configuration command. When you enter this command, the switch enters the policy-map configuration mode. In this mode, you specify the actions to take on a specific traffic class by using the **trust** or **set** policy-map configuration and policy-map class configuration commands. To make the policy map effective, you attach it to an interface by using the **service-policy** interface configuration command.

The policy map can also contain commands that define the policer, (the bandwidth limitations of the traffic) and the action to take if the limits are exceeded. For more information, see the “Policing and Marking” section on page 29-9.

A policy map also has these characteristics:

- A policy map can contain up to 255 class statements.
- You can have different classes within a policy-map.
- A policy-map trust state supersedes an interface trust state.

For configuration information, see the “Configuring a QoS Policy” section on page 29-27.

## Policing and Marking

After a packet is classified and has an internal DSCP value assigned to it, the policing and marking process can begin as shown in Figure 29-4.

Policing involves creating a policer that specifies the bandwidth limits for the traffic. Packets that exceed the limits are *out of profile* or *nonconforming*. Each policer specifies the action to take for packets that are in or out of profile. These actions, carried out by the marker, include passing through the packet without modification, dropping the packet, or marking down the packet with a new DSCP value that is obtained from the configurable policed-DSCP map. For information on the policed-DSCP map, see the “Mapping Tables” section on page 29-12.

You can create these types of policers:

- Individual

QoS applies the bandwidth limits specified in the policer separately to each matched traffic class for each port/VLAN to which the policy-map is attached to. You configure this type of policer within a policy map by using the **police** command under policy-map class configuration mode.

- Aggregate

QoS applies the bandwidth limits specified in an aggregate policer cumulatively to all matched traffic flows. You configure this type of policer by specifying the aggregate policer name within a policy map by using the **police aggregate** policy-map configuration command. You specify the bandwidth limits of the policer by using the **qos aggregate-policer** global configuration command. In this way, the aggregate policer is shared by multiple classes of traffic within a policy map.

When configuring policing and policers, keep these items in mind:

- For IP packets, only the length of the IP payload (the total length field in the IP header) is used by the policer for policing computation. The Layer 2 header and trailer length are not taken into account. For example, for a 64-byte Ethernet II IP packet, only 46 bytes are taken into account for policing (64 bytes - 14 byte Ethernet Header - 4 bytes Ethernet CRC).

For non-IP packets, the Layer 2 length as specified in the Layer 2 Header is used by the policer for policing computation. To specify additional Layer 2 encapsulation length when policing IP packets, use the **qos account layer2 encapsulation** command.

- By default, no policers are configured.
- Only the average rate and committed burst parameters are configurable.
- Policing can occur on ingress and egress interfaces:
  - 1020 policers are supported on ingress
  - 1020 policers are supported on egress



---

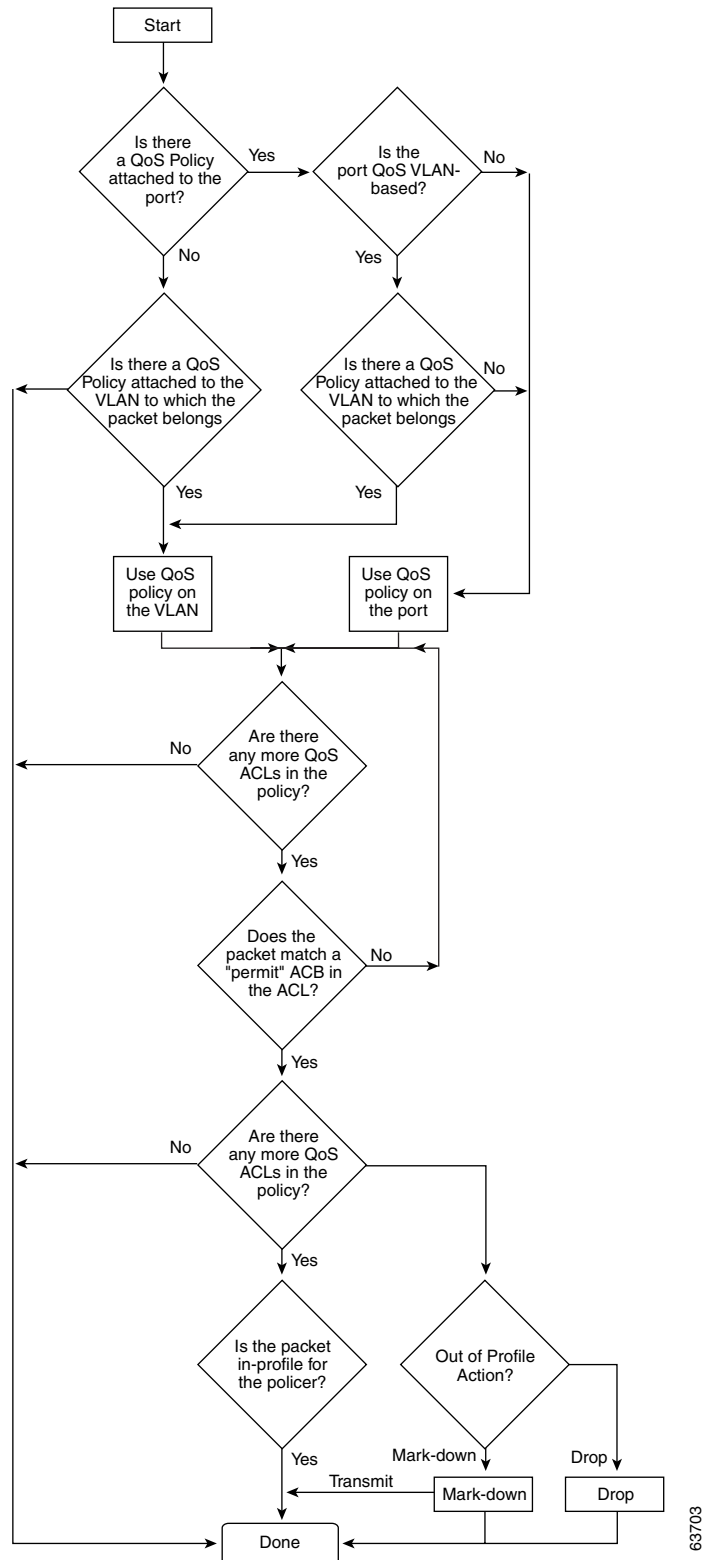
**Note** Policers 0 through 3 are reserved.

---

- All policers can be individual or aggregate.
- Two input and two output policers are reserved and used for “no policing” policers.
- On an interface configured for QoS, all traffic received or sent through the interface is classified, policed, and marked according to the policy-map attached to the interface. However, if the interface is configured to use VLAN-based QoS (using the **qos vlan-based** command), the traffic received or sent through the interface is classified, policed, and marked according to the policy-map attached to the VLAN (configured on the VLAN interface) to which the packet belongs. If there is no policy-map attached to the VLAN to which the packet belongs, the policy-map attached to the interface is used.

After you configure the policy map and policing actions, attach the policy to an ingress or egress interface by using the **service-policy** interface configuration command. For configuration information, see the “Configuring a QoS Policy” section on page 29-27 and the “Creating Named Aggregate Policers” section on page 29-25.

Figure 29-4 Policing and Marking Flowchart



63703

## Internal DSCP Values

The following sections describe the internal DSCP values:

- Internal DSCP Sources, page 29-12
- Egress ToS and CoS Sources, page 29-12

### Internal DSCP Sources

During processing, QoS represents the priority of all traffic (including non-IP traffic) with an internal DSCP value. QoS derives the internal DSCP value from the following:

- For trust-CoS traffic, from received or ingress interface Layer 2 CoS values
- For trust-DSCP traffic, from received or ingress interface DSCP values
- For untrusted traffic, from ingress interface DSCP value

The trust state of traffic is the trust state of the ingress interface unless set otherwise by a policy action for this traffic class.

QoS uses configurable mapping tables to derive the internal 6-bit DSCP value from CoS, which are 3-bit values (see the “Configuring DSCP Maps” section on page 29-40).

### Egress ToS and CoS Sources

For egress IP traffic, QoS creates a ToS byte from the internal DSCP value and sends it to the egress interface to be written into IP packets. For **trust-dscp** and **untrusted** IP traffic, the ToS byte includes the original 2 least-significant bits from the received ToS byte.

**Note**

The internal ToS value can mimic an IP precedence value (see Table 29-1 on page 29-4).

For all egress traffic, QoS uses a configurable mapping table to derive a CoS value from the internal ToS value associated with traffic (see the “Configuring the DSCP-to-CoS Map” section on page 29-42). QoS sends the CoS value to be written into ISL and 802.1Q frames.

For traffic received on an ingress interface configured to *trust CoS* using the **qos trust cos** command, the transmit CoS is always the incoming packet CoS (or the ingress interface default CoS if the packet is received untagged).

When the interface trust state is not configured to *trust dscp* using the **qos trust dscp** command, the security and QoS ACL classification will always use the interface DSCP and not the incoming packet DSCP.

## Mapping Tables

During QoS processing, the switch represents the priority of all traffic (including non-IP traffic) with an internal DSCP value:

- During classification, QoS uses configurable mapping tables to derive the internal DSCP (a 6-bit value) from received CoS. These maps include the CoS-to-DSCP map.
- During policing, QoS can assign another DSCP value to an IP or non-IP packet (if the packet is out of profile and the policer specifies a marked down DSCP value). This configurable map is called the policed-DSCP map.

- Before the traffic reaches the scheduling stage, QoS uses the internal DSCP to select one of the four egress queues for output processing. The DSCP-to-egress queue mapping can be configured using the **qos map dscp to tx-queue** command.

The CoS-to-DSCP and DSCP-to-CoS map have default values that might or might not be appropriate for your network.

For configuration information, see the “Configuring DSCP Maps” section on page 29-40.

## Queueing and Scheduling

Each physical port has four transmit queues (egress queues). Each packet that needs to be transmitted is enqueued to one of the transmit queues. The transmit queues are then serviced based on the transmit queue scheduling algorithm.

Once the final transmit DSCP is computed (including any markdown of DSCP), the transmit DSCP to transmit queue mapping configuration determines the transmit queue. The packet is placed in the transmit queue of the transmit port, determined from the transmit DSCP. Use the **qos map dscp to tx-queue** command to configure the transmit DSCP to transmit queue mapping. The transmit DSCP is the internal DSCP value if the packet is a non-IP packet as determined by the QoS policies and trust configuration on the ingress and egress ports.

For configuration information, see the “Configuring Transmit Queues” section on page 29-37.

## Active Queue Management

Active queue management (AQM) is the pro-active approach of informing you about congestion before a buffer overflow occurs. AQM is done using Dynamic buffer limiting (DBL). DBL tracks the queue length for each traffic flow in the switch. When the queue length of a flow exceeds its limit, DBL will drop packets or set the Explicit Congestion Notification (ECN) bits in the packet headers.

DBL classifies flows in two categories, adaptive and aggressive. Adaptive flows reduce the rate of packet transmission once it receives congestion notification. Aggressive flows do not take any corrective action in response to congestion notification. For every active flow the switch maintains two parameters, “buffersUsed” and “credits”. All flows start with “max-credits”, a global parameter. When a flow with credits less than “aggressive-credits” (another global parameter) it is considered an aggressive flow and is given a small buffer limit called “aggressiveBufferLimit”.

Queue length is measured by the number of packets. The number of packets in the queue determines the amount of buffer space that a flow is given. When a flow has a high queue length the computed value is lowered. This allows new incoming flows to receive buffer space in the queue. This allows all flows to get a proportional share of packets through the queue.

## Sharing Link Bandwidth Among Transmit Queues

The four transmit queues for a transmit port share the available link bandwidth of that transmit port. You can set the link bandwidth to be shared differently among the transmit queues using **bandwidth** command in interface transmit queue configuration mode. With this command, you assign the minimum guaranteed bandwidth for each transmit queue.

By default, all queues are scheduled in a round robin manner.

Bandwidth can only be configured on:

- Uplink ports on supervisor engines

- Ports on the WS-X4306-GB linecard.
- The 2 1000BASE-X ports on the WS-X4232-GB-RJ linecard
- The first 2 ports on the WS-X4418-GB linecard
- The two 1000BASE-X ports on the WS-X4412-2GB-TX linecard

## Strict Priority / Low Latency Queueing

You can configure transmit queue 3 on each port with higher priority using the **priority high** tx-queue configuration command in the interface configuration mode. When transmit queue 3 is configured with higher priority, packets in transmit queue 3 are scheduled ahead of packets in other queues.

When transmit queue 3 is configured at a higher priority, the packets are scheduled for transmission before the other transmit queues only if it has not met the allocated bandwidth sharing configuration. Any traffic that exceeds the configured shape rate will be queued and transmitted at the configured rate. If the burst of traffic, exceeds the size of the queue, packets will be dropped to maintain transmission at the configured shape rate.

## Traffic Shaping

Traffic Shaping provides the ability to control the rate of outgoing traffic in order to make sure that the traffic conforms to the maximum rate of transmission contracted for it. Traffic that meets certain profile can be shaped to meet the downstream traffic rate requirements to handle any data rate mismatches.

Each transmit queue can be configured to transmit a maximum rate using the **shape** command. The configuration allows you to specify the maximum rate of traffic. Any traffic that exceeds the configured shape rate will be queued and transmitted at the configured rate. If the burst of traffic exceeds the size of the queue, packets will be dropped to maintain transmission at the configured shape rate.

## Packet Modification

A packet is classified, policed, and queued to provide QoS. Packet modifications can occur during this process:

- For IP packets, classification involves assigning a DSCP to the packet. However, the packet is not modified at this stage; only an indication of the assigned DSCP is carried along. The reason for this is that QoS classification and ACL lookup occur in parallel, and it is possible that the ACL specifies that the packet should be denied and logged. In this situation, the packet is forwarded with its original DSCP to the CPU, where it is again processed through ACL software.
- For non-IP packets, classification involves assigning an internal DSCP to the packet, but because there is no DSCP in the non-IP packet, no overwrite occurs. Instead, the internal DSCP is used both for queueing and scheduling decisions and for writing the CoS priority value in the tag if the packet is being transmitted on either an ISL or 802.1Q trunk port.
- During policing, IP and non-IP packets can have another DSCP assigned to them (if they are out of profile and the policer specifies a markdown DSCP). Once again, the DSCP in the packet is not modified, but an indication of the marked-down value is carried along. For IP packets, the packet modification occurs at a later stage



# Configuring Auto-QoS

You can use the auto-QoS feature to simplify the deployment of existing QoS features. Auto-QoS makes assumptions about the network design, and as a result, the switch can prioritize different traffic flows and appropriately use the egress queues instead of using the default QoS behavior. (The default is that QoS is disabled. The switch then offers best-effort service to each packet, regardless of the packet content or size, and sends it from a single queue.)

When you enable auto-QoS, it automatically classifies traffic based on ingress packet label. The switch uses the resulting classification to choose the appropriate egress queue.

You use auto-QoS commands to identify ports connected to Cisco IP phones and to identify ports that receive trusted voice over IP (VoIP) traffic through an uplink. Auto-QoS then performs these functions:

- Detects the presence or absence of IP phones
- Configures QoS classification
- Configures egress queues

These sections describe how to configure auto-QoS on your switch:

- Generated Auto-QoS Configuration, page 29-15
- Effects of Auto-QoS on the Configuration, page 29-16
- Configuration Guidelines, page 29-16
- Enabling Auto-QoS for VoIP, page 29-17

## Generated Auto-QoS Configuration

By default, auto-QoS is disabled on all interfaces.

When you enable the auto-QoS feature on the first interface, these automatic actions 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 trust** interface configuration command, the ingress classification on the specified interface is set to trust the CoS label received in the packet if the specified interface is configured as Layer 2 (and is set to trust DSCP if the interface is configured as Layer 3). (See Table 29-2.)
- 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 interface is set to trust the cos label received in the packet, because some old phones do not mark dscp. When a Cisco IP phone is absent, the ingress classification is set to not trust the cos label in the packet.

For information about the trusted boundary feature, see the “Configuring a Trusted Boundary to Ensure Port Security” section on page 29-23.

When you enable auto-QoS by using the **auto qos voip cisco-phone** or the **auto qos voip trust** interface configuration commands, the switch automatically generates a QoS configuration based on the traffic type and ingress packet label and applies the commands listed in Table 29-2 to the interface.

**Table 29-2** Generated Auto-QoS Configuration

| Description                                                                                                                                                                                                                                                                                                  | Automatically Generated Command                                                                                                                                                                            |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| The switch automatically enables standard QoS and DBL configures the cos-to-DSCP map (maps CoS values in incoming packets to a DSCP value).                                                                                                                                                                  | Switch(config)# <b>qos</b><br>Switch(config)# <b>qos map cos 3 to 26</b><br>Switch(config)# <b>qos dbl</b><br>Switch(config)# <b>qos map cos 5 to 46</b>                                                   |
| The switch automatically configures the DSCP-to-Tx-queue mapping.                                                                                                                                                                                                                                            | Switch(config)# <b>qos map dscp 24 25 26 27 b28 29 30 31 to tx-queue 4</b><br>Switch(config)# <b>qos map dscp 32 33 34 35 36 37 38 39 to tx-queue 4</b>                                                    |
| The switch automatically sets the ingress classification on the interface to trust the CoS/DSCP value received in the packet.                                                                                                                                                                                | Switch(config-if)# <b>qos trust cos</b><br>or<br>Switch(config-if)# <b>qos trust dscp</b>                                                                                                                  |
| The switch automatically creates a QoS service policy, enables DBL on the policy, and attaches it to the interface.                                                                                                                                                                                          | Switch(config)# <b>policy-map autoqos-voip-policy</b><br>Switch(config-pmap)# <b>class class-default</b><br>Switch(config-pmap-c)# <b>dbl</b>                                                              |
| If you entered the <b>auto qos voip cisco-phone</b> command, the switch automatically enables the trusted boundary feature, which uses the CDP to detect the presence or absence of a Cisco IP phone.                                                                                                        | Switch(config-if)# <b>qos trust device cisco-phone</b>                                                                                                                                                     |
| The switch assigns a higher priority for queue 3. Limit for shaping on queue 3 is selected so that it is 33 percent of the link speed. Configure shaping as 33 percent on those ports where sharing is supported.<br><br>This procedure ensures that the higher-priority queue does not starve other queues. | Switch(config-if)# <b>tx-queue 3</b><br>Switch(config-if-tx-queue)# <b>priority high</b><br>Switch(config-if-tx-queue)# <b>shape percent 33</b><br>Switch(config-if-tx-queue)# <b>bandwidth percent 33</b> |

## Effects of Auto-QoS on the Configuration

When auto-QoS is enabled, the **auto qos voip** interface configuration command and the generated configuration are added to the running configuration.

## Configuration Guidelines

Before configuring auto-QoS, you should be aware of this information:

- In this release, auto-QoS configures the switch only for VoIP with Cisco IP phones.
- To take advantage of the auto-QoS defaults, do not configure any standard-QoS commands before entering the auto-QoS commands. If necessary, you can fine-tune the QoS configuration, but we recommend that you do so only after the auto-QoS configuration is completed.
- You can enable auto-QoS on static, dynamic-access, voice VLAN access, and trunk ports.
- By default, the CDP is enabled on all interfaces. For auto-QoS to function properly, do not disable the CDP.
- To enable **auto qos voip trust** on Layer 3 interfaces, change the port to Layer 3, then apply auto-QoS to make it trust DSCP.

## Enabling Auto-QoS for VoIP

To enable auto-QoS for VoIP within a QoS domain, perform this task:

|        | Command                                                                          | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------|----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch# <b>debug auto qos</b>                                                    | (Optional) Enables debugging for auto-QoS. When debugging is enabled, the switch displays the QoS commands that are automatically generated and applied when auto-QoS is enabled or disabled.                                                                                                                                                                                                                                           |
| Step 2 | Switch# <b>configure terminal</b>                                                | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                       |
| Step 3 | Switch(config)# <b>interface interface-id</b>                                    | Enters interface configuration mode, and specify the interface that is connected to a Cisco IP phone or the uplink interface that is connected to another switch or router in the interior of the network.                                                                                                                                                                                                                              |
| Step 4 | Switch(config-if)# <b>auto qos voip</b><br>{ <b>cisco-phone</b>   <b>trust</b> } | Enables auto-QoS.<br><br>The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>cisco-phone</b>—If the interface is connected to a Cisco IP phone, the cos labels of incoming packets are trusted only when the telephone is detected.</li> <li>• <b>trust</b>—The uplink interface is connected to a trusted switch or router, and the VoIP traffic classification in the ingress packet is trusted.</li> </ul> |
| Step 5 | Switch(config)# <b>end</b>                                                       | Returns to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                        |
| Step 6 | Switch# <b>show auto qos interface interface-id</b>                              | Verifies your entries.<br><br>This command displays the auto-QoS configuration that was initially applied; it does not display any user changes to the configuration that might be in effect.                                                                                                                                                                                                                                           |

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

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

```
Switch(config)# interface fastethernet1/1
Switch(config-if)# auto qos voip cisco-phone
```

This example shows how to enable auto-QoS and to trust the cos/dscp labels in incoming packets when the switch or router 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 display the QoS commands that are automatically generated when auto-QoS is enabled:

```
Switch# debug auto qos
AutoQoS debugging is on
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# auto qos voip cisco-phone
```

## Displaying Auto-QoS Information

To display the initial auto-QoS configuration, use the **show auto qos [interface *interface-id*]** privileged EXEC command. To display any user changes to that configuration, use the **show running-config** privileged EXEC command. You can compare the **show auto qos** and the **show running-config** command output to identify the user-defined QoS settings.

To display information about the QoS configuration that might be affected by auto-QoS, use one of these commands:

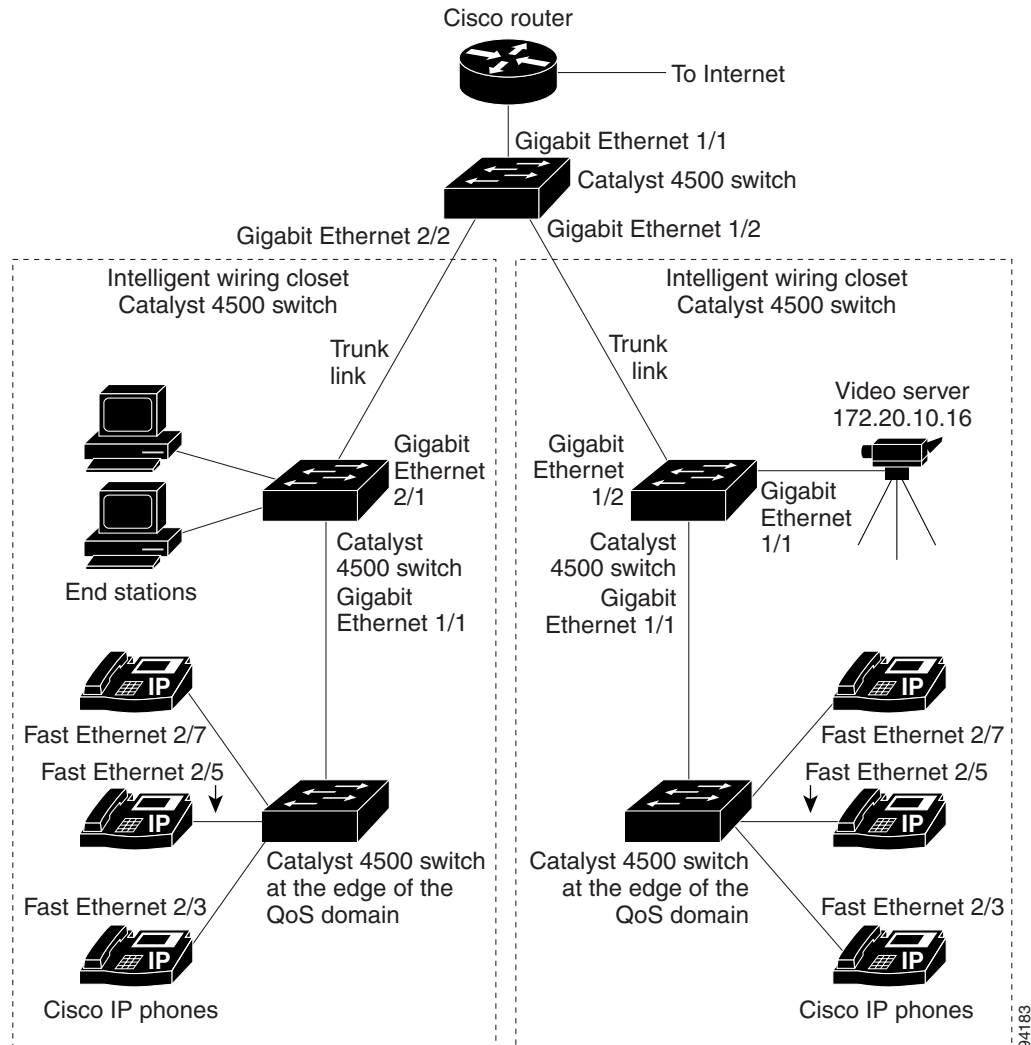
- **show qos**
- **show qos map**
- **show qos interface [interface-id]**

For more information about these commands, refer to the command reference for this release.

## Auto-QoS Configuration Example

This section describes how you could implement auto-QoS in a network, as shown in Figure 29-5.

**Figure 29-5 Auto-QoS Configuration Example Network**



The intelligent wiring closets in Figure 29-5 are composed of Catalyst 4500 switches. The object of this example is to prioritize the VoIP traffic over all other traffic. To do so, enable auto-QoS on the switches at the edge of the QoS domains in the wiring closets.



### Note

You should not configure any standard QoS commands before entering the auto-QoS commands. You can fine-tune the QoS configuration, but we recommend that you do so only after the auto-QoS configuration is completed.

To configure the switch at the edge of the QoS domain to prioritize the VoIP traffic over all other traffic, perform this task:

|         | Command                                             | Purpose                                                                                                                                                                                                                                                                                                                                              |
|---------|-----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1  | Switch# <b>debug auto qos</b>                       | Enables debugging for auto-QoS. When debugging is enabled, the switch displays the QoS configuration that is automatically generated when auto-QoS is enabled.                                                                                                                                                                                       |
| Step 2  | Switch# <b>configure terminal</b>                   | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                    |
| Step 3  | Switch(config)# <b>cdp enable</b>                   | Enables CDP globally. By default, CDP is enabled.                                                                                                                                                                                                                                                                                                    |
| Step 4  | Switch(config)# <b>interface fastethernet2/3</b>    | Enters interface configuration mode.                                                                                                                                                                                                                                                                                                                 |
| Step 5  | Switch(config-if)# <b>auto qos voip cisco-phone</b> | Enables auto-QoS on the interface, and specifies that the interface is connected to a Cisco IP phone.<br><br>The CoS labels of incoming packets are trusted only when the IP phone is detected.                                                                                                                                                      |
| Step 6  | Switch(config)# <b>interface fastethernet2/5</b>    | Enters interface configuration mode.                                                                                                                                                                                                                                                                                                                 |
| Step 7  | Switch(config)# <b>auto qos voip cisco-phone</b>    | Enables auto-QoS on the interface, and specifies that the interface is connected to a Cisco IP phone.                                                                                                                                                                                                                                                |
| Step 8  | Switch(config)# <b>interface fastethernet2/7</b>    | Enters interface configuration mode.                                                                                                                                                                                                                                                                                                                 |
| Step 9  | Switch(config)# <b>auto qos voip cisco-phone</b>    | Enables auto-QoS on the interface, and specifies that the interface is connected to a Cisco IP phone.                                                                                                                                                                                                                                                |
| Step 10 | Switch(config)# <b>interface gigabit1/1</b>         | Enters interface configuration mode.                                                                                                                                                                                                                                                                                                                 |
| Step 11 | Switch(config)# <b>auto qos voip trust</b>          | Enables auto-QoS on the interface, and specifies that the interface is connected to a trusted router or switch.                                                                                                                                                                                                                                      |
| Step 12 | Switch(config)# <b>end</b>                          | Returns to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                     |
| Step 13 | Switch# <b>show auto qos</b>                        | Verifies your entries.<br><br>This command displays the auto-QoS configuration that is initially applied; it does not display any user changes to the configuration that might be in effect.<br><br>For information about the QoS configuration that might be affected by auto-QoS, see the “Displaying Auto-QoS Information” section on page 29-18. |
| Step 14 | Switch# <b>show auto qos interface interface-id</b> | Verifies your entries.<br><br>This command displays the auto-QoS configuration that was initially applied; it does not display any user changes to the configuration that might be in effect.                                                                                                                                                        |
| Step 15 | Switch# <b>copy running-config startup-config</b>   | Saves the <b>auto qos voip</b> interface configuration commands and the generated auto-QoS configuration in the configuration file.                                                                                                                                                                                                                  |

# Configuring QoS

Before configuring QoS, you must have a thorough understanding of these items:

- The types of applications used and the traffic patterns on your network.
- Traffic characteristics and needs of your network. Is the traffic bursty? Do you need to reserve bandwidth for voice and video streams?
- Bandwidth requirements and speed of the network.
- Location of congestion points in the network.

These sections describe how to configure QoS on the Catalyst 4500 series switch:

- Default QoS Configuration, page 29-21
- Configuration Guidelines, page 29-22
- Enabling QoS Globally, page 29-23
- Configuring a Trusted Boundary to Ensure Port Security, page 29-23
- Enabling Dynamic Buffer Limiting, page 29-25
- Creating Named Aggregate Policers, page 29-25
- Configuring a QoS Policy, page 29-27
- Enabling or Disabling QoS on an Interface, page 29-34
- Configuring VLAN-Based QoS on Layer 2 Interfaces, page 29-34
- Configuring the Trust State of Interfaces, page 29-35
- Configuring the CoS Value for an Interface, page 29-36
- Configuring DSCP Values for an Interface, page 29-37
- Configuring Transmit Queues, page 29-37
- Configuring DSCP Maps, page 29-40

## Default QoS Configuration

Table 29-3 shows the QoS default configuration.

**Table 29-3 QoS Default Configuration**

| Feature                                  | Default Value                        |
|------------------------------------------|--------------------------------------|
| Global QoS configuration                 | Disabled                             |
| Interface QoS configuration (port based) | Enabled when QoS is globally enabled |
| Interface CoS value                      | 0                                    |
| Interface DSCP value                     | 0                                    |

**Table 29-3 QoS Default Configuration (continued)**

| Feature                                          | Default Value                                                                                                                                                                                  |
|--------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CoS to DSCP map<br>(DSCP set from CoS values)    | CoS 0 = DSCP 0<br>CoS 1 = DSCP 8<br>CoS 2 = DSCP 16<br>CoS 3 = DSCP 24<br>CoS 4 = DSCP 32<br>CoS 5 = DSCP 40<br>CoS 6 = DSCP 48<br>CoS 7 = DSCP 56                                             |
| DSCP to CoS map<br>(CoS set from DSCP values)    | DSCP 0–7 = CoS 0<br>DSCP 8–15 = CoS 1<br>DSCP 16–23 = CoS 2<br>DSCP 24–31 = CoS 3<br>DSCP 32–39 = CoS 4<br>DSCP 40–47 = CoS 5<br>DSCP 48–55 = CoS 6<br>DSCP 56–63 = CoS 7                      |
| Marked-down DSCP from DSCP map<br>(Policed-DSCP) | Marked-down DSCP value equals original DSCP value (no markdown)                                                                                                                                |
| Policers                                         | None                                                                                                                                                                                           |
| Policy maps                                      | None                                                                                                                                                                                           |
| Transmit queue sharing                           | 1/4 of the link bandwidth                                                                                                                                                                      |
| Transmit queue size                              | 1/4 of the transmit queue entries for the port. The transmit queue size of a port depends on the type of port, ranging from 240 packets per transmit queue to 1920 packets per transmit queue. |
| Transmit queue shaping                           | None                                                                                                                                                                                           |
| DCSP-to-Transmit queue map                       | DSCP 0–15 Queue 1<br>DSCP 16–31 Queue 2<br>DSCP 32–47 Queue 3<br>DSCP 48–63 Queue 4                                                                                                            |
| High priority transmit queue                     | Disabled                                                                                                                                                                                       |
| <b>With QoS disabled</b>                         |                                                                                                                                                                                                |
| Interface trust state                            | Trust DSCP                                                                                                                                                                                     |
| <b>With QoS enabled</b>                          | With QoS enabled and all other QoS parameters at default values, QoS sets IP DSCP to zero and Layer 2 CoS to zero in all traffic transmitted.                                                  |
| Interface trust state                            | Untrusted                                                                                                                                                                                      |

## Configuration Guidelines

Before beginning the QoS configuration, you should be aware of this information:

- If you have EtherChannel ports configured on your switch, you must configure QoS classification and policing on the EtherChannel. The transmit queue configuration must be configured on the individual physical ports that comprise the EtherChannel.



- It is not possible to match IP fragments against configured IP extended ACLs to enforce QoS. IP fragments are transmitted as best effort. IP fragments are denoted by fields in the IP header.
- It is not possible to match IP options against configured IP extended ACLs to enforce QoS. These packets are sent to the CPU and processed by software. IP options are denoted by fields in the IP header.
- Control traffic (such as spanning-tree BPDUs and routing update packets) received by the switch are subject to all ingress QoS processing.
- If you want to use the set command in the policy map, you must enable IP routing (disabled by default) and configure an IP default route to send traffic to the next-hop device that is capable of forwarding.

**Note**

QoS processes both unicast and multicast traffic.

## Enabling QoS Globally

To enable QoS globally, perform this task:

|               | Command                    | Purpose                                                |
|---------------|----------------------------|--------------------------------------------------------|
| <b>Step 1</b> | Switch(config)# <b>qos</b> | Enables QoS on the switch.                             |
|               |                            | Use the <b>no qos</b> command to globally disable QoS. |
| <b>Step 2</b> | Switch(config)# <b>end</b> | Exits configuration mode.                              |
| <b>Step 3</b> | Switch# <b>show qos</b>    | Verifies the configuration.                            |

This example shows how to enable QoS globally:

```
Switch(config)# qos
Switch(config)# end
Switch#
```

This example shows how to verify the configuration:

```
Switch# show qos
 QoS is enabled globally

Switch#
```

## Configuring a Trusted Boundary to Ensure Port Security

In a typical network, you connect a Cisco IP phone to a switch port as discussed in Chapter 35, “Configuring Voice Interfaces.” Traffic sent from the telephone to the switch is typically marked with a tag that uses the 802.1Q header. The header contains the VLAN information and the class of service (CoS) 3-bit field, which determines the priority of the packet. For most Cisco IP phone configurations, the traffic sent from the telephone to the switch is trusted to ensure that voice traffic is properly prioritized over other types of traffic in the network. By using the **qos trust cos** interface configuration command, you can configure the switch port to which the telephone is connected to trust the CoS labels of all traffic received on that port.

In some situations, you also might connect a PC or workstation to the IP phone. In this case, you can use the **switchport priority extend cos** interface configuration command to configure the telephone through the switch CLI to override the priority of the traffic received from the PC. With this command, you can prevent a PC from taking advantage of a high-priority data queue.

However, if a user bypasses the telephone and connects the PC directly to the switch, the CoS labels generated by the PC are trusted by the switch (because of the trusted CoS setting) and can allow misuse of high-priority queues. The trusted boundary feature solves this problem by using the CDP to detect the presence of a Cisco IP phone (such as the Cisco IP Phone 7910, 7935, 7940, and 7960) on a switch port.

**Note**

If CDP is not running on the switch globally or on the port in question, trusted boundary will not work.

When you configure trusted boundary on a port, trust is disabled. Then, when a phone is plugged in and detected, trust is enabled. (It may take a few minutes to detect the phone.) Now, when a phone is unplugged (and not detected), the trusted boundary feature disables the trusted setting on the switch port and prevents misuse of a high-priority queue.

To enable trusted boundary on a port, perform this task:

|               | Command                                                       | Purpose                                                                                                                                                                                                                   |
|---------------|---------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Switch# <b>configure terminal</b>                             | Enters global configuration mode.                                                                                                                                                                                         |
| <b>Step 2</b> | Switch(config)# <b>interface</b><br><i>interface-id</i>       | Enters interface configuration mode, and specifies the interface connected to the IP phone.<br><br>Valid interfaces include physical interfaces.                                                                          |
| <b>Step 3</b> | Switch(config)# <b>qos trust</b> [ <b>cos</b>   <b>dscp</b> ] | Configures the interface to trust the CoS value in received traffic. By default, the port is not trusted.                                                                                                                 |
| <b>Step 4</b> | Switch(config)# <b>qos trust device</b><br><b>cisco-phone</b> | Specifies that the Cisco IP phone is a trusted device.<br><br>You cannot enable both trusted boundary and auto-QoS ( <b>auto qos voip</b> interface configuration command) at the same time; they are mutually exclusive. |
| <b>Step 5</b> | Switch(config)# <b>end</b>                                    | Returns to privileged EXEC mode.                                                                                                                                                                                          |
| <b>Step 6</b> | Switch# <b>show qos interface</b><br><i>interface-id</i>      | Verifies your entries.                                                                                                                                                                                                    |
| <b>Step 7</b> | Switch# <b>copy running-config</b><br><b>startup-config</b>   | (Optional) Saves your entries in the configuration file.                                                                                                                                                                  |

To disable the trusted boundary feature, use the **no qos trust device cisco-phone** interface configuration command.

## Enabling Dynamic Buffer Limiting

To enable DBL globally on the switch, perform this task:

|        | Command                        | Purpose                                                                         |
|--------|--------------------------------|---------------------------------------------------------------------------------|
| Step 1 | Switch(config)# <b>qos db1</b> | Enables DBL on the switch.<br>Use the <b>no qos db1</b> command to disable AQM. |
| Step 2 | Switch(config)# <b>end</b>     | Exits configuration mode.                                                       |
| Step 3 | Switch# <b>show qos db1</b>    | Verifies the configuration.                                                     |

This example shows how to enable DBL globally:

```
Switch(config)# qos db1
Global DBL enabled
Switch(config)# end
Switch#
```

This example shows how to verify the configuration:

```
Switch# show qos db1
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
Switch#
```

## Creating Named Aggregate Policers

To create a named aggregate policer, perform this task:

| Command                                                                                                                                                                                                                                           | Purpose                            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|
| Switch(config)# <b>qos aggregate-policer</b> <i>policer_name</i><br><i>rate burst</i> [[ <b>conform-action</b> { <b>transmit</b>   <b>drop</b> }]<br>[ <b>exceed-action</b> { <b>transmit</b>   <b>drop</b>  <br><b>policed-dscp-transmit</b> }]] | Creates a named aggregate policer. |

An aggregate policer can be applied to one or more interfaces. However, if you apply the same policer to the input direction on one interface and to the output direction on a different interface, then you have created the equivalent of two different aggregate policers in the switching engine. Each policer has the same policing parameters, with one policing the ingress traffic on one interface and the other policing the egress traffic on another interface. If an aggregate policer is applied to multiple interfaces in the same direction, then only one instance of the policer is created in the switching engine.

Similarly, an aggregate policer can be applied to a port or to a VLAN. If you apply the same aggregate policer to a port and to a VLAN, then you have created the equivalent of two different aggregate policers in the switching engine. Each policer has the same policing parameters, with one policing the traffic on

the configured port and the other policing the traffic on the configured VLAN. If an aggregate policer is applied to only ports or only VLANs, then only one instance of the policer is created in the switching engine.

In effect, if you apply a single aggregate policer to ports and VLANs in different directions, then you have created the equivalent of four aggregate policers; one for all ports sharing the policer in input direction, one for all ports sharing the policer in output direction, one for all VLANs sharing the policer in input direction and one for all VLANs sharing the policer in output direction.

When creating a named aggregate policer, note the following:

- The valid range of values for the *rate* parameter is as follows:
  - Minimum—32 kilobits per second
  - Maximum—32 gigabits per second

See the “Configuration Guidelines” section on page 29-22.

- Rates can be entered in bits-per-second, or you can use the following abbreviations:
  - k to denote 1000 bps
  - m to denote 1000000 bps
  - g to denote 1000000000 bps




---

**Note** You can also use a decimal point. For example, a rate of 1,100,000 bps can be entered as 1.1m.

---

- The valid range of values for the *burst* parameter is as follows:
  - Minimum—1 kilobyte
  - Maximum—512 megabytes
- Bursts can be entered in bytes, or you can use the following abbreviation:
  - k to denote 1000 bytes
  - m to denote 1000000 bytes
  - g to denote 1000000000 bytes




---

**Note** You can also use a decimal point. For example, a burst of 1,100,000 bytes can be entered as 1.1m.

---

- Optionally, you can specify a conform action for matched in-profile traffic as follows:
  - The default conform action is **transmit**.
  - Enter the **drop** keyword to drop all matched traffic.




---

**Note** When you configure **drop** as the conform action, QoS configures **drop** as the exceed action.

---

- Optionally, for traffic that exceeds the CIR, you can specify an exceed action as follows:
  - The default exceed action is **drop**.
  - Enter the **policed-dscp-transmit** keyword to cause all matched out-of-profile traffic to be marked down as specified in the markdown map.

- For no policing, enter the **transmit** keyword to transmit all matched out-of-profile traffic.
- You can enter the **no qos aggregate-policer** *policer\_name* command to delete a named aggregate policer.

This example shows how to create a named aggregate policer with a 10 Mbps rate limit and a 1-MB burst size that transmits conforming traffic and marks down out-of-profile traffic.

```
Switch(config)# qos aggregate-policer aggr-1 10000000 1000000 conform-action transmit
exceed-action policed-dscp-transmit
Switch(config)# end
Switch#
```

This example shows how to verify the configuration:

```
Switch# show qos aggregate-policer aggr-1
Policer aggr-1
 Rate(bps):10000000 Normal-Burst(bytes):1000000
 conform-action:transmit exceed-action:policed-dscp-transmit
 Polymaps using this policer:
Switch#
```

## Configuring a QoS Policy

The following subsections describe QoS policy configuration:

- Overview of QoS Policy Configuration, page 29-27
- Configuring a Class Map (Optional), page 29-28
- Verifying Class-Map Configuration, page 29-29
- Configuring a Policy Map, page 29-29
- Verifying Policy-Map Configuration, page 29-32
- Attaching a Policy Map to an Interface, page 29-33



### Note

QoS policies process both unicast and multicast traffic.

## Overview of QoS Policy Configuration

Configuring a QoS policy requires you to configure traffic classes and the policies that will be applied to those traffic classes, and to attach the policies to interfaces using these commands:

- **access-list** (optional for IP traffic—you can filter IP traffic with **class-map** commands):
  - QoS supports these access list types:

| Protocol | Numbered Access Lists?          | Extended Access Lists?             | Named Access Lists? |
|----------|---------------------------------|------------------------------------|---------------------|
| IP       | Yes:<br>1 to 99<br>1300 to 1999 | Yes:<br>100 to 199<br>2000 to 2699 | Yes                 |

- See Chapter 24, “Configuring Network Security with ACLs,” for information about ACLs on the Catalyst 4500 series switches.

- **class-map** (optional)—Enter the **class-map** command to define one or more traffic classes by specifying the criteria by which traffic is classified (see the “Configuring a Class Map (Optional)” section on page 29-28).
- **policy-map**—Enter the **policy-map** command to define the following for each class of traffic:
  - Internal DSCP source
  - Aggregate or individual policing and marking
- **service-policy**—Enter the **service-policy** command to attach a policy map to an interface.

## Configuring a Class Map (Optional)

The following subsections describe class map configuration:

- Creating a Class Map, page 29-28
- Configuring Filtering in a Class Map, page 29-28

Enter the **class-map** configuration command to define a traffic class and the match criteria that will be used to identify traffic as belonging to that class. Match statements can include criteria such as an ACL, an IP precedence value, or a DSCP value. The match criteria are defined with one match statement entered within the class-map configuration mode.

### Creating a Class Map

To create a class map, perform this task:

| Command                                                                         | Purpose                                                                        |
|---------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| Switch(config)# [no] <b>class-map</b> [match-all   match-any] <i>class_name</i> | Creates a named class map.<br>Use the <b>no</b> keyword to delete a class map. |

### Configuring Filtering in a Class Map

To configure filtering in a class map, perform one of these tasks:

| Command                                                                                                            | Purpose                                                                                                                                                                                                                                                                                                         |
|--------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Switch(config-cmap)# [no] <b>match access-group</b> { <i>acl_index</i>   <b>name</b> <i>acl_name</i> }             | (Optional) Specifies the name of the ACL used to filter traffic.<br>Use the <b>no</b> keyword to remove the statement from a class map.<br><b>Note</b> Access lists are not documented in this publication. See the reference under <b>access-list</b> in the “Configuring a QoS Policy” section on page 29-27. |
| Switch (config-cmap)# [no] <b>match ip precedence</b> <i>ipp_value1</i> [ <i>ipp_value2</i> [ <i>ipp_valueN</i> ]] | (Optional—for IP traffic only) Specifies up to eight IP precedence values used as match criteria. Use the <b>no</b> keyword to remove the statement from a class map.                                                                                                                                           |
| Switch (config-cmap)# [no] <b>match ip dscp</b> <i>dscp_value1</i> [ <i>dscp_value2</i> [ <i>dscp_valueN</i> ]]    | (Optional—for IP traffic only) Specifies up to eight DSCP values used as match criteria. Use the <b>no</b> keyword to remove the statement from a class map.                                                                                                                                                    |
| Switch (config-cmap)# [no] <b>match any</b>                                                                        | (Optional) Matches any IP traffic or non-IP traffic.                                                                                                                                                                                                                                                            |

**Note**

Any Input or Output policy that uses a class-map with the **match ip precedence** or **match ip dscp** class-map commands, requires that the port on which the packet is received, be configured to **trust dscp**. If the incoming port trust state is not set to **trust dscp**, the IP packet DSCP/IP-precedence is not used for matching the traffic; instead the receiving port's default DSCP is used.

**Note**

The interfaces on the Catalyst 4500 series switch do not support the **match classmap**, **match destination-address**, **match input-interface**, **match mpls**, **match not**, **match protocol**, **match qos-group**, and **match source-address** keywords.

## Verifying Class-Map Configuration

To verify class-map configuration, perform this task:

|        | Command                                  | Purpose                     |
|--------|------------------------------------------|-----------------------------|
| Step 1 | Switch (config-cmap)# <b>end</b>         | Exits configuration mode.   |
| Step 2 | Switch# <b>show class-map class_name</b> | Verifies the configuration. |

This example shows how to create a class map named **ipp5** and how to configure filtering to match traffic with IP precedence 5:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# class-map ipp5
Switch(config-cmap)# match ip precedence 5
Switch(config-cmap)# end
Switch#
```

This example shows how to verify the configuration:

```
Switch# show class-map ipp5
Class Map match-all ipp5 (id 1)
 Match ip precedence 5

Switch#
```

## Configuring a Policy Map

You can attach only one policy map to an interface. Policy maps can contain one or more policy-map classes, each with different match criteria and policers.

Configure a separate policy-map class in the policy map for each type of traffic that an interface receives. Put all commands for each type of traffic in the same policy-map class. QoS does not attempt to apply commands from more than one policy-map class to matched traffic.

The following sections describe policy-map configuration:

- Creating a Policy Map, page 29-30
- Configuring Policy-Map Class Actions, page 29-30

## Creating a Policy Map

To create a policy map, perform this task:

| Command                                                   | Purpose                                                                                                 |
|-----------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| Switch(config)# [no] <b>policy-map</b> <i>policy_name</i> | Creates a policy map with a user-specified name.<br>Use the <b>no</b> keyword to delete the policy map. |

## Configuring Policy-Map Class Actions

These sections describe policy-map class action configuration:

- Configuring the Policy-Map Class Trust State, page 29-30
- Configuring the Policy Map Class DBL State, page 29-30
- Configuring Policy-Map Class Policing, page 29-31
- Using a Named Aggregate Policer, page 29-31
- Configuring a Per-Interface Policer, page 29-31

### Configuring the Policy-Map Class Trust State

To configure the policy-map class trust state, perform this task:

| Command                                                                  | Purpose                                                                                                                                                                                                                                                                     |
|--------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Switch(config-pmap-c)# [no] <b>trust</b><br>{ <b>cos</b>   <b>dscp</b> } | Configures the policy-map class trust state, which selects the value that QoS uses as the source of the internal DSCP value (see the “Internal DSCP Values” section on page 29-12).<br><br>Use the <b>no</b> keyword to clear a configured value and return to the default. |

When configuring the policy-map class trust state, note the following:

- You can enter the **no trust** command to use the trust state configured on the ingress interface (this is the default).
- With the **cos** keyword, QoS sets the internal DSCP value from received or interface CoS.
- With the **dscp** keyword, QoS uses received DSCP.

### Configuring the Policy Map Class DBL State

To configure the policy map class DBL state, perform this task:

| Command                                | Purpose                                                                                                                                                                                                                                |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Switch(config-pmap-c)# [no] <b>dbl</b> | Configures the policy-map class DBL state, which tracks the queue length of traffic flows (see the “Active Queue Management” section on page 29-13).<br><br>Use the <b>no</b> keyword to clear an DBL value and return to the default. |



When configuring the policy-map class DBL state, note the following:

- Any class that uses a named aggregate policer must have the same DBL configuration to work.

### Configuring Policy-Map Class Policing

These sections describe configuration of policy-map class policing:

- Using a Named Aggregate Policer, page 29-31
- Configuring a Per-Interface Policer, page 29-31

### Using a Named Aggregate Policer

To use a named aggregate policer (see the “Creating Named Aggregate Policers” section on page 29-25), perform this task:

| Command                                                                   | Purpose                                                                                                                    |
|---------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| Switch(config-pmap-c)# [no] <b>police aggregate</b> <i>aggregate_name</i> | Uses a previously defined aggregate policer.<br>Use the <b>no</b> keyword to delete the policer from the policy map class. |

### Configuring a Per-Interface Policer

To configure a per-interface policer (see the “Policing and Marking” section on page 29-9), perform this task:

| Command                                                                                                                                            | Purpose                                                                                                         |
|----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| Switch(config-pmap-c)# [no] <b>police rate burst</b> [[conform-action {transmit   drop}][exceed-action {transmit   drop   policed-dscp-transmit}]] | Configures a per-interface policer.<br>Use the <b>no</b> keyword to delete a policer from the policy map class. |

When configuring a per-interface policer, note the following:

- The valid range of values for the *rate* parameter is as follows:
  - Minimum—32 kilobits per second, entered as 32000
  - Maximum—32 gigabits per second, entered as 32000000000



**Note** See the “Configuration Guidelines” section on page 29-22.

- Rates can be entered in bits-per-second, or you can use the following abbreviations:
  - k to denote 1000 bps
  - m to denote 1000000 bps
  - g to denote 1000000000 bps



**Note** You can also use a decimal point. For example, a rate of 1,100,000 bps can be entered as 1.1m.

- The valid range of values for the *burst* parameter is as follows:
  - Minimum—1 kilobyte
  - Maximum—512 megabytes
- Bursts can be entered in bytes, or you can use the following abbreviation:
  - k to denote 1000 bytes
  - m to denote 1000000 bytes
  - g to denote 1000000000 bytes



**Note** You can also use a decimal point. For example, a burst of 1,100,000 bytes can be entered as 1.1m.

- Optionally, you can specify a conform action for matched in-profile traffic as follows:
  - The default conform action is **transmit**.
  - You can enter the **drop** keyword to drop all matched traffic.
- Optionally, for traffic that exceeds the CIR, you can enter the **policed-dscp-transmit** keyword to cause all matched out-of-profile traffic to be marked down as specified in the markdown map. See “Configuring the Policed-DSCP Map” section on page 29-41.
  - For no policing, you can enter the **transmit** keyword to transmit all matched out-of-profile traffic.

This example shows how to create a policy map named **ipp5-policy** that uses the class-map named **ipp5**, is configured to rewrite the packet precedence to 6 and to aggregate police the traffic that matches IP precedence value of 5:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# policy-map ipp5-policy
Switch(config-pmap)# class ipp5
Switch(config-pmap-c)# set ip precedence 6
Switch(config-pmap-c)# dbl
Switch(config-pmap-c)# police 2000000000 2000000 conform-action transmit exceed-action
policed-dscp-transmit
Switch(config-pmap-c)# end
```

## Verifying Policy-Map Configuration

To verify policy-map configuration, perform this task:

|        | Command                             | Purpose                                                                                                                                              |
|--------|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch(config-pmap-c)# end          | Exits policy-map class configuration mode.<br><br><b>Note</b> Enter additional <b>class</b> commands to create additional classes in the policy map. |
| Step 2 | Switch# show policy-map policy_name | Verifies the configuration.                                                                                                                          |

This example shows how to verify the configuration:

```
Switch# show policy-map ipp5-policy
show policy ipp5-policy
Policy Map ipp5-policy
class ipp5
 set ip precedence 6
 dbl
police 2000000000 2000000 conform-action transmit exceed-action
policed-dscp-transmit
Switch#
```

## Attaching a Policy Map to an Interface

To attach a policy map to an interface, perform this task:

|        | Command                                                                                                                 | Purpose                                                                                                                            |
|--------|-------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch(config)# <b>interface</b> {vlan vlan_ID   {fastethernet   gigabitethernet} slot/interface   Port-channel number} | Selects the interface to configure.                                                                                                |
| Step 2 | Switch(config-if)# [no] <b>service-policy</b> input policy_map_name                                                     | Attaches a policy map to the input direction of the interface. Use the <b>no</b> keyword to detach a policy map from an interface. |
| Step 3 | Switch(config-if)# <b>end</b>                                                                                           | Exits configuration mode.                                                                                                          |
| Step 4 | Switch# <b>show policy-map interface</b> {vlan vlan_ID   {fastethernet   gigabitethernet} slot/interface}               | Verifies the configuration.                                                                                                        |

This example shows how to attach the policy map named **pmap1** to Fast Ethernet interface 5/36:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 5/36
Switch(config-if)# service-policy input pmap1
Switch(config-if)# end
```

This example shows how to verify the configuration:

```
Switch# show policy-map interface fastethernet 5/36
FastEthernet6/1

 service-policy input:p1

 class-map:c1 (match-any)
 238474 packets
 match:access-group 100
 38437 packets
 police:aggr-1
 Conform:383934 bytes Exceed:949888 bytes

 class-map:class-default (match-any)
 0 packets
 match:any
 0 packets
Switch#
```

## Enabling or Disabling QoS on an Interface

The **qos** interface command reenables any previously configured QoS features. The **qos** interface command does not affect the interface queuing configuration.

To enable or disable QoS features for traffic from an interface, perform this task:

|        | Command                                                                                                                                                                      | Purpose                                                                                    |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| Step 1 | Switch(config)# <b>interface</b> { <b>vlan</b> <i>vlan_ID</i>   { <b>fastethernet</b>   <b>gigabitethernet</b> } <i>slot/interface</i>   <b>Port-channel</b> <i>number</i> } | Selects the interface to configure.                                                        |
| Step 2 | Switch(config-if)# [ <b>no</b> ] <b>qos</b>                                                                                                                                  | Enables QoS on the interface.<br>Use the <b>no</b> keyword to disable QoS on an interface. |
| Step 3 | Switch(config-if)# <b>end</b>                                                                                                                                                | Exits configuration mode.                                                                  |
| Step 4 | Switch# <b>show qos interface</b>                                                                                                                                            | Verifies the configuration.                                                                |

This example shows how to disable QoS on interface VLAN 5:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface vlan 5
Switch(config-if)# no qos
Switch(config-if)# end
Switch#
```

This example shows how to verify the configuration:

```
Switch# show qos | begin QoS is disabled
QoS is disabled on the following interfaces:
V15
<...Output Truncated...>
Switch#
```

## Configuring VLAN-Based QoS on Layer 2 Interfaces

By default, QoS uses policy maps attached to physical interfaces. For Layer 2 interfaces, you can configure QoS to use policy maps attached to a VLAN. See the “Attaching a Policy Map to an Interface” section on page 29-33.

To configure VLAN-based QoS on a Layer 2 interface, perform this task:

|        | Command                                                                                                                                     | Purpose                                                                                                                   |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch(config)# <b>interface</b> { <b>fastethernet</b>   <b>gigabitethernet</b> } <i>slot/interface</i>   <b>Port-channel</b> <i>number</i> | Selects the interface to configure.                                                                                       |
| Step 2 | Switch(config-if)# [ <b>no</b> ] <b>qos vlan-based</b>                                                                                      | Configures VLAN-based QoS on a Layer 2 interface.<br>Use the <b>no</b> keyword to disable VLAN-based QoS on an interface. |
| Step 3 | Switch(config-if)# <b>end</b>                                                                                                               | Exits configuration mode.                                                                                                 |
| Step 4 | Switch# <b>show qos</b>                                                                                                                     | Verifies the configuration.                                                                                               |

**Note**

If no input QoS policy is attached to a Layer 2 interface, then the input QoS policy attached to the VLAN (on which the packet is received), if any, is used even if the port is not configured as VLAN-based. If you do not want this default, attach a placeholder input QoS policy to the Layer 2 interface. Similarly, if no output QoS policy is attached to a Layer 2 interface, then the output QoS policy attached to the VLAN (on which the packet is transmitted), if any, is used even if the port is not configured as VLAN-based. If you do not want this default, attach a placeholder output QoS policy to the layer 2 interface.

This example shows how to configure VLAN-based QoS on Fast Ethernet interface 5/42:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 5/42
Switch(config-if)# qos vlan-based
Switch(config-if)# end
```

This example shows how to verify the configuration:

```
Switch# show qos | begin QoS is vlan-based
QoS is vlan-based on the following interfaces:
 Fa5/42
Switch#
```

**Note**

When a layer 2 interface is configured with VLAN-based QoS, and if a packet is received on the port for a VLAN on which there is no QoS policy, then the QoS policy attached to the port, if any is used. This applies for both Input and Output QoS policies.

## Configuring the Trust State of Interfaces

This command configures the trust state of interfaces. By default, all interfaces are untrusted.

To configure the trust state of an interface, perform this task;

|        | Command                                                                                                                 | Purpose                                                                                                                             |
|--------|-------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch(config)# <b>interface</b> {vlan vlan_ID   {fastethernet   gigabitethernet} slot/interface   Port-channel number} | Selects the interface to configure.                                                                                                 |
| Step 2 | Switch(config-if)# [no] <b>qos trust</b> [dscp   cos]                                                                   | Configures the trust state of an interface.<br><br>Use the <b>no</b> keyword to clear a configured value and return to the default. |
| Step 3 | Switch(config-if)# <b>end</b>                                                                                           | Exits configuration mode.                                                                                                           |
| Step 4 | Switch# <b>show qos</b>                                                                                                 | Verifies the configuration.                                                                                                         |

When configuring the trust state of an interface, note the following:

- You can use the **no qos trust** command to set the interface state to untrusted.
- For traffic received on an ingress interface configured to *trust CoS* using the **qos trust cos** command, the transmit CoS is always the incoming packet CoS (or the ingress interface default CoS if the packet is received untagged).

- When the interface trust state is not configured to *trust dscp* using the **qos trust dscp** command, the security and QoS ACL classification will always use the interface DSCP and not the incoming packet DSCP.

This example shows how to configure Gigabit Ethernet interface 1/1 with the **trust cos** keywords:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet 1/1
Switch(config-if)# qos trust cos
Switch(config-if)# end
Switch#
```

This example shows how to verify the configuration:

```
Switch# show qos interface gigabitethernet 1/1 | include trust
Trust state: trust COS
Switch#
```

## Configuring the CoS Value for an Interface

QoS assigns the CoS value specified with this command to untagged frames from ingress interfaces configured as trusted and to all frames from ingress interfaces configured as untrusted.

To configure the CoS value for an ingress interface, perform this task:

|        | Command                                                                                                 | Purpose                                                                                                                             |
|--------|---------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch(config)# <b>interface</b> {fastethernet   gigabitethernet} slot/interface   Port-channel number} | Selects the interface to configure.                                                                                                 |
| Step 2 | Switch(config-if)# [no] <b>qos cos</b> default_cos                                                      | Configures the ingress interface CoS value.<br><br>Use the <b>no</b> keyword to clear a configured value and return to the default. |
| Step 3 | Switch(config-if)# <b>end</b>                                                                           | Exits configuration mode.                                                                                                           |
| Step 4 | Switch# <b>show qos interface</b> {fastethernet   gigabitethernet} slot/interface                       | Verifies the configuration.                                                                                                         |

This example shows how to configure the CoS 5 as the default on Fast Ethernet interface 5/24:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 5/24
Switch(config-if)# qos cos 5
Switch(config-if)# end
Switch#
```

This example shows how to verify the configuration:

```
Switch# show qos interface fastethernet 5/24 | include Default COS
Default COS is 5
Switch#
```

## Configuring DSCP Values for an Interface

QoS assigns the DSCP value specified with this command to non IPv4 frames received on interfaces configured to trust DSCP and to all frames received on interfaces configured as untrusted.

To configure the DSCP value for an ingress interface, perform this task:

|        | Command                                                                                                                       | Purpose                                                                                                                          |
|--------|-------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch(config)# <b>interface</b> { <b>fastethernet</b>   <b>gigabitethernet</b> } <i>slot/interface   Port-channel number</i> | Selects the interface to configure.                                                                                              |
| Step 2 | Switch(config-if)# [no] <b>qos dscp</b> <i>default_dscp</i>                                                                   | Configures the ingress interface DSCP value.<br>Use the <b>no</b> keyword to clear a configured value and return to the default. |
| Step 3 | Switch(config-if)# <b>end</b>                                                                                                 | Exits configuration mode.                                                                                                        |
| Step 4 | Switch# <b>show qos interface</b> { <b>fastethernet</b>   <b>gigabitethernet</b> } <i>slot/interface</i>                      | Verifies the configuration.                                                                                                      |

This example shows how to configure the DSCP 5 as the default on Fast Ethernet interface 5/24:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 5/24
Switch(config-if)# qos dscp 5
Switch(config-if)# end
Switch#
```

This example shows how to verify the configuration:

```
Switch# show qos interface fastethernet 6/1
QoS is enabled globally
Port QoS is enabled
 Port Trust State:CoS
 Default DSCP:0 Default CoS:0

 Tx-Queue Bandwidth ShapeRate Priority QueueSize
 (bps) (bps) (bps) (packets)

 1 31250000 disabled N/A 240
 2 31250000 disabled N/A 240
 3 31250000 disabled normal 240
 4 31250000 disabled N/A 240
Switch#
```

## Configuring Transmit Queues

The following sections describes how to configure the transmit queues:

- Mapping DSCP Values to Specific Transmit Queues, page 29-38
- Allocating Bandwidth Among Transmit Queues, page 29-39
- Configuring Traffic Shaping of Transmit Queues, page 29-39
- Configuring a High Priority Transmit Queue, page 29-40

Depending on the complexity of your network and your QoS solution, you might need to perform all of the procedures in the next sections. Before You will need to make decisions about these characteristics:

- Which packets are assigned (by DSCP value) to each queue?
- What is the size of a transmit queue relative to other queues for a given port?
- How much of the available bandwidth is allotted to each queue?
- What is the maximum rate and burst of traffic that can be transmitted out of each transmit queue?

## Mapping DSCP Values to Specific Transmit Queues

To map the DSCP values to a transmit queue, perform this task:

|        | Command                                                                   | Purpose                                                                                                                                                                                                                                            |
|--------|---------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch(config)# <b>[no] qos map dscp dscp-values to tx-queue queue-id</b> | Maps the DSCP values to the transit queue. <i>dscp-list</i> can contain up to 8 DSCP values. The <i>queue-id</i> can range from 1 to 4.<br><br>Use the <b>no qos map dscp to tx-queue</b> command to clear the DSCP values from the transit queue. |
| Step 2 | Switch(config)# <b>end</b>                                                | Exits configuration mode.                                                                                                                                                                                                                          |
| Step 3 | Switch# <b>show qos maps dscp tx-queues</b>                               | Verifies the configuration.                                                                                                                                                                                                                        |

This example shows how to map DSCP values to transit queue 2.

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# qos map dscp 50 to tx-queue 2
Switch(config)# end
Switch#
```

This example shows how to verify the configuration.

```
Switch# show qos maps dscp tx-queue
DSCP-TxQueue Mapping Table (dscp = d1d2)
d1 :d2 0 1 2 3 4 5 6 7 8 9

0 : 02 02 02 01 01 01 01 01 01 01
1 : 01 01 01 01 01 01 01 02 02 02
2 : 02 02 02 02 02 02 02 02 02 02
3 : 02 02 03 03 03 03 03 03 03 03
4 : 03 03 03 03 03 03 03 03 04 04
5 : 04 04 04 04 04 04 04 04 04 04
6 : 04 04 04 04
Switch#
```



## Allocating Bandwidth Among Transmit Queues

To configure the transmit queue bandwidth, perform this task:

|        | Command                                                                                      | Purpose                                                                                                                                          |
|--------|----------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch(config)# <b>interface</b> <i>gigabitethernet slot/interface</i>                       | Selects the interface to configure.                                                                                                              |
| Step 2 | Switch(config-if)# <b>tx-queue</b> <i>queue_id</i>                                           | Selects the transmit queue to configure.                                                                                                         |
| Step 3 | Switch(config-if-tx-queue)# [ <b>no</b> ] [ <b>bandwidth rate</b>   <b>percent percent</b> ] | Sets the bandwidth rate for the transmit queue.<br>Use the <b>no</b> keyword to reset the transmit queue bandwidth ratios to the default values. |
| Step 4 | Switch(config-if-tx-queue)# <b>end</b>                                                       | Exits configuration mode.                                                                                                                        |
| Step 5 | Switch# <b>show qos interface</b>                                                            | Verifies the configuration.                                                                                                                      |

The bandwidth rate varies with the interface.

Bandwidth can only be configured on:

- Uplink ports on Supervisor Engine III (WS-X4014)
- Ports on the WS-X4306-GB linecard.
- The 2 1000BASE-X ports on the WS-X4232-GB-RJ linecard
- The first 2 ports on the WS-X4418-GB linecard
- The two 1000BASE-X ports on the WS-X4412-2GB-TX linecard

This example shows how to configure the bandwidth of 1 Mbps on transmit queue 2.

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet 1/1
Switch(config-if)# tx-queue 2
Switch(config-if-tx-queue)# bandwidth 1000000
Switch(config-if-tx-queue)# end
Switch#
```

## Configuring Traffic Shaping of Transmit Queues

To guarantee that packets transmitted from a transmit queue do not exceed a specified maximum rate, perform this task:

|        | Command                                                                                                 | Purpose                                                                                                               |
|--------|---------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch(config)# <b>interface</b> { <i>fastethernet</i>   <i>gigabitethernet</i> } <i>slot/interface</i> | Selects the interface to configure.                                                                                   |
| Step 2 | Switch(config-if)# <b>tx-queue</b> <i>queue_id</i>                                                      | Selects the transmit queue to configure.                                                                              |
| Step 3 | Switch(config-if-tx-queue)# [ <b>no</b> ] [ <b>shape rate</b>   <b>percent percent</b> ]                | Sets the transmit rate for the transmit queue.<br>Use the <b>no</b> keyword to clear the transmit queue maximum rate. |
| Step 4 | Switch(config-if-tx-queue)# <b>end</b>                                                                  | Exits configuration mode.                                                                                             |
| Step 5 | Switch# <b>show qos interface</b>                                                                       | Verifies the configuration.                                                                                           |

This example shows how to configure the shape rate to 1 Mbps on transmit queue 2.

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet 1/1
Switch(config-if-tx-queue)# tx-queue 2
Switch(config-if-tx-queue)# shape 1000000
Switch(config-if-tx-queue)# end
Switch#
```

## Configuring a High Priority Transmit Queue

To configure transmit queue 3 at a higher priority, perform this task:

|        | Command                                                                                                 | Purpose                                                                                                      |
|--------|---------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch(config)# <b>interface</b> { <b>fastethernet</b>   <b>gigabitethernet</b> } <i>slot/interface</i> | Selects the interface to configure.                                                                          |
| Step 2 | Switch(config-if)# <b>tx-queue</b> 3                                                                    | Selects transmit queue 3 to configure.                                                                       |
| Step 3 | Switch(config-if)# [ <b>no</b> ] <b>priority high</b>                                                   | Sets the transmit queue to high priority.<br>Use the <b>no</b> keyword to clear the transmit queue priority. |
| Step 4 | Switch(config-if)# <b>end</b>                                                                           | Exits configuration mode.                                                                                    |
| Step 5 | Switch# <b>show qos interface</b>                                                                       | Verifies the configuration.                                                                                  |

This example shows how to configure transmit queue 3 to high priority.

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet 1/1
Switch(config-if-tx-queue)# tx-queue 3
Switch(config-if-tx-queue)# priority high
Switch(config-if)# end
Switch#
```

## Configuring DSCP Maps

The following sections describes how to configure the DSCP maps. It contains this configuration information:

- Configuring the CoS-to-DSCP Map, page 29-40
- Configuring the Policed-DSCP Map, page 29-41
- Configuring the DSCP-to-CoS Map, page 29-42

All the maps are globally defined and are applied to all ports.

### Configuring the CoS-to-DSCP Map

You use the CoS-to-DSCP map to map CoS values in incoming packets to a DSCP value that QoS uses internally to represent the priority of the traffic.

Table 29-4 shows the default CoS-to-DSCP map.

**Table 29-4 Default CoS-to-DSCP Map**

|                   |   |   |    |    |    |    |    |    |
|-------------------|---|---|----|----|----|----|----|----|
| <b>CoS value</b>  | 0 | 1 | 2  | 3  | 4  | 5  | 6  | 7  |
| <b>DSCP value</b> | 0 | 8 | 16 | 24 | 32 | 40 | 48 | 56 |

If these values are not appropriate for your network, you need to modify them.

To modify the CoS-to-DSCP map, perform this task:

|               | <b>Command</b>                                                | <b>Purpose</b>                                                                                                                                                                                          |
|---------------|---------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Switch# <b>configure terminal</b>                             | Enters global configuration mode.                                                                                                                                                                       |
| <b>Step 2</b> | Switch(config)# <b>qos map cos cos1 ... cos8 to dscp dscp</b> | Modifies the CoS-to-DSCP map.<br><br>For <i>cos1...cos8</i> , you can enter up to 8 CoS; valid values range from 0 to 7. Separate each CoS value with a space.<br><br>The <i>dscp</i> range is 0 to 63. |
| <b>Step 3</b> | Switch(config)# <b>end</b>                                    | Returns to privileged EXEC mode.                                                                                                                                                                        |
| <b>Step 4</b> | Switch# <b>show qos maps cos-dscp</b>                         | Verifies your entries.                                                                                                                                                                                  |
| <b>Step 5</b> | Switch# <b>copy running-config startup-config</b>             | (Optional) Saves your entries in the configuration file.                                                                                                                                                |

To return to the default map, use the **no qos cos to dscp** global configuration command.

This example shows how to modify and display the CoS-to-DSCP map:

```
Switch# configure terminal
Switch(config)# qos map cos 0 to dscp 20
Switch(config)# end
Switch# show qos maps cos dscp
```

```
CoS-DSCP Mapping Table:
CoS: 0 1 2 3 4 5 6 7

DSCP: 20 8 16 24 32 40 48 56
Switch(config)#
```

## Configuring the Policed-DSCP Map

You use the policed-DSCP map to mark down a DSCP value to a new value as the result of a policing and marking action.

The default policed-DSCP map is a null map, which maps an incoming DSCP value to the same DSCP value.

To modify the CoS-to-DSCP map, perform this task:

|        | Command                                                                                | Purpose                                                                                                                                                                                                                                                                               |
|--------|----------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch# <b>configure terminal</b>                                                      | Enters global configuration mode.                                                                                                                                                                                                                                                     |
| Step 2 | Switch(config)# <b>qos map dscp policed</b><br><i>dscp-list to dscp mark-down-dscp</i> | Modifies the policed-DSCP map. <ul style="list-style-type: none"> <li>For <i>dscp-list</i>, enter up to 8 DSCP values separated by spaces. Then enter the <b>to</b> keyword.</li> <li>For <i>mark-down-dscp</i>, enter the corresponding policed (marked down) DSCP value.</li> </ul> |
| Step 3 | Switch(config)# <b>end</b>                                                             | Returns to privileged EXEC mode.                                                                                                                                                                                                                                                      |
| Step 4 | Switch# <b>show qos maps dscp policed</b>                                              | Verifies your entries.                                                                                                                                                                                                                                                                |
| Step 5 | Switch# <b>copy running-config startup-config</b>                                      | (Optional) Saves your entries in the configuration file.                                                                                                                                                                                                                              |

To return to the default map, use the **no qos dscp policed** global configuration command.

This example shows how to map DSCP 50 to 57 to a marked-down DSCP value of 0:

```
Switch# configure terminal
Switch(config)# qos map dscp policed 50 51 52 53 54 55 56 57 to dscp 0
Switch(config)# end
Switch# show qos maps dscp policed
Policed-dscp map:
 d1 : d2 0 1 2 3 4 5 6 7 8 9

 0 : 00 01 02 03 04 05 06 07 08 09
 1 : 10 11 12 13 14 15 16 17 18 19
 2 : 20 21 22 23 24 25 26 27 28 29
 3 : 30 31 32 33 34 35 36 37 38 39
 4 : 40 41 42 43 44 45 46 47 48 49
 5 : 00 00 00 00 00 00 00 00 58 59
 6 : 60 61 62 63
```



#### Note

In the above policed-DSCP map, the marked-down DSCP values are shown in the body of the matrix. The d1 column specifies the most-significant digit of the original DSCP; the d2 row specifies the least-significant digit of the original DSCP. The intersection of the d1 and d2 values provides the marked-down value. For example, an original DSCP value of 53 corresponds to a marked-down DSCP value of 0.

## Configuring the DSCP-to-CoS Map

You use the DSCP-to-CoS map to generate a CoS value.

Table 29-5 shows the default DSCP-to-CoS map.

**Table 29-5 Default DSCP-to-CoS Map**

| DSCP value | 0–7 | 8–15 | 16–23 | 24–31 | 32–39 | 40–47 | 48–55 | 56–63 |
|------------|-----|------|-------|-------|-------|-------|-------|-------|
| CoS value  | 0   | 1    | 2     | 3     | 4     | 5     | 6     | 7     |

If these values are not appropriate for your network, you need to modify them.

To modify the DSCP-to-CoS map, perform this task:

|        | Command                                                  | Purpose                                                                                                                                                                                                                                                                                                                           |
|--------|----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch# <b>configure terminal</b>                        | Enters global configuration mode.                                                                                                                                                                                                                                                                                                 |
| Step 2 | Switch(config)# <b>qos map dscp dscp-list to cos cos</b> | Modifies the DSCP-to-CoS map. <ul style="list-style-type: none"> <li>For <i>dscp-list</i>, enter up to 8 DSCP values separated by spaces. Then enter the <b>to</b> keyword.</li> <li>For <i>cos</i>, enter only one CoS value to which the DSCP values correspond.</li> </ul> The DSCP range is 0 to 63; the CoS range is 0 to 7. |
| Step 3 | Switch(config)# <b>end</b>                               | Returns to privileged EXEC mode.                                                                                                                                                                                                                                                                                                  |
| Step 4 | Switch# <b>show qos maps dscp to cos</b>                 | Verifies your entries.                                                                                                                                                                                                                                                                                                            |
| Step 5 | Switch# <b>copy running-config startup-config</b>        | (Optional) Saves your entries in the configuration file.                                                                                                                                                                                                                                                                          |

To return to the default map, use the **no qos dscp to cos** global configuration command.

This example shows how to map DSCP values 0, 8, 16, 24, 32, 40, 48, and 50 to CoS value 0 and to display the map:

```
Switch# configure terminal
Switch(config)# qos map dscp 0 8 16 24 32 40 48 50 to cos 0
Switch(config)# end
Switch# show qos maps dscp cos
Dscp-cos map:
d1 : d2 0 1 2 3 4 5 6 7 8 9

0 : 00 00 00 00 00 00 00 00 00 01
1 : 01 01 01 01 01 01 00 02 02 02
2 : 02 02 02 02 00 03 03 03 03 03
3 : 03 03 00 04 04 04 04 04 04 04
4 : 00 05 05 05 05 05 05 05 05 06
5 : 00 06 06 06 06 06 06 07 07 07
6 : 07 07 07 07
```



#### Note

In the above DSCP-to-CoS map, the CoS values are shown in the body of the matrix. The d1 column specifies the most-significant digit of the DSCP; the d2 row specifies the least-significant digit of the DSCP. The intersection of the d1 and d2 values provides the CoS value. For example, in the DSCP-to-CoS map, a DSCP value of 08 corresponds to a CoS value of 0.





## Configuring NetFlow Statistics Collection

This chapter describes how to configure NetFlow statistics on the Catalyst 4500 series switches. It also provides guidelines, procedures, and configuration examples.



**Note**

This feature is only available if the NetFlow Services Card (WS-F4531) is present.



**Note**

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference* and related publications at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/index.htm>. Refer to the “NetFlow Solutions Guide” for more detailed information on NetFlow usage and management.

The following topics are included:

- Overview of NetFlow Statistics Collection, page 30-1
- Checking for Required Hardware, page 30-4
- Caveat for the NetFlow Feature, page 30-3
- Configuring NetFlow Statistics Collection, page 30-4
- Configuring Netflow Aging Parameters, page 30-9
- NetFlow Statistics Collection Configuration Example, page 30-9
- NetFlow Configuration Examples, page 30-10

## Overview of NetFlow Statistics Collection

A network flow is defined as a unidirectional sequence of packets between a given source and destination endpoints. Network flows are highly granular; flow endpoints are identified both by an IP address and transport layer application port numbers. NetFlow also utilizes the IP type and the input interface identifier to uniquely identify flows.

NetFlow statistics is a global traffic monitoring feature that allows flow-level monitoring of all IPv4-routed traffic through the switch. Collected statistics can be exported to an external device (NetFlow Collector/Analyzer) through the NetFlow Data Export (NDE). Network planners can selectively enable NetFlow statistics (and NDE) on a per-device basis to gain traffic performance, control, or accounting benefits in specific network locations. Traffic monitoring does not need to be operating on each device in the network.

## Information Derived from Hardware

Information available in a typical NetFlow record from hardware includes the following:

- the packet and byte counts
- start and end timestamps
- source and destination IP addresses
- IP protocol
- source and destination port numbers.

## Information Derived from Software

The software infers the following fields:

- Input identifier
- Output identifier
- Routing information, including next-hop address, origin and peer AS, source and destination prefix mask

## Determining the Input and Output interface and AS Numbers

The input and output interface values are correct when Policy Based Routing (PBR) is not used. There are simple symmetric routing scenarios, and no load balancing schemes are applied by an adjacent upstream router. The input and output interface values determined by the software, however, are not guaranteed to be accurate in the specific situations explained below.

Software determines the output interface information by looking up the FIB (Forwarding Information Base) entry in the default FIB table (based on the destination IP address). From this FIB entry, the software gains access to the destination AS number for this destination IP address, as well as the appropriate adjacency that stores the interface information. Therefore, the output interface is based solely on the destination IP address. If load balancing is enabled on the switch, instead of looking at the adjacency in the FIB entry, the load balancing hash will be applied to access the appropriate FIB path and access the appropriate adjacency. Although this process will typically yield correct results, a potential inaccuracy can occur when using a PBR that shares IP addresses with the default FIB table. Under these circumstances, there would then be multiple FIB table entries and associated adjacencies for the same destination IP address.

Similarly, the input interface and the source AS number for the source IP address are determined by looking up the FIB entry in the default FIB table based on the source IP address. Therefore, the input interface is based solely on the source IP address and a reverse lookup is done to determine to which interface a packet with this IP destination address needs to be routed. This process assumes that the forwarding paths are symmetrical. However, if this process yields multiple input interfaces, a deterministic algorithm will be applied to pick one of them—the one with the lowest IP address. Although this process typically yields correct values, there are scenarios where the values are inaccurate:

- If load balancing is being applied by an upstream adjacent router, one input interface must be chosen arbitrarily out of the multiple input interfaces available. This action is necessary because the input interface that would be used depends on the type of load balancing algorithm being deployed by the



adjacent upstream router. It is not always feasible to know the algorithm. Therefore, all flow statistics will be attributed to one input interface. Software selects the interface with the lowest IP subnet number.

- In an asymmetric routing scheme, where the traffic for an IP subnet might be received on an interface that is different from the interface where packets are sent to this IP subnet, the inferences noted previously for selecting an input interface, based on a reverse lookup, would be incorrect and cannot be verified. The reason is that RPF-based forwarding is not supported in the Catalyst 4500 series switch Cisco IOS-based supervisor engines.
- If PBR (Policy Based Routing) is enabled on the switch and the flow is destined to an address that resides in the PBR range or is sourced from an address that resides in the PBR range, the information will be incorrect. In this case, the input and output interface will most likely point to the default route (if configured) or will have no value at all (NULL).
- In the case of detecting DOS attacks, even if the route is symmetrical, it might not yield the correct results because there may be multiple paths to the destination, which is the source of the attacks.



#### Note

NetFlow consumes additional memory and CPU resources; therefore, it is important that you understand the resources required on your switch before enabling NetFlow.

## VLAN Statistics

The NetFlow Services module, in combination with the Catalyst 4500 series switch Supervisor Engine IV, provides the capability of reporting VLAN statistics for routed traffic in and out of a VLAN, as well as Layer 2 output VLAN statistics. The CLI output for a specific VLAN is shown below:

```
cat4k-sup4-2# sh vlan counters or show vlan id 22 count
* Multicast counters include broadcast packets
Vlan Id :22
L2 Unicast Packets :38
L2 Unicast Octets :2432
L3 Input Unicast Packets :14344621
L3 Input Unicast Octets :659852566
L3 Output Unicast Packets :8983050
L3 Output Unicast Octets :413220300
L3 Output Multicast Packets :0
L3 Output Multicast Octets :0
L3 Input Multicast Packets :0
L3 Input Multicast Octets :0
L2 Multicast Packets :340
L2 Multicast Octets :21760
```

## Caveat for the NetFlow Feature

The NetFlow Services module has hardware limitations that restrict the platform support to a subset of all NetFlow fields. Specifically, the following fields will not be supported:

- TCP Flags
- ToS

# Configuring NetFlow Statistics Collection

To configure NetFlow Switching, complete the tasks in these sections:

- Checking for Required Hardware, page 30-4
- Enabling NetFlow Statistics Collection, page 30-5
- Exporting NetFlow Statistics, page 30-5
- Managing NetFlow Statistics Collection, page 30-6
- Configuring an Aggregation Cache, page 30-6
- Configuring a NetFlow Minimum Prefix Mask for Router-Based Aggregation, page 30-7

## Checking for Required Hardware



### Note

The Catalyst 4500 series switches require WS-F4531 daughter cards and the Catalyst 4500 series switch Supervisor Engine IV to support the NetFlow statistics collection.

To ensure that the necessary hardware is enabled, issue the **show module** command, as follows:

```
Switch# show module all
Chassis Type : WS-C4507R

Power consumed by backplane : 40 Watts

Mod Ports Card Type Model
Serial No.
-----+-----+-----+-----+-----+-----+-----+-----+-----+
1 2 1000BaseX (GBIC) Supervisor(active) WS-X4515
JAB062604KB
2 2 1000BaseX (GBIC) Supervisor(standby) WS-X4515
JAB062408CB
6 48 10/100BaseTX (RJ45) WS-X4148
JAB032305UH

M MAC addresses Hw Fw Sw Status
-----+-----+-----+-----+-----+-----+-----+-----+
1 0001.6442.2c00 to 0001.6442.2c01 0.4 12.1(14r)EW(12.1(20030513:00 Ok
2 0001.6442.2c02 to 0001.6442.2c03 0.4 12.1(14r)EW(12.1(20030513:00 Ok
6 0050.3ed8.6780 to 0050.3ed8.67af 1.6 12.1(14r)EW(12.1(20030513:00 Ok

Mod Submodule Model Serial No. Hw Status
-----+-----+-----+-----+-----+-----+-----+
1 Netflow Services Card WS-F4531 JAB062209CG 0.2 Ok
2 Netflow Services Card WS-F4531 JAB062209AG 0.2 Ok
```



### Note

Enabling this feature does not impact the hardware-forwarding performance of the switch.

The effective size of the hardware flow “cache” table is 64 kilobytes. If more than 64 kilobytes flows are active simultaneously, statistics may be lost for some of the flows.

The effective size of the software flow table is 256 kilobytes. The NetFlow software manages the consistency between the hardware and software tables, keeping the hardware table open by purging inactive hardware flows to the software table.

User-configured timeout settings dictate when the flows are purged and exported through NDE from the software cache. Hardware flow management ensures consistency between hardware flow purging and the user-configured timeout settings.

Software-forwarded flows are also monitored. Moreover, statistics will overflow if any flow receives traffic at a sustained rate exceeding 2 gigabits per second. Generally, this situation should not occur because a port cannot transmit at a rate higher than 1 gigabit per second.

**Note**

By design, even if the timeout settings are high, flows will automatically “age out” as they approach their statistics limit.

## Enabling NetFlow Statistics Collection

To enable NetFlow switching, first configure the switch for IP routing as described in the IP configuration chapters in the *Cisco IOS IP and IP Routing Configuration Guide*. After you configure IP routing, perform one of these tasks:

| Command                                                 | Purpose                                                                                                                                                                                        |
|---------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Switch(config)# <b>ip route-cache flow</b>              | Enables Netflow switching for IP routing.                                                                                                                                                      |
| Switch(config)# <b>ip route-cache flow infer-fields</b> | Enables Netflow with inferred input/output interfaces and source/destination BGP as information.<br><br>The <b>inter-fields</b> option must be configured for AS information to be determined. |

## Exporting NetFlow Statistics

To configure the switch to export NetFlow statistics to a workstation when a flow expires, perform one of these tasks:

| Command                                                                                   | Purpose                                                                                                                  |
|-------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| Switch(config)# <b>ip flow-export destination</b> {hostname   ip-address} <b>udp-port</b> | (Required) Configures the router to export NetFlow cache entries to a specific destination (for example, a workstation). |

| Command                                                                          | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Switch(config)# <b>ip flow-export version</b><br>{1   {5 [origin-as   peer-as]}} | (Optional) Configures the router to export NetFlow cache entries to a workstation if you are using receiving software that requires version 1 or 5. Version 1 is the default.<br><br><b>origin-as</b> causes NetFlow to determine the origin Border Gateway Protocol (BGP) autonomous system of both the source and the destination hosts of the flow.<br><br><b>peer-as</b> causes NetFlow to determine the peer BGP autonomous system of both the input and output interfaces of the flow. |
| Switch(config)# <b>ip flow-export source</b> <interface>                         | (Optional) Specifies an interface whose IP address will be used as the source IP address in the IP header of the NetFlow Data Export (NDE) packet. Default is the NDE output interface.                                                                                                                                                                                                                                                                                                      |

## Managing NetFlow Statistics Collection

You can display and clear NetFlow statistics, including IP flow switching cache information and flow information, such as the protocol, total flow, flows per second, and so forth. You can also use the resulting information to obtain information about your switch traffic.

To manage NetFlow switching statistics, perform one or both of following tasks:

| Command                            | Purpose                                    |
|------------------------------------|--------------------------------------------|
| Switch# <b>show ip cache flow</b>  | Displays the NetFlow switching statistics. |
| Switch# <b>clear ip flow stats</b> | Clears the NetFlow switching statistics.   |

## Configuring an Aggregation Cache

Aggregation of NetFlow statistics is typically performed by NetFlow collection tools on management workstations. By extending this support to the Catalyst 4500 series switch, you are now able to do the following:

- Reduce the required bandwidth between the router and workstations, as fewer NDE packets are exported.
- Reduce the number of collection workstations required.
- Provide visibility to aggregated flow statistics at the CLI.

To configure an aggregation cache, you must enter the aggregation cache configuration mode, and you must decide which type of aggregation scheme you would like to configure: autonomous system, destination prefix, protocol prefix, or source prefix aggregation cache. Once you define the aggregation scheme, define the operational parameters for that scheme. More than one aggregation cache can be configured concurrently.

To configure an aggregation cache, perform this task:

|        | Command                                                                 | Purpose                                                                                                                                                               |
|--------|-------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Router(config)# <b>ip flow-aggregation cache as</b>                     | Enters aggregation cache configuration mode and enables an aggregation cache scheme (autonomous system, destination-prefix, prefix, protocol-port, or source-prefix). |
| Step 2 | Router(config-flow-cache)#<br><b>cache timeout inactive 199</b>         | Specifies the number of seconds (in this example, 199) in which an inactive entry is allowed to remain in the aggregation cache before it is deleted.                 |
| Step 3 | Router(config-flow-cache)#<br><b>cache timeout active 45</b>            | Specifies the number of minutes (in this example, 45) in which an active entry is active.                                                                             |
| Step 4 | Router(config-flow-cache)#<br><b>export destination 10.42.41.1 9991</b> | Enables the data export.                                                                                                                                              |
| Step 5 | Router(config-flow-cache)# <b>enabled</b>                               | Enables aggregation cache creation.                                                                                                                                   |

## Verifying Aggregation Cache Configuration and Data Export

To verify the aggregation cache information, perform this task:

| Command                                                          | Purpose                                               |
|------------------------------------------------------------------|-------------------------------------------------------|
| Router# <b>show ip cache flow aggregation destination-prefix</b> | Displays the specified aggregation cache information. |

To confirm data export, perform the following task:

| Command                            | Purpose                                                                                            |
|------------------------------------|----------------------------------------------------------------------------------------------------|
| Router# <b>show ip flow export</b> | Displays the statistics for the data export including the main cache and all other enabled caches. |

## Configuring a NetFlow Minimum Prefix Mask for Router-Based Aggregation

The minimum prefix mask specifies the shortest subnet mask that will be used for aggregating flows within one of the IP-address based aggregation caches (e.g. source-prefix, destination-prefix, prefix). In these caches, flows are aggregated based upon the IP address (source, destination, or both, respectively) and masked by the longer of the Minimum Prefix mask and the subnet mask of the route to the source/destination host of the flow (as found in the switch routing table).



### Note

The default value of the minimum mask is zero. The configurable range for the minimum mask is from 1 to 32. You should choose an appropriate value depending on the traffic. A higher value for the minimum mask will provide more detailed network addresses, but it may also result in increased number of flows in the aggregation cache.

To configure a minimum prefix mask for the Router-Based Aggregation feature, perform the tasks described in the following sections. Each task is optional.

- Configuring the Minimum Mask of a Prefix Aggregation Scheme
- Configuring the Minimum Mask of a Destination-Prefix Aggregation Scheme
- Configuring the Minimum Mask of a Source-Prefix Aggregation Scheme
- Monitoring and Maintaining Minimum Masks for Aggregation Schemes

## Configuring the Minimum Mask of a Prefix Aggregation Scheme

To configure the minimum mask of a prefix aggregation scheme, perform this task:

|        | Command                                                          | Purpose                                           |
|--------|------------------------------------------------------------------|---------------------------------------------------|
| Step 1 | Router(config)# <b>ip flow-aggregation cache prefix</b>          | Configures the prefix aggregation cache.          |
| Step 2 | Router(config-flow-cache)# <b>mask source minimum value</b>      | Specifies the minimum value for the source mask.  |
| Step 3 | Router(config-flow-cache)# <b>mask destination minimum value</b> | Specifies minimum value for the destination mask. |

## Configuring the Minimum Mask of a Destination-Prefix Aggregation Scheme

To configure the minimum mask of a destination-prefix aggregation scheme, perform this task:

|        | Command                                                             | Purpose                                               |
|--------|---------------------------------------------------------------------|-------------------------------------------------------|
| Step 1 | Router(config)# <b>ip flow-aggregation cache destination-prefix</b> | Configures the destination aggregation cache.         |
| Step 2 | Router(config-flow-cache)# <b>mask destination minimum value</b>    | Specifies the minimum value for the destination mask. |

## Configuring the Minimum Mask of a Source-Prefix Aggregation Scheme

To configure the minimum mask of a source-prefix aggregation scheme, perform this task:

|        | Command                                                        | Purpose                                          |
|--------|----------------------------------------------------------------|--------------------------------------------------|
| Step 1 | Router(config)# <b>ip flow-aggregation cache source-prefix</b> | Configures the source-prefix aggregation cache.  |
| Step 2 | Router(config-flow-cache)# <b>mask source minimum value</b>    | Specifies the minimum value for the source mask. |

## Monitoring and Maintaining Minimum Masks for Aggregation Schemes

To view the configured value of the minimum mask, use the following commands for each aggregation scheme, as needed:

| Command                                                          | Purpose                                                                                         |
|------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
| Router# <b>show ip cache flow aggregation prefix</b>             | Displays the configured value of the minimum mask in the prefix aggregation scheme.             |
| Router# <b>show ip cache flow aggregation destination-prefix</b> | Displays the configured value of the minimum mask in the destination-prefix aggregation scheme. |
| Router# <b>show ip cache flow aggregation source-prefix</b>      | Displays the configured value of the minimum mask in the source-prefix aggregation scheme.      |

## Configuring Netflow Aging Parameters

You can control when flows are purged from the software flow cache (and, if configured, reported through NDE) with the configuration aging parameters, **Active** and **Inactive**, of the **ip flow-cache timeout** command.

Active Aging specifies the period of time in which a flow should be removed from the software flow cache after the flow is created. Generally, this parameter is used to periodically notify external collection devices about active flows. This parameter operates independently of existing traffic on the flow. Active timeout settings tend to be on the order of minutes (default is 30min).

Inactive Aging specifies how long after the last packet is seen a flow is removed. The Inactive parameter clears the flow cache of “stale” flows thereby preventing new flows from starving (due to lack of resources). Inactive timeout settings tend to be on the order of seconds (default is 15sec).

## NetFlow Statistics Collection Configuration Example

The following example shows how to modify the configuration to enable NetFlow switching. It also shows how to export the flow statistics for further processing to UDP port 9991 on a workstation with the IP address of 40.0.0.2. In this example, existing NetFlow statistics are cleared, thereby ensuring that the **show ip cache flow** command displays an accurate summary of the NetFlow switching statistics:

```
Switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip route-cache flow
Switch(config)# ip flow-export destination 40.0.0.2 9991
Switch(config)# ip flow-export version 5
Switch(config)# end
Switch# show ip flow export
Flow export is enabled
 Exporting flows to 40.0.0.2 (9991)
 Exporting using source IP address 40.0.0.1
 Version 5 flow records
 2 flows exported in 1 udp datagrams
 0 flows failed due to lack of export packet
 0 export packets were sent up to process level
```

```

0 export packets were dropped due to no fib
0 export packets were dropped due to adjacency issues
0 export packets were dropped due to fragmentation failures
0 export packets were dropped due to encapsulation fixup failures
Switch#
Switch# show ip cache flow

IP Flow Switching Cache, 17826816 bytes
0 active, 262144 inactive, 4 added
14 age polls, 0 flow alloc failures
Active flows timeout in 1 minutes
Inactive flows timeout in 10 seconds
last clearing of statistics 15:48:37

```

| Protocol  | Total<br>Flows | Flows<br>/Sec | Packets<br>/Flow | Bytes<br>/Pkt | Packets<br>/Sec | Active(Sec)<br>/Flow | Idle(Sec)<br>/Flow |
|-----------|----------------|---------------|------------------|---------------|-----------------|----------------------|--------------------|
| UDP-other | 1              | 0.0           | 3                | 46            | 0.0             | 0.0                  | 10.3               |
| IP-other  | 1              | 0.0           | 100              | 38            | 0.0             | 0.0                  | 10.2               |
| Total:    | 2              | 0.0           | 51               | 38            | 0.0             | 0.0                  | 10.2               |

```

SrcIf SrcIPaddress DstIf DstIPaddress Pr SrcP DstP Pkts
Switch#

```

## NetFlow Configuration Examples

This section provides the following basic configuration examples:

- Sample Netflow Enabling Schemes, page 30-10
- Sample NetFlow Aggregation Configurations, page 30-10
- Sample NetFlow Minimum Prefix Mask Router-Based Aggregation Schemes, page 30-12

## Sample Netflow Enabling Schemes



### Note

Enabling Netflow on a per interface basis is not supported on a Catalyst 4500 Switch.

This example shows how to enable Netflow globally:

```

Switch# configure terminal
Switch(config)# ip route-cache flow

```

This example shows how to enable Netflow with support for inferred fields:

```

Switch# configure terminal
Switch(config)# ip route-cache flow infer-fields

```

## Sample NetFlow Aggregation Configurations

This section provides the following aggregation cache configuration examples:

- Autonomous System Configuration, page 30-11
- Destination Prefix Configuration, page 30-11
- Prefix Configuration, page 30-11
- Protocol Port Configuration, page 30-11



- Source Prefix Configuration, page 30-12

## Autonomous System Configuration

This example shows how to configure an autonomous system aggregation cache with an inactive timeout of 200 seconds, a cache active timeout of 45 minutes, an export destination IP address of 10.42.42.1, and a destination port of 9992:

```
Switch(config)# ip flow-aggregation cache as
Switch(config-flow-cache)# cache timeout inactive 200
Switch(config-flow-cache)# cache timeout active 45
Switch(config-flow-cache)# export destination 10.42.42.1 9992
Switch(config-flow-cache)# enabled
```

## Destination Prefix Configuration

This example shows how to configure a destination prefix aggregation cache with an inactive timeout of 200 seconds, a cache active timeout of 45 minutes, an export destination IP address of 10.42.42.1, and a destination port of 9992:

```
Switch(config)# ip flow-aggregation cache destination-prefix
Switch(config-flow-cache)# cache timeout inactive 200
Switch(config-flow-cache)# cache timeout active 45
Switch(config-flow-cache)# export destination 10.42.42.1 9992
Switch(config-flow-cache)# enabled
```

## Prefix Configuration

This example shows how to configure a prefix aggregation cache with an inactive timeout of 200 seconds, a cache active timeout of 45 minutes, an export destination IP address of 10.42.42.1, and a destination port of 9992:

```
Switch(config)# ip flow-aggregation cache prefix
Switch(config-flow-cache)# cache timeout inactive 200
Switch(config-flow-cache)# cache timeout active 45
Switch(config-flow-cache)# export destination 10.42.42.1 9992
Switch(config-flow-cache)# enabled
```

## Protocol Port Configuration

This example shows how to configure a protocol port aggregation cache with an inactive timeout of 200 seconds, a cache active timeout of 45 minutes, an export destination IP address of 10.42.42.1, and a destination port of 9992:

```
Switch(config)# ip flow-aggregation cache protocol-port
Switch(config-flow-cache)# cache timeout inactive 200
Switch(config-flow-cache)# cache timeout active 45
Switch(config-flow-cache)# export destination 10.42.42.1 9992
Switch(config-flow-cache)# enabled
```

## Source Prefix Configuration

This example shows how to configure a source prefix aggregation cache with an inactive timeout of 200 seconds, a cache active timeout of 45 minutes, an export destination IP address of 10.42.42.1, and a destination port of 9992:

```
Switch(config)# ip flow-aggregation cache source-prefix
Switch(config-flow-cache)# cache timeout inactive 200
Switch(config-flow-cache)# cache timeout active 45
Switch(config-flow-cache)# export destination 10.42.42.1 9992
Switch(config-flow-cache)# enabled
```

## Sample NetFlow Minimum Prefix Mask Router-Based Aggregation Schemes

This section provides examples for the NetFlow minimum prefix mask aggregation cache configuration:

- Prefix Aggregation Scheme
- Destination-Prefix Aggregation Scheme
- Source-Prefix Aggregation Scheme

### Prefix Aggregation Scheme

This is an example of a prefix aggregation cache configuration:

```
!
ip flow-aggregation cache prefix
mask source minimum 24
mask destination minimum 28
```

In this example, assume the following configuration:

```
ip route 118.42.20.160 255.255.255.224 110.42.13.2
ip route 122.16.93.160 255.255.255.224 111.22.21.2
```

Both routes have a 27-bit subnet mask in the routing table on the switch.

Flows travelling from the 118.42.20.160 subnet to the 122.16.93.160 subnet whose source IP addresses match with a mask of 27 bits and whose destination IP addresses match with a mask of 28 bits are aggregated together in the cache statistics.

### Destination-Prefix Aggregation Scheme

This is an example of a destination-prefix aggregation cache configuration:

```
!
ip flow-aggregation cache destination-prefix
mask destination minimum 32
!
```

### Source-Prefix Aggregation Scheme

This is an example of a source-prefix aggregation cache configuration:

```
ip flow-aggregation cache source-prefix
mask source minimum 30
!
```



# Understanding and Configuring Dynamic ARP Inspection

This chapter describes how to configure Dynamic ARP Inspection (DAI) on the Catalyst 4500 series switch.

This chapter includes the following major sections:

- Overview of Dynamic ARP Inspection, page 31-1
- Configuring Dynamic ARP Inspection, page 31-5



## Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference* and the publications at this URL: <http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/index.htm>

## Overview of Dynamic ARP Inspection

Dynamic ARP Inspection (DAI) is a security feature that validates Address Resolution Protocol (ARP) packets in a network. DAI allows a network administrator to intercept, log, and discard ARP packets with invalid MAC address to IP address bindings. This capability protects the network from certain “man-in-the-middle” attacks.

This section contains the following subsections:

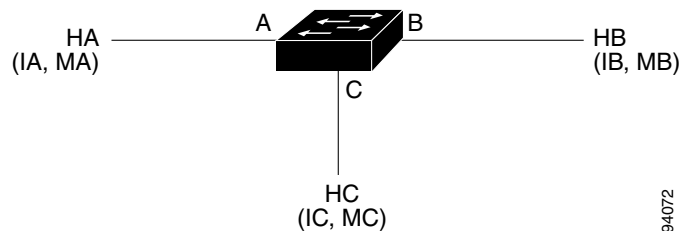
- ARP Cache Poisoning, page 31-2
- Dynamic ARP Inspection, page 31-2
- Interface Trust state, Security Coverage and Network Configuration, page 31-3
- Relative Priority of Static Bindings and DHCP Snooping Entries, page 31-4
- Logging of Denied Packets, page 31-4
- Rate Limiting of ARP Packets, page 31-4
- Port Channels and Their Behavior, page 31-4

## ARP Cache Poisoning

You can attack hosts, switches, and routers connected to your Layer 2 network by “poisoning” their ARP caches. For example, a malicious user might intercept traffic intended for other hosts on the subnet by poisoning the ARP caches of systems connected to the subnet.

Consider the following configuration:

**Figure 31-1 ARP Cache Poisoning**



Hosts HA, HB, and HC are connected to the switch on interfaces A, B and C, all of which are on the same subnet. Their IP and MAC addresses are shown in parentheses; for example, Host HA uses IP address IA and MAC address MA. When HA needs to communicate to HB at the IP Layer, HA broadcasts an ARP request for the MAC address associated with IB. As soon as HB receives the ARP request, the ARP cache on HB is populated with an ARP binding for a host with the IP address IA and a MAC address MA; for example, IP address IA is bound to MAC address MA. When HB responds, the ARP cache on HA is populated with a binding for a host with the IP address IB and a MAC address MB.

Host HC can “poison” the ARP caches of HA and HB by broadcasting forged ARP responses with bindings for a host with an IP address of IA (or IB) and a MAC address of MC. Hosts with poisoned ARP caches use the MAC address MC as the destination MAC address for traffic intended for IA or IB. This means that HC intercepts that traffic. Because HC knows the true MAC addresses associated with IA and IB, HC can forward the intercepted traffic to those hosts using the correct MAC address as the destination. HC has inserted itself into the traffic stream from HA to HB, the classic “man in the middle” attack.

## Dynamic ARP Inspection

To prevent ARP poisoning attacks such as the one described in the previous section, a switch must ensure that only valid ARP requests and responses are relayed. DAI prevents these attacks by intercepting all ARP requests and responses. Each of these intercepted packets is verified for valid MAC address to IP address bindings before the local ARP cache is updated or the packet is forwarded to the appropriate destination. Invalid ARP packets are dropped.

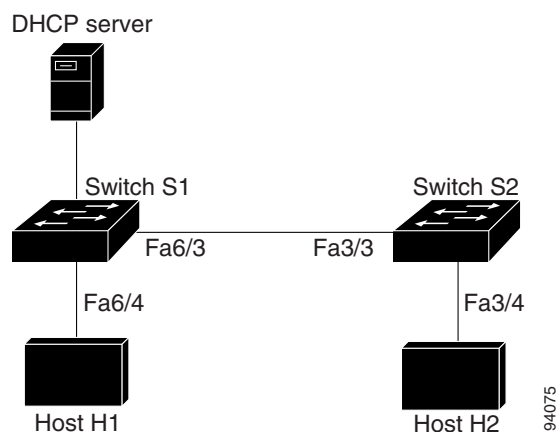
DAI determines the validity of an ARP packet based on valid MAC address to IP address bindings stored in a trusted database. This database is built at runtime by DHCP snooping, provided that it is enabled on the VLANs and on the switch in question. In addition, DAI can also validate ARP packets against user-configured ARP ACLs in order to handle hosts that use statically configured IP addresses.

DAI can also be configured to drop ARP packets when the IP addresses in the packet are invalid or when the MAC addresses in the body of the ARP packet do not match the addresses specified in the Ethernet header.

## Interface Trust state, Security Coverage and Network Configuration

DAI associates a trust state with each interface on the system. Packets arriving on trusted interfaces bypass all DAI validation checks, while those arriving on untrusted interfaces go through the DAI validation process. In a typical network configuration for DAI, all ports connected to host ports are configured as untrusted, while all ports connected to switches are configured as trusted. With this configuration, all ARP packets entering the network from a given switch will have passed the security check; it is unnecessary to perform a validation at any other place in the VLAN / network:

**Figure 31-2 Validation of ARP Packets on a DAI-enabled VLAN**



Use the trust state configuration carefully.

Configuring interfaces as untrusted when they should be trusted can result in a loss of connectivity. If we assume that both S1 and S2 (in Figure 31-2) run DAI on the VLAN that holds H1 and H2, and if H1 and H2 were to acquire their IP addresses from S1, then only S2 binds the IP to MAC address of H1. Therefore, if the interface between S1 and S2 is untrusted, the ARP packets from H1 get dropped on S2. This condition would result in a loss of connectivity between H1 and H2.

Configuring interfaces to be trusted when they are actually untrusted leaves a security hole in the network. If S1 were not running DAI, then H1 can easily poison the ARP of S2 (and H2, if the inter-switch link is configured as trusted). This condition can occur even though S2 is running DAI.

DAI ensures that hosts (on untrusted interfaces) connected to a switch running DAI do not poison the ARP caches of other hosts in the network. It does not, however, ensure that hosts from other portions of the network do not poison the caches of the hosts connected to it.

To handle cases in which some switches in a VLAN run DAI and other switches do not, the interfaces connecting such switches should be configured as untrusted. To validate the bindings of packets from non-DAI switches, however, the switch running DAI should be configured with ARP ACLs. When it is not feasible to determine such bindings, switches running DAI should be isolated from non-DAI switches at Layer 3.



### Note

Depending on the setup of DHCP server and the network, it may not be possible to perform validation of a given ARP packet on all switches in the VLAN.

## Relative Priority of Static Bindings and DHCP Snooping Entries

As mentioned previously, DAI populates its database of valid MAC address to IP address bindings through DHCP snooping. It also validates ARP packets against statically configured ARP ACLs. It is important to note that ARP ACLs have precedence over entries in the DHCP snooping database. ARP Packets are first compared to user-configured ARP ACLs. If the ARP ACL denies the ARP packet, then the packet will be denied even if a valid binding exists in the database populated by DHCP snooping.

## Logging of Denied Packets

DAI maintains a log of denied IP ARP packets. Log messages are generated at a controlled rate, and log entries are cleared once messages are generated on their behalf.

## Rate Limiting of ARP Packets

DAI performs validation checks in the CPU, so the number of incoming ARP packets is rate-limited to prevent a denial of service attack. By default, the rate for untrusted interfaces is set to 15 packets per second, whereas trusted interfaces have no rate limit. When the rate of incoming ARP packets exceeds the configured limit, the port is placed in the errdisable state. The port remains in that state until an administrator intervenes. You can enable errdisable recovery so that ports emerge from this state automatically after a specified timeout period.

Unless a rate limit is explicitly configured on an interface, changing the trust state of the interface will also change its rate limit to the default value for that trust state; that is, 15 packets per second for untrusted interfaces and unlimited for trusted interfaces. Once a rate limit is configured explicitly, the interface retains the rate limit even when its trust state is changed. At any time, the interface reverts to its default rate limit if the no form of the **rate limit** command is applied.

## Port Channels and Their Behavior

A given physical port can join a channel only when the trust state of the physical port and of the channel match. Otherwise, the physical port remains suspended in the channel. A channel inherits its trust state from the first physical port that joined the channel. Consequently, the trust state of the first physical port need not match the trust state of the channel.

Conversely, when the trust state is changed on the channel, the new trust state is configured on all the physical ports that comprise the channel.

The rate limit check on port channels is unique. The rate of incoming packets on a physical port is checked against the port channel configuration rather than the physical ports configuration.

The rate limit configuration on a port channel is independent of the configuration on its physical ports.

The rate limit is cumulative across all physical port; that is, the rate of incoming packets on a port channel equals the sum of rates across all physical ports.

When you configure rate limits for ARP packets on trunks, you must account for VLAN aggregation because a high rate limit on one VLAN can cause a “denial of service” attack to other VLANs when the port is errdisabled by software. Similarly, when a port channel is errdisabled, a high rate limit on one physical port can cause other ports in the channel to go down.

# Configuring Dynamic ARP Inspection

This section includes these scenarios:

- Scenario One: Two Switches Support Dynamic ARP Inspection, page 31-5
- Scenario Two: One Switch Supports Dynamic ARP Inspection, page 31-9

## Scenario One: Two Switches Support Dynamic ARP Inspection

Assume that there are two switches, S1 and S2 with hosts H1 and H2 attached, respectively. Both S1 and S2 are running DAI on VLAN 1 where the hosts are located. The S1 interface fa6/3 is connected to the S2 interface fa3/3, and a DHCP server is connected to S1. Both hosts acquire their IP addresses from the same DHCP server. Therefore, S1 has the binding for H1 and H2, and S2 has the binding for host H2.

To make the setup effective, you must configure the interface fa3/3 on S2 to be trusted. (You can leave interface fa6/3 on S1 as untrusted.) If the DHCP server is moved from S1 to a different location, however, the configuration will not work. To ensure that this setup works permanently, without compromising security, you must configure both interfaces fa6/3 on S1 and fa3/3 on S2 as trusted.

### Configuring Switch S1

To enable DAI and configure fa6/3 on S1 as trusted, follow these steps:

#### Step 1 Verify the connection between switches S1 and S2:

```
S1# 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
S2 Fas 6/3 177 R S I WS-C4006 Fas 3/3
S1#
```

#### Step 2 Enable DAI on VLAN 1 and verify the configuration:

```
S1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)# ip arp inspection vlan 1
S1(config)# end
S1# 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
S1#
```

**Step 3** Configure interface fa6/3 as trusted:

```

S1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)# in fa6/3
S1(config-if)# ip arp inspection trust
S1(config-if)# end
S1# show ip arp inspection interfaces fastEthernet 6/3

```

| Interface | Trust State | Rate (pps) |
|-----------|-------------|------------|
| -----     | -----       | -----      |
| Fa6/3     | Trusted     | None       |

S1#

**Step 4** Verify the bindings:

```

S1# show ip dhcp snooping binding

```

| MacAddress        | IpAddress | Lease(sec) | Type          | VLAN | Interface       |
|-------------------|-----------|------------|---------------|------|-----------------|
| -----             | -----     | -----      | -----         | ---- | -----           |
| 00:02:00:02:00:02 | 1.1.1.2   | 4993       | dhcp-snooping | 1    | FastEthernet6/4 |

S1#

**Step 5** Check the statistics before and after Dynamic ARP processes any packets:

```

S1# 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                      |

S1#

If H1 then sends out two ARP requests with an IP address of 1.1.1.2 and a MAC address of 0002.0002.0002, both requests are permitted, as reflected in the following statistics:

```

S1# show ip arp inspection statistics vlan 1

```

| Vlan | Forwarded | Dropped | DHCP Drops | ACL Drops |
|------|-----------|---------|------------|-----------|
| ---- | -----     | -----   | -----      | -----     |
| 1    | 2         | 0       | 0          | 0         |

| Vlan | DHCP Permits | ACL Permits | Source MAC Failures |
|------|--------------|-------------|---------------------|
| ---- | -----        | -----       | -----               |
| 1    | 2            | 0           | 0                   |

| Vlan | Dest MAC Failures | IP Validation Failures |
|------|-------------------|------------------------|
| ---- | -----             | -----                  |
| 1    | 0                 | 0                      |

S1#

If H1 then tries to send an ARP request with an IP address of 1.1.1.3, the packet is dropped and an error message is logged:

```

00:12:08: %SW_DAI-4-DHCP_SNOOPING_DENY: 2 Invalid ARPs (Req) on Fa6/4, vlan
1. ([0002.0002.0002/1.1.1.3/0000.0000.0000/0.0.0.0/02:42:35 UTC Tue Jul 10 2001])
S1# show ip arp inspection statistics vlan 1
S1#

```



The statistics will display as follows:

```

Vlan Forwarded Dropped DHCP Drops ACL Drops
---- -
1 2 2 2 0

Vlan DHCP Permits ACL Permits Source MAC Failures
---- -
1 2 0 0

Vlan Dest MAC Failures IP Validation Failures
---- -
1 0 0
S1#

```

## Configuring Switch S2

To enable DAI and configure fa3/3 on S2 as trusted, follow these steps:

### Step 1 Verify the connectivity:

```

S2# 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
S1 Fas 3/3 120 R S I WS-C4006 Fas 6/3
S2#

```

### Step 2 Enable DAI on VLAN 1, and verify the configuration:

```

S2# conf t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)# ip arp inspection vlan 1
S2(config)# end
S2# 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
S2#

```

### Step 3 Configure interface fa3/3 as trusted:

```

S2# conf t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)# interface fastEthernet 3/3
S2(config-if)# ip arp inspection trust
S2(config-if)# end
S2# show ip arp inspection interfaces

```

| Interface | Trust State | Rate (pps) |
|-----------|-------------|------------|
| -----     | -----       | -----      |
| Gi1/1     | Untrusted   | 15         |
| Gi1/2     | Untrusted   | 15         |
| Gi3/1     | Untrusted   | 15         |
| Gi3/2     | Untrusted   | 15         |
| Fa3/3     | Trusted     | None       |
| Fa3/4     | Untrusted   | 15         |
| Fa3/5     | Untrusted   | 15         |
| Fa3/6     | Untrusted   | 15         |
| Fa3/7     | Untrusted   | 15         |

&lt;output truncated&gt;

S2#

**Step 4** Verify the list of DHCP snooping bindings:

S2# show ip dhcp snooping binding

| MacAddress        | IpAddress | Lease (sec) | Type          | VLAN | Interface       |
|-------------------|-----------|-------------|---------------|------|-----------------|
| -----             | -----     | -----       | -----         | ---- | -----           |
| 00:01:00:01:00:01 | 1.1.1.1   | 4995        | dhcp-snooping | 1    | FastEthernet3/4 |

S2#

**Step 5** Check the statistics before and after Dynamic ARP processes any packets:

S2# 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                      |

S2#

If H2 then sends out an ARP request with the IP address 1.1.1.1 and the MAC address 0001.0001.0001, the packet is forwarded and the statistics are updated appropriately:

S2# show ip arp inspection statistics vlan 1

| Vlan | Forwarded | Dropped | DHCP Drops | ACL Drops |
|------|-----------|---------|------------|-----------|
| ---- | -----     | -----   | -----      | -----     |
| 1    | 1         | 0       | 0          | 0         |

| Vlan | DHCP Permits | ACL Permits | Source MAC Failures |
|------|--------------|-------------|---------------------|
| ---- | -----        | -----       | -----               |
| 1    | 1            | 0           | 0                   |

| Vlan | Dest MAC Failures | IP Validation Failures |
|------|-------------------|------------------------|
| ---- | -----             | -----                  |
| 1    | 0                 | 0                      |

S2#

Conversely, if H2 attempts to send an ARP request with the IP address 1.1.1.2, the request is dropped and an error message is logged:

```
00:18:08: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa3/4, vlan
1. ([0001.0001.0001/1.1.1.2/0000.0000.0000/0.0.0.0/01:53:21 UTC Fri May 23 2003])
S2#
```

The statistics will display as follows:

```
S2# show ip arp inspection statistics vlan 1
```

| Vlan | Forwarded | Dropped | DHCP Drops | ACL Drops |
|------|-----------|---------|------------|-----------|
| 1    | 1         | 1       | 1          | 0         |

| Vlan | DHCP Permits | ACL Permits | Source MAC Failures |
|------|--------------|-------------|---------------------|
| 1    | 1            | 0           | 0                   |

| Vlan | Dest MAC Failures | IP Validation Failures |
|------|-------------------|------------------------|
| 1    | 0                 | 0                      |

```
S2#
```

## Scenario Two: One Switch Supports Dynamic ARP Inspection

If switch S2 does not support DAI or DHCP snooping, configuring interface fa6/3 as trusted would leave a security hole because both S1 and H1 could be attacked by either S2 or H2. To prevent this possibility, you must configure interface fa6/3 as untrusted. To permit ARP packets from H2, you must set up an ARP ACL and apply it to VLAN 1. If the IP address of H2 is not static, such that it is impossible to apply the ACL configuration on S1, S1 and S2 must be separated at Layer 3, that is, have a router routing packets between S1 and S2.

To set up an ARP ACL on switch S1, follow these steps:

- Step 1** Set up the access list to permit the IP address 1.1.1.1 and the MAC address 0001.0001.0001, and verify the configuration:

```
S1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)# arp access-list H2
S1(config-arp-nacl)# permit ip host 1.1.1.1 mac host 1.1.1
S1(config-arp-nacl)# end
S1# show arp access-list
ARP access list H2
 permit ip host 1.1.1.1 mac host 0001.0001.0001
```

- Step 2** Apply the ACL to VLAN 1, and verify the configuration:

```
S1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)# ip arp inspection filter H2 vlan 1
S1(config)# end
S1#

S1# 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    | H2        | No         |

| Vlan | ACL Logging | DHCP Logging |
|------|-------------|--------------|
| ---- | -----       | -----        |
| 1    | Deny        | Deny         |

S1#

**Step 3** Establish the interface fa6/3 as untrusted, and verify the configuration:

```
S1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)# in fa6/3
S1(config-if)# no ip arp inspection trust
S1(config-if)# end
Switch# show ip arp inspection interfaces fastEthernet 6/3
```

| Interface | Trust State | Rate (pps) |
|-----------|-------------|------------|
| -----     | -----       | -----      |
| Fa6/3     | Untrusted   | 15         |

Switch#

When H2 sends 5 ARP requests through interface fa6/3 on S1 and a “get” is permitted by S1, the statistics are updated appropriately:

```
Switch# show ip arp inspection statistics vlan 1
Vlan Forwarded Dropped DHCP Drops ACL Drops

1 5 0 0 0
Vlan DHCP Permits ACL Permits Source MAC Failures

1 0 5 0
Vlan Dest MAC Failures IP Validation Failures

1 0 0
Switch#
```



## Configuring SPAN

---

This chapter describes how to configure the Switched Port Analyzer (SPAN) feature on the Catalyst 4500 series switches. SPAN selects network traffic for analysis by a network analyzer such as a SwitchProbe device or other Remote Monitoring (RMON) probe.

This chapter consists of the following sections:

- Overview of SPAN, page 32-1
- SPAN Configuration Guidelines and Restrictions, page 32-4
- Configuring SPAN, page 32-4
- CPU Port Sniffing, page 32-7
- Encapsulation Configuration, page 32-7
- Ingress Packets, page 32-7
- Packet Type Filtering, page 32-8
- Configuration Example, page 32-9



### Note

For complete syntax and usage information for the switch commands used in this chapter, refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference* and the publications at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/index.htm>

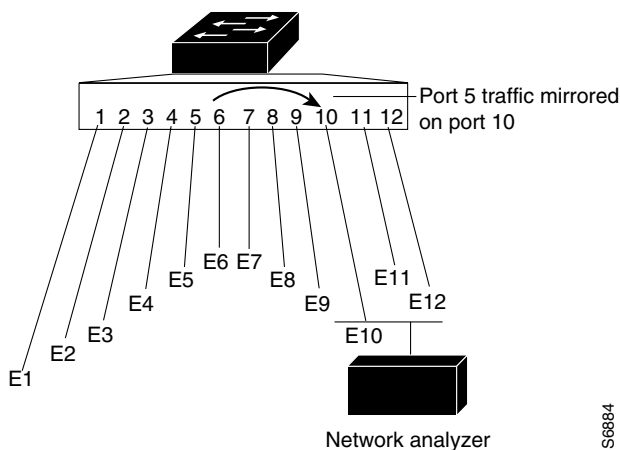
## Overview of SPAN

SPAN mirrors traffic from one or more source interfaces on any VLAN, or from one or more VLANs to a destination interface for analysis. In Figure 32-1, all traffic on Ethernet interface 5 (the source interface) is mirrored to Ethernet interface 10. A network analyzer on Ethernet interface 10 receives all network traffic from Ethernet interface 5 without being physically attached to it.

For SPAN configuration, the source interfaces and the destination interface must be on the same switch.

SPAN does not affect the switching of network traffic on source interfaces; copies of the packets received or transmitted by the source interfaces are sent to the destination interface.

Figure 32-1 Example SPAN Configuration



The following sections describe how SPAN works:

- SPAN Session, page 32-2
- Destination Interface, page 32-2
- Source Interface, page 32-3
- Traffic Types, page 32-3
- VLAN-Based SPAN, page 32-3
- SPAN Traffic, page 32-3

## SPAN Session

A SPAN session is an association of a destination interface with a set of source interfaces; you configure SPAN sessions using parameters that specify the type of network traffic to monitor. SPAN sessions allow you to monitor traffic on one or more interfaces, or one or more VLANs, and/or CPU (optionally with one or more queues), and send either ingress traffic, egress traffic, or both to a destination interface.

You can configure up to six separate SPAN sessions (2 ingress, 4 egress) with separate or overlapping sets of SPAN source interfaces or VLANs. A bi-directional SPAN session counts as both 1 ingress and 1 egress session. Both switched and routed interfaces can be configured as SPAN sources.

SPAN sessions do not interfere with the normal operation of the switch. When enabled, a SPAN session might become active or inactive based on various events or actions; a syslog message indicates this. The **show monitor session** command displays the administrative status of a SPAN session.

A SPAN session will remain inactive after system boot-up until the destination interface is operational.

## Destination Interface

A destination interface (also called a *monitor interface*) is a switched or routed interface where SPAN sends packets for analysis. Once an interface becomes an active destination interface, incoming traffic is disabled. For more information, see “Ingress Packets” section on page 32-7.

An interface specified as a destination interface in one SPAN session cannot be a destination interface for another SPAN session. An interface configured as a destination interface cannot be configured as a source interface. EtherChannel interfaces cannot be SPAN destination interfaces. For more information about the encapsulation of spanned packets, see “Encapsulation Configuration” section on page 32-7.

## Source Interface

A source interface is an interface monitored for network traffic analysis. One or more source interfaces can be monitored in a single SPAN session with user-specified traffic types (ingress, egress, or both) applicable for all the source interfaces.

You can configure source interfaces for any VLAN. You can configure VLANs as source interfaces, which means that all interfaces in the specified VLANs are source interfaces for the SPAN session.

Trunk interfaces can be configured as source interfaces and can be mixed with nontrunk source interfaces. For more information, see “Encapsulation Configuration” section on page 32-7.

## Traffic Types

Ingress SPAN (Rx) copies network traffic received by the source interfaces for analysis at the destination interface. Egress SPAN (Tx) copies network traffic transmitted from the source interfaces. Specifying the configuration option “both” copies network traffic received and transmitted by the source interfaces to the destination interface.

## VLAN-Based SPAN

VLAN-based SPAN analyzes the network traffic in one or more VLANs. You can configure VLAN based-SPAN as ingress SPAN, egress SPAN, or both. All of the interfaces in the source VLANs become source interfaces for the VLAN-based SPAN session.

Use the following guidelines for VLAN-based SPAN sessions:

- Trunk interfaces are included as source interfaces for VLAN-based SPAN sessions.
- For VLAN-based SPAN sessions with both ingress and egress SPAN configured, two packets are forwarded by the SPAN destination interface if the packets get switched on the same VLAN.
- When a VLAN is cleared, it is removed from the source list for VLAN-based SPAN sessions.
- Inactive and internal VLANs are not allowed for VLAN-based SPAN configuration.
- If a VLAN is being ingress monitored and the switch routes traffic from another VLAN to the monitored VLAN, that traffic is not monitored—it is not seen on the SPAN destination interface. Additionally, traffic that gets routed from an egress-monitored VLAN to some other VLAN does not get monitored. VLAN-based SPAN only monitors traffic that leaves or enters the switch, not traffic that gets routed between VLANs.

## SPAN Traffic

All network traffic, including multicast and bridge protocol data unit (BPDU) packets, can be monitored using SPAN.

In some SPAN configurations, multiple copies of the same source packet are sent to the SPAN destination interface. For example, a bidirectional (both ingress and egress) SPAN session is configured for sources a1 and a2 to a destination interface d1. If a packet enters the switch through a1 and gets switched to a2, both incoming and outgoing packets are sent to destination interface d1; both packets would be the same (unless a Layer-3 rewrite had occurred, in which case the packets would be different).

## SPAN Configuration Guidelines and Restrictions

Follow these guidelines and restrictions when configuring SPAN:

- Use a network analyzer to monitor interfaces.
- You cannot mix source VLANs and filter VLANs within a SPAN session. You can have source VLANs or filter VLANs, but not both at the same time.
- EtherChannel interfaces can be SPAN source interfaces; they cannot be SPAN destination interfaces.
- When you specify source interfaces and do not specify a traffic type (Tx, Rx, or both), “both” is used by default.
- If you specify multiple SPAN source interfaces, the interfaces can belong to different VLANs.
- Enter the **no monitor session** *number* command with no other parameters to clear the SPAN session *number*.
- The **no monitor** command clears all SPAN sessions.
- SPAN destinations never participate in any spanning tree instance. SPAN includes BPDUs in the monitored traffic, so any BPDUs seen on the SPAN destination are from the SPAN source.

## Configuring SPAN

The following sections describe how to configure SPAN:

- Configuring SPAN Sources, page 32-5
- Configuring SPAN Destinations, page 32-5
- Monitoring Source VLANs on a Trunk Interface, page 32-6
- Configuration Scenario, page 32-6
- Verifying a SPAN Configuration, page 32-6



### Note

Entering SPAN configuration commands does not clear previously configured SPAN parameters. You must enter the **no monitor session** command to clear configured SPAN parameters.



## Configuring SPAN Sources

To configure the source for a SPAN session, perform this task:

| Command                                                                                                                                                                                           | Purpose                                                                                                                                                                                                                                                                                                                           |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Switch(config)# <b>[no] monitor session</b><br><b>{session_number} {source {interface</b><br><b>&lt;interface_list&gt;   {vlan vlan_ids   cpu</b><br><b>[queue queue_ids ] } [rx   tx   both]</b> | Specifies the SPAN session number (1 through 6), the source interfaces (FastEthernet or GigabitEthernet), VLANs (1 through 4094), whether or not traffic received or sent from the CPU is copied to the session destination, and the traffic direction to be monitored.<br><br>Use the <b>no</b> keyword to restore the defaults. |

This example shows how to configure SPAN session 1 to monitor bidirectional traffic from source interface Fast Ethernet 5/1:

```
Switch(config)# monitor session 1 source interface fastethernet 5/1
```

This example shows how to configure sources with differing directions within a SPAN session:

```
Switch(config)# monitor session 1 source interface fa2/3 rx
Switch(config)# monitor session 1 source interface fa2/2 tx
Switch(config)#
```

## Configuring SPAN Destinations

To configure the destination for a SPAN session, perform this task:

| Command                                                                                                                                                                                         | Purpose                                                                                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| Switch(config)# <b>[no] monitor session</b><br><b>&lt;session_number&gt; destination interface</b><br><b>&lt;interface&gt; [encapsulation {isl   dot1q}]</b><br><b>[ingress [vlan vlan_ID]]</b> | Specifies the SPAN session number (1 through 6) and the destination interfaces or VLANs.<br><br>Use the <b>no</b> keyword to restore the defaults. |

This example shows how to configure interface Fast Ethernet 5/48 as the destination for SPAN session 1:

```
Switch(config)# monitor session 1 destination interface fastethernet 5/48
```

## Monitoring Source VLANs on a Trunk Interface

To monitor specific VLANs when the SPAN source is a trunk interface, perform this task:

| Command                                                                                                                                                                                           | Purpose                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Switch(config)# [no] monitor session {session_number} filter { vlan vlan_id [,   - ] }   { packet-type { good   bad } }   { address-type { unicast   multicast   broadcast } [ rx   tx   both ] } | Monitors specific VLANs when the SPAN source is a trunk interface. The filter keyword restricts monitoring to traffic that is on the specified VLANs; it is typically used when monitoring a trunk interface.<br><br>Monitoring is established through all the ports in the specified VLANs<br><br>Use the <b>no</b> keyword to restore the defaults. |

This example shows how to monitor VLANs 1 through 5 and VLAN 9 when the SPAN source is a trunk interface:

```
Switch(config)# monitor session 2 filter vlan 1 - 5 , 9
```

## Configuration Scenario

This example shows how to use the commands described in this chapter to completely configure and unconfigure a span session. Assume that you want to monitor bidirectional traffic from source interface Fast Ethernet 4/10, which is configured as a trunk interface carrying VLANs 1 through 4094. Moreover, you want to monitor only traffic in VLAN 57 on that trunk. Using Fast Ethernet 4/15 as your destination interface, you would enter the following commands:

```
Switch(config)# monitor session 1 source interface fastethernet 4/10
Switch(config)# monitor session 1 filter vlan 57
Switch(config)# monitor session 1 destination interface fastethernet 4/15
```

You are now monitoring traffic from interface Fast Ethernet 4/10 that is on VLAN 57 out of interface FastEthernet 4/15. To disable the span session enter the following command:

```
Switch(config)# no monitor session 1
```

## Verifying a SPAN Configuration

This example shows how to verify the configuration of SPAN session 2:

```
Switch# show monitor session 2
Session 2

Source Ports:
 RX Only: Fa5/12
 TX Only: None
 Both: None
Source VLANs:
 RX Only: None
 TX Only: None
 Both: None
Destination Ports: Fa5/45
Filter VLANs: 1-5,9
Switch#
```

## CPU Port Sniffing

When configuring a SPAN session, you can specify the CPU (or a subset of CPU queues) as a SPAN source. Queues may be specified either by number or by name. When such a source is specified, traffic going to the CPU through one of the specified queues is mirrored and sent out of the SPAN destination port in the session. This traffic includes both control packets and regular data packets that are sent to or from the CPU (due to software forwarding).

You can mix the CPU source with either regular port sources or VLAN sources.

To configure CPU source sniffing, perform this task:

| Command                                                                                                                                                            | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Switch(config)# <b>[no] monitor session</b> {session_number} {source {interface <interface_list>   {vlan <vlan_ids>   cpu [queue <queue_ids> ] } [rx   tx   both]} | Specifies that the CPU will cause traffic received by or sent from the CPU to be copied to the destination of the session. The <b>queue</b> identifier optionally allows sniffing-only traffic (received) on the specified CPU queue(s).<br><br>Queues may be identified either by number or by name. Queue names may subsume multiple numbered queues for convenience.<br><br>Use the <b>no</b> keyword to restore the defaults. |

This example shows how to configure a CPU source to sniff all packets received by the CPU:

```
Switch(config)# monitor session 1 source cpu rx
```

This example shows how to use queue names and queue number ranges for the CPU as a SPAN source:

```
Switch(config)# monitor session 2 source cpu queue control-packet rx
Switch(config)# monitor session 3 source cpu queue 21 -23 rx
```

## Encapsulation Configuration

When configuring a SPAN destination port, you can explicitly specify the encapsulation type used by the port. Packets sent out the port are tagged in accordance with the specified mode. (The encapsulation mode also controls how tagged packets are handled when the ingress packet option is enabled.) The Catalyst 4500 series switch supervisor engines support ISL encapsulation and 802.1q encapsulation, as well as untagged packets. The “replicate” encapsulation type (in which packets are transmitted from the destination port using whatever encapsulation applied to the original packet) is not supported. If no encapsulation mode is specified, the port default is untagged.

## Ingress Packets

When ingress is enabled, the SPAN destination port accepts incoming packets (potentially tagged depending on the specified encapsulation mode) and switches them normally. When configuring a SPAN destination port, you can specify whether or not the ingress feature is enabled and what VLAN to use to switch untagged ingress packets. (Specifying an ingress VLAN is not required when ISL encapsulation is configured, as all ISL encapsulated packets have VLAN tags.) Although the port is STP forwarding,

it does not participate in the STP, so use caution when configuring this feature lest a spanning-tree loop be introduced in the network. When both ingress and a trunk encapsulation are specified on a SPAN destination port, the port will go forwarding in all active VLANs. Configuring a non-existent VLAN as an ingress VLAN is not allowed.

Host learning is disabled on SPAN destination ports with ingress enabled, and the port is removed from VLAN floodsets, so regular traffic will not be switched out of the destination port. If it is necessary to send traffic to a host connected to the SPAN destination port with ingress enabled, a static host entry may be configured.

To configure ingress packets and encapsulation, perform this task:

| Command                                                                                                                                                 | Purpose                                                                                                                                                         |
|---------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Switch(config)# [no] monitor session<br><session_number> destination interface<br><interface> [encapsulation {isl   dot1q}]<br>[ingress [vlan vlan_ID]] | Specifies the configuration of the ingress packet and the encapsulation type of the destination port.<br><br>Use the <b>no</b> keyword to restore the defaults. |

This example shows how to configure a destination port with 802.1q encapsulation and ingress packets using native VLAN 7:

```
Switch(config)# monitor session 1 destination interface fastethernet 5/48
encapsulation dot1q ingress vlan 7
```

With this configuration, traffic from SPAN sources associated with session 1 would be copied out of interface Fast Ethernet 5/48, with 802.1q encapsulation. Incoming traffic would be accepted and switched, with untagged packets being classified into VLAN 7.

## Packet Type Filtering

When configuring a SPAN session, you can specify packet filter parameters similar to VLAN filters. When specified, the packet filters indicate types of packets that may be sniffed. If no packet filters are specified, packets of all types may be sniffed. Different types of packet filters may be specified for ingress and egress traffic.

There are two categories of packet filtering: packet-based (good, error) or address-based (unicast/multicast/broadcast). Packet-based filters can only be applied in the ingress direction. Packets are classified as broadcast, multicast, or unicast by the hardware based on the destination address.



### Note

When filters of both types are configured, only packets that pass both filters are spanned. For example, if you set both “error” and “multicast,” only multicast packets with errors will be spanned.

To configure packet type filtering, perform this task:

| Command                                                                                                                                                                                                     | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>Switch(config)# [no] monitor session {session_number} filter { vlan vlan_id [,   - ] }   { packet-type { good   bad } }   { address-type { unicast   multicast   broadcast } [ rx   tx   both ]}</pre> | <p>Specifies filter sniffing of the specified packet types in the specified directions.</p> <p>You can specify both Rx and Tx type filters, as well as specify multiple type filters at the same time (such as <b>good</b> and <b>unicast</b> to only sniff non-error unicast frames). As with VLAN filters, if no type or filter is specified, then the session will sniff all packet types.</p> <p>Use the <b>no</b> keyword to restore the defaults.</p> |

This example shows how to configure a session to accept only unicast packets in the ingress direction:

```
Switch(config)# monitor session 1 filter address-type unicast rx
```

## Configuration Example

The following is an example of SPAN configuration using some of the SPAN enhancements.

In the example below, you configure a session to sniff unicast traffic arriving on interface Gi1/1. The traffic is mirrored out of interface Gi1/2 with ISL encapsulation. Ingress traffic is permitted.

```
Switch(config)# monitor session 1 source interface gi1/1 rx
Switch(config)# monitor session 1 destination interface gi1/2 encapsulation isl ingress
Switch(config)# monitor session 1 filter address-type unicast rx
```

```
Switch# show monitor
```

```
Session 1

Type :Local Session
Source Ports :
 RX Only :Gi1/1
Destination Ports :Gi1/2
 Encapsulation :ISL
 Ingress :Enabled
Filter Addr Type :
 RX Only :Unicast
```





# Environmental Monitoring and Power Management

This chapter describes power management and environmental monitoring features in the Catalyst 4500 series switches. It provides guidelines, procedures, and configuration examples.

This chapter consists of the following major sections:

- Understanding Environmental Monitoring, page 33-1
- Power Management, page 33-3
- Configuring Inline Power, page 33-16



**Note**

For complete syntax and usage information for the switch commands used in this chapter, refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference* and related publications at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/index.htm>

## Understanding Environmental Monitoring

You can monitor your system with a few commands and an understanding of the system alarms. Environmental monitoring of chassis components provides early warning indications of possible component failure. This warning helps you to ensure the safe and reliable operation of your system and avoid network interruptions.

This section describes how to monitor these critical system components, so you can identify and rapidly correct hardware-related problems in your system.

## Using CLI Commands to Monitor your Environment

To monitor the system, you use the **show environment** CLI command. This section gives a basic overview of the command and keywords you are likely to need.

Enter the **show environment [alarm | status | temperature]** command to display system status information. Keyword descriptions are listed in Table 33-1.

**Table 33-1** show environment Keyword Descriptions

| Keyword            | Purpose                                                                                                     |
|--------------------|-------------------------------------------------------------------------------------------------------------|
| <b>alarm</b>       | Displays environmental alarms for the system.                                                               |
| <b>status</b>      | Displays field-replaceable unit (FRU) operational status and power and power supply fan sensor information. |
| <b>temperature</b> | Displays temperature of the chassis.                                                                        |

The following example shows how to display the environment conditions. Notice that this output indicates that the power supplies are different. The switch will only use one power supply and disable the other.

```
Switch# show environment
no alarm

Chassis Temperature = 35 degrees Celsius
Chassis Over Temperature Threshold = 75 degrees Celsius
Chassis Critical Temperature Threshold = 95 degrees Celsius

Power
Supply Model No Type Status Fan Inline
----- -----
PS1 PWR-C45-2800AC AC 2800W good good good
→ PS2 PWR-C45-1000AC AC 1000W err-disable good n.a.

*** Power Supplies of different types have been detected***
Switch#
```

## System Alarms

The system has two types of alarms: major and minor. A major alarm indicates a critical problem that could lead to system shutdown. A minor alarm is just informational—it alerts you to a problem that could turn critical if corrective action is not taken.

When the system issues an alarm (major or minor) indicating an over-temperature condition, the alarm is not canceled nor is any action taken (such as module reset or shutdown) for five minutes. If the temperature falls 5 degrees Celsius below the alarm threshold during this period, the alarm is canceled.

An LED is associated with each alarm. The LEDs are used as environmental indicators for the supervisor engine and switching modules. (See Table 33-2 for more information.)



### Note

Refer to the *Catalyst 4500 Series Switch Module Installation Guide* for additional information on LEDs, including the supervisor engine system LED.



**Table 33-2 Alarms for Supervisor Engine and Switching Modules**

| Event                                                                     | Alarm Type | LED Color                   | Description and Action                                                                                                                                                                                                                                                                                                               |
|---------------------------------------------------------------------------|------------|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Supervisor engine temperature sensor exceeds major threshold <sup>1</sup> | Major      | Status <sup>2</sup> LED red | <p>Syslog message.</p> <p>If the over-temperature condition is not corrected, the system shuts down after 5 min.</p> <p>Alarm thresholds:</p> <ul style="list-style-type: none"> <li>Chassis temperature = 32°C</li> <li>Chassis over temperature threshold = 75°C</li> <li>Chassis critical temperature threshold = 95°C</li> </ul> |
| Supervisor engine temperature sensor exceeds minor threshold              | Minor      | Status LED orange           | <p>Syslog message.</p> <p>Monitor the condition.</p>                                                                                                                                                                                                                                                                                 |

1. Temperature sensors monitor key supervisor engine components including daughter cards.

2. A Status LED is located on the supervisor engine front panel and all module front panels.

## Power Management

This section describes the power management feature in the Catalyst 4500 series switches.

The following major sections are included:

- Power Management for the Catalyst 4500 Series Switches, page 33-3
- Power Management for the Catalyst 4006 Switch, page 33-10
- Power Consumption of Chassis Components, page 33-15
- Configuring Inline Power, page 33-16

## Power Management for the Catalyst 4500 Series Switches

You can select from several different power supplies to ensure that you have enough power for the modules installed in your switch. The Catalyst 4500 series switches support the following power supplies:

- Fixed Wattage—This power supply always delivers a fixed amount of inline and system power.
  - 1000 W AC
  - 2800 W AC—Supports inline power.
- Variable Wattage—This power supply automatically adjusts the wattage to accommodate inline and system power requirements.
  - 1300 W AC—Supports inline power.
  - 1400 W DC—Supports up to 1400 W of system power and variable amounts of inline power, depending on the input feed to the power supply. See “Special Considerations for the 1400W DC Power Supply” section on page 33-9 for more information.

When you insert power supplies in your switch, use power supplies that are of the same wattage. If you mix power supplies, the switch will use the one it recognizes first; the other power supply is ignored. The power supply status displays as err-disable and the summary displays as all zeros (0) for wattage values in the output for the **show power** command.

The following example shows the output for the **show power** command for mixed power supplies:

```
Switch# show power
Power
Supply Model No Type Status Fan Inline
----- -
PS1 PWR-C45-2800AC AC 2800W good good good
→ PS2 PWR-C45-1000AC AC 1000W err-disable good n.a.

*** Power Supplies of different type have been detected***

Power Supply Max Min Max Min Absolute
(Nos in Watts) Inline Inline System System Maximum

PS1 1400 1400 1360 1360 2800
→ PS2 0 0 0 0 0
Switch#
```

## Power Management Modes

The Catalyst 4500 series switches support two power management modes:

- **Redundant mode**—Redundant mode uses one power supply as a primary power supply and the second power supply as a back-up. If the primary power supply fails, the second power supply immediately supports the switch without any disruption in the network. Both power supplies must be the same wattage. A single power supply must have enough power to support the switch configuration.
- **Combined mode**—Combined mode uses the power from all installed power supplies to support the switch configuration power requirements. However, combined mode has no power redundancy. If a power supply fails, one or more modules might shut down. The 1400W DC power supply does not support Combined mode.

## Selecting a Power Management Mode

By default, a switch is set to redundant mode. In the **show power** command, if the **power supplies needed by system** is 1, the switch is in redundant mode; if the **power supplies needed by system** is 2, the switch is in combined mode.

Your switch hardware configuration will dictate which power supply or supplies you should use. For example, if your switch configuration requires more power than a single power supply provides, use the combined mode. In combined mode, however, the switch has no power redundancy. Consider the following possibilities:

- The supervisor engine consumes 110 W, the fan boxes for the Catalyst 4503 switch consume 30 W each, the fan boxes for the Catalyst 4506 and Catalyst 4507 switches consume 50 W each, the backplane for the Catalyst 4503 and Catalyst 4506 switches consumes 10 W, and the backplane for the Catalyst 4507 switch consumes 40 W.
- 1000 W can support a fully loaded Catalyst 4503 switch with no IP phone support.
- 1300 W can support a fully loaded Catalyst 4503 switch with Cisco IP phones.
- 1300 W does not support a Catalyst 4507 fully loaded with Cisco IP phones in Redundant mode.

- 2800 W can support a fully loaded Catalyst 4503 switch with Cisco IP phones or a fully loaded Catalyst 4506 switch or Catalyst 4507 switch with limited Cisco IP phone support.
- Each inline power port on a WS-X4148-RJ45V module requires 6.3 W. Five fully loaded WS-X4148-RJ45V modules in a switch comprises 240 ports. This configuration will require 1512 W of inline power plus 300 W for the modules.

See Table 33-4 on page 33-15 for the power requirements of Catalyst 4500 series switch modules.

## Power Management Limitations in Catalyst 4500 Family Switches

It is possible that you can configure a switch that requires more power than the power supplies provide. The two ways you could configure a switch to exceed the power capabilities are as follows:

- The power requirements for the installed modules exceed the power provided by the power supplies.

If you insert a single power supply and then set the switch to Combined mode, the switch displays following error message:

```
Insufficient power supplies present for specified configuration.
```

This error message is also displayed in the output for the **show power** command. This error message displays because by definition, Combined mode requires two working power supplies installed in your switch.

If the power requirements for the installed modules exceeds the power provided by the power supplies, the switch displays following error message:

```
Insufficient power available for the current chassis configuration.
```

This error message also appears in the **show power** command output.

If you attempt to insert additional modules into your switch and exceed the power that the power supplies provide, the switch immediately places the newly inserted module into reset mode and the switch displays following error message:

```
Module has been inserted and Insufficient power supplies operating.
```

Additionally, if you power down a functioning switch, and you insert an additional module or change the module configuration so that the power requirements exceed the available power, once you power on the switch again one or more modules are placed in reset mode.

- The power requirements for the inline power exceed the inline power provided by the power supplies.

If you have too many IP phones drawing power from the system, power to IP phones is cut and some phones may be powered down to reduce the power requirements to match the power supplies.

In the first scenario (power requirements exceed the power supplied), the system initiates the five-minute evaluation countdown timer. When this timer runs out, the system attempts to resolve this power usage limitation by evaluating the type and number of modules installed.

During the evaluation cycle, the modules are in effect removed and re-inserted, thus disrupting network connectivity; the switch reactivates only the modules it is able to support with the limited power available and leaves the remaining modules in reset mode. The supervisor engine always remains enabled. Modules placed in reset mode still consume some power. If the chassis module combination, including the modules in reset, still require more power than is available, the five-minute evaluation countdown timer starts for another evaluation cycle, and additional modules are placed in reset mode until the power usage is stable. If the power requirement of the active modules and the modules in reset does not exceed the available power, the system is stable and no more evaluation cycles are run, until something again causes insufficient power usage. Multiple cycles may be required to stabilize the system. If you configure the chassis correctly, the system will not enter the evaluation cycle.

A module in reset continues to draw power as long as it is installed in the chassis; you can use the **show power module** command to find out how much power is required to bring the module online and when it is held in reset.

To compute the power requirements for your system and verify that your system has enough power, add the power consumed by the supervisor engine module(s), the fan box(es), and the installed modules (including inline power). For inline power, multiply the number of IP phones by 6.3W. See the “Power Consumption of Chassis Components” section on page 33-15 for more information on the power consumption for the various components of your switch.

You can use the **show module** command to verify which modules are active and which, if any, have been placed in reset.

The following example shows the **show module** command output for a system with inadequate power for all installed modules. The system does not have enough power for Module 5; the **Status** displays it as **PwrDeny**.

```
Switch# show module

Mod Ports Card Type Model Serial No.
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
1 2 1000BaseX (GBIC) Supervisor(active) WS-X4014 JAB054109GH
2 6 1000BaseX (GBIC) WS-X4306 00000110
3 18 1000BaseX (GBIC) WS-X4418 JAB025104WK
→ 5 0 Not enough power for module WS-X4148-FX-MT 00000000000
6 48 10/100BaseTX (RJ45) WS-X4148 JAB023402RP

M MAC addresses Hw Fw Sw Status
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
1 005c.9d1a.f9d0 to 005c.9d1a.f9df 0.5 12.1(11br)EW 12.1(20020313:00 Ok
2 0010.7bab.9920 to 0010.7bab.9925 0.2 Ok
3 0050.7356.2b36 to 0050.7356.2b47 1.0 Ok
→ 5 0001.64fe.a930 to 0001.64fe.a95f 0.0 PwrDeny
6 0050.0f10.28b0 to 0050.0f10.28df 1.0 Ok

Switch#
```

### Configuring Redundant Mode on a Catalyst 4500 Series Switch

By default, the power supplies in a Catalyst 4500 series switch are set to operate in redundant mode. To effectively use redundant mode, follow these guidelines:

- Use two power supplies that are the same type.
- If you have the power management mode set to redundant mode and only one power supply installed, your switch will accept the configuration, but operates without redundancy.



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. The switch will not have power redundancy.

- For fixed power supplies, choose a power supply that by itself is powerful enough to support the switch configuration.

- For variable power supplies, choose a power supply that supplies enough power so that the chassis and inline power requirements are less than the maximum available power for the chassis and inline power for the power supply. Variable power supplies automatically adjust the power resources to accommodate the chassis and inline power requirements when a system is booted up. Modules are brought up first, followed by IP phones.
- The maximum available power for chassis and inline power for each power supply is listed in Table 33-3 on page 33-9.

To configure redundant mode on your Catalyst 4500 series switch, perform this task:

|        | Command                                                | Purpose                                            |
|--------|--------------------------------------------------------|----------------------------------------------------|
| Step 1 | Switch# <b>configure terminal</b>                      | Enters configuration mode.                         |
| Step 2 | Switch(config)# <b>power redundancy-mode redundant</b> | Sets the power management mode to redundant mode.  |
| Step 3 | Switch(config)# <b>end</b>                             | Exits configuration mode.                          |
| Step 4 | Switch# <b>show power supplies</b>                     | Verifies the power redundancy mode for the switch. |



#### Note

The **power redundancy-mode redundant** command is not supported on a Catalyst 4006 switch.

The following example shows how to set the power management mode to redundant mode.

```
Switch (config)# power redundancy-mode redundant
Switch (config)# end
Switch#
```

The following example shows how to display the current power redundancy mode. The **Power supplies needed by system: 1** indicates that the switch is in redundant mode.

```
Switch# show power supplies
Power supplies needed by system :1
Switch#
```

## Configuring Combined Mode on a Catalyst 4500 Series Switch

If your switch configuration requires more power than a single power supply can provide, set the power management mode to combined mode. Combined mode utilizes the available power for both power supplies; however, your switch will have no power redundancy.

To effectively use combined mode, follow these guidelines:

- Use the power supplies that are the same type and wattage (fixed or variable and AC or DC).
- If you use power supplies with different types or wattages, the switch will utilize only one of the power supplies.
- For variable power supplies, choose a power supply that supplies enough power so that the chassis and inline power requirements are less than the maximum available power for the chassis and inline power for the power supply. Variable power supplies automatically adjust the power resources to accommodate the chassis and inline power requirements.
- The 1400 W DC power supply does not support Combined mode. If you set the power budget to 2, the switch disregards this setting.

- If you have the power management mode set to combined mode and only one power supply installed, your switch will accept the configuration, but power is available from only one power supply.
- When your switch is configured to combined mode, the total available power is not the mathematical sum of the individual power supplies. The power supplies have a predetermined current sharing ratio. See Table 33-3 on page 33-9 for more information.
- The maximum available power for chassis and inline power for each power supply is listed in Table 33-3 on page 33-9.

To configure combined mode on your Catalyst 4500 series switch, perform this task:

|        | Command                                               | Purpose                                            |
|--------|-------------------------------------------------------|----------------------------------------------------|
| Step 1 | Switch# <b>configure terminal</b>                     | Enters configuration mode.                         |
| Step 2 | Switch(config)# <b>power redundancy-mode combined</b> | Sets the power management mode to combined mode.   |
| Step 3 | Switch(config)# <b>end</b>                            | Exits configuration mode.                          |
| Step 4 | Switch# <b>show power supplies</b>                    | Verifies the power redundancy mode for the switch. |



**Note**

The **power redundancy-mode combined** command does not work on a Catalyst 4006 switch.

The following example shows how to set the power management mode to combined mode.

```
Switch (config)# power redundancy-mode combined
Switch (config)# end
Switch#
```

The following example shows how to display the current power redundancy mode. The **Power supplies needed by system: 2** indicates that the switch is in combined mode.

```
Switch# show power supplies
Power supplies needed by system :2
Switch#
```

## Available Power for Catalyst 4500 Series Switches Power Supplies

Table 33-3 lists the power available for use in the various Catalyst 4500 series switches power supplies. When your switch is configured to combined mode, the total available power is not the mathematical sum of the individual power supplies. The power supplies have a predetermined current sharing ratio. The total power available is  $P + (P * \text{ratio})$ .

**Table 33-3 Available Power**

| Power Supply | Redundant Mode (W)                                                                                                                                   | Combined Mode (W)                                                                                                                  | Sharing Ratio             |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|---------------------------|
| 1000 W AC    | Chassis <sup>1</sup> = 1000<br>Inline = 0                                                                                                            | Chassis = 1667<br>Inline = 0                                                                                                       | 2/3                       |
| 1300 W AC    | Chassis (max) = 1000<br>Inline (max) = 800<br>Chassis + Inline + Backplane<br>≤ 1300                                                                 | Chassis (min) = 767<br>Chassis (max) = 1667<br>Inline (min) = 433<br>Inline (max) = 1333<br>Chassis + Inline +<br>Backplane ≤ 2166 | 2/3                       |
| 1400 W DC    | Chassis (min) = 200<br>Chassis (max) = 1360<br>Inline (max) <sup>2</sup> = (DC Input <sup>3</sup> -<br>[Chassis (min) + Backplane] /<br>0.75) * 0.96 | N/A                                                                                                                                | 2/3                       |
| 2800 W AC    | Chassis = 1360<br>In-line = 1400                                                                                                                     | Chassis = 2473<br>In-line = 2545                                                                                                   | System—9/11<br>Inline—2/3 |

1. Chassis power includes power for the supervisor(s), all line cards, and the fan tray.
2. 0.75 is the efficiency for the 1400W DC power supply. 0.96 applied to inline power.
3. The DC Input can vary for the 1400W DC power supply and is configurable. For more information, see “Special Considerations for the 1400W DC Power Supply” on page 9.

## Special Considerations for the 1400W DC Power Supply



### Caution

Do not mix the 1400 W DC power supply with any other power supply, even for a hot swap or other short-term emergency. Doing so can seriously damage your switch.

Keep in mind the following guidelines when using a 1400 W DC power supply with your Catalyst 4500 series switch.

- The 1400 W DC power supply works with a variety of DC sources. The DC input can vary from 300 W to 7500 W. Refer to the power supply documentation for additional information.
- A Supervisor Engine III and Supervisor Engine IV cannot detect the DC source plugged into the 1400 W DC power supply. If you are using the 1400 W DC power supply with a Supervisor Engine III, use the **power dc input** command to set the DC input power. For more information on this command, see the “Configuring the DC Input for a Power Supply” section on page 33-10.
- The software automatically adjusts between system power (for modules, backplane, and fans) and inline power. Although inline power is 96 percent efficient, system power has only 75 percent efficiency. For example, each 120 W of system power requires 160 W from the DC input. This is reflected in the **Power Used** column of the output for the **show power available** command.
- The 1400 W DC power supply does not support Combined mode. If you set the power budget to 2 (Combined mode), the switch allows you to configure Combined modes, but disregards the setting and remains in Redundant mode.

- The 1400 W DC power supply has a separate power on/off switch for inline power. The power supply fan status and main power supply status are tied together. If either of them fails, both the power supply and its fan report as bad/off. You should verify that the main power is on before turning the power on for the inline switch. In addition, you should verify that the power for the inline switch is off before turning off the main power.

### Configuring the DC Input for a Power Supply

To configure the DC input power for the 1400 W DC power supply or a power shelf, perform the following procedure:

|        | Command                                           | Purpose                                   |
|--------|---------------------------------------------------|-------------------------------------------|
| Step 1 | Switch# <code>configure terminal</code>           | Enters configuration mode                 |
| Step 2 | Switch(config)# <code>power dc input watts</code> | Sets the capacity of the DC input source. |
| Step 3 | Switch(config)# <code>end</code>                  | Exits configuration mode.                 |

The same configuration is applied to both power slots. For example, if you set the dc power input to 1000 W, the switch expects 1000 W as the external DC source both for slot 1 and slot 2 (if present) respectively.

The following example shows how to set the external DC power source to 1000 W.

```
Switch# configure terminal
Switch (config)# power dc input 1000
Switch (config)# end
Switch#
```

## Power Management for the Catalyst 4006 Switch

The power management feature for the Catalyst 4006 switch is designed to support an optimized Catalyst 4006 chassis with a limited module configuration on a reduced number of power supplies.

The Catalyst 4006 chassis supports only the 400 W AC, 400W DC, and 650 W DC power supplies and allows you to mix AC-input and DC-input power supplies in the same chassis. In systems with redundant power supplies, both power supplies should be of the same wattage. If you mix a 400 W power supply and a 650 W power supply, the switch performs as if there were two 400 W power supplies. For detailed information on supported power supply configurations for each chassis, refer to the *Catalyst 4000 Family Installation Guide*.

Catalyst 4000 family modules have different power requirements; thus, some switch configurations require more power than 1+1 redundancy mode (a single power supply) can provide. In those configurations, redundancy requires three power supplies. Redundant and nonredundant power configurations are discussed in the following sections.

The Catalyst 4500 series switch contains holding bays for up to three power supplies. You need two primary power supplies to operate a fully loaded Catalyst 4006 chassis. You can set the power redundancy to two primary plus one redundant power supply (2+1 redundancy mode) or to one primary plus one redundant power supply (1+1 redundancy mode). The 1+1 redundancy mode might not support a fully loaded chassis.

If your switch has only two power supplies and is in 2+1 redundancy mode (the default mode), there is no redundancy. You can create redundancy with only two power supplies by setting the power redundancy to operate in 1+1 redundancy mode (one primary plus one redundant power supply). However, 1+1 redundancy will not support all configurations.



The 1+1 redundancy mode is designed and optimized for the following hardware configurations:

- One Catalyst 4006 chassis with a WS-X4013 supervisor engine with two 400 W power supplies (in 1+1 redundancy mode) and four WS-X4148-RJ or WS-X4148-RJ21 modules
- One Catalyst 4006 chassis with a WS-X4013 supervisor engine with two 650 W power supplies (in 1+1 redundancy mode) and five WS-X4148-RJ or WS-X4148-RJ21 modules

Although other configurations are possible, we do not recommend that you use them without careful consideration of the power usage in the system. For example, other similar and possible configurations may consist of four modules that consume less power, and the total module power usage does not exceed the absolute maximum power usage for the system.

The supervisor engine uses 110 W, the fan box uses 25 W, and the backplane does not consume any power. The system total load for the modules + supervisor + fan cannot total more than the power supplied by the power supply. The 1+1 redundancy mode might not support a fully loaded chassis and, therefore, one slot of the chassis *might be empty*. An attempt to use five modules risks an oversubscription of available power.

If you opt to use the 1+1 redundancy mode, the type and number of modules supported are limited by the power available from a single power supply. To determine the power consumption for each module in your chassis, see the “Power Consumption of Chassis Components” section on page 33-15.

To choose a 1+1 redundancy configuration, you must change the system configuration from the default 2+1 redundancy mode to 1+1 redundancy mode by using the **power supplies required 1** command. The **power supplies required 1** command sets the power redundancy to 1+1 redundancy mode. In the 1+1 redundancy mode, the nonredundant power available to the system is the power of the single weakest power supply. The second power supply installed in your switch provides full redundancy.

## Limitations of the 1+1 Redundancy Mode

If you attempt to configure the system to operate in 1+1 redundancy mode, and you have more modules installed in the chassis than a single power supply can handle, the system displays the following error message:

```
Insufficient power supplies for the specified configuration
```

This message will also appear in the **show power** command output.

If you are already operating in 1+1 redundancy mode with a valid module configuration and you attempt to insert additional modules that require more power than the single power supply provides, the system immediately places the newly inserted module into reset mode and issues these error messages:

```
Module has been inserted
```

```
Insufficient power supplies operating
```

Additionally, if a chassis that has been operating in 1+1 redundancy mode with a valid module configuration is powered down, and you insert a module or change the module configuration inappropriately and power on the switch again, the module(s) in the chassis (at boot up) that require more power than is available, are placed into reset mode.

Both of these scenarios initiate the five-minute evaluation countdown timer. When this timer runs out, the system attempts to resolve this power usage limitation by evaluating the type and number of modules installed. The evaluation process may require several cycles to stabilize the chassis' power usage.

During the evaluation cycle, the modules are in effect removed and re-inserted, thus causing disruption of network connectivity; the switch reactivates only the modules it is able to support with the limited power available and leaves the remaining modules in reset mode. The supervisor engine always remains enabled. Modules placed in reset mode still consume some power. If the chassis module combination,

including the modules in reset, still require more power than is available, the five-minute evaluation countdown timer starts for another evaluation cycle, and additional modules are placed in reset mode until the power usage is stable.

If the power requirement of the active modules and with the modules in reset does not exceed the available power, the system is stable and no more evaluation cycles are run, until something again causes insufficient power usage. One or possibly two cycles are required to stabilize the system. If you configure the chassis correctly, the system will not enter the evaluation cycle.


**Note**

If you have all three power supplies installed and you still choose to operate in 1+1 redundancy mode but later add additional modules which exceed the power available, the five-minute evaluation timer starts again. The switch may require several evaluation cycles to stabilize the system. To correct this power situation caused by the additional modules, you can either remove the extra modules or change the power redundancy to 2+1 redundancy mode. If you choose to return to the 2+1 redundancy mode, each module held in reset mode is brought up one-by-one to an operational state.

A module in reset continues to draw power as long as it is installed in the chassis; however, the **show module** command output indicates that there is not enough power for the module.

A single power supply provides 400 W or 650 W. Two 400 W power supplies provide 750 W. Two 650 W power supplies supply only 750 W, and is a restriction on the power supply cooling capacity for the Catalyst 4006 switches.

If you mix a 400 W power supply and a 650 W power supply, the switch performs as if there were two 400 W power supplies. If you have one 400 W power supply and one 650 W power supply in 1+1 redundancy mode, and a second 650 W power supply set as the backup, the system performs as if there were 400 W. If the 400 W power supply fails, the backup 650 W power supply comes into service; however, the switch still has only 400 W available. You need to remove the failed 400 W power supply for the switch to make use of the 650 W available.

To compute the power requirements for your system and verify that your system has enough power, add up the power consumed by the supervisor engine module, the fan box, and the installed modules. (See the “Power Consumption of Chassis Components” section on page 33-15 for more information on the power consumption for the various components of your switch.) For 1+1 redundancy mode, verify that the total is less than 400 W or 650 W, depending on the power supplies installed in your switch. The following examples are provided to further explain the use of power supplies.

The following configuration requires a minimum of 395 W:

- WS-X4013 supervisor engine—110 W
- Four WS-X4148-RJ modules—65 W each (260 W total—the optimized module configuration)
- Fan box—25 W

This configuration requires less than the maximum that a single power supply can provide in 1+1 redundancy mode.

The following configuration requires more power than a single 400 W power supply can provide:

- WS-X4013 supervisor engine—110 W
- Two WS-X4148-RJ modules in slots 2 and 3—65 W each (130 W total)
- Two WS-X4448-GB-LX modules in slots 4 and 5—90 W each (180 W total)
- Fan box—25 W

This configuration requires 445 W and cannot be used in 1+1 redundancy mode for a 400 W power supply. A single 650 W power supply provides enough power for 1+1 redundancy mode for this configuration.

The following configuration requires more power than either a single 400 W or 650 W power supply can provide:

- WS-X4013 supervisor engine—110 W
- Five 48-port 100BASE-FX modules in slots 2 through 6—120 W each (600 W total)
- Fan box—25 W

This configuration requires 735 W and cannot be used in 1+1 redundancy mode for either a 400 W or 650 W power supply.

Remember, when considering the 1+1 redundancy mode, you must carefully plan the configuration of the module power usage of your chassis. An incorrect configuration will momentarily disrupt your system during the evaluation cycle. To avoid this disruption, carefully plan your configuration to ensure it is within the power limits, or return to the default 2+1 redundancy configuration by installing a third power supply in your switch and set the power redundancy to 2+1 redundancy mode.

Use the **power supplies required 2** command to set the power redundancy to the 2+1 redundancy mode.

## Setting the Power Redundancy Mode

To configure the power redundancy mode on a Catalyst 4006 switch, perform this task:

|        | Command                                                | Purpose                                                                        |
|--------|--------------------------------------------------------|--------------------------------------------------------------------------------|
| Step 1 | Switch# <b>configure terminal</b>                      | Enters configuration mode.                                                     |
| Step 2 | Switch(config)# <b>power supplies required {1   2}</b> | Sets the power redundancy mode.                                                |
| Step 3 | Switch(config)# <b>end</b>                             | Exits configuration mode.                                                      |
| Step 4 | Switch# <b>show power</b>                              | Verifies the power redundancy mode and the current power usage for the switch. |



### Note

The **power supplies required** command is not supported on a Catalyst 4500 series switch.

The default power redundancy mode is 2 (2+1) redundancy mode.

The following example shows how to set the power redundancy mode to 1 (1+1 redundancy mode).

```
Switch (config)# power supplies required 1
Switch (config)# end
Switch#
```

The following example shows how to display the current power status of system components and the power redundancy mode. The **Power supplies needed by system: 1** indicates that the switch is in 1+1 redundancy mode:

```
Switch# show power
Power
Supply Model No Type Status Fan Sensor Inline Status

PS1 WS-X4008 AC 400W good good n.a.
PS2 WS-X4008 AC 400W good good n.a.
PS3 none -- -- -- --
PEM none -- -- -- --

Power Supply Max Min Max Min Absolute
(Nos in Watts) Inline Inline System System Maximum

PS1 0 0 400 400 400
PS2 0 0 400 400 400
PS3 -- -- -- -- --

Power Summary
(in Watts) Available Used Remaining

System Power 400 260 140
Inline Power 0 0 0
Maximum Power 400 260 140
```

→ Power supplies needed by system :1

```
Mod Model Power Used Power Used
 (online) (in Reset)

1 WS-X4014 110 110
3 WS-X4306 35 30
6 WS-X4424-GB-RJ45 90 50
Switch#
```

The following example shows the **show module** command output for a system with inadequate power for all installed modules. The system does not have enough power for Module 5; the **Status** displays it as **PwrDeny**.

```
Switch# show module

Mod Ports Card Type Model Serial No.

1 2 1000BaseX (GBIC) Supervisor(active) WS-X4014 JAB054109GH
2 6 1000BaseX (GBIC) WS-X4306 00000110
3 18 1000BaseX (GBIC) WS-X4418 JAB025104WK
→ 5 0 Not enough power for module WS-X4148-FX-MT 00000000000
6 48 10/100BaseTX (RJ45) WS-X4148 JAB023402RP

M MAC addresses Hw Fw Sw Status

1 005c.9d1a.f9d0 to 005c.9d1a.f9df 0.5 12.1(11br)EW 12.1(20020313:00 Ok
2 0010.7bab.9920 to 0010.7bab.9925 0.2 Ok
3 0050.7356.2b36 to 0050.7356.2b47 1.0 Ok
→ 5 0001.64fe.a930 to 0001.64fe.a95f 0.0 PwrDeny
6 0050.0f10.28b0 to 0050.0f10.28df 1.0 Ok
Switch#
```

## Power Consumption of Chassis Components

For power consumption of common Catalyst 4000 family modules, see Table 33-4.

Enter the **show power** command to display the current power redundancy and the current system power usage.

**Table 33-4 Power Consumption for Catalyst 4000 Family Components**

| Module                                                                                           | Power Consumed During Operation (W) | Power Consumed in Reset Mode (W) |
|--------------------------------------------------------------------------------------------------|-------------------------------------|----------------------------------|
| Supervisor Engine II-Plus                                                                        | 110                                 | 110                              |
| Supervisor Engine III                                                                            | 110                                 | 110                              |
| Supervisor Engine IV                                                                             | 145                                 | 145                              |
| Catalyst 4006 fan box                                                                            | 25                                  | 25                               |
| Catalyst 4503 fan box                                                                            | 30                                  | 30                               |
| Catalyst 4506 and 4507 fan box                                                                   | 50                                  | 50                               |
| Catalyst 4006 switch backplane                                                                   | 0                                   | 0                                |
| Catalyst 4503 switch backplane                                                                   | 10                                  | 10                               |
| Catalyst 4506 switch backplane                                                                   | 10                                  | 10                               |
| Catalyst 4507 switch backplane                                                                   | 40                                  | 40                               |
| 6-port 1000BASE-X (GBIC) Gigabit Ethernet WS-X4306-GB                                            | 35                                  | 30                               |
| 32-port 10/100 Fast Ethernet RJ-45 WS-X4232-RJ-XX                                                | 50                                  | 35                               |
| 24-port 100BASE-FX Fast Ethernet switching module WS-X4124-FX-MT                                 | 90                                  | 75                               |
| 32-port 10/100 Fast Ethernet RJ-45, plus 2-port 1000BASE-X (GBIC) Gigabit Ethernet WS-4232-GB-RJ | 55                                  | 35                               |
| 48-port 100BASE-FX Fast Ethernet switching module WS-4148-FX-MT                                  | 120                                 | 10                               |
| 18-port server switching 1000BASE-X (GBIC) Gigabit Ethernet WS-4418-GB                           | 80                                  | 50                               |
| Catalyst 4006 Backplane Channel Module WS-X4019                                                  | 10                                  | 10                               |
| 48-port 10/100 Fast Ethernet RJ-45 WS-X4148-RJ                                                   | 65                                  | 40                               |
| 12-port 1000BASE-T Gigabit Ethernet, plus 2-port 1000BASE-X (GBIC) Gigabit Ethernet WS-X4416     | 110                                 | 70                               |
| 24-port 1000BASE-X Gigabit Ethernet WS-X4424-GB-RJ45                                             | 90                                  | 50                               |

**Table 33-4 Power Consumption for Catalyst 4000 Family Components (continued)**

| Module                                                                | Power Consumed During Operation (W) | Power Consumed in Reset Mode (W) |
|-----------------------------------------------------------------------|-------------------------------------|----------------------------------|
| 48-port 1000BASE-X Gigabit Ethernet<br>WS-X4448-GB-RJ45               | 120                                 | 72                               |
| 48-port 1000BASE-X Gigabit Ethernet<br>WS-X4448-GB-LX                 | 90                                  | 50                               |
| 48-port Telco 10/100BASE-TX switching module<br>WS-X4148-RJ21         | 65                                  | 40                               |
| 48-port inline power 10/100BASE-TX switching module<br>WS-X4148-RJ45V | 60                                  | 50                               |
| 4-port MT-RJ Uplink module<br>WS-U4504-FX-MT                          | 10                                  | 10                               |
| 48-port 10/100/1000BASE-T switching module<br>WS-X4548-GB-RJ45        | 58                                  | 15                               |

## Configuring Inline Power

The Catalyst 4006 switch and Catalyst 4500 series switches can sense if a powered device is connected to an inline power module. The Catalyst 4006 switch and Catalyst 4500 series switches can supply inline power to the powered device if there is no power on the circuit. The powered device can also be connected to an AC power source and supply its own power to the voice circuit. If there is power on the circuit, the switch does not supply it.



### Note

A powered device is any device connected to the switch that requires external power or can utilize inline power. For example, an access point or IP phone.

## Power Management Modes

If your switch has a module capable of providing inline power to end stations, you can set each interface on the module to automatically detect and apply inline power if the end station requires power.

The Catalyst 4500 series switch has three inline power modes:

- **auto**—The supervisor engine directs the switching module to power up the interface *only* if the switching module discovers the phone and the switch has enough power. You can specify the maximum wattage that is allowed on the interface. If you do not specify a wattage, then the switch will deliver no more than the hardware-supported maximum value.
- **static**—The supervisor engine directs the switching module to power up the interface to the wattage you specify *only* if the switching module discovers the phone. You can specify the maximum wattage that is allowed on the interface. If you do not specify a wattage, then the switch allows the hardware-supported maximum value. The maximum wattage, whether determined by the switch or specified by you, is preallocated to the interface. If the switch does not have enough power for the allocation, the command will fail.

- **never**—The supervisor engine does not direct the switching module to power up the interface even if an unpowered phone is connected.

The switch allocates inline power to the interfaces configured to **static** mode before it allocates power to the interfaces configured to **auto** mode. In the event of insufficient inline power due to a partial power supply failure, interfaces configured to **auto** mode are shutdown before interfaces configured to **static** mode.

To set an interface to automatically detect an end station requiring power and apply the inline power, perform this task:

|        | Command                                                                                                                                                                           | Purpose                                                                                                                                                                                                                                                                                                                                                                            |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch(config)# <b>interface</b> { <b>fastethernet</b>   <b>gigabitethernet</b> } <i>slot/port</i>                                                                                | Selects the interface to configure.                                                                                                                                                                                                                                                                                                                                                |
| Step 2 | Switch(config-if)# <b>power inline</b> { <b>auto</b> [ <b>max</b> [ <i>milli-watts</i> ]   <b>never</b>   <b>static</b> [ <b>max</b> [ <i>milli-watts</i> ]   <b>allocation</b> ] | Sets the interface to automatically detect if the end device requires power and apply inline power to the end device if necessary. If necessary, you can use the <b>max</b> keyword to specify the maximum wattage allowed on the interface (2000 to 15400 milliwatts).<br><br>Use the <b>never</b> keyword to disable detection and power for the inline-power capable interface. |
| Step 3 | Switch(config-if)# <b>end</b>                                                                                                                                                     | Exits configuration mode.                                                                                                                                                                                                                                                                                                                                                          |
| Step 4 | Switch# <b>show power inline</b> { <b>fastethernet</b>   <b>gigabitethernet</b> } <i>slot/port</i>                                                                                | Displays the inline power state for the switch.                                                                                                                                                                                                                                                                                                                                    |

If you set a non-inline-power-capable interface to automatically detect and apply power, an error message indicates that the configuration is not valid.

The following example shows how to set the Fast Ethernet interface 4/1 to automatically detect inline power and send power through that interface:

```
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
```

This example shows how to verify the inline power configuration for the Fast Ethernet interface 5/8:

```
Switch# show power inline fastethernet 4/1
Available:665(w) Used:663(w) Remaining:2(w)
Interface Admin Oper Power Device Class
 (Watts)

Fa4/1 auto on 5.0 Cisco IP Phone 7960 n/a
Interface AdminPowerMax AdminAllocation
 (milli-watts) (milli-watts)

Fa4/1 15400 15400
Switch#
```

The following example shows to configure an interface so that it never supplies power through the interface:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 5/2
Switch(config-if)# power inline never
Switch(config-if)# end
Switch#
```

## Configuring Power Allocation for an Interface

By default, the switch allocates 15.4 W to an interface when it discovers a powered device on the interface. This number automatically adjusts downward to the amount the powered device actually requires, when the switch receives a CDP packet from the powered device. Normally, this automatic method works well, and no further configuration is required. However, if CDP is disabled or you want the switch to allocate less power to a powered device than the amount requested by the powered device (not recommended), you can specify the power allocation for the entire switch or by interface.

You can change the power allocation for the entire switch by performing this procedure in configuration mode:

|        | Command                                                          | Purpose                                                                                                                                                                                   |
|--------|------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch(config)# [no] power inline allocation default milli-watts | Sets the inline power allocation (in milliwatts) for the switch. The power allocation can range from 2000 to 15,200.<br><br>Use the <b>no</b> keyword to disable inline power allocation. |
| Step 2 | Switch(config)# end                                              | Exits configuration mode.                                                                                                                                                                 |
| Step 3 | Switch# show power inline allocation default                     | Displays the inline power state for the switch.                                                                                                                                           |

The following example shows how to set the inline power allocation to 5000 milliwatts.

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# power inline allocation default 5000
Switch(config)# end
Switch#
```

This example shows how to verify the inline power allocation.

```
Switch# show power inline allocation default
Default inline power allocation : 5000 mW
Switch#
```



You can change the power allocation for a single interface by performing this procedure in interface configuration mode:

|        | Command                                                                                                       | Purpose                                                                                                                                                                                      |
|--------|---------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch(config)# <b>interface</b> { <b>fastethernet</b>   <b>gigabitethernet</b> } <i>slot/port</i>            | Selects the interface to configure.                                                                                                                                                          |
| Step 2 | Switch(config-if)# [no] <b>power inline allocation</b> <i>milli-watts</i>                                     | Sets the inline power allocation (in milliwatts) for the interface. The power allocation can range from 2000 to 15,200.<br><br>Use the <b>no</b> keyword to disable inline power allocation. |
| Step 3 | Switch(config-if)# <b>end</b>                                                                                 | Exits configuration mode.                                                                                                                                                                    |
| Step 4 | Switch# <b>show power inline allocation</b> { <b>fastethernet</b>   <b>gigabitethernet</b> } <i>slot/port</i> | Displays the inline power state for the interface.                                                                                                                                           |

The following example shows how to set the inline power allocation to 5000 milliwatts for Fast Ethernet interface 4/1:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 5/2
Switch(config-if)# power inline allocation 5000
Switch(config-if)# end
Switch#
```

This example shows how to verify the inline power allocation.

```
Switch# show power inline fastethernet 4/1
Available:665(w) Used:663(w) Remaining:2(w)
Interface Admin Oper Power Device Class
 (Watts)

Fa4/1 auto on 5.0 Cisco IP Phone 7960 n/a
Interface AdminPowerMax AdminAllocation
 (milli-watts) (milli-watts)

Fa4/1 15400 5000
Switch#
```

## Displaying the Operational Status for an Interface

Each interface has an operational status which reflects the inline power status for an interface. The operational status for an interface is defined as one of the following:

- on—Power is supplied by the port.
- off—Power is not supplied by the port. 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 **show power inline** command displays as n/a.
- Power-deny—The supervisor engine does not have enough power to allocate to the port, or the power that is configured for the port is less than the power required by the port; power is not being supplied by the port.

- **err-disable**—The port is unable to provide power to the connected device that is configured in **Static** mode.
- **faulty**—The port failed diagnostics tests.

You can use the **show inline power** command to view the operational status for an interface.

This example shows how to display the operational status for all interfaces on module 4:

```
Switch# show power inline module 4
Available:665(w) Used:663(w) Remaining:2(w)
Interface Admin Oper Power Device Class
 (Watts)

Fa4/1 auto on 5.0 Cisco IP Phone 7960 n/a
Fa4/2 static on 7.0 Cisco IP Phone 7910 n/a
Fa4/3 auto off 0 n/a n/a
Fa4/4 static off 7.0 n/a n/a
Fa4/5 static off 7.0 n/a n/a
Fa4/6 static off 7.0 n/a n/a
Switch#
```

This example shows how to display the operational status for Fast Ethernet interface 4/1:

```
Switch#show power inline fa4/1
Available:665(w) Used:663(w) Remaining:2(w)
Interface Admin Oper Power Device Class
 (Watts)

Fa4/1 auto on 5.0 Cisco IP Phone 7960 n/a
Interface AdminPowerMax AdminAllocation
 (milli-watts) (milli-watts)

Fa4/1 15400 5000
Switch#
```



# Configuring Supervisor Engine Redundancy on the Catalyst 4507R Switch

This chapter describes how to configure supervisor engine redundancy on the Catalyst 4507R switch.

This chapter consists of the following major sections:

- Overview of Supervisor Engine Redundancy, page 34-1
- Understanding Supervisor Engine Redundancy, page 34-2
- Supervisor Engine Redundancy Guidelines and Restrictions, page 34-3
- Configuring Supervisor Engine Redundancy, page 34-4
- Synchronizing the Supervisor Engine Configurations, page 34-4
- Performing a Software Upgrade, page 34-5
- Copying Files to the Standby Supervisor Engine, page 34-7



## Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference* and related publications at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/index.htm>

## Overview of Supervisor Engine Redundancy

Catalyst 4500 series switches allow a standby supervisor engine to take over if the primary supervisor engine fails, thereby allowing the switch to resume operation quickly and efficiently in the event of a supervisor engine failure. This capability is called supervisor engine redundancy. In software, this capability is enabled by route processor redundancy (RPR) operating mode. RPR is a generic term for the feature.

The standby supervisor engine runs in RPR mode. When RPR mode is used, the standby supervisor engine partially boots and keeps synchronized copies of the active configuration, which shortens the time needed to bring up the standby supervisor engine and have it start handling traffic from 1.5 minutes (for a cold boot on the standby) to 30 seconds (to finish the boot and re establish links).

In addition to the reduced switchover time, supervisor engine redundancy supports the following:

- Online insertion and removal (OIR) of the standby supervisor engine.
- Software upgrade (See the “Performing a Software Upgrade” section on page 34-5)
- Auto-startup and bootvar synchronization

- Hardware signals that detect and decide the active or standby status of supervisor engines
- Clock synchronization every 60 seconds from the active to the standby supervisor engine
- Automatic switchover to the standby supervisor engine if the active supervisor engine ever fails

When the switch is powered on, the two supervisor engines automatically determine between themselves which will serve as the primary and which will be the standby. Usually, the supervisor engine that boots first, either in slot 1 or 2, becomes the active supervisor engine.

A switchover will occur when one or more of the following events take place:

- The active supervisor engine fails or is removed
- A user forces a switchover
- A user reloads the active supervisor engine
- A core dump occurs

**Note**

In a switchover, there is a disruption of traffic because some address states are lost and then restored after they are dynamically redetermined.

## Understanding Supervisor Engine Redundancy

These sections describe supervisor engine redundancy:

- Operation, page 34-2
- Supervisor Engine Synchronization, page 34-3

### Operation

With supervisor engine redundancy enabled, the standby supervisor engine automatically takes over for the primary supervisor engine if the active supervisor engine fails or if a manual switchover is performed. The standby supervisor engine has already been automatically initialized and configured, shortening the switchover time. Supervisor engine redundancy provides the following additional benefits:

- Online insertion and removal (OIR) of the standby supervisor engine  
Supervisor engine redundancy allows OIR of the standby supervisor engine for maintenance. When the standby supervisor engine is inserted, the active supervisor engine detects its presence and begins to transition the standby supervisor engine to the fully initialized state.
- Software upgrade  
To minimize software upgrade and downgrade times, you can preload the standby supervisor engine with the software version you want to upgrade or downgrade to and then configure the system to switch over to the standby supervisor engine.

Supervisor engine redundancy also supports manual user-initiated switchover. You can initiate a switchover with the **redundancy force-switchover** command.

## Supervisor Engine Synchronization

Because the standby supervisor engine is not fully initialized, it interacts with the active supervisor engine only to receive configuration changes as they occur, keeping the configuration information on both supervisor engines identical. This synchronization of the startup configuration file is enabled by default in RPR mode. You cannot enter CLI commands on the standby supervisor engine.

When a standby supervisor engine is running in RPR mode, the following operations trigger synchronization of the configuration information:

- When a standby supervisor engine first comes online, the configuration information is synchronized from the active supervisor engine to the standby supervisor engine. This synchronization overwrites any existing startup configuration file on the standby supervisor engine.
- If the **auto-synch** command is enabled, changes to the startup configuration on the active supervisor engine are automatically synchronized on the standby supervisor.

## Supervisor Engine Redundancy Guidelines and Restrictions

The following guidelines and restrictions apply to supervisor engine redundancy:

- Supervisor engine redundancy does not provide supervisor engine load balancing or any other feature requiring two active supervisor engines. Only one supervisor engine is active. Network services are disrupted until the standby supervisor engine takes over and the switch recovers.
- The two Gigabit Ethernet interfaces available in RPR mode are the first Gigabit Ethernet ports on each supervisor. That is, only Gig 1/1 and Gig 2/1 are available. The other two ports, Gig 1/2 and Gig 2/2, are not available.
- With supervisor engine redundancy enabled, the supervisor engines may run different versions of the Cisco IOS software, if both are Cisco IOS Release 12.1(12c)EW or later releases.
- The Forwarding Information Base (FIB) tables are cleared on a switchover. As a result, routed traffic is interrupted until route tables reconverge.
- Static IP routes are maintained across a switchover because they are configured from entries in the configuration file.
- Information about dynamic states maintained on the active supervisor engine is not synchronized to the standby supervisor engine and is lost on switchover. Dynamic state information (such as border gateway protocol [BGP] session information) is lost at switchover.
- The Catalyst 4507R switch is the only Catalyst 4500 series switch that supports supervisor engine redundancy.
- The active and standby supervisor engines must be in slots 1 and 2.
- Both the active and standby supervisor engines must be Supervisor Engine IV modules. Earlier versions are not supported.
- Each supervisor engine must have the resources to run the switch on its own, which means all supervisor engine resources are duplicated. In other words, each supervisor engine has its own Flash device and console port connections.
- Make separate console connections to each supervisor engine. Do not connect a Y cable to the console ports.
- You must set the configuration register in the startup-config to autoboot. (See the “Modifying the Boot Field” section on page 3-15.)

**Note**

There is no support for booting from the network.

If these requirements are met, the switch functions in RPR mode by default.

## Configuring Supervisor Engine Redundancy

Supervisor engine redundancy is configured by default when a second supervisor engine is detected.

This example shows how to display the redundancy state:

```
Switch#show redundancy states
 my state = 13 -ACTIVE
 peer state = 4 -STANDBY COLD
 Mode = Duplex
 Unit = Primary
 Unit ID = 1

Redundancy Mode (Operational) = RPR
Redundancy Mode (Configured) = RPR
 Split Mode = Disabled
 Manual Swact = Enabled
 Communications = Up

 client count = 4
 client_notification_TMR = 30000 milliseconds
 keep_alive TMR = 4000 milliseconds
 keep_alive count = 1
 keep_alive threshold = 7
 RF debug mask = 0x0
Switch#
```

## Synchronizing the Supervisor Engine Configurations

During normal operation, the startup-config, boot variables, config-registers, and VLAN database configuration are synchronized by default between the two supervisor engines. In a switchover, the new active supervisor engine uses the current configuration.

To manually synchronize the configurations used by the two supervisor engines, perform this task on the active supervisor engine:

|               | Command                                                                                       | Purpose                                  |
|---------------|-----------------------------------------------------------------------------------------------|------------------------------------------|
| <b>Step 1</b> | Switch(config)# <b>redundancy</b>                                                             | Enters redundancy configuration mode.    |
| <b>Step 2</b> | Switch(config-red)# <b>main-cpu</b>                                                           | Enters main-cpu configuration submode.   |
| <b>Step 3</b> | Switch(config-r-mc)# <b>auto-sync {startup-config   config-register   bootvar   standard}</b> | Synchronizes the configuration elements. |

|        | Command                                           | Purpose                                                                                                                                                                                                 |
|--------|---------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 4 | Switch(config-r-mc)# <b>end</b>                   | Returns to privileged EXEC mode.                                                                                                                                                                        |
| Step 5 | Switch# <b>copy running-config startup-config</b> | Forces a manual synchronization of the configuration files in NVRAM.<br><br><b>Note</b> This step is not required to synchronize the running configuration file in dynamic random-access memory (DRAM). |

**Note**

The **auto-sync** command controls the synchronization of the CONFIG-REG, BOOTVAR and STARTUP/PRIVATE configuration files only. The calendar and **vlan** database files are always synchronized when they change.

This example shows how to reenable the default automatic synchronization feature using the **auto-sync standard** command to synchronize the **startup-config** and **config-register** configuration of the active supervisor engine with the standby supervisor engine: Updates for the boot variables are automatic and cannot be disabled.

```
Switch(config)# redundancy
Switch(config-red)# main-cpu
Switch(config-r-mc)# auto-sync standard
Switch(config-r-mc)# end
Switch# copy running-config startup-config
```

**Note**

To manually synchronize only individual elements of the standard auto-sync configuration, disable the default automatic synchronization feature.

This example shows how to disable default automatic synchronization and allow only automatic synchronization of the config-registers of the active supervisor engine to the standby supervisor engine while disallowing synchronization of the startup configuration:

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

## Performing a Software Upgrade

The software upgrade procedure supported by supervisor engine redundancy allows you to upgrade the Cisco IOS software image on the supervisor engines without reloading the system.

To perform a software upgrade, perform this task:

|               | Command                                                                                                                                                                                                                                                                                                            | Purpose                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <pre>Switch# copy source_device:source_filename slot0:target_filename  Or:  Switch# copy source_device:source_filename bootflash:target_filename  Or:  Switch# copy source_device:source_filename slaveslot0:target_filename  Or:  Switch# copy source_device:source_filename slavebootflash:target_filename</pre> | Copies the new Cisco IOS software image to bootflash on both supervisor engines.                                                                                                                                                                                                                                                                                                                 |
| <b>Step 2</b> | <pre>Switch# config terminal Switch(config)# config-register 0x2 Switch(config)# boot system flash device:file_name</pre>                                                                                                                                                                                          | Configures the supervisor engines to boot the new image.                                                                                                                                                                                                                                                                                                                                         |
| <b>Step 3</b> | <pre>Switch# copy running-config start-config</pre>                                                                                                                                                                                                                                                                | Saves the configuration.                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Step 4</b> | <pre>Switch# redundancy reload peer</pre>                                                                                                                                                                                                                                                                          | <p>Reloads the standby supervisor engine and bring it back online (running the new version of the Cisco IOS software).</p> <p><b>Note</b> Before reloading the standby supervisor engine, make sure you wait long enough to ensure that all configuration synchronization changes have completed.</p>                                                                                            |
| <b>Step 5</b> | <pre>Switch# redundancy force-switchover</pre>                                                                                                                                                                                                                                                                     | <p>Conducts a manual switchover to the standby supervisor engine. The standby supervisor engine becomes the new active supervisor engine running the new Cisco IOS software image. The modules reload and the module software downloads from the new active supervisor engine.</p> <p>The old active supervisor engine reboots with the new image and becomes the standby supervisor engine.</p> |

This example shows how to perform a software upgrade:

```
Switch# config terminal
Switch(config)# config-register 0x2
Switch(config)# boot system flash slot0: cat4000-is-mz.121-11b.EW
Switch# copy running-config start-config
Switch# hw-module reset
Switch# redundancy force-switchover
Switch#
```



## Copying Files to the Standby Supervisor Engine

If you want to manually copy a file from the active supervisor engine to the **slot0:** device on the standby supervisor engine, use the following command:

```
Switch# copy source_device:source_filename slaveslot0:target_filename
```

Use the following command to copy a file to the **bootflash:** device on a standby supervisor engine:

```
Switch# copy source_device:source_filename slavebootflash:target_filename
```





## Configuring Voice Interfaces

This chapter describes how to configure voice interfaces for the Catalyst 4500 series switches.

This chapter consists of these major sections:

- Overview of Voice Interfaces, page 35-1
- Configuring a Port to Connect to a Cisco 7960 IP Phone, page 35-2
- Configuring Voice Ports for Voice and Data Traffic, page 35-2
- Overriding the CoS Priority of Incoming Frames, page 35-3
- Configuring Inline Power, page 35-4



**Note**

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference* and related publications at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/index.htm>

## Overview of Voice Interfaces

Catalyst 4500 series switches can connect to a Cisco 7960 IP Phone and carry IP voice traffic. If necessary, the switch can supply electrical power to the circuit connecting it to the Cisco 7960 IP Phone.

Because the sound quality of an IP telephone call can deteriorate if the data is unevenly sent, the switch uses quality of service (QoS) based on IEEE 802.1p class of service (CoS). QoS uses classification and scheduling to transmit network traffic from the switch in a predictable manner. See Chapter 29, “Configuring QoS” for more information on QoS.

You can configure the Cisco 7960 IP Phone to forward traffic with an 802.1p priority. You can use the CLI to configure a Catalyst 4500 series switch to honor or ignore a traffic priority assigned by a Cisco 7960 IP Phone.

The Cisco 7960 IP Phone contains an integrated three-port 10/100 switch. The ports are dedicated connections as described below:

- Port 1 connects to the Catalyst 4500 series switch or other device that supports voice-over-IP.
- Port 2 is an internal 10/100 interface that carries the phone traffic.
- Port 3 connects to a PC or other device.

Figure 35-1 shows one way to configure a Cisco 7960 IP Phone.

**Figure 35-1 Cisco 7960 IP Phone Connected to a Catalyst 4000 Family Switch**



## Configuring a Port to Connect to a Cisco 7690 IP Phone

Because a Cisco 7960 IP Phone also supports connection to a PC or another device, an interface connecting a Catalyst 4500 series switch to a Cisco 7960 IP Phone can carry a mix of voice and data traffic.

There are three configurations for a port connected to a Cisco 7960 IP Phone:

- All traffic is transmitted according to the default COS priority of the port. This is the default.
- Voice traffic is given a higher priority by the phone (CoS priority is always 5), and all traffic is in the same VLAN.
- Voice and data traffic are carried on separate VLANs.

To configure a port to instruct the phone to give voice traffic a higher priority and to forward all traffic through the 802.1Q native VLAN, perform this task:

|               | Command                                                                                    | Purpose                                                                                                                             |
|---------------|--------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Switch# <b>configure terminal</b>                                                          | Enters configuration mode.                                                                                                          |
| <b>Step 2</b> | Switch(config)# <b>interface</b> {fastethernet   gigabitethernet} slot/port                | Specifies the interface to configure.                                                                                               |
| <b>Step 3</b> | Switch(config-if)# <b>switchport voice vlan dot1p</b>                                      | Instructs the switch to use 802.1p priority tagging for voice traffic and to use VLAN 1 (default native VLAN) to carry all traffic. |
| <b>Step 4</b> | Switch(config-if)# <b>end</b>                                                              | Returns to privileged EXEC mode.                                                                                                    |
| <b>Step 5</b> | Switch# <b>show interface</b> {fastethernet   gigabitethernet} slot/port <b>switchport</b> | Verifies the port configuration.                                                                                                    |

## Configuring Voice Ports for Voice and Data Traffic

Because voice and data traffic can travel through the same voice port, you should specify a different VLAN for each type of traffic. You can configure a switch port to forward voice and data traffic on different VLANs.

To configure a port to receive voice and data from a Cisco IP Phone on different VLANs, perform this task:

|        | Command                                                                                                           | Purpose                                                                                                                                                   |
|--------|-------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch# <b>configure terminal</b>                                                                                 | Enters configuration mode.                                                                                                                                |
| Step 2 | Switch(config)# <b>interface</b> { <b>fastethernet</b>   <b>gigabitethernet</b> } <i>slot/port</i>                | Specifies the interface to configure.                                                                                                                     |
| Step 3 | Switch(config-if)# <b>switchport voice vlan</b> <i>vlan_num</i>                                                   | Instructs the Cisco IP Phone to forward all voice traffic through a specified VLAN. The Cisco IP Phone forwards the traffic with an 802.1p priority of 5. |
| Step 4 | Switch(config-if)# <b>end</b>                                                                                     | Returns to privileged EXEC mode.                                                                                                                          |
| Step 5 | Switch# <b>show interface</b> { <b>fastethernet</b>   <b>gigabitethernet</b> } <i>slot/port</i> <b>switchport</b> | Verifies the configuration.                                                                                                                               |

In the following example, VLAN 1 carries data traffic, and VLAN 2 carries voice traffic. In this configuration, you must connect all Cisco IP Phones and other voice-related devices to switch ports that belong to VLAN 2.

```
Switch# configure terminal
Switch(config)# interface fastethernet 2/5
Switch(config-if)# switchport voice vlan 2
switchport voice vlan 2
Switch(config-if)# end
Switch# show interface fastethernet 2/5 switchport
show interface fastethernet 2/5 switchport
Name: Fa2/5
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)
Voice VLAN: 2 ((Inactive))
Appliance trust: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Switch#
```

## Overriding the CoS Priority of Incoming Frames

A PC or another data device can connect to a Cisco 7960 IP Phone port. The PC can generate packets with an assigned CoS value. You can also use the switch CLI to override the priority of frames arriving on the phone port from connected devices, and you can set the phone port to accept (trust) the priority of frames arriving on the port.

To override the CoS priority setting received from the non-voice port on the Cisco 7960 IP Phone, perform this task:

|        | Command                                                                                                           | Purpose                                                                                                                                                                                                                  |
|--------|-------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Switch# <b>configure terminal</b>                                                                                 | Enters configuration mode.                                                                                                                                                                                               |
| Step 2 | Switch(config)# <b>interface</b> { <b>fastethernet</b>   <b>gigabitethernet</b> } <i>slot/port</i>                | Specifies the interface to configure.                                                                                                                                                                                    |
| Step 3 | Switch(config-if)# [ <b>no</b> ] <b>qos trust extend cos 3</b>                                                    | Sets the phone port to override the priority received from the PC or the attached device and forward the received data with a priority of 3.<br><br>Use the <b>no</b> keyword to return the port to its default setting. |
| Step 4 | Switch(config-if)# <b>end</b>                                                                                     | Returns to privileged EXEC mode.                                                                                                                                                                                         |
| Step 5 | Switch# <b>show interface</b> { <b>fastethernet</b>   <b>gigabitethernet</b> } <i>slot/port</i> <b>switchport</b> | Verifies the change.                                                                                                                                                                                                     |

## Configuring Inline Power

The Catalyst 4500 series switch senses if it is connected to a Cisco 7960 IP Phone. The Catalyst 4500 series switch can supply inline power to the Cisco 7960 IP Phone if there is no power on the circuit. The Cisco 7960 IP Phone can also be connected to an AC power source and supply its own power to the voice circuit. If there is power on the circuit, the switch does not supply it.

You can configure the switch not to supply power to the Cisco 7960 IP Phone and to disable the detection mechanism. See the “Configuring Inline Power” section on page 33-16 for the CLI commands that you can use to supply inline power to a Cisco 7960 IP Phone.



# Acronyms

Table A-1 defines the acronyms used in this publication.

**Table A-1** *Acronyms*

| Acronym | Expansion                                         |
|---------|---------------------------------------------------|
| ACE     | access control entry                              |
| ACL     | access control list                               |
| AFI     | authority and format identifier                   |
| Agport  | aggregation port                                  |
| ALPS    | Airline Protocol Support                          |
| AMP     | Active Monitor Present                            |
| APaRT   | Automated Packet Recognition and Translation      |
| ARP     | Address Resolution Protocol                       |
| AV      | attribute value                                   |
| AVVID   | Architecture for Voice, Video and Integrated Data |
| BDD     | binary decision diagrams                          |
| BECN    | backward explicit congestion notification         |
| 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                    |
| CAM     | content-addressable memory                        |
| CAR     | committed access rate                             |
| CCA     | circuit card assembly                             |
| CDP     | Cisco Discovery Protocol                          |
| CEF     | Cisco Express Forwarding                          |
| CGMP    | Cisco Group Management Protocol                   |

**Table A-1** *Acronyms (continued)*

| <b>Acronym</b> | <b>Expansion</b>                                  |
|----------------|---------------------------------------------------|
| CHAP           | Challenge Handshake Authentication Protocol       |
| CIR            | committed information rate                        |
| CIST           | Common and Internal Spanning Tree                 |
| 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                              |
| CUDD           | University of Colorado Decision Diagram           |
| DBL            | Dynamic Buffer Limiting                           |
| DCC            | Data Country Code                                 |
| dCEF           | distributed Cisco Express Forwarding              |
| DDR            | dial-on-demand routing                            |
| DE             | discard eligibility                               |
| DEC            | Digital Equipment Corporation                     |
| DFI            | Domain-Specific Part Format Identifier            |
| DFP            | Dynamic Feedback Protocol                         |
| DISL           | Dynamic Inter-Switch Link                         |
| DLC            | Data Link Control                                 |
| DLSw           | Data Link Switching                               |
| DMP            | data movement processor                           |
| DNS            | Domain Name System                                |
| DoD            | Department of Defense                             |
| DOS            | denial of service                                 |
| DRAM           | dynamic RAM                                       |
| DSAP           | destination service access point                  |
| DSCP           | differentiated services code point                |
| DSPU           | downstream SNA Physical Units                     |
| DTP            | Dynamic Trunking Protocol                         |
| DTR            | data terminal ready                               |
| DXI            | data exchange interface                           |



**Table A-1** *Acronyms (continued)*

| <b>Acronym</b> | <b>Expansion</b>                                                        |
|----------------|-------------------------------------------------------------------------|
| EAP            | Extensible Authentication Protocol                                      |
| EARL           | Enhanced Address Recognition Logic                                      |
| EEPROM         | electrically erasable programmable read-only memory                     |
| EHSA           | enhanced high system availability                                       |
| EIA            | Electronic Industries Association                                       |
| ELAN           | Emulated Local Area Network                                             |
| EOBC           | Ethernet out-of-band channel                                            |
| ESI            | end-system identifier                                                   |
| 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                                         |
| HSRP           | Hot Standby Routing 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                       |
| IFS            | IOS File System                                                         |
| IGMP           | Internet Group Management Protocol                                      |
| IGRP           | Interior Gateway Routing Protocol                                       |
| ILMI           | Integrated Local Management Interface                                   |
| IP             | Internet Protocol                                                       |
| IPC            | interprocessor communication                                            |
| IPX            | Internetwork Packet Exchange                                            |
| IS-IS          | Intermediate System-to-Intermediate System Intradomain Routing Protocol |
| ISL            | Inter-Switch Link                                                       |
| ISO            | International Organization of Standardization                           |
| LAN            | local area network                                                      |
| LANE           | LAN Emulation                                                           |
| LAPB           | Link Access Procedure, Balanced                                         |
| LDA            | Local Director Acceleration                                             |

**Table A-1** *Acronyms (continued)*

| <b>Acronym</b> | <b>Expansion</b>                     |
|----------------|--------------------------------------|
| 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                   |
| MAC            | Media Access Control                 |
| MACL           | MAC Access Control                   |
| MD5            | Message Digest 5                     |
| MFD            | multicast fast drop                  |
| 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                   |
| MLSE           | maintenance loops signaling entity   |
| MRM            | multicast routing monitor            |
| MSDP           | Multicast Source Discovery Protocol  |
| MST            | Multiple Spanning Tree               |
| MSTI           | MST instance                         |
| MTU            | maximum transmission unit            |
| MVAP           | multiple VLAN access port            |
| NBP            | Name Binding Protocol                |
| NCIA           | Native Client Interface Architecture |
| NDE            | NetFlow Data Export                  |
| NET            | network entity title                 |
| NetBIOS        | Network Basic Input/Output System    |
| NFFC           | NetFlow Feature Card                 |
| NMP            | Network Management Processor         |
| NSAP           | network service access point         |
| NTP            | Network Time Protocol                |
| NVRAM          | nonvolatile RAM                      |

**Table A-1** *Acronyms (continued)*

| <b>Acronym</b> | <b>Expansion</b>                           |
|----------------|--------------------------------------------|
| OAM            | Operation, Administration, and Maintenance |
| ODM            | order dependent merge                      |
| OSI            | Open System Interconnection                |
| OSPF           | open shortest path first                   |
| PACL           | Port Access Control List                   |
| PAE            | port access entity                         |
| PAgP           | Port Aggregation Protocol                  |
| PBD            | packet buffer daughterboard                |
| PBR            | Policy Based Routing                       |
| PC             | Personal Computer                          |
| PCM            | pulse code modulation                      |
| PCR            | peak cell rate                             |
| PDP            | policy decision point                      |
| PDU            | protocol data unit                         |
| PEP            | policy enforcement point                   |
| PGM            | Pragmatic General Multicast                |
| PHY            | physical sublayer                          |
| PIB            | policy information base                    |
| PIM            | Protocol Independent Multicast             |
| PPP            | Point-to-Point Protocol                    |
| PRID           | Policy Rule Identifiers                    |
| PVST+          | Per VLAN Spanning Tree+                    |
| QM             | QoS manager                                |
| QoS            | quality of service                         |
| RADIUS         | Remote Access Dial-In User Service         |
| RAM            | random-access memory                       |
| RCP            | Remote Copy Protocol                       |
| RGMP           | Router-Ports Group Management Protocol     |
| RIB            | routing information base                   |
| RIF            | Routing Information Field                  |
| RMON           | remote network monitor                     |
| ROM            | read-only memory                           |
| ROMMON         | ROM monitor                                |
| RP             | route processor or rendezvous point        |
| RPC            | remote procedure call                      |
| RPF            | reverse path forwarding                    |

**Table A-1** *Acronyms (continued)*

| <b>Acronym</b> | <b>Expansion</b>                                                |
|----------------|-----------------------------------------------------------------|
| RPR            | Route Processor Redundancy                                      |
| RSPAN          | remote SPAN                                                     |
| RST            | reset                                                           |
| RSVP           | ReSerVation Protocol                                            |
| 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                                          |
| SSTP           | Cisco Shared Spanning Tree                                      |
| STP            | Spanning Tree Protocol                                          |
| 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                         |
| TopN           | Utility that allows the user to analyze port traffic by reports |
| TOS            | type of service                                                 |
| TLV            | type-length-value                                               |

**Table A-1** *Acronyms (continued)*

| <b>Acronym</b> | <b>Expansion</b>                       |
|----------------|----------------------------------------|
| TTL            | Time To Live                           |
| TVX            | valid transmission                     |
| UDLD           | UniDirectional Link Detection Protocol |
| UDP            | User Datagram Protocol                 |
| UNI            | User-Network Interface                 |
| UTC            | Coordinated Universal Time             |
| VACL           | VLAN access control list               |
| VCC            | virtual channel circuit                |
| VCI            | virtual circuit identifier             |
| VCR            | Virtual Configuration Register         |
| VINES          | Virtual Network System                 |
| VLAN           | virtual LAN                            |
| VMPS           | VLAN Membership Policy Server          |
| VPN            | virtual private network                |
| VRF            | VPN routing and forwarding             |
| 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                   |





---

## Numerics

- 802.10 SAID (default) **8-4**
- 802.1Q trunks **12-6**
- 802.1Q VLANs
  - encapsulation **6-3**
  - trunk restrictions **6-5**
- 802.1s
  - See MST
- 802.1w
  - See MST
- 802.1X
  - See port-based authentication
- 802.1x authentication
  - support for guest VLANs **26-5**
- 802.3ad
  - See LACP

---

## A

- AAA
  - disabling **26-8**
  - enabling **26-8**
- abbreviating commands **2-5**
- access control entries
  - See ACEs
- access ports, configuring **6-8**
- access VLANs **6-6**
- ACEs
  - ACLs **24-2**
  - Ethernet **24-2**
  - IP **24-2**
  - Layer 4 operation restrictions **24-6**

## ACLs

- ACEs **24-2**
  - applying on routed packets **24-19**
  - applying on switched packets **24-19**
  - compatibility on the same switch **24-3**
  - configuring with VLAN maps **24-18**
- CPU impact **24-8**
- IP
  - matching criteria for port ACLs **24-4**
- MAC extended **24-9**
- matching criteria for router ACLs **24-3**
- port
  - and voice VLAN **24-4**
  - defined **24-2**
  - limitations **24-4**
  - processing **24-8**
  - types supported **24-2**
- acronyms, list of **A-1**
- active queue management **29-13**
- addresses
  - See MAC addresses
- adjacency tables
  - description **21-2**
  - displaying statistics **21-10**
- advertisements, VTP
  - See VTP advertisements
- alarms
  - major **33-2**
  - minor **33-2**
- audience **xix**
- authentication
  - See also port-based authentication
- authentication server

- defined 26-2
- RADIUS server 26-2
- authorized and unauthorized ports 26-4
- authorized ports with 802.1X 26-4
- automatic QoS
  - See QoS
- Auto-QoS
  - configuring 29-15

---

## B

- BackboneFast
  - adding a switch (figure) 13-2
  - and MST 14-2
  - configuring 13-15
  - link failure (figure) 13-7, 13-8
  - not supported MST 14-2
  - understanding 13-6
  - See also STP
- BGP 1-8
- blocking packets 27-1
- blocking state (STP)
  - RSTP comparisons (table) 14-4
- boot bootldr command 3-18
- boot command 3-15
- boot fields
  - See configuration register boot fields
- boot system command 3-13, 3-18
- boot system flash command 3-15
- Border Gateway Protocol
  - See BGP
- boundary ports
  - description 14-6
- BPDU Guard
  - and MST 14-2
  - configuring 13-12
  - overview 13-4
- BPDU
  - and media speed 12-2

- pseudobridges and 14-5
  - what they contain 12-3
- bridge ID
  - See STP bridge ID
- bridge priority (STP) 12-16
- bridge protocol data units
  - See BPDUs
- broadcast storm control
  - disabling 28-4
- BSR
  - configuration example 23-21
- burst rate 29-39
- burst size 29-26

---

## C

- cautions for passwords
  - encrypting 3-9
  - TACACS+ 3-9
- CDP
  - and trusted boundary 29-24
  - configuration 16-1
  - displaying configuration 16-3
  - enabling on interfaces 16-2
  - maintaining 16-3
  - monitoring 16-3
  - overview 1-2, 16-1
- cdp enable command 16-2
- CEF
  - adjacency tables 21-2
  - configuring load balancing 21-7
  - disabling per-destination load balancing 21-7
  - display statistics 21-9
  - enabling 21-7
  - hardware switching 21-4
  - load balancing 21-6
  - overview 21-1
  - software switching 21-4
- CGMP



- overview **15-1**
- channel-group group command **17-7, 17-9**
- Cisco Discovery Protocol
  - See CDP
- Cisco Express Forwarding
  - See CEF
- Cisco Group Management Protocol
  - See CGMP
- Cisco IP Phones
  - configuring **35-2**
  - sound quality **35-1**
- CIST
  - description **14-2**
- class-map command **29-28**
- class of service
  - See CoS
- clear cdp counters command **16-3**
- clear cdp table command **16-3**
- clear counters command **4-13**
- clearing
  - IP multicast table entries **23-20**
- clear ip flow stats command **30-6**
- CLI
  - accessing **2-1**
  - backing out one level **2-5**
  - getting commands **2-5**
  - history substitution **2-3**
  - modes **2-5**
  - monitoring environments **32-1**
  - ROM monitor **2-6**
  - software basics **2-4**
- clients
  - in 802.1x authentication **26-2**
- command-line processing **2-3**
- command modes **2-5**
- commands
  - listing **2-5**
- command switches
  - in VMPS **9-1**
- common and internal spanning tree
  - See CIST
- common spanning tree
  - See CST
- community ports
  - description **10-1**
- community VLANs
  - description **10-2**
- config-register command **3-16**
- config terminal command **3-2**
- configuration
  - 802.1X with Guest-VLAN **26-10**
- configuration example, SPAN enhancement **32-9**
- configuration files
  - saving **3-3**
- configuration guidelines
  - for VMPS **9-3**
- configuration register
  - changing settings **3-15 to 3-16**
  - configuring **3-13**
  - settings at startup **3-14**
- configuration register boot fields
  - listing value **3-16**
  - modifying **3-15**
- configure terminal command **3-15, 4-2**
- configuring
  - inline power **33-16**
- console configuration mode **2-5**
- console port
  - disconnecting user sessions **5-5**
  - monitoring user sessions **5-4**
- copy running-config startup-config command **3-3**
- copy system:running-config nvram:startup-config command **3-18**
- CoS
  - configuring port value **29-36**
  - definition **29-3**
  - figure **29-2**
  - overriding on Cisco IP Phones **35-3**

- priority **35-3**
- CoS-to-DSCP maps **29-40**
- counters
  - clearing MFIB **23-20**
  - clearing on interfaces **4-13**
- CPU port sniffing, SPAN enhancement **32-7**
- CST
  - description **14-5**
  - IST and **14-2**
  - MST and **14-2**

## D

- default configuration
  - 802.1X **26-7**
  - auto-QoS **29-15**
  - IGMP filtering **15-12**
- default gateway
  - configuring **3-4**
  - verifying configuration **3-5**
- default ports
  - 802.1x authentication not supported on **26-8**
- description command **4-8**
- detecting unidirectional links **18-1**
- DHCP snooping
  - configuration guidelines **19-3**
  - configuring **19-3**
  - default configuration **19-3**
  - displaying binding tables **19-9**
  - displaying configuration **19-10**
  - enabling **19-4**
  - enabling on private VLAN **19-5**
  - enabling the database agent **19-5**
  - monitoring **19-9, 19-12, 19-13**
  - overview **19-1**
  - Snooping database agent **19-2**
- DHCP Snooping Database Agent
  - adding to the database (example) **19-9**
  - enabling (example) **19-6**
- overview **19-2**
- reading from a TFTP file (example) **19-7**
- Differentiated Services Code Point values
  - See DSCP values
- DiffServ architecture, QoS **29-2**
- disabled state
  - RSTP comparisons (table) **14-4**
- disabling
  - broadcast storm control **28-4**
- disconnect command **5-5**
- documentation
  - organization **xix**
  - related **xxi**
- DSCP maps **29-40**
- DSCP-to-CoS maps
  - configuring **29-42**
- DSCP values
  - configuring maps **29-40**
  - configuring port value **29-37**
  - definition **29-3**
  - IP precedence **29-2**
  - mapping markdown **29-22**
  - mapping to transmit queues **29-38**
- DTP
  - VLAN trunks and **6-3**
- duplex command **4-7**
- duplex mode
  - configuring interface **4-6**
- Dynamic Host Configuration Protocol snooping
  - See DHCP snooping
- dynamic port VLAN membership
  - configuring **9-5**
  - example **9-9**
  - overview **9-2**
  - reconfirming **9-7**
  - troubleshooting **9-8**
- Dynamic Trunking Protocol
  - See DTP

## E

### EAP

- request/identity frame **26-3**
- response/identity frame **26-3**

### EAP frames

- changing retransmission time **26-13**
- exchanging (figure) **26-3**
- setting retransmission number **26-14**

### EAPOL frames

- 802.1x authentication and **26-2**
- OTP authentication, example (figure) **26-3**

### EAPOL-start frame **26-3**

### edge ports

- description **14-7**

### EGP

- overview **1-8**

### EIGRP

- overview **1-7**

### enable command **3-2, 3-15**

### enable mode **2-5**

### encapsulation configuration, SPAN enhancements **32-7**

### encapsulation types **6-3**

### Enhanced Interior Gateway Routing Protocol

- See EIGRP

### environmental monitoring

- LED indications **33-2**
- SNMP traps **33-2**
- supervisor engine **33-2**
- switching modules **33-2**
- using CLI commands **33-1**

### EtherChannel

- channel-group group command **17-7, 17-9**
- configuration guidelines **17-5**
- configuring **17-6 to 17-14**
- configuring Layer 2 **17-9**
- configuring Layer 3 **17-6**
- interface port-channel command **17-7**
- lacp system-priority

- command example **17-12**

### modes **17-3**

### overview **17-1**

### PAgP

- Understanding **17-3**

### physical interface configuration **17-7**

### port-channel interfaces **17-2**

### port-channel load-balance

- command **17-11**

### port-channel load-balance command **17-12**

### removing **17-13**

### removing interfaces **17-13**

### EtherChannel ports

- 802.1x authentication not supported in **26-8**

### extended range VLANs

- See VLANs

### Extensible Authentication Protocol over LAN **26-1**

### Exterior Gateway Protocol

- See EGP

## F

### FastDrop

- clearing entries **23-20**
- displaying entries **23-19**
- overview **23-10**

### fast-leave processing

- enabling **15-6**

### FIB

- description **21-2**

- See also MFIB

### filtering

- in a VLAN **24-10**
- non-IP traffic **24-9**

### flags **23-11**

### Flash memory

- configuring router to boot from **3-18**
- loading system images from **3-17**
- security precautions **3-17**

flooded traffic, blocking **27-2**  
 forward-delay time (STP)  
     configuring **12-18**  
 forwarding information base  
     See FIB

## G

gateway  
     See default gateway  
 global configuration mode **2-5**

## H

hardware switching **21-5**  
 hello time (STP)  
     configuring **12-17**  
 history  
     CLI **2-3**  
 hop counts  
     configuring MST bridges **14-7**  
 hosts, limit on dynamic port **9-8**  
 Hot Standby Routing Protocol  
     See HSRP  
 HSRP  
     description **1-6**

## I

ICMP  
     enabling **5-10**  
     ping **5-5**  
     running IP traceroute **5-7**  
     time exceeded messages **5-7**  
 IEEE 802.1s  
     See MST  
 IEEE 802.1w  
     See MST

IEEE 802.3ad

    See LACP

IGMP

    description **23-3**  
     enabling **23-13**  
     immediate-leave processing **15-2**  
     overview **15-1**

IGMP filtering

    configuring **15-12**  
     default configuration **15-12**  
     described **15-12**  
     monitoring **15-16**

IGMP groups, setting the maximum number **15-14**

IGMP profile

    applying **15-13**  
     configuration mode **15-12**  
     configuring **15-13**

IGMP snooping

    configuration guidelines **15-3**  
     enabling **15-4**  
     IP multicast and **23-4**  
     monitoring **15-10**  
     overview **15-1**

IGRP

    description **1-7**

ingress packets, SPAN enhancement **32-7**

inline power

    configuring on Cisco IP phones **35-4**

interface command **3-2, 4-1**

interface port-channel command **17-6, 17-7**

interface range command **4-4**

interface range macro command **4-5**

interfaces

    adding descriptive name **4-8**  
     clearing counters **4-13**  
     configuring **4-2**  
     configuring ranges **4-4**  
     displaying information about **4-12**  
     Layer 2 modes **6-4**

- maintaining **4-12**
- monitoring **4-12**
- naming **4-8**
- numbers **4-2**
- overview **4-1**
- restarting **4-13**
- See also Layer 2 interfaces
- Interior Gateway Routing Protocol
  - See IGRP
- Internet Control Message Protocol
  - See ICMP
- Internet Group Management Protocol
  - See IGMP
- Inter-Switch Link encapsulation
  - See ISL encapsulation
- IP
  - configuring default gateway **3-4**
  - configuring static routes **3-5**
  - displaying statistics **21-8**
  - flow switching cache **30-6**
  - ip cef command **21-7**
  - ip flow-aggregation cache destination-prefix command **30-8**
  - ip flow-aggregation cache prefix command **30-8**
  - ip flow-aggregation cache source-prefix command **30-8**
  - ip flow-export command **30-6**
  - ip icmp rate-limit unreachable command **5-11**
  - ip igmp profile command **15-12**
  - ip igmp snooping tcn flood command **15-9**
  - ip igmp snooping tcn flood query count command **15-9**
  - ip igmp snooping tcn query solicit command **15-10**
  - ip load-sharing per-destination command **21-7, 21-8**
  - ip local policy route-map command **22-4**
  - ip mask-reply command **5-12**
  - IP multicast
    - clearing table entries **23-20**
    - configuring **23-12**
    - default configuration **23-13**
    - displaying PIM information **23-15**
    - displaying the routing table information **23-16**
    - enabling **23-13**
    - enabling dense-mode PIM **23-14**
    - enabling sparse-mode **23-14**
    - features not supported **23-12**
    - hardware forwarding **23-8**
    - IGMP snooping and **15-3, 23-4**
    - monitoring **23-15**
    - overview **23-1**
    - routing protocols **23-2**
    - software forwarding **23-8**
    - See also Auto-RP; IGMP; PIM; RP; RPF
  - ip multicast-routing command **23-13**
  - IP Phones
    - configuring voice ports **35-2**
    - See Cisco IP Phones **35-1**
  - IP phones
    - automatic classification and queueing **29-15**
    - trusted boundary for QoS **29-23**
  - ip pim command **23-14**
  - ip pim dense-mode command **23-14**
  - ip pim sparse-dense-mode command **23-15**
  - ip policy route-map command **22-3**
  - ip redirects command **5-11**
  - ip route-cache flow command **30-5**
  - IP routing tables
    - deleting entries **23-20**
  - IP Source Guard
    - configuring **19-11**
    - configuring on private VLANs **19-12**
    - displaying **19-12, 19-13**
    - overview **19-10**
  - IP statistics
    - displaying **21-9**
  - IP traceroute
    - executing **5-7**
    - overview **5-7**
  - IP unicast
    - displaying statistics **21-9**

ip unreachable command 5-10

## IPX

redistribution of route information with EIGRP 1-7

ISL encapsulation 6-3

isolated ports

description 10-1

isolated VLANs

description 10-2

## IST

description 14-2

MST regions and 14-2

IST master

description 14-7

## J

jumbo frames

and ethernet ports 4-10

configuring MTU sizes for 4-11

ports and linecards that support 4-9

understanding 4-9

VLAN interfaces 4-10

## K

keyboard shortcuts 2-3

## L

labels

definition 29-3

## LACP

system ID 17-4

Layer 2

show interfaces 4-11

Layer 2 access ports 6-8

Layer 2 frames, classification with CoS 29-2

Layer 2 interfaces

assigning VLANs 8-8

configuring 6-5

configuring as PVLAN host ports 10-8

configuring as PVLAN promiscuous ports 10-7

configuring as PVLAN trunk ports 10-9

defaults 6-5

disabling configuration 6-9

modes 6-4

show interfaces command 6-7

Layer 2 interface type

resetting 10-11

setting 10-11

Layer 2 switching

overview 6-1

Layer 2 Traceroute

and ARP 5-9

and CDP 5-8

described 5-8

host-to-host paths 5-8

IP addresses and subnets 5-9

MAC addresses and VLANs 5-9

multicast traffic 5-9

multiple devices on a port 5-9

unicast traffic 1-3, 5-8

usage guidelines 5-8

Layer 2 trunks

configuring 6-6

overview 6-3

Layer 3 packets, classification methods 29-2

Layer 4 port operations

configuration guidelines 24-6

restrictions 24-6

leave processing, IGMP

See fast-leave processing

LEDs

description (table) 33-2

limit of hosts on dynamic ports 9-8

listening state (STP)

RSTP comparisons (table) 14-4

- load balancing
  - configuring for CEF **21-7**
  - configuring for EtherChannel **17-12**
  - overview **17-5, 21-6**
  - per-destination **21-7**
- login timer
  - changing **5-4**
- logoutwarning command **5-4**
- loop guard
  - and MST **14-2**
  - configuring **13-9**
  - overview **13-2**

## M

- MAC addresses
  - allocating **12-5**
  - building tables **6-2**
  - displaying **5-3**
  - displaying in DHCP snooping binding table **19-10**
  - in ACLs **24-9**
- MAC extended access lists **24-9**
- mapping
  - DSCP markdown values **29-22**
  - DSCP values to transmit queues **29-38**
- mapping tables
  - configuring DSCP **29-40**
  - described **29-12**
- mask destination command **30-8**
- mask source command **30-8**
- match ip address command **22-3**
- maximum aging time (STP)
  - configuring **12-18**
- member switches
  - in VMPS **9-1**
- MFIB
  - CEF and **23-5**
  - displaying **23-18**
  - overview **23-11**
- modules
  - checking status **5-1**
- monitoring
  - ACL information **24-26**
  - IGMP filters **15-16**
  - IGMP snooping **15-10**
  - VLAN
    - maps **24-17**
    - VLAN filters **24-17**
- M-record **14-2**
- MST
  - and multiple spanning trees **1-3, 14-2**
  - boundary ports **14-6**
  - BPDUs **14-2**
  - configuration **14-5**
  - configuring **14-9**
  - displaying configurations **14-13**
  - edge ports **14-7**
  - enabling **14-9**
  - hop count **14-7**
  - instances **14-5**
  - interoperability **14-4**
  - interoperability with PVST+ **14-2**
  - link type **14-7**
  - master **14-7**
  - message age **14-7**
  - regions **14-5, 14-6**
  - restrictions **14-8**
- MST instances
  - configuring parameters **14-11**
  - description **14-2**
  - number supported **14-5**
- MSTP
  - M-record **14-2**
  - M-tree **14-2**
- M-tree **14-2**
- MTU size (default) **8-4**
- multicast
  - See IP multicast

multicast packets  
     blocking **27-2**

multicast routers  
     displaying routing tables **23-16**  
     flood suppression **15-7**  
     specifying port for **15-7**

Multicast Storm Control, enabling **28-6**

multiple forwarding paths **1-3, 14-2**

Multiple Spanning Tree  
     See MST

---

## N

native VLAN  
     specifying **6-6**

NetFlow  
     destination-prefix aggregation  
         configuration (example) **30-12**  
         minimum mask, configuring **30-8**

IP  
     flow switching cache **30-6**

prefix aggregation  
     configuration (example) **30-10**  
     minimum mask, configuring **30-8**

source-prefix aggregation  
     minimum mask, configuring **30-8**

switching  
     configuration (example) **30-9**  
     configuring **30-5**  
     exporting cache entries **30-5**  
     statistics **30-6**

NetFlow aggregation  
     minimum mask  
         default value **30-7**

NetFlow statistics  
     caveats on supervisor **30-4**  
     configuring collection **30-4**  
     implementing collection **30-4**  
     overview of collection **30-1**

network fault tolerance **1-3, 14-2**

network management  
     configuring **16-1**

Next Hop Resolution Protocol  
     See NHRP

NFFC/NFFC II  
     IGMP snooping and **15-3**

NHRP  
     support **1-7**

non-IP traffic filtering **24-9**

non-RPF traffic  
     description **23-9**  
     in redundant configurations (figure) **23-10**

nonvolatile random-access memory  
     See NVRAM

normal-range VLANs  
     See VLANs

NVRAM  
     saving settings **3-3**

---

## O

OIR  
     overview **4-12**

online insertion and removal  
     See OIR

Open Shortest Path First  
     See OSPF

operating system images  
     See system images

OSPF  
     area concept **1-7**  
     description **1-6**

overview of NetFlow statistics collection **30-1**

---

## P

packets



- modifying **29-14**
- packet type filtering, SPAN enhancement **32-8**
- PAgP
  - understanding **17-3**
- passwords
  - configuring enable password **3-7**
  - configuring enable secret password **3-7**
  - encrypting **3-9**
  - recovering lost enable password **3-12**
  - setting line password **3-8**
  - setting TACACS+ **3-8**
- PBR (policy-based routing)
  - configuration (example) **22-4**
  - enabling **22-2**
  - features **22-1**
  - overview **22-1**
  - route maps **22-2**
  - when to use **22-2**
- Per-VLAN Rapid Spanning Tree **12-6**
  - enabling **12-20**
- PIM
  - configuring dense mode **23-14**
  - configuring sparse mode **23-14**
  - displaying information **23-15**
  - displaying statistics **23-20**
  - enabling sparse-dense mode **23-14, 23-15**
  - overview **23-3**
- PIM-DM **23-3**
- PIM-SM **23-3**
- ping
  - executing **5-6**
  - overview **5-5**
- ping command **5-6, 23-15**
- point-to-point
  - in 802.1x authentication (figure) **26-2**
- police command **29-31**
- policed-DSCP map **29-41**
- policers
  - description **29-5**
  - number of **29-10**
  - types of **29-9**
- policies
  - See QoS policies
- policing
  - See QoS policing
- policy-map command **29-28, 29-30**
- policy maps
  - attaching to interfaces **29-33**
  - configuring **29-29**
- port ACLs
  - and voice VLAN **24-4**
  - defined **24-2**
  - limitations **24-4**
- Port Aggregation Protocol
  - see PAgP
- port-based authentication
  - client, defined **26-2**
  - configuration guidelines **26-8**
  - configuring
    - quiet period **26-12**
  - configuring Guest-VLAN **26-10**
  - configuring manual re-authentication of a client **26-12**
  - controlling authorization state **26-4**
  - default configuration **26-7**
  - described **26-1**
  - device roles **26-2**
  - disabling **26-9**
  - displaying statistics **26-16**
  - enabling **26-8**
  - enabling multiple hosts **26-15**
  - enabling periodic re-authentication **26-11**
  - encapsulation **26-2**
  - initiation and message exchange **26-3**
  - method lists **26-8**
  - ports not supported **26-4**
  - resetting to default values **26-15**
  - setting retransmission number **26-14**
  - setting retransmission time **26-13**

- switch as proxy **26-2**
- switch as RADIUS client **26-2**
- topologies, supported **26-6**
- with VLAN assignment **26-4**
- port-based QoS features
  - See QoS
- port-channel interfaces
  - See also EtherChannel
  - creating **17-6**
  - overview **17-2**
- port-channel load-balance
  - command **17-11**
  - command example **17-12**
- port-channel load-balance command **17-12**
- port cost (STP)
  - configuring **12-15**
- PortFast
  - and MST **14-2**
  - BPDU filter
    - configuring **13-12**
  - configuring or enabling **13-11**
  - overview **13-3**
- PortFast BPDU filtering
  - overview **13-4**
- Portfast BPDU filtering
  - and MST **14-2**
  - enabling **13-12**
- PortFast STP parameter **9-3**
- port priority
  - configuring MST instances **14-11**
- port priority (STP) **12-13**
- ports
  - blocking **27-1**
  - checking status **5-2**
  - community **10-1**
  - dynamic VLAN membership
    - configuring **9-5**
    - example **9-9**
    - overview **9-2**
  - reconfirming **9-7**
  - forwarding, resuming **27-3**
  - isolated **10-1**
  - PVLAN types **10-1**
  - secure **25-1**
  - See also interfaces
- port security
  - aging **25-5**
  - and QoS trusted boundary **29-23**
  - configuring **25-3**
  - default configuration **25-2**
  - described **25-1**
  - displaying **25-7**
  - violations **25-2**
  - with other features **25-3**
- port states
  - description **12-5**
- port trust state
  - See trust states
- power, inline **33-16, 35-4**
- power dc input command **33-10**
- power inline command **33-17**
- power management
  - 1+1 redundancy mode **33-10**
  - 2+1 redundancy mode **33-10**
  - Catalyst 4006 switch **33-10**
  - Catalyst 4500 series **33-3**
  - Catalyst 4500 Series power supplies **33-8**
  - combined mode **33-4**
  - configuring combined mode **33-7**
  - configuring redundant mode **33-6**
  - overview **33-1**
  - redundancy **33-10**
  - redundant mode **33-4**
- power redundancy
  - setting on Catalyst 4006 **33-13**
- power redundancy-mode comand **33-7**
- power supplies
  - fixed **33-3**

- variable **33-3**
- power supplies required command **33-13**
- primary VLANs
  - associating with secondary VLANs **10-6**
  - description **10-1**
- priority
  - overriding **35-3**
- privileged EXEC mode **2-5**
- privileges
  - changing default **3-10**
  - configuring levels **3-10**
  - exiting **3-11**
  - logging in **3-11**
- promiscuous ports
  - configuring PVLAN **10-7**
  - description **10-1**
  - setting mode **10-11**
- protocol timers **12-4**
- pruning, VTP
  - See VTP pruning
- pseudobridges
  - description **14-5**
- PVLANs
  - 802.1q support **10-3**
  - configuration guidelines **10-4**
  - configuring **10-4**
  - configuring promiscuous ports **10-7**
  - host ports
    - setting **10-11**
  - isolated VLANs **10-2**
  - overview **10-1**
  - permitting routing, example **10-10**
  - promiscuous mode
    - setting **10-11**
  - setting
    - interface mode **10-11**

## Q

### QoS

- allocating bandwidth **29-39**
- auto-QoS
  - configuration and defaults display **29-18**
  - configuration guidelines **29-16**
  - described **29-15**
  - displaying **29-18**
  - effects on NVRAM configuration **29-16**
  - enabling for VoIP **29-17**
- basic model **29-5**
- burst size **29-26**
- classification **29-5 to 29-9**
- configuration guidelines **29-22**
  - auto-QoS **29-16**
- configuring
  - auto-QoS **29-15**
  - trusted boundary **29-23**
- configuring DSCP maps **29-40**
- configuring traffic shaping **29-39**
- configuring VLAN-based **29-34**
- creating policing rules **29-27**
- default auto configuration **29-15**
- default configuration **29-21**
- definitions **29-3**
- disabling on interfaces **29-33**
- enabling on interfaces **29-33**
- flowcharts **29-7, 29-11**
- IP phones
  - automatic classification and queueing **29-15**
  - detection and trusted settings **29-15, 29-23**
- overview **29-1**
- packet modification **29-14**
- port-based **29-34**
- priority **29-14**
- traffic shaping **29-14**
- transmit rate **29-39**
- trust states

- trusted device **29-23**
- VLAN-based **29-34**
- See also COS; DSCP values; transmit queues
- QoS active queue management
  - tracking queue length **29-13**
- QoS labels
  - definition **29-3**
- QoS mapping tables
  - CoS-to-DSCP **29-40**
  - DSCP-to-CoS **29-42**
  - policed-DSCP **29-41**
  - types **29-12**
- QoS marking
  - description **29-4**
- QoS policers
  - burst size **29-26**
  - numbers of **29-10**
  - types of **29-9**
- QoS policies
  - attaching to interfaces **29-10**
  - overview **29-27**
- QoS policing
  - definition **29-4**
  - described **29-5, 29-9**
- QoS transmit queues
  - allocating bandwidth **29-39**
  - burst **29-14**
  - configuring **29-37**
  - configuring traffic shaping **29-39**
  - mapping DHCP values to **29-38**
  - maximum rate **29-14**
  - overview **29-13**
  - sharing link bandwidth **29-13**
- Quality of service
  - See QoS
- queueing **29-5, 29-13**

---

## R

- RADIUS server
  - configuring settings **26-11**
  - parameters on the switch **26-10**
- range command **4-4**
- range macros
  - defining **4-5**
- ranges of interfaces
  - configuring **4-4**
- Rapid Spanning Tree
  - See RSTP
- re-authentication
  - configuring manual **26-12**
  - enabling periodic **26-11**
- reduced MAC address **12-2**
- redundancy (RPR)
  - configuring **34-4**
  - route processor redundancy **34-2**
  - supervisor engine and Cisco IOS software **34-3**
- related documentation **xxi**
- reload command **3-15, 3-16**
- replication
  - description **23-8**
- reserved-range VLANs
  - See VLANs
- retransmission number
  - setting in 802.1x authentication **26-14**
- retransmission time
  - changing in 802.1x authentication **26-13**
- RIP
  - description **1-6**
- rommon, command **3-16**
- ROM monitor
  - boot process and **3-13**
  - CLI **2-6**
- root bridge
  - selecting in MST **14-2**
- root bridge (STP)

- configuring 12-9
- root guard
  - and MST 14-2
  - enabling 13-8
  - overview 13-2
- routed packets, ACLs on 24-19
- route-map (IP) command 22-3
- route maps
  - defining 22-3
  - PBR 22-2
- route processor redundancy
  - See redundancy (RPR+)
- router ACLs
  - description 24-2
  - using with VLAN maps 24-18
- routers, multicast
  - See multicast routers
- Routing Information Protocol
  - See RIP
- RPR+
  - See redundancy (RPR+)
- RSTP
  - compatibility 14-3
  - description 14-2
  - port roles 14-3
  - port states 14-4

## S

- SAID
  - See 802.10 SAID
- scheduling 29-13
  - defined 29-4
  - overview 29-5
- secondary root switch 12-12
- secondary VLANs
  - associating with primary 10-6
  - description 10-2
  - permitting routing 10-10
- secure ports, configuring 25-1
- security, port 25-1
- Security Association Identifier
  - See 802.10 SAID
- servers, VTP
  - See VTP servers
- service-policy command 29-28
- service-policy input command 7-1, 29-33
- set default interface command 22-3
- set interface command 22-3
- set ip default next-hop command 22-3
- set ip next-hop command 22-3
- show adjacency command 21-10
- show boot command 3-18
- show catalyst4000 chassis-mac-address command 12-3
- show cdp command 16-2, 16-3
- show cdp entry command 16-3
- show cdp interface command 16-3
- show cdp neighbors command 16-3
- show cdp traffic command 16-4
- show configuration command 4-8
- show debugging command 16-4
- show environment command 33-1
- show history command 2-4
- show inlinepower command 33-17, 33-18, 33-19
- show interfaces command 4-11, 4-12
- show interfaces status command 5-2
- show ip cache flow aggregation destination-prefix command 30-9
- show ip cache flow aggregation prefix command 30-9
- show ip cache flow aggregation source-prefix command 30-9
- show ip cache flow command 30-6
- show ip cef command 21-8
- show ip interface command 23-15
- show ip local policy command 22-4
- show ip mroute command 23-15
- show ip pim interface command 23-15
- show mac-address-table address command 5-3

- show mac-address-table interface command **5-3**
- show mls entry command **21-9**
- show module command **5-1, 12-5**
- show power command **33-13**
- show power supplies command **33-7**
- show protocols command **4-12**
- show running-config command
  - adding description for an interface **4-8**
  - checking your settings **3-3**
  - displaying ACLs **24-12, 24-14, 24-21, 24-22**
- show startup-config command **3-4**
- show users command **5-4**
- show version command **3-16**
- shutdown, command **4-13**
- shutting down
  - interfaces **4-13**
- single spanning tree
  - See SST
- slot numbers, description **4-1**
- SNMP
  - documentation **1-11**
  - support **1-11**
- software
  - upgrading **34-5**
- software configuration register **3-13**
- software switching
  - description **21-5**
  - interfaces **21-6**
  - key data structures used **23-7**
- SPAN
  - configuration guidelines **32-4**
  - configuring **32-4 to 32-6**
  - overview **32-1**
- SPAN destination ports
  - 802.1x authentication not supported **26-8**
- SPAN enhancements
  - configuration example **32-9**
  - CPU port sniffing **32-7**
  - encapsulation configuration **32-7**
  - ingress packets **32-7**
  - packet type filtering **32-8**
- spanning-tree backbonefast command **13-15**
- spanning-tree cost command **12-15**
- spanning-tree guard root command **13-8**
- spanning-tree portfast bpdu-guard command **13-12**
- spanning-tree portfast command **13-11**
- spanning-tree port-priority command **12-13**
- spanning-tree uplinkfast command **13-14**
- spanning-tree vlan
  - command **12-9**
  - command example **12-9**
- spanning-tree vlan command **12-8**
- spanning-tree vlan cost command **12-15**
- spanning-tree vlan forward-time command **12-19**
- spanning-tree vlan hello-time command **12-17**
- spanning-tree vlan max-age command **12-18**
- spanning-tree vlan port-priority command **12-13**
- spanning-tree vlan priority command **12-17**
- spanning-tree vlan root primary command **12-10**
- spanning-tree vlan root secondary command **12-12**
- SPAN session **32-2**
- speed
  - configuring interface **4-6**
- speed command **4-7**
- SST
  - description **14-2**
  - interoperability **14-4**
- static routes
  - configuring **3-5**
  - verifying **3-6**
- statistics
  - displaying 802.1X **26-16**
  - displaying PIM **23-20**
  - NetFlow accounting **30-6**
- Storm Control
  - disabling **28-4**
  - displaying **28-5**
  - enabling **28-3**

- storm control **xx**
  - Storm Control, enabling multicast **28-6**
  - STP
    - configuring **12-7 to 12-20**
    - creating topology **12-4**
    - defaults **12-6**
    - disabling **12-19**
    - enabling **12-7**
    - enabling extended system ID **12-8**
    - enabling Per-VLAN Rapid Spanning Tree **12-20**
    - forward-delay time **12-18**
    - hello time **12-17**
    - maximum aging time **12-18**
    - overview **12-1, 12-3**
    - per-VLAN rapid spanning tree **12-6**
    - port cost **12-15**
    - Port Fast parameter **9-3**
    - port priority **12-13**
    - root bridge **12-9**
  - STP bridge ID **12-2**
  - supervisor engine
    - configuring **3-2 to 3-6**
    - copying files to standby **34-7**
    - default configuration **3-1**
    - default gateways **3-4**
    - environmental monitoring **33-1**
    - redundancy **34-1**
    - ROM monitor **3-13**
    - startup configuration **3-12**
    - static routes **3-5**
    - synchronizing configurations **34-4**
  - SVIs
    - and router ACLs **24-3**
  - switched packets, ACLs on **24-19**
  - Switched Port Analyzer
    - See SPAN
  - switching
    - NetFlow
      - configuration (example) **30-9**
      - configuring **30-5**
      - exporting cache entries **30-5**
    - switchport
      - show interfaces **4-11**
      - switchport access vlan command **6-6, 6-8**
      - switchport block multicast command **27-2**
      - switchport block unicast command **27-2**
      - switchport mode access command **6-8**
      - switchport mode dynamic command **6-6**
      - switchport mode trunk command **6-6**
    - switch ports
      - See access ports
    - switchport trunk allowed vlan command **6-6**
    - switchport trunk encapsulation command **6-6**
    - switchport trunk encapsulation dot1q command **6-3**
    - switchport trunk encapsulation isl command **6-3**
    - switchport trunk encapsulation negotiate command **6-3**
    - switchport trunk native vlan command **6-6**
    - switchport trunk pruning vlan command **6-6**
  - syslog messages **33-2**
  - system
    - reviewing configuration **3-4**
    - settings at startup **3-14**
  - system images
    - loading from Flash memory **3-17**
    - modifying boot field **3-14**
    - specifying **3-17**
- 
- ## T
- TACACS+
    - setting passwords **3-8**
  - Telnet
    - accessing CLI **2-2**
    - disconnecting user sessions **5-5**
    - executing **5-3**
    - monitoring user sessions **5-4**
  - telnet command **5-4**
  - time exceeded messages **5-7**

timer  
     See login timer

Token Ring  
     media not supported (note) **8-4, 11-3**

TOS  
     description **29-3**

trace command **5-7**

Traceroute  
     See Layer 2 Traceroute

traceroute  
     See IP traceroute

traceroute mac command **5-9**

traceroute mac ip command **5-9**

traffic  
     blocking flooded **27-2**

traffic control  
     using ACLs (figure) **24-4**  
     using VLAN maps (figure) **24-5**

traffic shaping **29-14**

translational bridge numbers (defaults) **8-4**

transmit queues  
     See QoS transmit queues

transmit rate **29-39**

troubleshooting  
     with traceroute **5-7**

trunk ports  
     802.1x authentication not supported on **26-8**  
     configuring PVLAN **10-9 to 10-10**

trunks  
     802.1Q restrictions **6-5**  
     configuring **6-6**  
     configuring access VLANs **6-6**  
     configuring allowed VLANs **6-6**  
     default interface configuration **6-6**  
     different VTP domains **6-3**  
     enabling to non-DTP device **6-4**  
     encapsulation **6-3**  
     specifying native VLAN **6-6**  
     understanding **6-3**

trusted boundary for QoS **29-23**

trust states  
     configuring **29-35**

type of service  
     See TOS

---

## U

UDLD  
     default configuration **18-2**  
     disabling **18-3**  
     enabling **18-3**  
     overview **18-1, 31-1**

unauthorized ports with 802.1X **26-4**

unicast  
     See IP unicast

unicast flood blocking  
     configuring **27-1**

unicast traffic, blocking **27-2**

unidirectional ethernet  
     enabling **7-1**  
     example of setting **7-1**  
     overview **7-1**

UniDirectional Link Detection Protocol  
     See UDLD

UplinkFast  
     and MST **14-2**  
     enabling **13-14**  
     MST and **14-3**  
     overview **13-5**

user EXEC mode **2-5**

user sessions  
     disconnecting **5-5**  
     monitoring **5-4**

---

## V

VACLs



- Layer 4 port operations **24-6**
- virtual LANs
  - See VLANs
- VLAN ACLs
  - See VLAN maps
- vlan command **8-6, 8-7**
- vlan database command **8-7**
- VLAN Management Policy Server
  - see VMPS
- VLAN map
  - order of entries **24-11**
- VLAN maps
  - applying **24-14, 24-22**
  - common uses for **24-15**
  - configuration example **24-15**
  - configuration guidelines **24-11**
  - configuring **24-10**
  - creating entries **24-12**
  - defined **24-3**
  - denying access example **24-16**
  - denying packets **24-12**
  - displaying **24-17**
  - examples **24-16**
  - permitting packets **24-12**
  - router ACLs and **24-18**
  - using (figure) **24-5**
- VLAN Query Protocol (VQP) **9-1**
- VLANs
  - allowed on trunk **6-6**
  - configuration guidelines **8-3**
  - configuring **8-4**
  - default configuration **8-4**
  - description **1-4**
  - extended range **8-3**
  - IDs (default) **8-4**
  - interface assignment **8-8**
  - name (default) **8-4**
  - normal range **8-3**
  - overview **8-1**
  - reserved range **8-3**
  - See also PVLANS
  - See also private VLANs
- VLAN Trunking Protocol
  - See VTP
- VLAN trunks
  - overview **6-3**
- VMPS
  - administering **9-5**
  - configuration file example **9-8**
  - database configuration file **9-8**
  - dynamic port membership
    - configuring **9-5**
    - example **9-9**
    - overview **9-2**
    - reconfirming **9-7**
  - in a cluster of switches **9-1**
  - monitoring **9-5**
  - overview **9-1**
  - reconfirming membership **9-7**
  - reconfirming membership information **9-7**
- voice interfaces
  - configuring **35-1**
- Voice over IP
  - configuring **35-1**
- voice ports
  - configuring VVID **35-2**
- voice traffic **33-16, 35-4**
- VTP
  - configuration guidelines **11-5**
  - configuring **11-6 to 11-10**
  - configuring transparent mode **11-9**
  - default configuration **11-5**
  - disabling **11-9**
  - monitoring **11-10**
  - overview **11-1**
  - See also VTP version 2
- VTP advertisements
  - description **11-3**

## VTP clients

- configuring **11-8**

## VTP domains

- description **11-2**

VTP modes **11-2**

## VTP pruning

- enabling **11-6**
- overview **11-3**

## VTP servers

- configuring **11-7**

## VTP statistics

- displaying **11-10**

## VTP version 2

- enabling **11-7**
- overview **11-3**
- See also VTP

## VVID

- configuring **35-2**