

Cisco Reader Comment Card

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 (CCO) _____ % CD-ROM
_____ % Printed docs _____ % Other: _____
- 7 I prefer this access method: _____
- 8 I use the following three product features the most:

Document Information

Document Title: Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide

Part Number: OL-3999-01

S/W Release (if applicable): 12.2(14)SX

On a scale of 1–5 (5 being the best), please let us know how we rate in the following areas:

- ____ The document is written at my technical level of understanding. ____ The information is accurate.
- ____ The document is complete. ____ The information I wanted was easy to find.
- ____ The information is well organized. ____ The information I found was useful to my job.

Please comment on our lowest scores:

Mailing Information

Company Name

Date

Contact Name

Job Title

Mailing Address

City

State/Province

ZIP/Postal Code

Country

Phone ()

Extension

Fax ()

E-mail

Can 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.

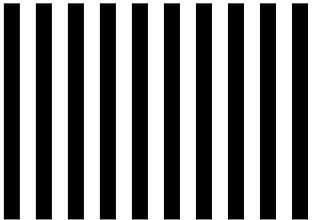
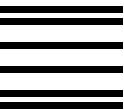
BUSINESS REPLY MAIL

FIRST-CLASS MAIL

PERMIT NO. 4631 SAN JOSE CA

POSTAGE WILL BE PAID BY ADDRESSEE

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES



DOCUMENT RESOURCE CONNECTION

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

||||||||||||||||||||||||||



Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide

Cisco IOS 12.2(14)SX

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-7814099=
Text Part Number: OL-3999-01



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.

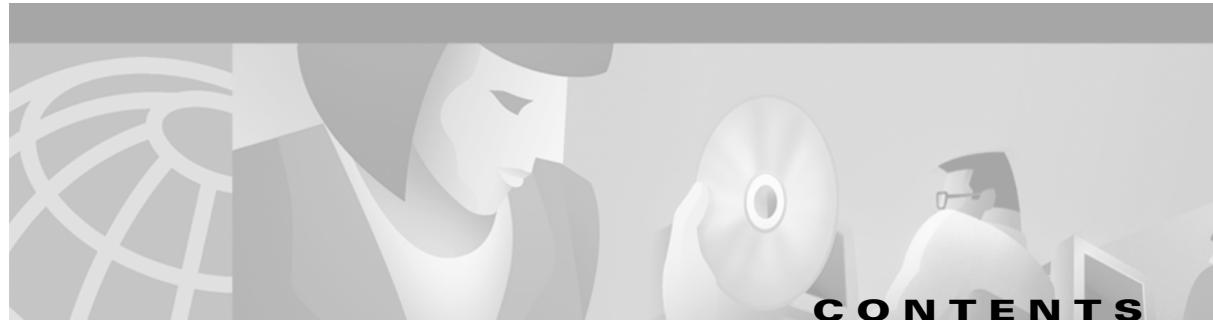
The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

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.



Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide
Copyright © 2003, Cisco Systems, Inc.
All rights reserved.



Preface xvii

Audience xvii

Organization xvii

Related Documentation xix

Conventions xx

Obtaining Documentation xxi

Cisco.com xxi

Documentation CD-ROM xxi

Ordering Documentation xxi

Documentation Feedback xxi

Obtaining Technical Assistance xxii

Cisco.com xxii

Technical Assistance Center xxii

Obtaining Additional Publications and Information xxiii

CHAPTER 1

Product Overview 1-1

Supported Hardware and Software 1-1

User Interfaces 1-1

Software Features Supported in Hardware by the PFC3 and DFC3 1-2

CHAPTER 2

Command-Line Interfaces 2-1

Accessing the CLI 2-1

Accessing the CLI through 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

Cisco IOS Command Modes 2-4

Displaying a List of Cisco IOS Commands and Syntax 2-5

ROM-Monitor Command-Line Interface 2-6

CHAPTER 3

Configuring the Switch for the First Time 3-1

Default Configuration 3-1

Configuring the Switch 3-2

Using the Setup Facility or the setup Command	3-2
Using Configuration Mode	3-10
Checking the Running Configuration Before Saving	3-10
Saving the Running Configuration Settings	3-11
Reviewing the Configuration	3-11
Configuring a Default Gateway	3-11
Configuring a Static Route	3-12
Configuring a BOOTP Server	3-13
Protecting Access to Privileged EXEC Commands	3-15
Setting or Changing a Static Enable Password	3-15
Using the enable password and enable secret Commands	3-15
Setting or Changing a Line Password	3-16
Setting TACACS+ Password Protection for Privileged EXEC Mode	3-16
Encrypting Passwords	3-17
Configuring Multiple Privilege Levels	3-17
Recovering a Lost Enable Password	3-19
Modifying the Supervisor Engine Startup Configuration	3-20
Understanding the Supervisor Engine Boot Configuration	3-20
Configuring the Software Configuration Register	3-21
Specifying the Startup System Image	3-24
Understanding Flash Memory	3-24
CONFIG_FILE Environment Variable	3-25
Controlling Environment Variables	3-26

CHAPTER 4

Configuring a Supervisor Engine 720	4-1
Using the Slots on a Supervisor Engine 720	4-1
Configuring Supervisor Engine 720 Ports	4-1
Configuring and Monitoring the Switch Fabric Module Functionality	4-2
Understanding How the Switch Fabric Module Functionality Works	4-2
Configuring the Switch Fabric Module Functionality	4-4
Monitoring the Switch Fabric Module Functionality	4-4

CHAPTER 5

Configuring Interfaces	5-1
Understanding Interface Configuration	5-1
Using the Interface Command	5-2
Configuring a Range of Interfaces	5-4
Defining and Using Interface-Range Macros	5-5
Configuring Optional Interface Features	5-6

Configuring Ethernet Interface Speed and Duplex Mode	5-6
Configuring Jumbo Frame Support	5-10
Configuring IEEE 802.3Z Flow Control	5-13
Configuring the Port Debounce Timer	5-14
Adding a Description for an Interface	5-15
Understanding Online Insertion and Removal	5-15
Monitoring and Maintaining Interfaces	5-16
Monitoring Interface Status	5-16
Clearing Counters on an Interface	5-17
Resetting an Interface	5-17
Shutting Down and Restarting an Interface	5-18

CHAPTER 6

Configuring RPR and RPR+ Supervisor Engine Redundancy	6-1
Understanding Supervisor Engine Redundancy	6-1
Supervisor Engine Redundancy Overview	6-1
RPR Operation	6-2
RPR+ Operation	6-2
Supervisor Engine Synchronization	6-3
Supervisor Engine Redundancy Guidelines and Restrictions	6-4
RPR+ Guidelines and Restrictions	6-4
Hardware Configuration Guidelines and Restrictions	6-5
Configuration Mode Restrictions	6-5
Configuring Supervisor Engine Redundancy	6-5
Configuring RPR and RPR+	6-6
Synchronizing the Supervisor Engine Configurations	6-6
Displaying the Redundancy States	6-7
Performing a Fast Software Upgrade	6-8
Copying Files to the Redundant Supervisor Engine	6-9

CHAPTER 7

Configuring LAN Ports for Layer 2 Switching	7-1
Understanding How Layer 2 Switching Works	7-1
Understanding Layer 2 Ethernet Switching	7-1
Understanding VLAN Trunks	7-2
Layer 2 LAN Port Modes	7-4
Default Layer 2 LAN Interface Configuration	7-4
Layer 2 LAN Interface Configuration Guidelines and Restrictions	7-5
Configuring LAN Interfaces for Layer 2 Switching	7-6
Configuring a LAN Port for Layer 2 Switching	7-6

Configuring a Layer 2 Switching Port as a Trunk	7-7
Configuring a LAN Interface as a Layer 2 Access Port	7-13

CHAPTER 8

Configuring EtherChannels 8-1

Understanding How EtherChannels Work	8-1
EtherChannel Feature Overview	8-1
Understanding How EtherChannels Are Configured	8-2
Understanding Port Channel Interfaces	8-4
Understanding Load Balancing	8-4
EtherChannel Feature Configuration Guidelines and Restrictions	8-5
Configuring EtherChannels	8-6
Configuring Port Channel Logical Interfaces for Layer 3 EtherChannels	8-6
Configuring Channel Groups	8-7
Configuring the LACP System Priority and System ID	8-9
Configuring EtherChannel Load Balancing	8-10

CHAPTER 9

Configuring VTP 9-1

Understanding How VTP Works	9-1
Understanding the VTP Domain	9-2
Understanding VTP Modes	9-2
Understanding VTP Advertisements	9-2
Understanding VTP Version 2	9-3
Understanding VTP Pruning	9-3
VTP Default Configuration	9-5
VTP Configuration Guidelines and Restrictions	9-5
Configuring VTP	9-6
Configuring VTP Global Parameters	9-6
Configuring the VTP Mode	9-8
Displaying VTP Statistics	9-10

CHAPTER 10

Configuring VLANs 10-1

Understanding How VLANs Work	10-1
VLAN Overview	10-1
VLAN Ranges	10-2
Configurable VLAN Parameters	10-3
Understanding Token Ring VLANs	10-3
VLAN Default Configuration	10-6
VLAN Configuration Guidelines and Restrictions	10-8

Configuring VLANs	10-9
VLAN Configuration Options	10-9
Creating or Modifying an Ethernet VLAN	10-10
Assigning a Layer 2 LAN Interface to a VLAN	10-12
Configuring the Internal VLAN Allocation Policy	10-12
Mapping 802.1Q VLANs to ISL VLANs	10-12

CHAPTER 11

Configuring Private VLANs	11-1
Understanding How Private VLANs Work	11-1
Private VLAN Configuration Guidelines	11-2
Configuring Private VLANs	11-4
Configuring a VLAN as a Private VLAN	11-5
Associating Secondary VLANs with a Primary VLAN	11-6
Mapping Secondary VLANs to the Layer 3 VLAN Interface of a Primary VLAN	11-7
Configuring a Layer 2 Interface as a Private VLAN Host Port	11-8
Configuring a Layer 2 Interface as a Private VLAN Promiscuous Port	11-9

CHAPTER 12

Configuring Cisco IP Phone Support	12-1
Understanding Cisco IP Phone Support	12-1
Cisco IP Phone Connections	12-1
Cisco IP Phone Voice Traffic	12-2
Cisco IP Phone Data Traffic	12-3
Cisco IP Phone Power Configurations	12-3
Default Cisco IP Phone Support Configuration	12-4
Cisco IP Phone Support Configuration Guidelines and Restrictions	12-4
Configuring Cisco IP Phone Support	12-5
Configuring Voice Traffic Support	12-5
Configuring Data Traffic Support	12-7
Configuring Inline Power Support	12-8

CHAPTER 13

Configuring IEEE 802.1Q Tunneling and Layer 2 Protocol Tunneling	13-1
Understanding How 802.1Q Tunneling Works	13-1
802.1Q Tunneling Configuration Guidelines and Restrictions	13-3
Configuring 802.1Q Tunneling	13-5
Configuring 802.1Q Tunnel Ports	13-5
Configuring the Switch to Tag Native VLAN Traffic	13-6
Understanding How Layer 2 Protocol Tunneling Works	13-6
Configuring Support for Layer 2 Protocol Tunneling	13-7

CHAPTER 14

Configuring STP and IEEE 802.1s MST	14-1
Understanding How STP Works	14-1
STP Overview	14-2
Understanding the Bridge ID	14-2
Understanding Bridge Protocol Data Units	14-3
Election of the Root Bridge	14-4
STP Protocol Timers	14-4
Creating the Spanning Tree Topology	14-5
STP Port States	14-5
STP and IEEE 802.1Q Trunks	14-11
Understanding How IEEE 802.1w RSTP Works	14-12
IEEE 802.1w RSTP Overview	14-12
RSTP Port Roles	14-12
RSTP Port States	14-13
Rapid-PVST	14-13
Understanding How IEEE 802.1s MST Works	14-13
IEEE 802.1s MST Overview	14-14
MST-to-PVST Interoperability	14-15
Common Spanning Tree	14-16
MST Instances	14-17
MST Configuration Parameters	14-17
MST Regions	14-17
Message Age and Hop Count	14-19
Default STP Configuration	14-19
STP and MST Configuration Guidelines and Restrictions	14-20
Configuring STP	14-20
Enabling STP	14-21
Enabling the Extended System ID	14-22
Configuring the Root Bridge	14-23
Configuring a Secondary Root Bridge	14-24
Configuring STP Port Priority	14-25
Configuring STP Port Cost	14-27
Configuring the Bridge Priority of a VLAN	14-28
Configuring the Hello Time	14-30
Configuring the Forward-Delay Time for a VLAN	14-30
Configuring the Maximum Aging Time for a VLAN	14-31
Enabling Rapid-PVST	14-31
Configuring IEEE 802.1s MST	14-32
Enabling MST	14-32

CHAPTER 14

Displaying MST Configurations	14-34
Configuring MST Instance Parameters	14-37
Configuring MST Instance Port Parameters	14-38
Restarting Protocol Migration	14-38

CHAPTER 15

Configuring Optional STP Features	15-1
Understanding How PortFast Works	15-2
Understanding How BPDU Guard Works	15-2
Understanding How PortFast BPDU Filtering Works	15-2
Understanding How UplinkFast Works	15-3
Understanding How BackboneFast Works	15-4
Understanding How EtherChannel Guard Works	15-6
Understanding How Root Guard Works	15-6
Understanding How Loop Guard Works	15-6
Enabling PortFast	15-8
Enabling PortFast BPDU Filtering	15-10
Enabling BPDU Guard	15-11
Enabling UplinkFast	15-12
Enabling BackboneFast	15-13
Enabling EtherChannel Guard	15-14
Enabling Root Guard	15-14
Enabling Loop Guard	15-15

CHAPTER 16

Configuring Layer 3 Interfaces	16-1
Configuring IP Routing and Addresses	16-1
Configuring IPX Routing and Network Numbers	16-4
Configuring AppleTalk Routing, Cable Ranges, and Zones	16-5
Configuring Other Protocols on Layer 3 Interfaces	16-6

CHAPTER 17

Configuring IP Unicast Layer 3 Switching on Supervisor Engine 720	17-1
Understanding How Layer 3 Switching Works	17-2
Understanding Hardware Layer 3 Switching on PFC3 and DFC3s	17-2
Understanding Layer 3-Switched Packet Rewrite	17-2
Default Hardware Layer 3 Switching Configuration	17-4
Configuration Guidelines and Restrictions	17-5
Configuring Hardware Layer 3 Switching	17-5

Displaying Hardware Layer 3 Switching Statistics	17-6
<hr/>	
Configuring IP Multicast Layer 3 Switching on Supervisor Engine 720	18-1
Understanding How IP Multicast Layer 3 Switching Works	18-1
IP Multicast Layer 3 Switching Overview	18-2
Multicast Layer 3 Switching Cache	18-2
Layer 3-Switched Multicast Packet Rewrite	18-3
Partially and Completely Switched Flows	18-3
Non-RPF Traffic Processing	18-5
Understanding How Bidirectional PIM Works	18-6
Default IP Multicast Layer 3 Switching Configuration	18-6
IP Multicast Layer 3 Switching Configuration Guidelines and Restrictions	18-7
Restrictions	18-7
Unsupported Features	18-8
Configuring IP Multicast Layer 3 Switching	18-8
Source-Specific Multicast with IGMPv3, IGMP v3lite, and URD	18-9
Enabling IP Multicast Routing Globally	18-9
Enabling IP PIM on Layer 3 Interfaces	18-9
Enabling IP Multicast Layer 3 Switching Globally	18-10
Enabling IP Multicast Layer 3 Switching on Layer 3 Interfaces	18-10
Enabling Ingress Replication Mode	18-11
Specifying the Maximum Number of Multicast Routes	18-11
Configuring the Layer 3 Switching Global Threshold	18-12
Enabling Installation of Directly Connected Subnets	18-12
Specifying the Flow Statistics Message Interval	18-13
Enabling Shortcut-Consistency Checking	18-13
Configuring ACL-Based Filtering of RPF Failures	18-14
Displaying RPF Failure Rate-Limiting Information	18-14
Displaying IP Multicast Layer 3 Hardware Switching Summary	18-14
Displaying the IP Multicast Routing Table	18-17
Displaying IP Multicast Layer 3 Switching Statistics	18-18
Configuring Bidirectional PIM	18-19
Enabling Bidirectional PIM Globally	18-20
Configuring the Rendezvous Point for Bidirectional Groups	18-20
Setting the Bidirectional PIM Scan Interval	18-21
Displaying Bidirectional PIM Information	18-21
Using Debug Commands	18-23
Clearing IP Multicast Layer 3 Switching Statistics	18-23

CHAPTER 19**Configuring IGMP Snooping 19-1**

Understanding How IGMP Snooping Works	19-1
IGMP Snooping Overview	19-2
Joining a Multicast Group	19-2
Leaving a Multicast Group	19-4
Understanding IGMP Version 3 Support	19-5
Default IGMP Snooping Configuration	19-7
IGMP Snooping Configuration Guidelines and Restrictions	19-7
IGMP Snooping Querier Configuration Guidelines and Restrictions	19-7
Enabling the IGMP Snooping Querier	19-8
Configuring IGMP Snooping	19-8
Enabling IGMP Snooping	19-9
Configuring a Member Port Statically	19-10
Configuring a Multicast Router Port Statically	19-10
Configuring the IGMP Query Interval	19-11
Enabling IGMP Fast-Leave Processing	19-11
Enabling SSM Safe Reporting	19-12
Configuring IGMPv3 Explicit Host Tracking	19-12
Displaying IGMP Snooping Information	19-13

CHAPTER 20**Configuring RGMP 20-1**

Understanding How RGMP Works	20-1
Default RGMP Configuration	20-2
RGMP Configuration Guidelines and Restrictions	20-2
Enabling RGMP on Layer 3 Interfaces	20-3

CHAPTER 21**Configuring Network Security 21-1**

Configuring MAC Address-Based Traffic Blocking	21-1
Configuring TCP Intercept	21-2
Configuring Unicast Reverse Path Forwarding Check	21-2
Understanding Unicast RPF Check Support	21-2
Configuring Unicast RPF Check	21-3

CHAPTER 22**Understanding Cisco IOS ACL Support 22-1**

Cisco IOS ACL Configuration Guidelines and Restrictions	22-1
Hardware and Software ACL Support	22-2
Guidelines and Restrictions for Using Layer 4 Operators in ACLs	22-2

Determining Layer 4 Operation Usage	22-3
Determining Logical Operation Unit Usage	22-3

CHAPTER 23**Configuring VLAN ACLs** **23-1**

Understanding VACLs	23-1
VACL Overview	23-1
Bridged Packets	23-2
Routed Packets	23-2
Multicast Packets	23-3
Configuring VACLs	23-4
VACL Configuration Overview	23-4
Defining a VLAN Access Map	23-5
Configuring a Match Clause in a VLAN Access Map Sequence	23-6
Configuring an Action Clause in a VLAN Access Map Sequence	23-6
Applying a VLAN Access Map	23-7
Verifying VLAN Access Map Configuration	23-7
VLAN Access Map Configuration and Verification Examples	23-7
Configuring VACL Logging	23-8

CHAPTER 24**Configuring PFC QoS** **24-1**

Understanding How PFC QoS Works	24-1
QoS Terminology	24-2
PFC QoS Feature Flowcharts	24-4
PFC QoS Feature Summary	24-8
Ingress LAN Port Features	24-9
PFC3 Marking and Policing	24-13
LAN Egress Port Features	24-18
PFC QoS Default Configuration	24-21
PFC QoS Configuration Guidelines and Restrictions	24-28
Configuring PFC QoS	24-30
Enabling PFC QoS Globally	24-31
Enabling or Disabling Microflow Policing	24-31
Enabling Microflow Policing of Bridged Traffic	24-32
Enabling VLAN-Based PFC QoS on Layer 2 LAN Ports	24-33
Enabling or Disabling PFC Features on an Interface	24-33
Creating Named Aggregate Policers	24-34
Configuring a PFC QoS Policy	24-37
Configuring Egress DSCP Mutation	24-49
Configuring DSCP Value Maps	24-51

Configuring the Trust State of 1p1q0t, 1p1q8t, Gigabit Ethernet, and OSM Ports	24-56
Configuring the Ingress LAN Port CoS Value	24-56
Configuring LAN-Port Drop Threshold Percentages	24-57
Enabling and Disabling WRED-Drop Thresholds	24-62
Mapping CoS Values to LAN-Port Drop Thresholds	24-62
Allocating Bandwidth Between LAN-Port Transmit Queues	24-67
Setting the Receive-Queue Size Ratio on a 1p1q0t or 1p1q8t Ingress LAN Ports	24-67
Setting the LAN-Port Transmit-Queue Size Ratio	24-68

CHAPTER 25**Configuring PFC QoS Statistics Data Export** **25-1**

Understanding PFC QoS Statistics Data Export	25-1
PFC QoS Statistics Data Export Default Configuration	25-1
Configuring PFC QoS Statistics Data Export	25-2

CHAPTER 26**Configuring the Cisco IOS Firewall Feature Set** **26-1**

Cisco IOS Firewall Feature Set Support Overview	26-1
Cisco IOS Firewall Guidelines and Restrictions	26-2
Additional CBAC Configuration	26-3

CHAPTER 27**Configuring IEEE 802.1X Port-Based Authentication** **27-1**

Understanding 802.1X Port-Based Authentication	27-1
Device Roles	27-2
Authentication Initiation and Message Exchange	27-3
Ports in Authorized and Unauthorized States	27-4
Supported Topologies	27-4
Default 802.1X Port-Based Authentication Configuration	27-5
802.1X Port-Based Authentication Guidelines and Restrictions	27-6
Configuring 802.1X Port-Based Authentication	27-7
Enabling 802.1X Port-Based Authentication	27-7
Configuring Switch-to-RADIUS-Server Communication	27-8
Enabling Periodic Reauthentication	27-10
Manually Reauthenticating the Client Connected to a Port	27-11
Initializing Authentication for the Client Connected to a Port	27-11
Changing the Quiet Period	27-11
Changing the Switch-to-Client Retransmission Time	27-12
Setting the Switch-to-Client Retransmission Time for EAP-Request Frames	27-13
Setting the Switch-to-Authentication-Server Retransmission Time for Layer 4 Packets	27-13
Setting the Switch-to-Client Frame Retransmission Number	27-14

Enabling Multiple Hosts	27-14
Resetting the 802.1X Configuration to the Default Values	27-15
Displaying 802.1X Status	27-15

CHAPTER 28

Configuring Port Security 28-1

Understanding Port Security	28-1
Default Port Security Configuration	28-2
Port Security Guidelines and Restrictions	28-2
Configuring Port Security	28-3
Configuring Port Security on an Interface	28-3
Configuring Port Security Aging	28-5
Displaying Port Security Settings	28-5

CHAPTER 29

Configuring Traffic Storm Control 29-1

Understanding Traffic Storm Control	29-1
Default Traffic Storm Control Configuration	29-2
Enabling Traffic Storm Control	29-2
Displaying Traffic Storm Control Settings	29-3

CHAPTER 30

Configuring CDP 30-1

Understanding How CDP Works	30-1
Configuring CDP	30-1
Enabling CDP Globally	30-2
Displaying the CDP Global Configuration	30-2
Enabling CDP on a Port	30-2
Displaying the CDP Interface Configuration	30-3
Monitoring and Maintaining CDP	30-3

CHAPTER 31

Configuring UDLD 31-1

Understanding How UDLD Works	31-1
UDLD Overview	31-1
UDLD Aggressive Mode	31-2
Default UDLD Configuration	31-3
Configuring UDLD	31-3
Enabling UDLD Globally	31-3
Enabling UDLD on Individual LAN Interfaces	31-4
Disabling UDLD on Fiber-Optic LAN Interfaces	31-4

CHAPTER 32

- Configuring the UDLD Probe Message Interval **31-5**
 Resetting Disabled LAN Interfaces **31-5**

CHAPTER 33

- Configuring NetFlow and NDE** **32-1**
- Understanding How NetFlow and NDE Work **32-1**
 - NetFlow and NDE Overview **32-2**
 - NetFlow and NDE on the MSFC3 **32-2**
 - NetFlow and NDE on the PFC3 **32-2**
 - Default NetFlow and NDE Configuration **32-8**
 - Configuring NetFlow and NDE **32-8**
 - Configuring NetFlow and NDE on the PFC3 **32-8**
 - Configuring NetFlow and NDE on the MSFC3 **32-14**
 - Displaying the NDE Address and Port Configuration **32-16**
 - Configuring NDE Flow Filters **32-17**
 - Displaying the NDE Configuration **32-19**
- Configuring Local SPAN and RSPAN** **33-1**
- Understanding How Local SPAN and RSPAN Work **33-1**
 - Local SPAN and RSPAN Overview **33-1**
 - Local SPAN and RSPAN Sessions **33-3**
 - Monitored Traffic **33-4**
 - SPAN Sources **33-4**
 - Destination Ports **33-5**
 - Local SPAN and RSPAN Configuration Guidelines and Restrictions **33-5**
 - Local SPAN and RSPAN Session Limits **33-5**
 - Local SPAN and RSPAN Source and Destination Limits **33-6**
 - Local SPAN and RSPAN Guidelines and Restrictions **33-6**
 - VSPAN Guidelines and Restrictions **33-7**
 - RSPAN Guidelines and Restrictions **33-7**
 - Configuring Local SPAN and RSPAN **33-8**
 - Local SPAN and RSPAN Configuration Overview **33-8**
 - Configuring RSPAN VLANs **33-8**
 - Configuring Local or RSPAN Sources **33-9**
 - Monitoring Specific Source VLANs on a Source Trunk Port **33-10**
 - Configuring Local SPAN and RSPAN Destinations **33-10**
 - Verifying the Configuration **33-12**
 - Configuration Examples **33-12**

CHAPTER 34

Configuring SNMP IfIndex Persistence	35-1
Understanding SNMP IfIndex Persistence	35-1
Configuring SNMP IfIndex Persistence	35-1
Enabling SNMP IfIndex Persistence Globally	35-2
Disabling SNMP IfIndex Persistence Globally	35-2
Enabling and Disabling SNMP IfIndex Persistence on Specific Interfaces	35-2
Clearing SNMP IfIndex Persistence Configuration from a Specific Interface	35-3

CHAPTER 35

Power Management and Environmental Monitoring	36-1
Understanding How Power Management Works	36-1
Enabling or Disabling Power Redundancy	36-2
Powering Modules Off and On	36-3
Viewing System Power Status	36-3
Power Cycling Modules	36-4
Determining System Power Requirements	36-4
Understanding How Environmental Monitoring Works	36-4
Monitoring System Environmental Status	36-4
Understanding LED Environmental Indications	36-6

CHAPTER 36

Configuring Online Diagnostics	36-1
Understanding How Online Diagnostics Work	36-1
Configuring Online Diagnostics	36-2
Setting Bootup Online Diagnostics Level	36-2
Configuring On-Demand Online Diagnostics	36-2
Scheduling Online Diagnostics	36-3
Configuring Health-Monitoring Diagnostics	36-4
Running Online Diagnostic Tests	36-4
Starting and Stopping Online Diagnostic Tests	36-4
Displaying Online Diagnostic Tests and Test Results	36-5

APPENDIX A

Acronyms	A-1
-----------------	------------

INDEX



Preface

This preface describes who should read the *Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide*, how it is organized, and its document conventions.

Audience

This guide is for experienced network administrators who are responsible for configuring and maintaining Catalyst 6500 series switches.

Organization

This guide is organized as follows:

Chapter	Title	Description
Chapter 1	Product Overview	Presents an overview of the Catalyst 6500 series switches.
Chapter 2	Command-Line Interfaces	Describes how to use the command-line interface (CLI).
Chapter 3	Configuring the Switch for the First Time	Describes how to perform a baseline configuration.
Chapter 4	Configuring a Supervisor Engine 720	Describes how to configure a Supervisor Engine 720.
Chapter 5	Configuring Interfaces	Describes how to configure non-layer-specific features on LAN interfaces.
Chapter 6	Configuring RPR and RPR+ Supervisor Engine Redundancy	Describes how to configure RPR and RPR+ supervisor engine redundancy.
Chapter 7	Configuring LAN Ports for Layer 2 Switching	Describes how to configure LAN interfaces to support Layer 2 features, including VLAN trunks.
Chapter 8	Configuring EtherChannels	Describes how to configure Layer 2 and Layer 3 EtherChannel port bundles.
Chapter 9	Configuring VTP	Describes how to configure the VLAN Trunking Protocol (VTP).

Chapter	Title	Description
Chapter 10	Configuring VLANs	Describes how to configure VLANs.
Chapter 11	Configuring Private VLANs	Describes how to configure private VLANs.
Chapter 12	Configuring Cisco IP Phone Support	Describes how to configure Cisco IP Phone support.
Chapter 13	Configuring IEEE 802.1Q Tunneling and Layer 2 Protocol Tunneling	Describes how to configure IEEE 802.1Q tunneling and Layer 2 protocol tunneling.
Chapter 14	Configuring STP and IEEE 802.1s MST	Describes how to configure the Spanning Tree Protocol (STP) and explains how STP works.
Chapter 15	Configuring Optional STP Features	Describes how to configure the STP PortFast, UplinkFast, and BackboneFast features.
Chapter 16	Configuring Layer 3 Interfaces	Describes how to configure LAN interfaces to support Layer 3 features.
Chapter 17	Configuring IP Unicast Layer 3 Switching on Supervisor Engine 720	Describes how to configure IP unicast Layer 3 switching for Supervisor Engine 720.
Chapter 18	Configuring IP Multicast Layer 3 Switching on Supervisor Engine 720	Describes how to configure IP Multicast Multilayer Switching (MMLS).
Chapter 19	Configuring IGMP Snooping	Describes how to configure Internet Group Management Protocol (IGMP) snooping.
Chapter 20	Configuring RGMP	Describes how to configure Router-Port Group Management Protocol (RGMP).
Chapter 21	Configuring Network Security	Describes how to configure network security features that are unique to the Catalyst 6500 series switches.
Chapter 22	Understanding Cisco IOS ACL Support	Describes how Catalyst 6500 series switches support Cisco IOS ACLs.
Chapter 23	Configuring VLAN ACLs	Describes how to configure VLAN ACLs.
Chapter 24	Configuring PFC QoS	Describes how to configure quality of service (QoS).
Chapter 25	Configuring PFC QoS Statistics Data Export	Describes how to configure PFC QoS statistics data export.
Chapter 26	Configuring the Cisco IOS Firewall Feature Set	Describes how to configure the Cisco IOS Firewall feature set.
Chapter 27	Configuring IEEE 802.1X Port-Based Authentication	Describes how to configure IEEE 802.1X port-based authentication.
Chapter 28	Configuring Port Security	Describes how to configure port security.
Chapter 29	Configuring Traffic Storm Control	Describes how to configure traffic storm control.
Chapter 30	Configuring CDP	Describes how to configure Cisco Discovery Protocol (CDP).
Chapter 31	Configuring UDLD	Describes how to configure the UniDirectional Link Detection (UDLD) protocol.
Chapter 32	Configuring NetFlow and NDE	Describes how to configure NetFlow and NDE.

Chapter	Title	Description
Chapter 33	Configuring Local SPAN and RSPAN	Describes how to configure the Switch Port Analyzer (SPAN).
Chapter 34	Configuring SNMP IfIndex Persistence	Describes how to configure SNMP ifIndex persistence.
Chapter 35	Power Management and Environmental Monitoring	Describes how to configure power management and environmental monitoring features.
Chapter 36	Configuring Online Diagnostics	Describes how to configure online diagnostics and run diagnostic tests.

Related Documentation

The following publications are available for the Catalyst 6500 series switches:

- *Catalyst 6500 Series Switch Installation Guide*
- *Catalyst 6500 Series Switch Module Installation Guide*
- *Catalyst 6500 Series Switch Cisco IOS Command Reference*
- *Catalyst 6500 Series Switch Cisco IOS System Message Guide*
- *Release Notes for Cisco IOS Release 12.2SX on the Catalyst 6500 and Cisco 7600*
- *Cisco IOS Configuration Guides and Command References*—Use these publications to help you configure Cisco IOS software features not described in the Catalyst 6500 series switch publications:
 - *Configuration Fundamentals Configuration Guide*
 - *Configuration Fundamentals Command Reference*
 - *Bridging and IBM Networking Configuration Guide*
 - *Bridging and IBM Networking 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 Home Applications Configuration Guide*
 - *Voice, Video, and Home Applications Command Reference*
 - *Software Command Summary*
 - *Software System Error Messages*
 - *Debug Command Reference*
 - *Internetwork Design Guide*
 - *Internetwork Troubleshooting Guide*

- *Configuration Builder Getting Started Guide*

The Cisco IOS Configuration Guides and Command References are located at this URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/index.htm>

- For information about MIBs, go to this URL:

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

Conventions

This document uses the following conventions:

Convention	Description
boldface font	Commands, command options, and keywords are in boldface .
<i>italic</i> font	Arguments for which you supply values are in <i>italics</i> .
[]	Elements in square brackets are optional.
{ x y z }	Alternative keywords 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 or the string will include the quotation marks.
screen font	Terminal sessions and information the system displays are in <i>screen</i> font.
boldface screen font	Information you must enter 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.
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords are in angle brackets.

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.

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-CONDODCD=) 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_inpck/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.

■ Obtaining Technical Assistance

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

■ Obtaining Additional Publications and Information

- 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



CHAPTER

1

Product Overview

This chapter consists of these sections:

- [Supported Hardware and Software, page 1-1](#)
- [User Interfaces, page 1-1](#)
- [Configuring Embedded CiscoView Support, page 1-2](#)
- [Software Features Supported in Hardware by the PFC3 and DFC3, page 1-3](#)

Supported Hardware and Software

Refer to the *Release Notes for Cisco IOS Release 12.2SX on the Catalyst 6500 and Cisco 7600* publication for complete information about the chassis, modules, and software features supported by the Catalyst 6500 series switches:

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/index.htm>

User Interfaces

Release 12.2(14)SX supports configuration using the following interfaces:

- CLI—See [Chapter 2, “Command-Line Interfaces.”](#)
- SNMP—Refer to the *Release 12.2 IOS Configuration Fundamentals Configuration Guide* and *Command Reference* at this URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/index.htm
- IOS web browser interface—Refer to “Using the Cisco Web Browser” in the *IOS Configuration Fundamentals Configuration Guide* at this URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/ffcprt1/fcf005.htm
- Embedded CiscoView—See the “[Configuring Embedded CiscoView Support](#)” section on page 1-2.

Configuring Embedded CiscoView Support

These sections describe configuring Embedded CiscoView support:

- [Understanding Embedded CiscoView, page 1-2](#)
- [Installing and Configuring Embedded CiscoView, page 1-2](#)
- [Displaying Embedded CiscoView Information, page 1-3](#)

Understanding Embedded CiscoView

The Embedded CiscoView network management system is a web-based interface that uses HTTP and SNMP to provide a graphical representation of the switch and to provide a GUI-based management and configuration interface. You can download the Java Archive (JAR) files for Embedded CiscoView at this URL:

<http://www.cisco.com/kobayashi/sw-center/netmgmt/ciscoview/embed-cview-planner.shtml>

Installing and Configuring Embedded CiscoView

To install and configure Embedded CiscoView, perform the following steps:

	Command	Purpose
Step 1	<code>Router# dir device_name</code>	Displays the contents of the device. If you are installing Embedded CiscoView for the first time, or if the CiscoView directory is empty, skip to Step 4 .
Step 2	<code>Router# delete device_name:cv/*</code>	Removes existing files from the CiscoView directory.
Step 3	<code>Router# squeeze device_name:</code>	Recovers the space in the file system.
Step 4	<code>Router# archive tar /xtract tftp:// ip address of tftp server/ciscoview.tar device_name:cv</code>	Extracts the CiscoView files from the tar file on the TFTP server to the CiscoView directory.
Step 5	<code>Router# dir device_name:</code>	Displays the contents of the device. In a redundant configuration, repeat Step 1 through Step 5 for the file system on the redundant supervisor engine.
Step 6	<code>Router# configure terminal</code>	Enters global configuration mode.
Step 7	<code>Router(config)# ip http server</code>	Enables the HTTP web server.
Step 8	<code>Router(config)# snmp-server community string ro</code>	Configures the SNMP password for read-only operation.
Step 9	<code>Router(config)# snmp-server community string rw</code>	Configures the SNMP password for read/write operation.



Note The default password for accessing the switch web page is the enable-level password of the switch.

For more information about web access to the switch, refer to “Using the Cisco Web Browser” in the *IOS Configuration Fundamentals Configuration Guide* at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fun_c/ffcprt1/fcf005.htm

Displaying Embedded CiscoView Information

To display the Embedded CiscoView information, enter the following EXEC commands:

Command	Purpose
Router# show ciscoview package	Displays information about the Embedded CiscoView files.
Router# show ciscoview version	Displays the Embedded CiscoView version.

Software Features Supported in Hardware by the PFC3 and DFC3

The Policy Feature Card 3 (PFC3) and Distributed Forwarding Card 3 (DFC3) provide hardware support for these Cisco IOS software features:

- Access Control Lists (ACLs) for Layer 3 ports and VLAN interfaces
 - Permit and deny actions of input and output standard and extended ACLs



Note Flows that require ACL logging are processed in software on the MSFC3.

- Reflexive ACL flows after the first packet in a session are processed in software on the MSFC3
- Dynamic ACL flows



Note Idle timeout is processed in software on the MSFC3.

For more information about PFC3 and DFC3 support for ACLs, see [Chapter 22, “Understanding Cisco IOS ACL Support.”](#)

For complete information about configuring ACLs, refer to the Cisco IOS Security Configuration Guide, Release 12.2, "Traffic Filtering and Firewalls," at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/ftrafwl/index.htm

- VLAN ACLs (VACLs)—To configure VACLs, see [Chapter 23, “Configuring VLAN ACLs.”](#)

■ Software Features Supported in Hardware by the PFC3 and DFC3

- Policy-based routing (PBR) for route-map sequences that use the **match ip address**, **set ip next-hop**, and **ip default next-hop** PBR keywords.

To configure PBR, refer to the *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.2, “Classification,” “Configuring Policy-Based Routing,” at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgr/fqos_c/fqcpmt1/qcfpbr.htm



Note If the MSFC3 address falls within the range of a PBR ACL, traffic addressed to the MSFC3 is policy routed in hardware instead of being forwarded to the MSFC3. To prevent policy routing of traffic addressed to the MSFC3, configure PBR ACLs to deny traffic addressed to the MSFC3.

- TCP intercept—To configure TCP intercept, see the “[Configuring TCP Intercept](#)” section on [page 21-2](#).
- Hardware-assisted NetFlow Aggregation—Refer to this URL:
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/nde.htm#1081085>
- Unicast Reverse Path Forwarding (RPF) Check—To configure Unicast RPF Check, see the “[Configuring Unicast Reverse Path Forwarding Check](#)” section on [page 21-2](#).
- Network Address Translation (NAT) for IPv4 unicast and multicast traffic.

Note the following information about hardware-assisted NAT:

- The PFC3 does not support NAT translation of multicast traffic.
- The PFC3 does not support NAT translation of UDP traffic.
- The PFC3 does not support NAT configured with a route-map that specifies length.
- When you configure NAT and NDE on an interface, the PFC3 sends all traffic in fragmented packets to the MSFC3 to be processed in software. (CSCdz51590)

To configure NAT, refer to the *Cisco IOS IP Configuration Guide*, Release 12.2, “IP Addressing and Services,” “Configuring IP Addressing,” “Configuring Network Address Translation,” at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgr/fipr_c/IPCPT1/1cfipadr.htm#1042290

To prevent a significant volume of NAT traffic from being sent to the MSFC3, due to either a DoS attack or a misconfiguration, enter the **mls rate-limit unicast acl {ingress | egress}** command described at this URL:

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/cmdref/m1.htm#56404>

(CSCe23296)

- GRE Tunneling and IP in IP Tunneling—The PFC3 and DFC3s support the following **tunnel** commands:
 - **tunnel destination**
 - **tunnel mode gre**
 - **tunnel mode ipip**
 - **tunnel source**
 - **tunnel ttl**
 - **tunnel tos**

The MSFC3 supports tunneling configured with any other **tunnel** commands.

The **tunnel ttl** command (default 255) sets the TTL of encapsulated packets.

The **tunnel tos** command, if present, sets the ToS byte of a packet when it is encapsulated. If the **tunnel tos** command is not present and QoS is not enabled, the ToS byte of a packet sets the ToS byte of the packet when it is encapsulated. If the **tunnel tos** command is not present and QoS is enabled, the ToS byte of a packet as modified by PFC QoS sets the ToS byte of the packet when it is encapsulated.

To configure GRE Tunneling and IP in IP Tunneling, refer to these publications:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/finter_c/icflogin.htm#1012601

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/finter_r/irfshtoip.htm

To configure the **tunnel tos** and **tunnel ttl** commands, refer to this publication:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s17/12s_tos.htm

Note the following information about tunnels:

- Each tunnel interface uses one internal VLAN.
- Each tunnel interface uses one additional router MAC address entry per router MAC address.
- You cannot configure any PFC QoS features on tunnel interfaces.
- The MSFC3 supports tunnels configured with egress features on the tunnel interface. Examples of egress features are output Cisco IOS ACLs, NAT (for inside to outside translation), TCP intercept, CBAC, WCCP, and encryption.
- The PFC3 does not support GRE tunnel encapsulation and de-encapsulation of multicast traffic.
- Firewall feature set images provide these features:
 - Context-Based Access Control (CBAC) —The PFC3 installs entries in the Netflow table to direct flows that require CBAC to the MSFC3 where the CBAC is applied in software on the MSFC3.
 - Authentication Proxy—After authentication on the MSFC3, the PFC3 provides TCAM support for the authentication policy.
 - Port-to-Application Mapping (PAM)—PAM is done in software on the MSFC3.

To configure firewall features, see [Chapter 26, “Configuring the Cisco IOS Firewall Feature Set.”](#)

■ Software Features Supported in Hardware by the PFC3 and DFC3



CHAPTER

2

Command-Line Interfaces

This chapter describes the command-line interfaces (CLIs) you use to configure the Catalyst 6500 series switches.



Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication and the Release 12.2 publications at this URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/index.htm>

This chapter consists of these sections:

- [Accessing the CLI, page 2-1](#)
- [Performing Command Line Processing, page 2-3](#)
- [Performing History Substitution, page 2-3](#)
- [Cisco IOS Command Modes, page 2-4](#)
- [Displaying a List of Cisco IOS Commands and Syntax, page 2-5](#)
- [ROM-Monitor Command-Line Interface, page 2-6](#)

Accessing the CLI

These sections describe accessing the CLI:

- [Accessing the CLI through the EIA/TIA-232 Console Interface, page 2-1](#)
- [Accessing the CLI through Telnet, page 2-2](#)

Accessing the CLI through 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).

■ Accessing the CLI

Perform initial configuration over a connection to the EIA/TIA-232 console interface. Refer to the *Catalyst 6500 Series Switch Module Installation Guide* for console interface cable connection procedures.

To make a console connection, perform this task:

Command	Purpose
Step 1 Press Return .	Brings up the prompt.
Step 2 Router> enable	Initiates enable mode enable.
Step 3 Password: <i>password</i> Router#	Completes enable mode enable.
Step 4 Router# quit	Exits the session when finished.

After making a console connection, you see this display:

```
Press Return for Console prompt
Router> enable
Password:
Router#
```

Accessing the CLI through Telnet



Note Before you can make a Telnet connection to the switch, you must configure an IP address (see the “Configuring IP Routing and Addresses” section on page 16-1).

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

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

Command	Purpose
Step 1 telnet {hostname ip_addr}	Makes a Telnet connection from the remote host, to the switch you want to access.
Step 2 Password: <i>password</i> Router#	Initiates authentication. Note If no password has been configured, press Return .
Step 3 Router> enable	Initiates enable mode enable.
Step 4 Password: <i>password</i> Router#	Completes enable mode enable.
Step 5 Router# quit	Exits the session when finished.

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

```
unix_host% telnet Router_1
Trying 172.20.52.40...
Connected to 172.20.52.40.
Escape character is '^]'.

User Access Verification

Password:
Router_1> enable
Password:
Router_1#
```

Performing Command Line Processing

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 the command at the prompt. [Table 2-1](#) lists the keyboard shortcuts for entering and editing commands.

Table 2-1 Keyboard Shortcuts

Keystrokes	Purpose
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 commands you entered. History substitution allows you to access these commands without retyping them, by using special abbreviated commands. [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 successively older commands.
Ctrl-N or the down arrow key. ¹	Returns to more recent commands in the history buffer after recalling commands with Ctrl-P or the up arrow key. Repeat the key sequence to recall successively more recent commands.
Router# show history	While in EXEC mode, lists the last several commands you have just entered.

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

Cisco IOS Command Modes



Note For complete information about Cisco IOS command modes, refer to the *Cisco IOS Configuration Fundamentals Configuration Guide* at this URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/index.htm

The Cisco IOS user interface is divided into many different modes. The commands available to you depend on which mode you are currently in. To get a list of the commands in a given mode, type a question mark (?) at the system prompt. See the “[Displaying a List of Cisco IOS Commands and Syntax](#)” section on page 2-5.

When you start a session on the switch, you begin in user mode, often called user EXEC mode. Only a limited subset of the commands are available in EXEC mode. To have access to all commands, you must enter privileged EXEC mode. Normally, you must type in a password to access privileged EXEC mode. From privileged EXEC mode, you can type in any EXEC command or access global configuration mode.

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



Note With Release 12.1(11b)E and later, when you are in configuration mode you can enter EXEC mode-level commands by entering the **do** keyword before the EXEC mode-level command.

ROM-monitor mode is a separate mode used when the switch cannot boot properly. For example, the switch might enter ROM-monitor mode if it does not find a valid system image when it is booting, or if its configuration file is corrupted at startup. See the “[ROM-Monitor 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	Description of Use	How to Access	Prompt
User EXEC	Connect to remote devices, change terminal settings on a temporary basis, perform basic tests, and display system information.	Log in.	Router>
Privileged EXEC (enable)	Set operating parameters. The privileged command set includes the commands in user EXEC mode, as well as the configure command. Use this command to access the other command modes.	From the user EXEC mode, enter the enable command and the enable password.	Router#
Global configuration	Configure features that affect the system as a whole.	From the privileged EXEC mode, enter the configure terminal command.	Router (config)#
Interface configuration	Many features are enabled for a particular interface. Interface commands enable or modify the operation of an interface.	From global configuration mode, enter the interface type slot/port command.	Router (config-if)#
Console configuration	From the directly connected console or the virtual terminal used with Telnet, use this configuration mode to configure the console interface.	From global configuration mode, enter the line console 0 command.	Router (config-line)#

The Cisco IOS command interpreter, called the EXEC, interprets and executes 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 **config 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**.

Displaying a List of Cisco IOS Commands and Syntax

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

```
Router> ?
```

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

```
Router# co?
configure
```

To display 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.

For example:

```
Router# 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.

Enter **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.

ROM-Monitor Command-Line Interface

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

You can also enter ROM-monitor mode by restarting and pressing the **Break** key during the first 60 seconds of startup.



Note The **Break** key is always enabled for 60 seconds after rebooting, regardless of whether the **Break** key is configured to be off by configuration register settings.

To access the ROM-monitor mode through a terminal server, you can escape to the Telnet prompt and enter the **send break** command for your terminal emulation program to break into ROM-monitor mode.

Once you are in ROM-monitor mode, the prompt changes to rommon 1>. Enter a question mark (?) to see the available ROM-monitor commands.

For more information about the ROM-monitor commands, refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication.



CHAPTER

3

Configuring the Switch for the First Time

This chapter contains information about how to initially configure the Catalyst 6500 series switch, which supplements the administration information and procedures in these publications:

- *Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.2, at this URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/index.htm
- *Cisco IOS Configuration Fundamentals Configuration Command Reference*, Release 12.2, at this URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_r/index.htm



Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication and the Release 12.2 publications at this URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/index.htm>

This chapter consists of these sections:

- [Default Configuration, page 3-1](#)
- [Configuring the Switch, page 3-2](#)
- [Protecting Access to Privileged EXEC Commands, page 3-15](#)
- [Recovering a Lost Enable Password, page 3-19](#)
- [Modifying the Supervisor Engine Startup Configuration, page 3-20](#)

Default Configuration

[Table 3-1](#) shows the default configuration.

Table 3-1 Default Configuration

Feature	Default Value
Administrative connection	Normal mode
Global information	No value for the following: <ul style="list-style-type: none"> • System name • System contact • Location
System clock	No value for system clock time
Passwords	No passwords configured for normal mode or enable mode (press the Return key)
Prompt	Router>

Configuring the Switch

These sections describe how to configure the switch:

- [Using the Setup Facility or the setup Command, page 3-2](#)
- [Using Configuration Mode, page 3-10](#)
- [Checking the Running Configuration Before Saving, page 3-10](#)
- [Saving the Running Configuration Settings, page 3-11](#)
- [Reviewing the Configuration, page 3-11](#)
- [Configuring a Default Gateway, page 3-11](#)
- [Configuring a Static Route, page 3-12](#)
- [Configuring a BOOTP Server, page 3-13](#)

Using the Setup Facility or the **setup** Command

These sections describe the setup facility and the **setup** command:

- [Setup Overview, page 3-2](#)
- [Configuring the Global Parameters, page 3-3](#)
- [Configuring Interfaces, page 3-8](#)

Setup Overview

At initial startup, the switch automatically defaults to the setup facility. (The **setup** command facility functions exactly the same as a completely unconfigured system functions when you first boot it up.) You can run the setup facility by entering the **setup** command at the enable prompt (#).

When you enter the **setup** command, current system configuration defaults are displayed in square brackets [] as you move through the **setup** command process and are queried by the system to make changes.

For example, you will see this display when you use the setup facility:

```
Configuring interface FastEthernet3/1:  
Is this interface in use?: yes  
Configure IP on this interface?: yes
```

When you use the **setup** command, you see this display:

```
Configuring interface FastEthernet4/1:  
Is this interface in use? [yes] : yes  
Configure IP on this interface? [yes] : yes
```

Configuring the Global Parameters

When you first start the setup facility or enter the **setup** command, you are queried by the system to configure the global parameters, which are used for controlling system-wide settings.

To boot the switch and enter the global parameters, follow these steps:

- Step 1** Connect a console terminal to the console interface on the supervisor engine, and then boot the system to the user EXEC prompt (Router>).

The following display appears after you boot the Catalyst 6500 series switch (depending on your configuration, your display might not exactly match the example):

```
System Bootstrap, Version 6.1(2)  
Copyright (c) 1994-2000 by cisco Systems, Inc.  
c6k_sup2 processor with 131072 Kbytes of main memory
```

```
rommon 1 > boot slot0:c6sup22-jsv-mz.121-5c.EX.bin
```

```
Self decompressing the image : #####  
#####  
#####  
#####  
#####  
#####  
#####  
#####  
#####  
#####  
#####  
[OK]
```

Restricted Rights Legend

Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

```
Cisco Internetwork Operating System Software  
IOS (tm) c6sup2_sp Software (c6sup2_sp-SPV-M), Version 12.1(5c)EX, EARLY DEPLOYMENT RELEASE SOFTWARE (fc1)  
Synced to mainline version: 12.1(5c)  
TAC:Home:Software:Ios General:CiscoIOSRoadmap:12.1  
Copyright (c) 1986-2001 by cisco Systems, Inc.  
Compiled Wed 28-Mar-01 18:36 by hqluong  
Image text-base: 0x30020980, data-base: 0x306B8000
```

Configuring the Switch

```

Start as Primary processor

00:00:05: %SYS-3-LOGGER_FLUSHING: System pausing to ensure console debugging output.

00:00:03: Currently running ROMMON from S (Gold) region
00:00:05: %OIR-6-CONSOLE: Changing console ownership to route processor


System Bootstrap, Version 12.1(3r)E2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.
Cat6k-MSFC2 platform with 131072 Kbytes of main memory

rommon 1 > boot

Self decompressing the image : #####
#####
## [OK]

Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706


Cisco Internetwork Operating System Software
IOS (tm) MSFC2 Software (C6MSFC2-BOOT-M), Version 12.1(3a)E4, EARLY DEPLOYMENT R
ELEASE SOFTWARE (fc1)
Copyright (c) 1986-2000 by cisco Systems, Inc.
Compiled Sat 14-Oct-00 05:33 by eaarmas
Image text-base: 0x30008980, data-base: 0x303B6000

cisco Cat6k-MSFC2 (R7000) processor with 114688K/16384K bytes of memory.
Processor board ID SAD04430J9K
R7000 CPU at 300Mhz, Implementation 39, Rev 2.1, 256KB L2, 1024KB L3 Cache
Last reset from power-on
X.25 software, Version 3.0.0.
509K bytes of non-volatile configuration memory.

16384K bytes of Flash internal SIMM (Sector size 512K).

Press RETURN to get started!

```



Note The first two sections of the configuration script (the banner and the installed hardware) appear only at initial system startup. On subsequent uses of the **setup** command facility, the setup script begins with the following System Configuration Dialog.

```
--- System Configuration Dialog ---
```

```
Continue with configuration dialog? [yes/no]: y
```

At any point you may enter a question mark '?' for help.
Use **ctrl-c** to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system



Note The examples in this section are intended as examples only. Your configuration might look differently depending on your system configuration.

- Step 2** Enter **yes** or press **Return** when asked if you want to enter the configuration dialog and if you want to see the current interface summary. Press **Return** to accept the default (yes):

Would you like to enter the initial configuration dialog? [yes]:

First, would you like to see the current interface summary? [yes]:

This example of a **yes** response (displayed during the setup facility) shows a switch at first-time startup; that is, nothing has been configured:

Current interface summary

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	unassigned	YES	TFTP	administratively down	down
GigabitEthernet1/1	unassigned	YES	TFTP	administratively down	down
GigabitEthernet1/2	unassigned	YES	TFTP	administratively down	down
GigabitEthernet3/1	unassigned	YES	TFTP	administratively down	down
GigabitEthernet3/2	unassigned	YES	TFTP	administratively down	down
GigabitEthernet3/3	unassigned	YES	TFTP	administratively down	down
GigabitEthernet3/4	unassigned	YES	TFTP	administratively down	down
GigabitEthernet3/5	unassigned	YES	TFTP	administratively down	down
GigabitEthernet3/6	unassigned	YES	TFTP	administratively down	down
GigabitEthernet3/7	unassigned	YES	TFTP	administratively down	down
GigabitEthernet3/8	unassigned	YES	TFTP	administratively down	down

(Additional displayed text omitted from this example.)

This example of a **yes** response (displayed during the setup command facility) shows a switch with some interfaces already configured:

Current interface summary

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	unassigned	YES	TFTP	administratively down	down
GigabitEthernet1/1	172.20.52.34	YES	NVRAM	up	up
GigabitEthernet1/2	unassigned	YES	TFTP	administratively down	down

Configuring the Switch

```

GigabitEthernet3/1      unassigned     YES TFTP    administratively down down
GigabitEthernet3/2      unassigned     YES TFTP    administratively down down
GigabitEthernet3/3      unassigned     YES TFTP    administratively down down
GigabitEthernet3/4      unassigned     YES TFTP    administratively down down
GigabitEthernet3/5      unassigned     YES TFTP    administratively down down
GigabitEthernet3/6      unassigned     YES TFTP    administratively down down
GigabitEthernet3/7      unassigned     YES TFTP    administratively down down
GigabitEthernet3/8      unassigned     YES TFTP    administratively down down
<...output truncated...>

```

- Step 3** Choose which protocols to support on your interfaces. On IP installations only, you can accept the default values for most of the questions.

A typical minimal configuration using IP follows and continues through [Step 8](#):

Configuring global parameters:

```
Enter host name [Router]: Router
```

- Step 4** Enter the enable secret password when the following is displayed (remember this password for future reference):

The enable secret is a password used to protect access to privileged EXEC and configuration modes. This password, after entered, becomes encrypted in the configuration.

Enter enable secret: **barney**

- Step 5** Enter the enable password when the following is displayed (remember this password for future reference):

The enable password is used when you do not specify an enable secret password, with some older software versions, and some boot images.

Enter enable password: **wilma**

The commands available at the user EXEC level are a subset of those available at the privileged EXEC level. Because many privileged EXEC commands are used to set operating parameters, you should protect these commands with passwords to prevent unauthorized use.

You must enter the correct password to gain access to privileged EXEC commands. When you are running from the boot ROM monitor, the enable password might be the correct one to use, depending on your boot ROM level.

The enable and enable secret passwords need to be different for effective security. You can enter the same password for both enable and enable secret during the setup script, but you receive a warning message indicating that you should enter a different password.

**Note**

An enable secret password can contain from 1 to 25 uppercase and lowercase alphanumeric characters; an enable password can contain any number of uppercase and lowercase alphanumeric characters. In both cases, a number cannot be the first character. Spaces are also valid password characters; for example, “two words” is a valid password. Leading spaces are ignored; trailing spaces are recognized.

- Step 6** Enter the virtual terminal password when the following is displayed (remember this password for future reference):

```
The virtual terminal password is used to protect
access to the router over a network interface.
Enter virtual terminal password: bambam
```

- Step 7** In most cases you will use IP routing. If so, you must also select an interior routing protocol, for example, the Enhanced Interior Gateway Routing Protocol (EIGRP).

Enter **yes** (the default) or press **Return** to configure IP, and then select EIGRP:

```
Configure IP? [yes]:
Configure EIGRP routing? [yes]:
Your IGRP autonomous system number [1]: 301
```

- Step 8** Enter **yes** or **no** to accept or refuse SNMP management:

```
Configure SNMP Network Management? [yes]:
Community string [public]:
```

For complete SNMP information and procedures, refer to these publications:

- *Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.2, “Cisco IOS System Management,” “Configuring SNMP Support,” at this URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/fcfprt3/fcf014.htm
- *Cisco IOS Configuration Fundamentals Configuration Command Reference*, Release 12.2, at this URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_r/index.htm

To provide a review of what you have done, a display similar to the following appears and lists all of the configuration parameters you selected in Steps 3 through 8. These parameters and their defaults are shown in the order in which they appeared on your console terminal:

The following configuration command script was created:

```
hostname router
enable secret 5 $1$S3Lx$uiTYg2UrFK1U0dgWdjvxw.
enable password lab
line vty 0 4
password lab
no snmp-server
!
ip routing eigrp 301

!
interface Vlan1
shutdown
no ip address
!
interface GigabitEthernet1/1
shutdown
no ip address
!
interface GigabitEthernet1/2
shutdown
no ip address
!
.
<...output truncated...>
```

```

.!
end

[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]: 2
% You can enter the setup, by typing setup at IOS command prompt
Router#

```

This completes the procedure on how to configure global parameters. The setup facility continues with the process to configure interfaces in the next section “[Configuring Interfaces](#).”

Configuring Interfaces

This section provides steps for configuring installed interfaces (using the setup facility or **setup** command facility) to allow communication over your external networks. To configure the interface parameters, you need your interface network addresses, subnet mask information, and which protocols you want to configure. (For additional interface configuration information on each of the modules available, refer to the individual configuration notes that shipped with your modules.)



Note The examples in this section are intended as examples only. Your configuration might look differently depending on your system configuration.

To configure interfaces, follow these steps:

- Step 1** At the prompt for the Gigabit Ethernet interface configuration, enter the appropriate responses for your requirements, using your own address and subnet mask:

```

Do you want to configure GigabitEthernet1/1 interface? [no]: yes
Configure IP on this interface? [no]: yes
IP address for this interface: 172.20.52.34
Subnet mask for this interface [255.255.0.0] : 255.255.255.224
Class B network is 172.20.0.0, 27 subnet bits; mask is /27

```

- Step 2** At the prompt for all other interface types, enter the appropriate responses for your requirements:

```

Do you want to configure FastEthernet5/1 interface? [no]: y
Configure IP on this interface? [no]: y
IP address for this interface: 172.20.52.98
Subnet mask for this interface [255.255.0.0] : 255.255.255.248
Class B network is 172.20.0.0, 29 subnet bits; mask is /29

```

Repeat this step for each interface you need to configure. Proceed to Step 3 to check and verify your configuration parameters.

When you reach and respond to the configuration dialog for the last installed interface, your interface configuration is complete.

- Step 3** Check and verify the entire list of configuration parameters, which should display on your console terminal and end with the following query:

```
Use this configuration? [yes/no] :
```

A **no** response returns you to the enable prompt (#). You will need to reenter the **setup** command to reenter your configuration. A **yes** response saves the running configuration to NVRAM as follows:

```
Use this configuration? [yes/no] : yes
[OK]
Use the enabled mode 'configure' command to modify this configuration.
Press RETURN to get started!
```

After you press the **Return** key, this prompt appears:

```
Router>
```

This completes the procedures for configuring global parameters and interface parameters in your system. Your interfaces are now available for limited use.

If you want to modify the currently saved configuration parameters after the initial configuration, enter the **setup** command. To perform more complex configurations, enter configuration mode and use the **configure** command. Check the current state of the switch using the **show version** command, which displays the software version and the interfaces, as follows:

```
Router# show version
Cisco Internetwork Operating System Software
IOS (tm) c6sup2_rp Software (c6sup2_rp-JSV-M), Version 12.1(5c)EX, EARLY DEPLOY
Synced to mainline version: 12.1(5c)
TAC:Home:Software:Ios General:CiscoIOSRoadmap:12.1
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Wed 28-Mar-01 17:52 by hqluong
Image text-base: 0x30008980, data-base: 0x315D0000

ROM: System Bootstrap, Version 12.1(3r)E2, RELEASE SOFTWARE (fc1)
BOOTFLASH: c6sup2_rp Software (c6sup2_rp-JSV-M), Version 12.1(5c)EX, EARLY DEPL

Router uptime is 2 hours, 33 minutes
System returned to ROM by power-on (SP by power-on)
Running default software

cisco Catalyst 6000 (R7000) processor with 114688K/16384K bytes of memory.
Processor board ID SAD04430J9K
R7000 CPU at 300Mhz, Implementation 39, Rev 2.1, 256KB L2, 1024KB L3 Cache
Last reset from power-on
Bridging software.
X.25 software, Version 3.0.0.
SuperLAT software (copyright 1990 by Meridian Technology Corp).
TN3270 Emulation software.
1 Virtual Ethernet/IEEE 802.3 interface(s)
48 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)
381K bytes of non-volatile configuration memory.

16384K bytes of Flash internal SIMM (Sector size 512K).
Configuration register is 0x2
Router#
```

For detailed interface configuration information, refer to the *Cisco IOS Interface Configuration Guide* at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/finter_c/index.htm

Using Configuration Mode

If you prefer not to use the setup facility, you can configure the switch from configuration mode as follows:

-
- Step 1** Connect a console terminal to the console interface of your supervisor engine.
 - Step 2** When you are asked if you want to enter the initial dialog, answer **no** to enter the normal operating mode as follows:

```
Would you like to enter the initial dialog? [yes]: no
```

- Step 3** After a few seconds you will see the user EXEC prompt (`Router>`). Type **enable** to enter enable mode:

```
Router> enable
```



Note Configuration changes can only be made in enable mode.

The prompt will change to the privileged EXEC prompt (#) as follows:

```
Router#
```

- Step 4** At the prompt (#), enter the **configure terminal** command to enter configuration mode as follows:

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

At the prompt, enter the **interface type slot/interface** command to enter interface configuration mode as follows:

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

In either of these configuration modes, you can enter any changes to the configuration. Enter the **end** command to exit configuration mode.

- Step 5** Save your settings. (See the “[Saving the Running Configuration Settings](#)” section on page 3-11.)
-

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 Before Saving

You can check the configuration settings you entered or changes you made by entering the **show running-config** command at the privileged EXEC prompt (#) as follows:

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

Current configuration:
Current configuration : 3441 bytes
!
version 12.1
service timestamps debug datetime localtime
service timestamps log datetime localtime
```

```

no service password-encryption
!
hostname Router
!
boot bufsize 522200
boot system flash slot0:c6sup22-jsv-mz.121-5c.EX.bin
boot bootldr bootflash:c6msfc2-boot-mz.121-3a.E4
enable password lab
!
redundancy
  main-cpu
    auto-sync standard
  ip subnet-zero
  no ip finger
!
cns event-service server
!
<...output truncated...>
!
interface FastEthernet3/3
  ip address 172.20.52.19 255.255.255.224
!
<...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 mop telnet rlogin udptn nasi
!
end
Router#

```

Saving the Running Configuration Settings

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

```
Router# copy running-config startup-config
```

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.

Reviewing the Configuration

To display information stored in NVRAM, enter the **show startup-config** EXEC command. The display should be similar to the display from the **show running-config** EXEC command.

Configuring a Default Gateway



Note

The switch uses the default gateway only when it is not configured to route.

Configuring the Switch

To send data to another subnet when the switch is not configured with a routing protocol, configure a default gateway. The default gateway must be the IP address of an interface on a router in the same subnet.

To configure a default gateway, perform this task:

Command	Purpose
Step 1 Router(config)# ip default-gateway A.B.C.D	Configures a default gateway.
Step 2 Router# show ip route	Verifies that the default gateway appears correctly in the IP routing table.

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

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

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

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 Router(config)# ip route dest_IP_address mask {forwarding_IP vlan vlan_ID}	Configures a static route.
Step 2 Router# show running-config	Verifies the static route configuration.

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:

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

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

```
Router# 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

Router#

```

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

```

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

```

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

```

Router# show running-config
Building configuration...
.
<...output truncated...>
.
ip default-gateway 172.20.52.35
ip classless
ip route 171.20.52.3 255.255.255.255 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

Router#

```

Configuring a BOOTP Server

The Bootstrap Protocol (BOOTP) automatically assigns an IP address by adding the MAC and IP addresses of the interface to the BOOTP server configuration file. When the switch boots, it automatically retrieves the IP address from the BOOTP server.

The switch performs a BOOTP request *only* if the current IP address is set to 0.0.0.0. (This address is the default address for a new switch or a switch that has had its startup-config file cleared using the **erase** command.)

To allow your switch to retrieve its IP address from a BOOTP server, you must first determine the MAC address of the switch and add that MAC address to the BOOTP configuration file on the BOOTP server. To create a BOOTP server configuration file, follow these steps:

-
- Step 1** Install the BOOTP server code on the workstation, if it is not already installed.
 - Step 2** Determine the MAC address from the label on the chassis.
 - Step 3** Add an entry in the BOOTP configuration file (usually /usr/etc/bootptab) for each switch. Press **Return** after each entry to create a blank line between each entry. See the example BOOTP configuration file that follows in Step 4.
 - Step 4** Enter the **reload** command to reboot and automatically request the IP address from the BOOTP server.

This example BOOTP configuration file shows the added entry:

```
# /etc/bootptab: database for bootp server (/etc/bootpd)
#
# Blank lines and lines beginning with '#' are ignored.
#
# Legend:
#
#      first field -- hostname
#                      (may be full domain name and probably should be)
#
#      hd -- home directory
#      bf -- bootfile
#      cs -- cookie servers
#      ds -- domain name servers
#      gw -- gateways
#      ha -- hardware address
#      ht -- hardware type
#      im -- impress servers
#      ip -- host IP address
#      lg -- log servers
#      lp -- LPR servers
#      ns -- IEN-116 name servers
#      rl -- resource location protocol servers
#      sm -- subnet mask
#      tc -- template host (points to similar host entry)
#      to -- time offset (seconds)
#      ts -- time servers
#
<information deleted>
#
#####
# Start of individual host entries
#####
Router:          tc=netcisco0:    ha=0000.0ca7.ce00:    ip=172.31.7.97:
dross:           tc=netcisco0:    ha=00000c000139:    ip=172.31.7.26:
<information deleted>
```

Protecting Access to Privileged EXEC Commands

The following tasks provide a way to control access to the system configuration file and privileged EXEC commands:

- [Setting or Changing a Static Enable Password, page 3-15](#)
- [Using the enable password and enable secret Commands, page 3-15](#)
- [Setting or Changing a Line Password, page 3-16](#)
- [Setting TACACS+ Password Protection for Privileged EXEC Mode, page 3-16](#)
- [Encrypting Passwords, page 3-17](#)
- [Configuring Multiple Privilege Levels, page 3-17](#)

Setting or Changing a Static Enable Password

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

Command	Purpose
Router(config)# enable password password	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:

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

To display the password or access level configuration, see the “[Displaying the Password, Access Level, and Privilege Level Configuration](#)” section on page 3-19.

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 enable mode (the default) or to access a specified privilege level. 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 of these tasks:

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

■ Protecting Access to Privileged EXEC Commands

Use either of these commands with the **level** option to 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 it with the **more system:running-config** command, it displays in encrypted form.

If you specify an encryption type, you must provide an encrypted password that you copy from another Catalyst 6500 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 3-19 if you lose or forget your password.

To display the password or access level configuration, see the “[Displaying the Password, Access Level, and Privilege Level Configuration](#)” section on page 3-19.

Setting or Changing a Line Password

To set or change a password on a line, perform this task:

Command	Purpose
Router(config-line)# password password	Sets a new password or change an existing password for the privileged level.

To display the password or access level configuration, see the “[Displaying the Password, Access Level, and Privilege Level Configuration](#)” section on page 3-19.

Setting TACACS+ Password Protection for Privileged EXEC Mode

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

- *Cisco IOS Security Configuration Guide*, Release 12.2, “Authentication, Authorization, and Accounting (AAA),” at this URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgr/fsecur_c/fsaaa/index.htm
- *Cisco IOS Security Command Reference*, Release 12.2, at this URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgr/fsecur_r/index.htm

To set the TACACS+ protocol to determine whether or not a user can access privileged EXEC mode, perform this task:

Command	Purpose
Router(config)# enable use-tacacs	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 for both a new username and a password. This information is then sent to the TACACS+ server for authentication. If you are using the extended TACACS+, it also sends any existing UNIX user identification code to the TACACS+ server.

**Caution**

If you enter the **enable use-tacacs** command, you must also enter **tacacs-server authenticate enable**, or you are locked out of the privileged EXEC mode.

**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 problem. This problem occurs because the switch cannot tell the difference between a query resulting from entering the **enable** command and 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
<code>Router(config)# service password-encryption</code>	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 you lose or forget the encrypted password. See the “[Recovering a Lost Enable Password](#)” section on page 3-19 if you lose or forget your password.

To display the password or access level configuration, see the “[Displaying the Password, Access Level, and Privilege Level Configuration](#)” section on page 3-19.

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.

■ Protecting Access to Privileged EXEC 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 widely. If you want more restricted access to the **configure** command, you can assign it level 3 security and distribute that password to more restricted users.

These tasks describe how to configure additional levels of security:

- [Setting the Privilege Level for a Command, page 3-18](#)
- [Changing the Default Privilege Level for Lines, page 3-18](#)
- [Logging In to a Privilege Level, page 3-18](#)
- [Exiting a Privilege Level, page 3-19](#)
- [Displaying the Password, Access Level, and Privilege Level Configuration, page 3-19](#)

Setting the Privilege Level for a Command

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

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

To display the password or access level configuration, see the “[Displaying the Password, Access Level, and Privilege Level Configuration](#)” section on page 3-19.

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
Router(config-line)# privilege level level	Changes the default privilege level for the line.

To display the password or access level configuration, see the “[Displaying the Password, Access Level, and Privilege Level Configuration](#)” section on page 3-19.

Logging In to a Privilege Level

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

Command	Purpose
Router# enable level	Logs into a specified privilege level.

Exiting a Privilege Level

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

Command	Purpose
Router# disable level	Exits to a specified privilege level.

Displaying the Password, Access Level, and Privilege Level Configuration

To display the password, access level, and privilege level configuration, perform this task:

Command	Purpose
Step 1 Router# show running-config	Displays the password and the access level configuration.
Step 2 Router# show privilege	Shows the privilege level configuration.

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

```
Router# show running-config
<...output truncated...>
enable password lab
<...output truncated...>
```

This example shows how to display the privilege level configuration:

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

Recovering a Lost Enable Password

To recover a lost enable password, follow these steps:

-
- Step 1** Connect to the console interface.
 - Step 2** Configure the switch to boot up without reading the configuration memory (NVRAM).
 - Step 3** Reboot the system.
 - Step 4** Access enable mode (which can be done without a password when one is not configured).
 - Step 5** View or change the password, or erase the configuration.
 - Step 6** Reconfigure the switch to boot up and read the NVRAM as it normally does.
 - Step 7** Reboot the system.
-



Note

Password recovery requires the Break signal. You must be familiar with how your terminal or PC terminal emulator issues this signal. For example, in ProComm, the Alt-B keys generate the Break signal. In a Windows terminal session, you press the **Break** or **Ctrl** and **Break** keys simultaneously.

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 3-20](#)
- [Configuring the Software Configuration Register, page 3-21](#)
- [Specifying the Startup System Image, page 3-24](#)
- [Understanding Flash Memory, page 3-24](#)
- [CONFIG_FILE Environment Variable, page 3-25](#)
- [Controlling Environment Variables, page 3-26](#)

Understanding the Supervisor Engine Boot Configuration

These next sections describe how the boot configuration works on the supervisor engine.

Understanding the Supervisor Engine Boot Process

The supervisor engine boot process involves two software images: ROM monitor and supervisor engine software. When the switch is powered up or reset, the ROM-monitor code is executed. Depending on the NVRAM configuration, the supervisor engine either stays in ROM-monitor 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 3-22. The BOOT environment variable is described in the “[Specifying the Startup System Image](#)” section on page 3-24.

Understanding the ROM Monitor

The ROM monitor executes upon power-up, reset, or when a fatal exception occurs. The switch enters ROM-monitor 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 ROM-monitor mode. From ROM-monitor mode, you can manually load a software image from bootflash or a Flash PC card.


Note

For complete syntax and usage information for the ROM monitor commands, refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication.

You can also enter ROM-monitor mode by restarting and then pressing the **Break** key during the first 60 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 ROM-monitor mode.


Note

The **Break** key is always enabled for 60 seconds after rebooting, regardless of whether the configuration-register setting has the **Break** key disabled.

The ROM monitor has these features:

- Power-on confidence test
- Hardware initialization
- Boot capability (manual boot and autoboot)
- Debug utility and crash analysis
- Monitor call interface (EMT calls—the ROM monitor provides information and some functionality to the running software images through EMT calls)
- File system (the ROM monitor knows the simple file system and supports the newly developed file system through the dynamic linked file system library [MONLIB])
- Exception handling

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 written into NVRAM.

Following are some reasons for changing the software configuration register settings:

- To select a boot source and default boot filename.
- To enable or disable the Break function.
- To control broadcast addresses.
- To set the console terminal baud rate.
- To load operating software from Flash memory.
- To recover a lost password.
- To allow you to manually boot the system using the **boot** command at the bootstrap program prompt.
- To force an automatic boot 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.

[Table 3-2](#) lists the meaning of each of the software configuration memory bits, and [Table 3-3](#) defines the boot field.



Caution

The recommended configuration register setting is 0x2102. If you configure a setting that leaves break enabled and you send a break sequence over a console connection, the switch drops into ROMMON.

Table 3-2 Software Configuration Register Bit Meaning

Bit Number ¹	Hexadecimal	Meaning
00 to 03	0x0000 to 0x000F	Boot field (see Table 3-3)
06	0x0040	Causes system software to ignore NVRAM contents
07	0x0080	OEM ² bit enabled
08	0x0100	Break disabled
09	0x0200	Use secondary bootstrap
10	0x0400	Internet Protocol (IP) broadcast with all zeros

Table 3-2 Software Configuration Register Bit Meaning (continued)

Bit Number ¹	Hexadecimal	Meaning
11 to 12	0x0800 to 0x1000	Console line speed (default is 9600 baud)
13	0x2000	Boot default Flash software if network boot fails
14	0x4000	IP broadcasts do not have network numbers
15	0x8000	Enable diagnostic messages and ignore NVRAM contents

1. The factory default value for the configuration register is 0x2102.

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
01	Boots the first system image in onboard Flash memory
02 to 0F	Specifies a default filename for booting over the network; enables boot system commands that override the default filename

Modifying the Boot Field and Using the **boot** Command

The configuration register boot field determines whether or not the switch loads an operating system image, and if so, where it obtains this system image. The following sections describe using and setting the configuration register boot field, and the tasks you must perform to modify the configuration register boot field.

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



Note The factory default configuration register setting for systems and spares is 0x2102.

When the boot field is set to either 0 or 1 (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 0, you must boot the operating system manually by entering the **boot** command to the system bootstrap program or ROM monitor.
- When the boot field is set to 1, the system boots the first image in the onboard 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 from a specific Flash image (using the **boot system flash filename** command).

You can also use the **boot** command to boot images stored in the Flash PC cards located in Flash PC card slot 0 or slot 1 on the supervisor engine. If you set the boot field to any bit pattern other than 0 or 1, the system uses the resulting number to form a filename for booting over the network.

You must set the boot field for the boot functions you require.

Modifying the Boot Field

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

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

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

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

```
Router> enable
Password:
Router#
```

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

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

- Step 3** Configure the configuration register to 0x2102 as follows:

```
Router(config)# config-register 0x2102
```

Set the contents of the configuration register by entering the **config-register value** configuration command, where *value* is a hexadecimal number preceded by 0x (see [Table 3-2 on page 3-21](#)).

- 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 software is reloaded by rebooting the system.

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

```
Configuration register is 0x141 (will be 0x2102 at next reload)
```

- Step 6** Save your settings.

See the “[Saving the Running Configuration Settings](#)” section on page 3-11. However, 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.

Verifying the Configuration Register Setting

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

To verify the configuration register setting, perform this task:

Command	Purpose
Router# show version include Configuration register	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 ROM-monitor mode and waits for user-entered ROM monitor commands. The new setting instructs the switch to load a system image from commands in the startup configuration file or from a default system image stored on a network server.

```
Router1# show version | include Configuration register
Configuration register is 0x2102
Router#
```

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.



Note Store the system software image in the **sup-bootflash:** or **slot0:** device, not in the **bootflash:** device. Store the boot loader image in the **bootflash:** device.

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*.

Understanding Flash Memory

The following sections describe Flash memory:

- [Flash Memory Features, page 3-25](#)
- [Security Features, page 3-25](#)
- [Flash Memory Configuration Process, page 3-25](#)



Note The descriptions in the following sections applies to both the bootflash device and to removable Flash memory cards.

Flash Memory Features

The Flash memory components allow you to do the following:

- Copy the system image to Flash memory using TFTP.
- Copy the system image to Flash memory using rcp.
- Boot the system from Flash memory either automatically or manually.
- Copy the Flash memory image to a network server using TFTP or rcp.
- Boot manually or automatically from a system software image stored in Flash memory.

Security Features

The Flash memory components support the following security features:

- Flash memory cards contain a write-protect switch that you can use to protect data. You must set the switch to *unprotected* to write data to the Flash PC card.
- The system image stored in Flash memory can be changed only from privileged EXEC level on the console terminal.

Flash Memory Configuration Process

To configure your switch to boot from Flash memory, follow these steps:

-
- Step 1** Copy a system image to Flash memory using TFTP or rcp (refer to the *Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.2, “Cisco IOS File Management,” “Loading and Maintaining System Images,” at this URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/ffcprt2/fcf008.htm
- Step 2** Configure the system to boot automatically from the 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 3-22, for more information on modifying the configuration register.
- Step 3** Save your configurations.
- Step 4** Power cycle and reboot your system to ensure that all is working as expected.
-

CONFIG_FILE Environment Variable

For Class A Flash file systems, the CONFIG_FILE environment variable specifies the file system and filename of the configuration file to use for initialization (startup). Valid file systems can include **nvrwam:**, **slot0:**, and **sup-bootflash:**.

For detailed file management configuration information, refer to the *Cisco IOS Configuration Fundamentals Configuration Guide* at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/index.htm

After you save the CONFIG_FILE environment variable to your startup configuration, the switch checks the variable upon startup to determine the location and filename of the configuration file to use for initialization.

The switch uses the NVRAM configuration during initialization when the CONFIG_FILE environment variable does not exist or when it is null (such as at first-time startup). If the switch detects a problem with NVRAM or a checksum error, the switch enters **setup** mode. See the “[Using the Setup Facility or the setup Command](#)” section on page 3-2 for more information on the **setup** command facility.

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, BOOTLDR, and CONFIG_FILE environment variables, use the **boot system**, **boot bootldr**, and **boot config** global configuration commands.

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. Refer to the “Specify the Startup Configuration File” section in the “Modifying, Downloading, and Maintaining Configuration Files” chapter of the *Configuration Fundamentals Configuration Guide* for details on setting the CONFIG_FILE variable.


Note

When you use the **boot system**, **boot bootldr**, and **boot config** global configuration commands, you affect only the running configuration. You must save the environment variable settings to your startup configuration to place the information under ROM monitor control and for the environment variables to function as expected. 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, BOOTLDR, and the CONFIG_FILE environment variables using the **show bootvar** command. This command displays the settings for these variables as they exist in the startup configuration as well as in the running configuration if a running configuration setting differs from a startup configuration setting.

This example shows how to check the BOOT, BOOTLDR, and the CONFIG_FILE environment variables:

```
Router# show bootvar
BOOT variable = slot0:c6sup22-jsv-mz.121-5c.EX.bin,1;
CONFIG_FILE variable does not exist
BOOTLDR variable = bootflash:c6msfc2-boot-mz.121-3a.E4
Configuration register is 0x2
Router#
```

To display the contents of the configuration file pointed to by the CONFIG_FILE environment variable, enter the **more nvram:startup-config** command.

Setting the BOOTLDR Environment Variable

To set the BOOTLDR environment variable, perform this task:

Command	Purpose
Step 1 Router# dir bootflash:	Verifies that bootflash contains the boot loader image.
Step 2 Router# configure terminal	Enters the configuration mode from the terminal.

Command	Purpose
Step 3 Router(config)# boot bootldr bootflash:boot_loader	Sets the BOOTLDR environment variable to specify the Flash device and filename of the boot loader image. This step modifies the runtime BOOTLDR environment variable.
Step 4 Router# end	Exits configuration mode.
Step 5 Router# copy system:running-config nvram:startup-config	Saves this runtime BOOTLDR environment variable to your startup configuration.
Step 6 Router# show bootvar	(Optional) Verifies the contents of the BOOTLDR environment variable.

This example shows how to set the BOOTLDR variable:

```
Router# dir bootflash:  
Directory of bootflash:/  
  
1 -rw-    1599488   Nov 29 1999 11:12:29  c6msfc-boot-mz.120-7.XE.bin  
  
15990784 bytes total (14391168 bytes free)  
Router# configure terminal  
Router (config)# boot bootldr bootflash:c6msfc-boot-mz.120-7.XE.bin  
Router (config)# end  
Router# copy system:running-config nvram:startup-config  
[ok]  
Router# show bootvar  
BOOT variable = sup-bootflash:c6sup-js-mz.120-7.XE.bin,1;  
CONFIG_FILE variable does not exist  
BOOTLDR variable = bootflash:c6msfc-boot-mz.120-7.XE.bin  
Configuration register is 0x2102
```

■ Modifying the Supervisor Engine Startup Configuration



Configuring a Supervisor Engine 720

This chapter describes how to configure a Supervisor Engine 720 in a Catalyst 6500 series switch. This chapter contains these sections:

- [Using the Slots on a Supervisor Engine 720, page 4-1](#)
- [Configuring Supervisor Engine 720 Ports, page 4-1](#)
- [Configuring and Monitoring the Switch Fabric Module Functionality, page 4-2](#)

**Note**

- For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication.
- With a 3-slot chassis, install the Supervisor Engine 720 in either slot 1 or 2.
- With a 6-slot or a 9-slot chassis, install the Supervisor Engine 720 in either slot 5 or 6.
- With a 13-slot chassis, install the Supervisor Engine 720 in either slot 7 or 8.

Using the Slots on a Supervisor Engine 720

The Supervisor Engine 720 has two CompactFlash Type II slots. The CompactFlash Type II slots support CompactFlash Type II Flash PC cards, including Microdrive cards. The keywords for the slots on the active Supervisor Engine 720 are **disk0:** and **disk1:**. The keywords for the slots on a redundant Supervisor Engine 720 are **slavedisk0:** and **slavedisk1:**.

Configuring Supervisor Engine 720 Ports

Supervisor Engine 720 port 1 has a small form-factor pluggable (SFP) connector and has no unique configuration options.

Supervisor Engine 720 port 2 has an RJ-45 connector and an SFP connector (default). To use the RJ-45 connector, you must change the configuration.

Configuring and Monitoring the Switch Fabric Module Functionality

To configure port 2 on a Supervisor Engine 720 to use either the RJ-45 connector or the SFP connector, perform this task:

Command	Purpose
Step 1 Router(config)# interface gigabitethernet slot/2	Selects the Ethernet port to be configured.
Step 2 Router(config-if)# media-type {rj45 sfp}	Selects the connector to use.
Router(config-if)# no media-type	Reverts to the default configuration (SFP).

This example shows how to configure port 2 on a Supervisor Engine 720 in slot 5 to use the RJ-45 connector:

```
Router(config)# interface gigabitethernet 5/2
Router(config-if)# media-type rj45
```

Configuring and Monitoring the Switch Fabric Module Functionality

These sections describe how to configure the switching mode and monitor the Switch Fabric Module 3 (SFM3) functionality that is included on a Supervisor Engine 720:

- [Understanding How the Switch Fabric Module Functionality Works, page 4-2](#)
- [Configuring the Switch Fabric Module Functionality, page 4-4](#)
- [Monitoring the Switch Fabric Module Functionality, page 4-4](#)

Understanding How the Switch Fabric Module Functionality Works

These sections describe how the Switch Fabric Module functionality works:

- [Switch Fabric Module Functionality Overview, page 4-2](#)
- [Switch Fabric Redundancy, page 4-2](#)
- [Forwarding Decisions for Layer 3-Switched Traffic, page 4-3](#)
- [Switching Modes, page 4-3](#)

Switch Fabric Module Functionality Overview

The SFM3 is built into the Supervisor Engine 720 and creates a dedicated connection between fabric-enabled modules and provides uninterrupted transmission of frames between these modules. In addition to the direct connection between fabric-enabled modules provided by the SFM3, fabric-enabled modules also have a direct connection to the 32-Gbps forwarding bus.

Switch Fabric Redundancy

No configuration is required for SFM3 redundancy. The SFM3 installed in the active Supervisor Engine 3 functions as the primary SFM3. A supervisor engine switchover will also cause an SFM3 switchover.

Forwarding Decisions for Layer 3-Switched Traffic

Either a PFC3 or a Distributed Feature Card 3 (DFC3) makes the forwarding decision for Layer 3-switched traffic as follows:

- A PFC3 makes all forwarding decisions for each packet that enters the switch through a module without a DFC3.
- A DFC3 makes all forwarding decisions for each packet that enters the switch on a DFC3-enabled module in these situations:
 - If the egress port is on the same module as the ingress port, the DFC3 forwards the packet locally (the packet never leaves the module).
 - If the egress port is on a different fabric-enabled module, the DFC3 sends the packet across the SFM3 to the egress module, which sends it out the egress port.
 - If the egress port is on a different nonfabric-enabled module, the DFC3 sends the packet across the SFM3 to the Supervisor Engine 720. The Supervisor Engine 720 fabric interface transfers the packet to the 32-Gbps switching bus where it is received by the egress module and is sent out the egress port.

Switching Modes

With a Supervisor Engine 720, traffic is forwarded to and from modules in one of the following modes:

- Compact mode—The switch uses this mode for all traffic when only fabric-enabled modules are installed. In this mode, a compact version of the DBus header is forwarded over the switch fabric channel, which provides the best possible performance.
- Truncated mode—The switch uses this mode for traffic between fabric-enabled modules when there are both fabric-enabled and nonfabric-enabled modules installed. In this mode, the switch sends a truncated version of the traffic (the first 64 bytes of the frame) over the switch fabric channel.
- Bus mode—The switch uses this mode for traffic between nonfabric-enabled modules and for traffic between a nonfabric-enabled module and a fabric-enabled module. In this mode, all traffic passes between the local bus and the supervisor engine bus.

[Table 4-1](#) shows the switch modes used with fabric-enabled and nonfabric-enabled modules installed.

Table 4-1 Switch Fabric Module Functionality Switching Modes

Modules	Switching Modes
Between fabric-enabled modules (when no nonfabric-enabled modules are installed)	Compact ¹
Between fabric-enabled modules (when nonfabric-enabled modules are also installed)	Truncated ²
Between fabric-enabled and nonfabric-enabled modules	Bus
Between non-fabric-enabled modules	Bus

1. In **show** commands, displayed as dcef mode for fabric-enabled modules with DFC3 installed; displayed as fabric mode for other fabric-enabled modules.
2. Displayed as fabric mode in **show** commands.

Configuring the Switch Fabric Module Functionality

To configure the switching mode, perform this task:

Command	Purpose
Router(config)# [no] fabric switching-mode allow {bus-mode {truncated [{threshold [number]}]}}	Configures the switching mode.

When configuring the switching mode, note the following syntax information:

- To allow use of nonfabric-enabled modules or to allow fabric-enabled modules to use bus mode, enter the **fabric switching-mode allow bus-mode** command.
- To prevent use of nonfabric-enabled modules or to prevent fabric-enabled modules from using bus mode, enter the **no fabric switching-mode allow bus-mode** command.



Caution

When you enter the **no fabric switching-mode allow bus-mode** command, power is removed from any nonfabric-enabled modules installed in the switch.

- To allow fabric-enabled modules to use truncated mode, enter the **fabric switching-mode allow truncated** command.
- To prevent fabric-enabled modules from using truncated mode, enter the **no fabric switching-mode allow truncated** command.
- To configure how many fabric-enabled modules must be installed before they use truncated mode instead of bus mode, enter the **fabric switching-mode allow truncated threshold number** command.
- To return to the default truncated-mode threshold, enter the **no fabric switching-mode allow truncated threshold** command.

Monitoring the Switch Fabric Module Functionality

The Switch Fabric Module supports a number of **show** commands for monitoring purposes. A fully automated startup sequence brings the module online and runs the connectivity diagnostics on the ports.

These sections describe how to monitor the Switch Fabric Module:

- [Displaying the Switch Fabric Module Functionality Redundancy Status, page 4-5](#)
- [Displaying Fabric Channel Switching Modes, page 4-5](#)
- [Displaying the Fabric Status, page 4-5](#)
- [Displaying the Fabric Utilization, page 4-6](#)
- [Displaying Fabric Errors, page 4-6](#)

Displaying the Switch Fabric Module Functionality Redundancy Status

To display the switch fabric module redundancy status, perform this task:

Command	Purpose
Router# show fabric active	Displays switch fabric module redundancy status.

```
Router# show fabric active
Active fabric card in slot 5
No backup fabric card in the system
Router#
```

Displaying Fabric Channel Switching Modes

To display the fabric channel switching mode of one or all modules, perform this task:

Command	Purpose
Router# show fabric switching-mode [module {slot_number all}]	Displays fabric channel switching mode of one or all modules.

This example shows how to display the fabric channel switching mode of all modules:

```
Router# show fabric switching-mode all
%Truncated mode is allowed
%System is allowed to operate in legacy mode

Module Slot      Switching Mode      Bus Mode
      5              DCEF             Compact
      9              Crossbar         Compact
Router#
```

Displaying the Fabric Status

To display the fabric status of one or all switching modules, perform this task:

Command	Purpose
Router# show fabric status [slot_number all]	Displays fabric status.

This example shows how to display the fabric status of all modules:

```
Router# show fabric status
  slot    channel      speed          module      fabric
           0        8G          status      status
           1        0        8G          OK          OK
           5        0        8G          OK          Up- Timeout
           6        0       20G          OK          Up- BufError
           8        0        8G          OK          OK
           8        1        8G          OK          OK
           9        0        8G          Down- DDRsync      OK
Router#
```

Displaying the Fabric Utilization

To display the fabric utilization of one or all modules, perform this task:

Command	Purpose
Router# show fabric utilization [slot_number all]	Displays fabric utilization.

This example shows how to display the fabric utilization of all modules:

```
Router#show fabric utilization all
Lo% Percentage of Low-priority traffic.
Hi% Percentage of High-priority traffic.

  slot    channel      speed  Ingress Lo%   Egress Lo%  Ingress Hi% Egress Hi%
    5        0       20G          0          0          0          0          0
    9        0       8G          0          0          0          0          0
Router#
```

Displaying Fabric Errors

To display fabric errors of one or all modules, perform this task:

Command	Purpose
Router# show fabric errors [slot_number all]	Displays fabric errors.

This example shows how to display fabric errors on all modules:

```
Router# show fabric errors

Module errors:
  slot    channel      crc     hbeat      sync    DDR sync
    1        0       0          0          0          0
    8        0       0          0          0          0
    8        1       0          0          0          0
    9        0       0          0          0          0

Fabric errors:
  slot    channel      sync     buffer    timeout
    1        0       0          0          0
    8        0       0          0          0
    8        1       0          0          0
    9        0       0          0          0
Router#
```



Configuring Interfaces

This chapter describes how to configure interfaces on the Catalyst 6500 series switches. This chapter consists of these sections:

- [Understanding Interface Configuration, page 5-1](#)
- [Using the Interface Command, page 5-2](#)
- [Configuring a Range of Interfaces, page 5-4](#)
- [Defining and Using Interface-Range Macros, page 5-5](#)
- [Configuring Optional Interface Features, page 5-6](#)
- [Understanding Online Insertion and Removal, page 5-15](#)
- [Monitoring and Maintaining Interfaces, page 5-16](#)

**Note**

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication and the Release 12.2 publications at this URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/index.htm>

Understanding Interface Configuration

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

- Interface type:
 - Ethernet (use the **ethernet** keyword)
 - Fast Ethernet (use the **fastethernet** keyword)
 - Gigabit Ethernet (use the **gigabitethernet** keyword)
 - 10-Gigabit Ethernet (use the **tengigabitethernet** keyword)

**Note**

For WAN interfaces, refer to the configuration note for the WAN module.

- Slot number—The slot in which the module is installed. On the Catalyst 6500 series switch, slots are numbered starting with 1, from top to bottom.

Using the Interface Command

- Port number—The physical port number on the module. On the Catalyst 6500 series switch, the port numbers always begin with 1. When facing the rear of the switch, ports are numbered from the left to the right.

You can identify ports from the physical location. You also can use **show** commands to display information about a specific port, or all the ports.

Using the Interface Command



Note You use the commands described in this section to configure both physical ports and logical interfaces.

These procedures apply to all interface configuration processes. Begin the interface configuration process in global configuration mode.

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

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

- Step 2** In the global configuration mode, enter the **interfaces** command. Identify the interface type and the number of the connector or interface card.

The following example shows how to select Fast Ethernet, slot 5, interface 1:

```
Router(config)# interfaces fastethernet 5/1
Router(config-if)#
```

- Step 3** Enter the **show interfaces** EXEC command to see a list of all interfaces that are installed. A report is provided for each interface that the device supports, as shown in this display:

```
Router# show interfaces fastethernet 5/48
FastEthernet5/48 is up, line protocol is up
  Hardware is C6k 100Mb 802.3, address is 0050.f0ac.3083 (bia 0050.f0ac.3083)
  Internet address is 172.20.52.18/27
  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)
  Half-duplex, 100Mb/s
  ARP type: ARPA, ARP Timeout 04:00:00
  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 1000 bits/sec, 1 packets/sec
  5 minute output rate 1000 bits/sec, 1 packets/sec
    4834677 packets input, 329545368 bytes, 0 no buffer
    Received 4796465 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
    51926 packets output, 15070051 bytes, 0 underruns
    0 output errors, 2 collisions, 2 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
Router#
```

- Step 4** Enter the **show hardware** EXEC command to see a list of the system software and hardware:

```

Router# show hardware
Cisco Internetwork Operating System Software
IOS (tm) c6sup2_rp Software (c6sup2_rp-JSV-M), Version 12.1(5c)EX, EARLY DEPLOY)
Synced to mainline version: 12.1(5c)
TAC:Home:Software:Ios General:CiscoIOSRoadmap:12.1
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Wed 28-Mar-01 17:52 by hqluong
Image text-base: 0x30008980, data-base: 0x315D0000

ROM: System Bootstrap, Version 12.1(3r)E2, RELEASE SOFTWARE (fc1)
BOOTFLASH: c6sup2_rp Software (c6sup2_rp-JSV-M), Version 12.1(5c)EX, EARLY DEPL)

Router uptime is 2 hours, 55 minutes
System returned to ROM by power-on (SP by power-on)
Running default software

cisco Catalyst 6000 (R7000) processor with 114688K/16384K bytes of memory.
Processor board ID SAD04430J9K
R7000 CPU at 300Mhz, Implementation 39, Rev 2.1, 256KB L2, 1024KB L3 Cache
Last reset from power-on
Bridging software.
X.25 software, Version 3.0.0.
SuperLAT software (copyright 1990 by Meridian Technology Corp).
TN3270 Emulation software.
1 Virtual Ethernet/IEEE 802.3 interface(s)
48 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)
381K bytes of non-volatile configuration memory.

16384K bytes of Flash internal SIMM (Sector size 512K).
Configuration register is 0x2

Router#

```

- Step 5** To begin configuring Fast Ethernet port 5/5, enter the **interface** keyword, interface type, and slot number/port number at the privileged EXEC prompt, as shown in the following example:

```

Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fastethernet 5/5
Router(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 enter either **fastethernet 5/5** or **fastethernet5/5**.

- Step 6** After each **interface** command, enter 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 get out of interface configuration mode and return to privileged EXEC mode.

- Step 7** After you configure an interface, check its status by using the EXEC **show** commands listed in “[Monitoring and Maintaining Interfaces](#)” section on page 5-16.

Configuring a Range of Interfaces

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

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

Command	Purpose
<pre>Router(config)# interface range { {vlan vlan_ID - vlan_ID [, vlan vlan_ID - vlan_ID] } {type¹ slot/port - port [, type¹ slot/port - port] } {macro_name [, macro_name]} }</pre>	<p>Selects the range of interfaces to be configured.</p> <p>Note You cannot use the no keyword with the range keyword.</p>

1. *type* = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

When configuring a range of interfaces, note the following syntax information:

- The space before the dash is required.
- You can enter up to five comma-separated ranges.
- You are not required to enter spaces before or after the comma.

For information about macros, see the “Defining and Using Interface-Range Macros” section on page 5-5.



Note You must add a space between the interface numbers and the dash when using the **interface range** command. For example, **interface range fastethernet 1 - 5** is valid syntax; **interface range fastethernet 1-5** is invalid.



Note For VLAN interfaces, the **interface range** command works only with those 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 reenable all Fast Ethernet ports 5/1 to 5/5:

```
Router(config)# interface range fastethernet 5/1 - 5
Router(config-if)# no shutdown
Router(config-if)#
*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
Router(config-if)#

```

**Note**

The link state messages (LINK-3-UPDOWN and LINEPROTO-5-UPDOWN) are disabled by default. Enter the **logging event link status** command on each interface where you want the messages enabled.

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

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

```

**Note**

The link state messages (LINK-3-UPDOWN and LINEPROTO-5-UPDOWN) are disabled by default. Enter the **logging event link status** command on each interface where you want the messages enabled.

If you enter multiple configuration commands while you are in interface-range configuration mode, each command is executed as it is entered (they are not batched together and executed after you exit interface-range configuration mode).

If you exit interface-range configuration mode while the commands are being executed, some commands may not be executed on all interfaces in the range. Wait until the command prompt reappears 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
<pre>Router(config)# define interface-range macro_name {v1an v1an_ID - v1an_ID} {type¹ slot/port - port} [, {type¹ slot/port - port}]</pre>	Defines the interface-range macro and save it in NVRAM.
<pre>Router(config)# no define interface-range macro_name</pre>	Deletes a macro.

1. *type* = **ethernet**, **fastethernet**, **gigabitetherent**, or **tengigabitetherent**

Configuring Optional Interface Features

This example shows how to define an interface-range macro named enet_list to select Fast Ethernet ports 5/1 through 5/4:

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

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

Command	Purpose
Router# show running-config	Shows the defined interface-range macro configuration.

This example shows how to display the defined interface-range macro named enet_list:

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

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

Command	Purpose
Router(config)# interface range macro macro_name	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:

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

Configuring Optional Interface Features

These sections describe optional interface features:

- [Configuring Ethernet Interface Speed and Duplex Mode, page 5-6](#)
- [Configuring Jumbo Frame Support, page 5-10](#)
- [Configuring IEEE 802.3Z Flow Control, page 5-13](#)
- [Configuring the Port Debounce Timer, page 5-14](#)
- [Adding a Description for an Interface, page 5-15](#)

Configuring Ethernet Interface Speed and Duplex Mode

These sections describe how to configure Ethernet port speed and duplex mode:

- [Speed and Duplex Mode Configuration Guidelines, page 5-7](#)
- [Setting the Ethernet Interface Speed, page 5-7](#)
- [Setting the Interface Duplex Mode, page 5-8](#)
- [Configuring Link Negotiation on Gigabit Ethernet Ports, page 5-8](#)
- [Displaying the Speed and Duplex Mode Configuration, page 5-9](#)

Speed and Duplex Mode Configuration Guidelines

You usually configure Ethernet port speed and duplex mode parameters to auto and allow the Catalyst 6500 series switch to negotiate the speed and duplex mode between ports. If you decide to configure the port speed and duplex modes manually, consider the following information:

- If you set the Ethernet port speed to auto, the switch automatically sets the duplex mode to auto.
- If you enter the **no speed** command, the switch automatically configures both speed and duplex to auto.
- If you configure an Ethernet port speed to a value other than auto (for example, 10, 100, or 1000 Mbps), configure the connecting port to match. Do not configure the connecting port to negotiate the speed.
- If you manually configure the Ethernet port speed to either 10 or 100 Mbps, the switch prompts you to also configure the duplex mode on the port.


Note

Catalyst 6500 series switches cannot automatically negotiate Ethernet port speed and duplex mode if the connecting port is configured to a value other than auto.


Caution

Changing the Ethernet port speed and duplex mode configuration might shut down and reenable the interface during the reconfiguration.

Setting the Ethernet Interface Speed


Note

If you set the Ethernet port speed to **auto** on a 10/100-Mbps or 10/100/1000-Mbps Ethernet port, both speed and duplex are autonegotiated.

To set the port speed for a 10/100 or a 10/100/1000-Mbps Ethernet port, perform this task:

Command	Purpose
Step 1 Router(config)# interface fastethernet slot/port	Selects the Ethernet port to be configured.
Step 2 Router(config-if)# speed {10 100 1000 auto}	Sets the speed of the Ethernet interface.
Router(config-if)# no speed	Reverts to the default configuration (speed auto).

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

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

Setting the Interface Duplex Mode

**Note**

- 10-Gigabit Ethernet and Gigabit Ethernet are full duplex only. You cannot change the duplex mode on 10-Gigabit Ethernet or Gigabit Ethernet ports or on a 10/100/1000-Mbps port configured for Gigabit Ethernet.
- If you set the port speed to auto on a 10/100-Mbps or a 10/100/1000-Mbps Ethernet port, both speed and duplex are autonegotiated. You cannot change the duplex mode of autonegotiation ports.

To set the duplex mode of an Ethernet or Fast Ethernet port, perform this task:

Command	Purpose
Step 1 Router(config)# interface fastethernet slot/port	Selects the Ethernet port to be configured.
Step 2 Router(config-if)# duplex [auto full half]	Sets the duplex mode of the Ethernet port.
Router(config-if)# no duplex	Reverts to the default configuration (duplex auto).

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

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

Configuring Link Negotiation on Gigabit Ethernet Ports

**Note**

Link negotiation does not negotiate port speed.

On Gigabit Ethernet ports, link negotiation exchanges flow-control parameters, remote fault information, and duplex information. Link negotiation is enabled by default.

The ports on both ends of a link must have the same setting. The link will not come up if the ports at each end of the link are set inconsistently (link negotiation enabled on one port and disabled on the other port).

Table 5-1 shows the four possible link negotiation configurations and the resulting link status for each configuration.

Table 5-1 Link Negotiation Configuration and Possible Link Status

Link Negotiation State		Link Status	
Local Port	Remote Port	Local Port	Remote Port
Off	Off	Up	Up
On	On	Up	Up
Off	On	Up	Down
On	Off	Down	Up

To configure link negotiation on a port, perform this task:

Command	Purpose
Step 1 Router(config)# interface gigabitethernet slot/port	Selects the port to be configured.
Step 2 Router(config-if)# speed nonegotiate Router(config-if)# no speed nonegotiate	Disables link negotiation. Reverts to the default configuration (link negotiation enabled).

This example shows how to enable link negotiation on Gigabit Ethernet port 5/4:

```
Router(config)# interface gigabitethernet 5/4
Router(config-if)# no speed nonegotiate
```

Displaying the Speed and Duplex Mode Configuration

To display the speed and duplex mode configuration for a port, perform this task:

Command	Purpose
Router# show interfaces type¹ slot/port	Displays the speed and duplex mode configuration.

1. *type* = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

This example shows how to display the speed and duplex mode of Fast Ethernet port 5/4:

```
Router# show interfaces fastethernet 5/4
FastEthernet5/4 is up, line protocol is up
    Hardware is Cat6K 100Mb Ethernet, address is 0050.f0ac.3058 (bia 0050.f0ac.3058)
    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 00:00:33, output never, output hang never
    Last clearing of "show interface" counters never
    Queueing strategy: fifo
    Output queue 0/40, 0 drops; input queue 0/75, 0 drops
    5 minute input rate 0 bits/sec, 0 packets/sec
    5 minute output rate 0 bits/sec, 0 packets/sec
        1238 packets input, 273598 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
        1380 packets output, 514382 bytes, 0 underruns
        0 output errors, 0 collisions, 2 interface resets
        0 babbles, 0 late collision, 0 deferred
        0 lost carrier, 0 no carrier
        0 output buffer failures, 0 output buffers swapped out
Router#
```

Configuring Jumbo Frame Support

These sections describe jumbo frame support:

- [Understanding Jumbo Frame Support, page 5-10](#)
- [Configuring MTU Sizes, page 5-12](#)


Caution

The following switching modules support a maximum ingress frame size of 8092 bytes:

- WS-X6516-GE-TX when operating at 100 Mbps
- WS-X6148-RJ-45, WS-X6148-RJ-45V and WS-X6148-RJ21, WS-X6148-RJ21V
- WS-X6248-RJ-45 and WS-X6248-TEL
- WS-X6248A-RJ-45 and WS-X6248A-TEL
- WS-X6348-RJ-45, WS-X6348-RJ45V and WS-X6348-RJ-21, WX-X6348-RJ21V

When jumbo frame support is configured, these modules drop ingress frames larger than 8092 bytes.

Understanding Jumbo Frame Support

These sections describe jumbo frame support:

- [Jumbo Frame Support Overview, page 5-10](#)
- [Ethernet Ports, page 5-11](#)
- [VLAN Interfaces, page 5-12](#)

Jumbo Frame Support Overview

A jumbo frame is a frame larger than the default Ethernet size. You enable jumbo frame support by configuring a larger-than-default maximum transmission unit (MTU) size on a port or VLAN interface and configuring the global LAN port MTU size.


Note

-
- Jumbo frame support fragments routed traffic in software on the MSFC.
 - Jumbo frame support does not fragment bridged traffic.
-

Bridged and Routed Traffic Size Check at Ingress 10, 10/100, and 100 Mbps Ethernet and 10 Gigabit Ethernet Ports

Jumbo frame support compares ingress traffic size with the global LAN port MTU size at ingress 10, 10/100, and 100 Mbps Ethernet and 10 Gigabit Ethernet LAN ports that have a nondefault MTU size configured. The port drops traffic that is oversized. You can configure the global LAN port MTU size (see the “[Configuring the Global Egress LAN Port MTU Size](#)” section on page 5-13).

Bridged and Routed Traffic Size Check at Ingress Gigabit Ethernet Ports

Gigabit Ethernet LAN ports configured with a nondefault MTU size accept frames containing packets of any size larger than 64 bytes. With a nondefault MTU size configured, Gigabit Ethernet LAN ports do not check for oversize ingress frames.

Routed Traffic Size Check on the PFC

For traffic that needs to be routed, Jumbo frame support on the PFC compares traffic sizes to the configured MTU sizes and provides Layer 3 switching for jumbo traffic between interfaces configured with MTU sizes large enough to accommodate the traffic. Between interfaces that are not configured with large enough MTU sizes, if the “do not fragment bit” is not set, the PFC sends the traffic to the MSFC to be fragmented and routed in software. If the “do not fragment bit” is set, the PFC drops the traffic.

Bridged and Routed Traffic Size Check at Egress 10, 10/100, and 100 Mbps Ethernet Ports

10, 10/100, and 100 Mbps Ethernet LAN ports configured with a nondefault MTU size transmit frames containing packets of any size larger than 64 bytes. With a nondefault MTU size configured, 10, 10/100, and 100 Mbps Ethernet LAN ports do not check for oversize egress frames.

Bridged and Routed Traffic Size Check at Egress Gigabit Ethernet and 10 Gigabit Ethernet Ports

Jumbo frame support compares egress traffic size with the global egress LAN port MTU size at egress Gigabit Ethernet and 10 Gigabit Ethernet LAN ports that have a nondefault MTU size configured. The port drops traffic that is oversized. You can configure the global LAN port MTU size (see the “[Configuring the Global Egress LAN Port MTU Size](#)” section on page 5-13).

Ethernet Ports

These sections describe configuring nondefault MTU sizes on Ethernet ports:

- [Ethernet Port Overview, page 5-11](#)
- [Layer 3 Ethernet Ports, page 5-11](#)
- [Layer 2 Ethernet Ports, page 5-11](#)

Ethernet Port Overview

Configuring a nondefault MTU size on a 10, 10/100, or 100 Mbps Ethernet port limits ingress packets to the global LAN port MTU size and permits egress traffic of any size larger than 64 bytes.

Configuring a nondefault MTU size on a Gigabit Ethernet port permits ingress packets of any size larger than 64 bytes and limits egress traffic to the global LAN port MTU size.

Configuring a nondefault MTU size on a 10 Gigabit Ethernet port limits ingress and egress packets to the global LAN port MTU size.

Configuring a nondefault MTU size on an Ethernet port limits routed traffic to the configured MTU size. You can configure the MTU size on any Ethernet port.

Layer 3 Ethernet Ports

On a Layer 3 port, you can configure an MTU size on each Layer 3 Ethernet port that is different than the global LAN port MTU size.



Traffic through a Layer 3 Ethernet LAN port that is configured with a nondefault MTU size is also subject to the global LAN port MTU size (see the “[Configuring the Global Egress LAN Port MTU Size](#)” section on page 5-13).

Layer 2 Ethernet Ports

On a Layer 2 port, you can only configure an MTU size that matches the global LAN port MTU size (see the “[Configuring the Global Egress LAN Port MTU Size](#)” section on page 5-13).

VLAN Interfaces

You can configure a different MTU size on each Layer 3 VLAN interface. Configuring a nondefault MTU size on a VLAN interface limits traffic to the nondefault MTU size. You can configure the MTU size on VLAN interfaces to support jumbo frames.

Configuring MTU Sizes

These sections describe how to configure MTU sizes:

- [Configuring MTU Sizes, page 5-12](#)
- [Configuring the Global Egress LAN Port MTU Size, page 5-13](#)

Configuring the MTU Size

To configure the MTU size, perform this task:

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

1. *type* = ethernet, fastethernet, gigabitethernet, tengigabitethernet, or ge-wan

When configuring the MTU size, note the following syntax information:

- For VLAN interfaces and Layer 3 Ethernet ports, supported MTU values are from 64 to 9216 bytes.
- For Layer 2 Ethernet ports, you can configure only the global egress LAN port MTU size (see the “[Configuring the Global Egress LAN Port MTU Size](#)” section on page 5-13).

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

```
Router# configure terminal
Router(config)# interface gigabitethernet 1/2
Router(config-if)# mtu 9216
Router(config-if)# end
```

This example shows how to verify the configuration:

```
Router# 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...>
Router#
```

Configuring the Global Egress LAN Port MTU Size

To configure the global egress LAN port MTU size, perform this task:

Command	Purpose
Step 1 Router(config)# system jumbomtu mtu_size	Configures the global egress LAN port MTU size.
	Router(config)# no system jumbomtu
Step 2 Router(config)# end	Exits configuration mode.

Configuring IEEE 802.3Z Flow Control

Gigabit Ethernet and 10-Gigabit Ethernet ports on the Catalyst 6500 series switches use flow control to stop the transmission of frames to the port for a specified time; other Ethernet ports use flow control to respond to flow-control requests.

If a Gigabit Ethernet or 10-Gigabit Ethernet port receive buffer becomes full, the port transmits an IEEE 802.3Z pause frame that requests remote ports to delay sending frames for a specified time. All Ethernet ports (10 Gbps, 1 Gbps, 100 Mbps, and 10 Mbps) can receive and respond to IEEE 802.3Z pause frames from other devices.

To configure flow control on an Ethernet port, perform this task:

Command	Purpose
Step 1 Router(config)# interface type¹ slot/port	Selects the port to configure.
Step 2 Router(config-if)# flowcontrol {receive send} {desired off on}	Configures a port to send or respond to pause frames.
	Router(config-if)# no flowcontrol {receive send}
Step 3 Router# show interfaces [type¹ slot/port] flowcontrol	Displays the flow-control configuration for all ports.

1. *type* = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

When configuring flow control, note the following syntax information:

- 10-Gigabit Ethernet ports are permanently configured to respond to pause frames.
- When the configuration of the remote ports is unknown, use the **receive desired** keywords to configure a Gigabit Ethernet port to respond to received pause frames.
- Use the **receive on** keywords to configure a Gigabit Ethernet port to respond to received pause frames.
- Use the **receive off** keywords to configure a Gigabit Ethernet port to ignore received pause frames.
- When configuring transmission of pause frames, note the following information:
 - When the configuration of the remote ports is unknown, use the **send desired** keywords to configure a port to send pause frames.
 - Use the **send on** keywords to configure a port to send pause frames.
 - Use the **send off** keywords to configure a port not to send pause frames.

This example shows how to turn on receive flow control and how to verify the flow-control configuration:

```
Router# configure terminal
Router(config)# interface gigabitethernet 1/2
Router(config-if)# flowcontrol receive on
Router(config-if)# end
Router# show interfaces flowcontrol

Interface Send           Receive
Gi1/1    Desired        OFF
Gi1/2    Desired        ON
Fa5/1    Not capable   OFF
<output truncated>
```

Configuring the Port Debounce Timer

The port debounce timer delays notification of a link change, which can decrease traffic loss due to network reconfiguration. You can configure the port debounce timer separately on each LAN port.



Caution

Enabling the port debounce timer causes link up and link down detections to be delayed, resulting in loss of traffic during the debouncing period. This situation might affect the convergence and reconvergence of some Layer 2 and Layer 3 protocols.

[Table 5-2](#) lists the time delay that occurs before notification of a link change.

Table 5-2 Port Debounce Timer Delay Time

Port Type	Debounce Timer Disabled	Debounce Timer Enabled
10BASE-FL ports	300 milliseconds	3100 milliseconds
10/100BASE-TX ports	300 milliseconds	3100 milliseconds
100BASE-FX ports	300 milliseconds	3100 milliseconds
10/100/1000BASE-TX ports	300 milliseconds	3100 milliseconds
1000BASE-TX ports	300 milliseconds	3100 milliseconds
Fiber Gigabit ports	10 milliseconds	100 milliseconds
10-Gigabit ports except WS-X6501-10GEX4 and WS-X6502-10GE	1000 milliseconds	3100 milliseconds

To configure the debounce timer on a port, perform this task:

Command	Purpose
Step 1 Router(config)# interface type¹ slot/port	Selects the port to configure.
Step 2 Router(config-if)# link debounce [time debounce_time]	Configures the debounce timer. Note The time keyword is supported only on fiber Gigabit Ethernet ports.
Router(config-if)# no link debounce	Reverts to the default setting.
Step 3 Router# show interfaces debounce	Verifies the configuration.

1. *type* = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

On fiber Gigabit Ethernet ports, you can increase the port debounce timer value in increments of 100 milliseconds up to 5000 milliseconds.

This example shows how to enable the port debounce timer on Fast Ethernet port 5/12:

```
Router(config)# interface fastethernet 5/12
Router(config-if)# link debounce
Router(config-if)# end
```

This example shows how to display the port debounce timer settings:

```
Router# show interfaces debounce | include enable
Fa5/12    enable          3100
```

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, perform this task:

Command	Purpose
Router(config-if)# description string	Adds a description for an interface.
Router(config-if)# no description	Deletes a description from an interface.

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

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

Understanding Online Insertion and Removal

The online insertion and removal (OIR) feature supported on the Catalyst 6500 series switches allows you to remove and replace modules while the system is online. You can shut down the modules before removal and restart it after insertion without causing other software or interfaces to shut down.

**Note**

Do not remove or install more than one module at a time. After you remove or install a module, check the LEDs before continuing. For module LED descriptions, refer to the *Catalyst 6500 Series Switch Installation Guide*.

When a module has been removed or installed, the Catalyst 6500 series switch stops processing traffic for the module and scans the system for a configuration change. Each interface type is verified against the system configuration, and then the system runs diagnostics on the new module. There is no disruption to normal operation during module insertion or removal.

The switch can bring only an identical replacement module online. If the replacement module is different from the removed module, you must configure it before the switch can bring it online.

Layer 2 MAC addresses are stored in an EEPROM, which allows modules to be replaced online without requiring the system to update switching tables and data structures. Regardless of the types of modules installed, the Layer 2 MAC addresses do not change unless you replace the supervisor engine. If you do replace the supervisor engine, the Layer 2 MAC addresses of *all* ports change to those specified in the address allocator on the new supervisor engine.

Monitoring and Maintaining Interfaces

You can perform the tasks in the following sections to monitor and maintain interfaces:

- [Monitoring Interface Status, page 5-16](#)
- [Clearing Counters on an Interface, page 5-17](#)
- [Resetting an Interface, page 5-17](#)
- [Shutting Down and Restarting an Interface, page 5-18](#)

Monitoring Interface Status

The software 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 and statistics about interfaces. The following table lists some of the interface monitoring commands. (You can display the complete list of **show** commands by using the **show ?** command at the EXEC prompt.) These commands are described in the *Cisco IOS Interface Command Reference* publication.

To display information about the interface, perform these tasks:

Command	Purpose
Router# show ibc	Displays current internal status information.
Router# show eobc	Displays current internal out-of-band information.
Router# show interfaces [type slot/port]	Displays the status and configuration of all or a specific interface.
Router# show running-config	Displays the currently running configuration.
Router# show rif	Displays the current contents of the routing information field (RIF) cache.

Command	Purpose
Router# show protocols [type slot/port]	Displays the global (system-wide) and interface-specific status of any configured protocol.
Router# show version	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 port 5/5:

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

Clearing Counters on an Interface

To clear the interface counters shown with the **show interfaces** command, perform this task:

Command	Purpose
Router# clear counters {{vlan vlan_ID} {type ¹ slot/port} {port-channel channel_ID}}	Clears interface counters.

1. *type* = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

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

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

The **clear counters** command clears all the current counters from the interface unless the optional arguments specify a specific interface.



Note The **clear counters** command clears counters displayed with the EXEC **show interfaces** command, not counters retrieved using SNMP.

Resetting an Interface

To reset an interface, perform this task:

Command	Purpose
Router# clear interface type ¹ slot/port	Resets an interface.

1. *type* = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

This example shows how to reset Fast Ethernet port 5/5:

```
Router# clear interface fastethernet 5/5
Router#
```

Shutting Down and Restarting an Interface

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

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

Command	Purpose
Step 1 Router(config)# interface {{vlan <i>vlan_ID</i> } {type ¹ <i>slot/port</i> } {port-channel <i>channel_ID</i> }}	Selects the interface to be configured.
Step 2 Router(config-if)# shutdown	Shuts down the interface.
Step 3 Router(config-if)# no shutdown	Reenables the interface.

1. *type* = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

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

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

This example shows how to reenable Fast Ethernet port 5/5:

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

To check if an interface is disabled, enter the EXEC **show interfaces** command. An interface that has been shut down is shown as administratively down in the **show interfaces** command display.



CHAPTER

6

Configuring RPR and RPR+ Supervisor Engine Redundancy

This chapter describes how to configure supervisor engine redundancy with RPR and RPR+. This chapter consists of these sections:

- [Understanding Supervisor Engine Redundancy, page 6-1](#)
- [Supervisor Engine Redundancy Guidelines and Restrictions, page 6-4](#)
- [Configuring Supervisor Engine Redundancy, page 6-5](#)
- [Performing a Fast Software Upgrade, page 6-8](#)
- [Copying Files to the Redundant Supervisor Engine, page 6-9](#)



For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication.

Understanding Supervisor Engine Redundancy

These sections describe supervisor engine redundancy:

- [Supervisor Engine Redundancy Overview, page 6-1](#)
- [RPR+ Operation, page 6-2](#)
- [Supervisor Engine Synchronization, page 6-3](#)

Supervisor Engine Redundancy Overview

Catalyst 6500 series switches support fault resistance by allowing a redundant supervisor engine to take over if the primary supervisor engine fails. RPR supports a switchover time of 2 to 4 minutes and RPR+ supports a switchover time of 30 to 60 seconds.

When RPR+ mode is used, the redundant supervisor engine is fully initialized and configured, which shortens the switchover time. The active supervisor engine checks the image version of the redundant supervisor engine when the redundant supervisor engine comes online. If the image on the redundant supervisor engine does not match the image on the active supervisor engine, RPR redundancy mode is used.

RPR Operation

RPR supports the following features:

- Auto-startup and bootvar synchronization between active and redundant supervisor engines
- Hardware signals that detect and decide the active or redundant status of supervisor engines
- Clock synchronization every 60 seconds from the active to the redundant supervisor engine
- A redundant supervisor engine that is booted but not all subsystems are up: if the active supervisor engine fails, the redundant supervisor engine become fully operational
- An operational supervisor engine present in place of the failed unit becomes the redundant supervisor engine
- Support for fast software upgrade (FSU) (See the “[Performing a Fast Software Upgrade](#)” section on [page 6-8](#).)



Note The two Gigabit Ethernet interfaces on the redundant supervisor engine are always active.

When the switch is powered on, RPR runs between the two supervisor engines. The supervisor engine that boots first, either in slot 1 or 2, becomes the RPR active supervisor engine. The Multilayer Switch Feature Card (MSFC or MSFC2) and Policy Feature Card (PFC or PFC2) become fully operational. The MSFC and PFC on the redundant supervisor engine come out of reset but are not operational.

The following events cause an RPR switchover:

- Clock synchronization failure between supervisor engines
- MSFC or PFC failure on the active supervisor engine
- A manual switchover

In a switchover, the redundant supervisor engine become fully operational and the following occurs:

- All switching modules power up again
- Remaining subsystems on the MSFC (including Layer 2 and Layer 3 protocols) are brought up
- Access control lists (ACLs) are reprogrammed into supervisor engine hardware



Note In a switchover, there is a disruption of traffic because some address states are lost and then restored after they are dynamically redetermined.

RPR+ Operation

With RPR+, the redundant supervisor engine is fully initialized and configured, which shortens the switchover time if the active supervisor engine fails or if a manual switchover is performed.

When the switch is powered on, RPR+ runs between the two supervisor engines. The supervisor engine that boots first, either in slot 1 or 2, becomes the active supervisor engine. The Multilayer Switch Feature Card (MSFC or MSFC2) and Policy Feature Card (PFC or PFC2) become fully operational. The MSFC and PFC on the redundant supervisor engine come out of reset but are not operational.

RPR+ enhances RPR by providing the following additional benefits:

- Reduced switchover time

Depending on the configuration, the switchover time is in the range of 30 to 60 seconds.

- Installed modules are not reloaded

Because both the startup configuration and the running configuration are continually synchronized from the active to the redundant supervisor engine, installed modules are not reloaded during a switchover.

- Online insertion and removal (OIR) of the redundant supervisor engine

RPR+ allows OIR of the redundant supervisor engine for maintenance. When the redundant supervisor engine is inserted, the active supervisor engine detects its presence and begins to transition the redundant supervisor engine to fully initialized state.

- Synchronization of OIR events

- Manual user-initiated switchover using the **redundancy force-switchover** command

The following events cause an RPR+ switchover:

- Clock synchronization failure between supervisor engines
- MSFC or PFC failure on the active supervisor engine

Supervisor Engine Synchronization

During RPR mode operation, the startup-config and config-registers configuration are synchronized by default between the two supervisor engines. In a switchover, the new active supervisor engine uses the current configuration.



Note

Unless auto-synchronization has been disabled, the boot variables are synchronized by default.

When a redundant supervisor engine configuration is running in RPR+ mode, the following operations trigger synchronization:

- When a redundant supervisor engine first comes online, the configuration information is synchronized in bulk from the active supervisor engine to the redundant supervisor engine. This synchronization overwrites any existing startup configuration file on the redundant supervisor engine.
- When configuration changes occur during normal operation, RPR+ performs an incremental synchronization from the active supervisor engine to the redundant supervisor engine. RPR+ synchronizes user-entered CLI commands incrementally line-by-line from the active supervisor engine to the redundant supervisor engine.



Note

- Even though the redundant supervisor engine is fully initialized, it only interacts with the active supervisor engine to receive incremental changes to the configuration files as they occur. You cannot enter CLI commands on the redundant supervisor engine.
- Synchronization of the startup configuration file is enabled by default in RPR+ mode.

Supervisor Engine Redundancy Guidelines and Restrictions

These sections describe supervisor engine redundancy guidelines and restrictions:

- [RPR+ Guidelines and Restrictions, page 6-4](#)
- [Hardware Configuration Guidelines and Restrictions, page 6-5](#)
- [Configuration Mode Restrictions, page 6-5](#)

RPR+ Guidelines and Restrictions

The following guidelines and restrictions apply to RPR+:

- Supervisor engine redundancy does not support nondefault VLAN data file names or locations. Do not enter the **vtp file file_name** command on a switch that has a redundant supervisor engine.
- Before installing a redundant supervisor engine, enter the **no vtp file** command to return to the default configuration.
- RPR+ redundancy does not support configuration entered in VLAN database mode. Use global configuration mode with RPR+ redundancy (see [Chapter 10, “Configuring VLANs”](#)).
- Configuration changes made through SNMP are not synchronized to the redundant supervisor engine. Enter a **copy running-config startup-config** command to synchronize the configuration on the redundant supervisor engine.
- Supervisor engine redundancy does not provide supervisor engine mirroring or supervisor engine load balancing. Only one supervisor engine is active. Network services are disrupted until the redundant supervisor engine takes over and the switch recovers.
- The two Gigabit Ethernet interfaces on the redundant supervisor engine are always active.
- With RPR+, both supervisor engines must run the same version of Cisco IOS software. If the supervisor engines are not running the same version of Cisco IOS software, the redundant supervisor engine comes online in RPR mode.
- RPR+ switchover takes place after the failed supervisor engine completes a core dump. A core dump can take up to 15 minutes. To get faster switchover time, disable core dump on the supervisor engines.
- 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 redundant supervisor engine and is lost on switchover.

These are examples of dynamic state information that is lost at switchover:

- Frame Relay Switched Virtual Circuits (SVCs)



Note Frame Relay-switched DLCI information is maintained across a switchover because Frame Relay-switched DLCI configuration is in the configuration file.

- All terminated PPP sessions
- All ATM SVC information

- All terminated TCP and other connection-oriented Layer 3 and Layer 4 sessions
- BGP sessions
- All Automatic Protection System (APS) state information

Hardware Configuration Guidelines and Restrictions

For redundant operation, the following guidelines and restrictions must be met:

- Cisco IOS running on the supervisor engine and the MSFC supports redundant configurations where the supervisor engines and MSFC routers are identical. If they are not identical, one will boot first and become active and hold the other supervisor engine and MSFC in a reset condition.
- 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.
- Both supervisor engines must have the same system image (see the “[Copying Files to the Redundant Supervisor Engine](#)” section on page 6-9).

**Note**

If the redundant supervisor engine is running Catalyst software, remove the active supervisor engine and boot the switch with only the redundant supervisor engine installed. Follow the procedures in the current release notes to convert the redundant supervisor engine from Catalyst software.

- The configuration register in the startup-config must be set to autoboot (see the “[Modifying the Boot Field](#)” section on page 3-23).

**Note**

There is no support for booting from the network.

If these requirements are met, the switch functions in RPR+ mode by default.

Configuration Mode Restrictions

The following configuration restrictions apply during the startup synchronization process:

- You cannot perform configuration changes during the startup (bulk) synchronization. If you attempt to make configuration changes during this process, the following message is generated:

```
Config mode locked out till standby initializes
```
- If configuration changes occur at the same time as a supervisor engine switchover, these configuration changes are lost.

Configuring Supervisor Engine Redundancy

These sections describe how to configure supervisor engine redundancy:

- Configuring RPR and RPR+, page 6-6
- Synchronizing the Supervisor Engine Configurations, page 6-6
- Displaying the Redundancy States, page 6-7

Configuring RPR and RPR+

To configure RPR or RPR+, perform this task:

	Command	Purpose
Step 1	Router(config)# redundancy	Enters redundancy configuration mode.
Step 2	Router(config-red)# mode {rpr rpr-plus}	Configures RPR or RPR+. When this command is entered, the redundant supervisor engine is reloaded and begins to work in RPR or RPR+ mode.
Step 3	Router# show running-config	Verifies that RPR or RPR+ is enabled.
Step 4	Router# show redundancy states	Displays the operating redundancy mode.

This example shows how to configure the system for RPR+ and display the redundancy state:

```

Router> enable
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# redundancy
Router(config-red)# mode rpr-plus
Router(config-red)# ^Z
Router# show redundancy states
    my state = 13 -ACTIVE
    peer state = 1 -DISABLED
        Mode = Simplex
        Unit = Primary
        Unit ID = 1

    Redundancy Mode (Operational) = Route Processor Redundancy Plus
    Redundancy Mode (Configured) = Route Processor Redundancy Plus
        Split Mode = Disabled
        Manual Swact = Disabled Reason: Simplex mode
        Communications = Down Reason: Simplex mode

        client count = 11
        client_notification_TMR = 30000 milliseconds
            keep_alive TMR = 4000 milliseconds
            keep_alive count = 0
            keep_alive threshold = 7
            RF debug mask = 0x0

Router#

```

Synchronizing the Supervisor Engine Configurations

During normal operation, the startup-config and config-registers 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
Step 1 Router(config)# redundancy	Enters redundancy configuration mode.
Step 2 Router(config-red)# main-cpu	Enters main-cpu configuration submode.
Step 3 Router(config-r-mc)# auto-sync {startup-config config-register bootvar standard}	Synchronizes the configuration elements.
Step 4 Router(config-r-mc)# end	Returns to privileged EXEC mode.
Step 5 Router# copy running-config startup-config	Forces a manual synchronization of the configuration files in NVRAM. Note This step is not required to synchronize the running configuration file in DRAM.



Note The **auto-sync standard** command does not synchronize the boot variables.

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 redundant supervisor engine:

```
Router(config)# redundancy
Router(config-red)# main-cpu
Router(config-r-mc)# auto-sync standard
Router(config-r-mc)# auto-sync bootvar
Router(config-r-mc)# end
Router# 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 only allow automatic synchronization of the config-registers of the active supervisor engine to the redundant supervisor engine while disallowing synchronization of the startup configuration:

```
Router(config)# redundancy
Router(config-red)# main-cpu
Router(config-r-mc)# no auto-sync standard
Router(config-r-mc)# auto-sync config-register
Router(config-r-mc)# end
Router# copy running-config startup-config
```

Displaying the Redundancy States

To display the redundancy states, perform this task:

Command	Purpose
Router# show redundancy states	Displays the redundancy states.

■ Performing a Fast Software Upgrade

This example shows how to display the redundancy states:

```
Router# show redundancy states
my state = 13 -ACTIVE
    peer state = 8 -STANDBY HOT
        Mode = Duplex
        Unit = Primary
        Unit ID = 1

Redundancy Mode (Operational) = Route Processor Redundancy Plus
Redundancy Mode (Configured) = Route Processor Redundancy Plus
    Split Mode = Disabled
    Manual Swact = Enabled
    Communications = Up

    client count = 11
    client_notification_TMR = 30000 milliseconds
        keep_alive TMR = 9000 milliseconds
            keep_alive count = 0
            keep_alive threshold = 18
            RF debug mask = 0x0

Router#
```

Performing a Fast Software Upgrade

The fast software upgrade (FSU) procedure supported by RPR+ allows you to upgrade the Cisco IOS image on the supervisor engines without reloading the system.



Note If you are performing a first-time upgrade to RPR+ from EHSA, you must reload both supervisor engines. FSU from EHSA is not supported.

To perform an FSU, perform this task:

	Command	Purpose
Step 1	<pre>Router# copy source_device:source_filename {disk0 disk1}:target_filename</pre> <p>Or:</p> <pre>Router# copy source_device:source_filename sup-bootflash:target_filename</pre> <p>Or:</p> <pre>Router# copy source_device:source_filename slavedisk0:target_filename</pre> <p>Or:</p> <pre>Router# copy source_device:source_filename slavesup-bootflash:target_filename</pre>	Copies the new Cisco IOS image to bootflash on both supervisor engines.
Step 2	<pre>Router# config terminal Router(config)# config-register 0x2102 Router(config)# boot system flash device:file_name</pre>	Configures the supervisor engines to boot the new image.

Command	Purpose
Step 3 Router# <code>copy running-config start-config</code>	Saves the configuration.
Step 4 Router# <code>hw-module {module num} reset</code>	Reloads the redundant supervisor engine and brings it back online (running the new version of the Cisco IOS software). Note Before reloading the redundant supervisor engine, make sure you wait long enough to ensure that all configuration synchronization changes have completed.
Step 5 Router# <code>redundancy force-switchover</code>	Conducts a manual switchover to the redundant supervisor engine. The redundant supervisor engine becomes the new active supervisor engine running the new Cisco IOS image. The modules are reloaded and the module software is downloaded from the new active supervisor engine. The old active supervisor engine reboots with the new image and becomes the redundant supervisor engine. Note To perform an EHSA to RPR+ FSU, use the <code>reload</code> command in Step 5.

This example shows how to perform an FSU:

```
Router# config terminal
Router(config)# config-register 0x2102
Router(config)# boot system flash disk0:c6k333-js-mz.122-14.SX
Router# copy running-config start-config
Router# hw-module reset
Router# redundancy force-switchover
Router#
```

Copying Files to the Redundant Supervisor Engine

Use the following command to copy a file to the **disk0:** device on a redundant supervisor engine:

```
Router# copy source_device:source_filename slavedisk0:target_filename
```

Use the following command to copy a file to the **bootflash:** device on a redundant supervisor engine:

```
Router# copy source_device:source_filename slavesup-bootflash:target_filename
```

Use the following command to copy a file to the **bootflash:** device on a redundant MSFC:

```
Router# copy source_device:source_filename slavebootflash:target_filename
```

■ Copying Files to the Redundant Supervisor Engine



Configuring LAN Ports for Layer 2 Switching

This chapter describes how to use the command-line interface (CLI) to configure Ethernet, Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet LAN ports for Layer 2 switching on the Catalyst 6500 series switches. The configuration tasks in this chapter apply to LAN ports on LAN switching modules and to the LAN ports on the supervisor engine.



For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication.

This chapter consists of these sections:

- [Understanding How Layer 2 Switching Works, page 7-1](#)
- [Default Layer 2 LAN Interface Configuration, page 7-4](#)
- [Layer 2 LAN Interface Configuration Guidelines and Restrictions, page 7-5](#)
- [Configuring LAN Interfaces for Layer 2 Switching, page 7-6](#)



To configure Layer 3 interfaces, see Chapter 16, “Configuring Layer 3 Interfaces.”

Understanding How Layer 2 Switching Works

These sections describe how Layer 2 switching works on the Catalyst 6500 series switches:

- [Understanding Layer 2 Ethernet Switching, page 7-1](#)
- [Understanding VLAN Trunks, page 7-2](#)
- [Layer 2 LAN Port Modes, page 7-4](#)

Understanding Layer 2 Ethernet Switching

These sections describe Layer 2 Ethernet switching:

- [Layer 2 Ethernet Switching Overview, page 7-2](#)
- [Switching Frames Between Segments, page 7-2](#)
- [Building the Address Table, page 7-2](#)

Layer 2 Ethernet Switching Overview

Catalyst 6500 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 the next packet.

Catalyst 6500 series switches solve 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 collision domain. Because each LAN port connects to a separate Ethernet collision domain, 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 stations can transmit and receive at the same time. When packets can flow in both directions simultaneously, effective Ethernet bandwidth doubles.

Switching Frames Between Segments

Each LAN port on a Catalyst 6500 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 stations 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 considers each LAN port to be an individual segment. When stations connected to different LAN ports need to communicate, the switch forwards frames from one LAN port to the other at wire speed to ensure that each session receives full bandwidth.

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

Building the Address Table

Catalyst 6500 series switches build the 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 address table, it floods the frame to all LAN ports of the same VLAN except the port that received the frame. When the destination station replies, the switch adds its relevant source address and port ID to the address table. The switch then forwards subsequent frames to a single LAN port without flooding to all LAN ports.

The address table can store at least 16,000 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

These sections describe VLAN trunks on the Catalyst 6500 series switches:

- [Trunking Overview, page 7-3](#)
- [Encapsulation Types, page 7-3](#)

Trunking Overview


Note

For information about VLANs, see [Chapter 10, “Configuring VLANs.”](#)

A trunk is a point-to-point link between the switch and another networking device. 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 ports:

- Inter-Switch Link (ISL)—ISL is a Cisco-proprietary trunking encapsulation (10-Gigabit Ethernet ports do not support ISL encapsulation).
- 802.1Q—802.1Q is an industry-standard trunking encapsulation.

You can configure a trunk on a single Ethernet port or on an EtherChannel. For more information about EtherChannel, see [Chapter 8, “Configuring EtherChannels.”](#)

Ethernet trunk ports support several trunking modes (see [Table 7-2 on page 7-4](#)). You can specify whether the trunk uses ISL or 802.1Q encapsulation, and if the encapsulation type is autonegotiated.


Note

You can configure LAN ports to negotiate the encapsulation type. You cannot configure WAN interfaces to negotiate the encapsulation type.

The Dynamic Trunking Protocol (DTP) manages trunk autonegotiation on LAN ports. DTP supports autonegotiation of both ISL and 802.1Q trunks.

To autonegotiate trunking, the LAN ports must be in the same VTP domain. Use the **trunk** or **nonegotiate** keywords to force LAN ports in different domains to trunk. For more information on VTP domains, see [Chapter 9, “Configuring VTP.”](#)

Encapsulation Types

[Table 7-1](#) lists the Ethernet trunk encapsulation types.

Table 7-1 Ethernet Trunk Encapsulation Types

Encapsulation	Function
switchport trunk encapsulation isl	Specifies ISL encapsulation on the trunk link. Note 10-Gigabit Ethernet ports do not support ISL encapsulation.
switchport trunk encapsulation dot1q	Specifies 802.1Q encapsulation on the trunk link.
switchport trunk encapsulation negotiate	Specifies that the LAN port negotiate with the neighboring LAN port to become an ISL (preferred) or 802.1Q trunk, depending on the configuration and capabilities of the neighboring LAN port.

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

■ Default Layer 2 LAN Interface Configuration

Layer 2 LAN Port Modes

Table 7-2 lists the Layer 2 LAN port modes and describes how they function on LAN ports.

Table 7-2 Layer 2 LAN Port Modes

Mode	Function
switchport mode access	Puts the LAN port into permanent nontrunking mode and negotiates to convert the link into a nontrunk link. The LAN port becomes a nontrunk port even if the neighboring LAN port does not agree to the change.
switchport mode dynamic desirable	Makes the LAN port actively attempt to convert the link to a trunk link. The LAN port becomes a trunk port if the neighboring LAN port is set to trunk , desirable , or auto mode. This is the default mode for all LAN ports.
switchport mode dynamic auto	Makes the LAN port willing to convert the link to a trunk link. The LAN port becomes a trunk port if the neighboring LAN port is set to trunk or desirable mode.
switchport mode trunk	Puts the LAN port into permanent trunking mode and negotiates to convert the link into a trunk link. The LAN port becomes a trunk port even if the neighboring port does not agree to the change.
switchport nonegotiate	Puts the LAN port into permanent trunking mode but prevents the port from generating DTP frames. You must configure the neighboring port manually as a trunk port to establish a trunk link.



Note

DTP is a point-to-point protocol. However, some internetworking devices might forward DTP frames improperly. To avoid this problem, ensure that LAN ports 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 LAN port to become a trunk but not generate DTP frames.

Default Layer 2 LAN Interface Configuration

Table 7-3 shows the Layer 2 LAN port default configuration.

Table 7-3 Layer 2 LAN Interface Default Configuration

Feature	Default
Interface mode:	
• Before entering the switchport command	Layer 3 (unconfigured)
• After entering the switchport command	switchport mode dynamic desirable
Trunk encapsulation	switchport trunk encapsulation negotiate
Allowed VLAN range	VLANs 1 to 4094, except reserved VLANs (see Table 10-1 on page 10-2)
VLAN range eligible for pruning	VLANs 2 to 1001
Default VLAN (for access ports)	VLAN 1
Native VLAN (for 802.1Q trunks)	VLAN 1

Table 7-3 Layer 2 LAN Interface Default Configuration (continued)

Feature	Default
Spanning Tree Protocol (STP)	Enabled for all VLANs
STP port priority	128
STP port cost	<ul style="list-style-type: none"> • 100 for 10-Mbps Ethernet LAN ports • 19 for 10/100-Mbps Fast Ethernet LAN ports • 19 for 100-Mbps Fast Ethernet LAN ports • 4 for 1,000-Mbps Gigabit Ethernet LAN ports • 2 for 10,000-Mbps 10-Gigabit Ethernet LAN ports

Layer 2 LAN Interface Configuration Guidelines and Restrictions

Follow these guidelines and restrictions when configuring Layer 2 LAN ports:

- 10-Gigabit Ethernet ports do not support ISL encapsulation.
- The following configuration guidelines and restrictions apply when using 802.1Q trunks and impose some limitations on the trunking strategy for a network. Note these restrictions when using 802.1Q trunks:
 - When connecting Cisco switches through an 802.1q trunk, make sure the native VLAN for an 802.1Q trunk is the same on both ends of the trunk link. If the native VLAN on one end of the trunk is different from the native VLAN on the other end, spanning tree loops might result.
 - Disabling spanning tree on the native VLAN of an 802.1Q trunk without disabling spanning tree on every VLAN in the network can cause spanning tree loops. We recommend that you leave spanning tree enabled on the native VLAN of an 802.1Q trunk. If this is not possible, disable spanning tree on every VLAN in the network. Make sure your network is free of physical loops before disabling spanning tree.
 - When you connect two Cisco switches through 802.1Q trunks, the switches exchange spanning tree BPDUs on each VLAN allowed on the trunks. The BPDUs on the native VLAN of the trunk are sent untagged to the reserved IEEE 802.1d spanning tree multicast MAC address (01-80-C2-00-00-00). The BPDUs on all other VLANs on the trunk are sent tagged to the reserved Cisco Shared Spanning Tree (SSTP) multicast MAC address (01-00-0c-cc-cc-cd).
 - Non-Cisco 802.1Q switches maintain only a single instance of spanning tree (the Mono Spanning Tree, or MST) that defines the spanning tree topology for all VLANs. When you connect a Cisco switch to a non-Cisco switch through an 802.1Q trunk, the MST of the non-Cisco switch and the native VLAN spanning tree of the Cisco switch combine to form a single spanning tree topology known as the Common Spanning Tree (CST).
 - Because Cisco switches transmit BPDUs to the SSTP multicast MAC address on VLANs other than the native VLAN of the trunk, non-Cisco switches do not recognize these frames as BPDUs and flood them on all ports in the corresponding VLAN. Other Cisco switches connected to the non-Cisco 802.1Q cloud receive these flooded BPDUs. This allows Cisco switches to maintain a per-VLAN spanning tree topology across a cloud of non-Cisco 802.1Q switches. The non-Cisco 802.1Q cloud separating the Cisco switches is treated as a single broadcast segment between all switches connected to the non-Cisco 802.1Q cloud through 802.1Q trunks.

■ Configuring LAN Interfaces for Layer 2 Switching

- Make certain that the native VLAN is the same on all of the 802.1q trunks connecting the Cisco switches to the non-Cisco 802.1q cloud.
- If you are connecting multiple Cisco switches to a non-Cisco 802.1q cloud, all of the connections must be through 802.1q trunks. You cannot connect Cisco switches to a non-Cisco 802.1q cloud through ISL trunks or through access ports. Doing so will cause the switch to place the ISL trunk port or access port into the spanning tree “port inconsistent” state and no traffic will pass through the port.

Configuring LAN Interfaces for Layer 2 Switching

These sections describe how to configure Layer 2 switching on the Catalyst 6500 series switches:

- [Configuring a LAN Port for Layer 2 Switching, page 7-6](#)
- [Configuring a Layer 2 Switching Port as a Trunk, page 7-7](#)
- [Configuring a LAN Interface as a Layer 2 Access Port, page 7-13](#)



Note Use the **default interface { ethernet | fastethernet | gigabitethernet | tengigabitethernet } slot/port** command to revert an interface to its default configuration.

Configuring a LAN Port for Layer 2 Switching

To configure a LAN port for Layer 2 switching, perform this task:

Command	Purpose
Step 1 Router(config)# interface type¹ slot/port	Selects the LAN port to configure.
Step 2 Router(config-if)# shutdown	(Optional) Shuts down the interface to prevent traffic flow until configuration is complete.
Step 3 Router(config-if)# switchport	Configures the LAN port for Layer 2 switching. Note You must enter the switchport command once without any keywords to configure the LAN port as a Layer 2 port before you can enter additional switchport commands with keywords.
Router(config-if)# no switchport	Clears Layer 2 LAN port configuration.
Step 4 Router(config-if)# no shutdown	Activates the interface. (Required only if you shut down the interface.)
Step 5 Router(config-if)# end	Exits configuration mode.
Step 6 Router# show running-config interface [type¹ slot/port]	Displays the running configuration of the interface.
Step 7 Router# show interfaces [type¹ slot/port] switchport	Displays the switch port configuration of the interface.
Step 8 Router# show interfaces [type¹ slot/port] trunk	Displays the trunk configuration of the interface.

1. *type* = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

After you enter the **switchport** command, the default mode is **switchport mode dynamic desirable**. If the neighboring port supports trunking and is configured to allow trunking, the link becomes a Layer 2 trunk when you enter the **switchport** command. By default, LAN trunk ports negotiate encapsulation. If the neighboring port supports ISL and 802.1Q encapsulation and both ports are set to negotiate the encapsulation type, the trunk uses ISL encapsulation (10-Gigabit Ethernet ports do not support ISL encapsulation).

Configuring a Layer 2 Switching Port as a Trunk

These section describe configuring a Layer 2 switching port as a trunk:

- [Preparing a Layer 2 Switching Port for Configuration as a Trunk, page 7-7](#)
- [Configuring the Layer 2 Switching Port as an ISL or 802.1Q Trunk, page 7-8](#)
- [Configuring the Layer 2 Trunk to Use DTP, page 7-8](#)
- [Configuring the Layer 2 Trunk Not to Use DTP, page 7-9](#)
- [Configuring the Default VLAN, page 7-9](#)
- [Configuring the 802.1Q Native VLAN, page 7-10](#)
- [Configuring the List of VLANs Allowed on a Trunk, page 7-10](#)
- [Configuring the List of Prune-Eligible VLANs, page 7-11](#)
- [Completing Trunk Configuration, page 7-12](#)
- [Verifying Layer 2 Trunk Configuration, page 7-12](#)
- [Configuration and Verification Examples, page 7-12](#)

Preparing a Layer 2 Switching Port for Configuration as a Trunk

To prepare a Layer 2 switching port for configuration as a trunk, perform this task:

Command	Purpose
Step 1 Router(config)# interface type ¹ slot/port	Selects the LAN port to configure.
Step 2 Router(config-if)# shutdown	(Optional) Shuts down the interface to prevent traffic flow until configuration is complete.
Step 3 Router(config-if)# switchport	(Optional) Configures the LAN port for Layer 2 switching (required only if the LAN port is not already configured for Layer 2 switching; see the “ Configuring a LAN Port for Layer 2 Switching ” section on page 7-6)

1. *type* = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

Configuring the Layer 2 Switching Port as an ISL or 802.1Q Trunk



Note Complete the steps in the “[Preparing a Layer 2 Switching Port for Configuration as a Trunk](#)” section on [page 7-7](#) before performing the tasks in this section.

To configure the Layer 2 switching port as an ISL or 802.1Q trunk, perform this task:

Command	Purpose
<pre>Router(config-if)# switchport trunk encapsulation {isl dot1q negotiate}</pre>	(Optional) Configures the encapsulation, which configures the Layer 2 switching port as either an ISL or 802.1Q trunk. Note To support the switchport mode trunk command, you must configure the encapsulation.
<pre>Router(config-if)# no switchport trunk encapsulation</pre>	Reverts to the default trunk encapsulation mode (negotiate).



Note Complete the steps in the “[Completing Trunk Configuration](#)” section on [page 7-12](#) after performing the tasks in this section.

Configuring the Layer 2 Trunk to Use DTP



Note Complete the steps in the “[Preparing a Layer 2 Switching Port for Configuration as a Trunk](#)” section on [page 7-7](#) before performing the tasks in this section.

To configure the Layer 2 trunk to use DTP, perform this task:

Command	Purpose
<pre>Router(config-if)# switchport mode dynamic {auto desirable}</pre>	(Optional) Configures the trunk to use DTP.
<pre>Router(config-if)# no switchport mode</pre>	Reverts to the default trunk trunking mode (switchport mode dynamic desirable).

When configuring the Layer 2 trunk to use DTP, note the following syntax information:

- Required only if the interface is a Layer 2 access port or to specify the trunking mode.
- See [Table 7-2 on page 7-4](#) for information about trunking modes.



Note Complete the steps in the “[Completing Trunk Configuration](#)” section on [page 7-12](#) after performing the tasks in this section.

Configuring the Layer 2 Trunk Not to Use DTP



Note Complete the steps in the “Preparing a Layer 2 Switching Port for Configuration as a Trunk” section on page 7-7 before performing the tasks in this section.

To configure the Layer 2 trunk not to use DTP, perform this task:

Command	Purpose
Step 1 Router(config-if)# switchport mode trunk Router(config-if)# no switchport mode	(Optional) Configures the port to trunk unconditionally. Reverts to the default trunk trunking mode (switchport mode dynamic desirable).
Step 2 Router(config-if)# switchport nonegotiate Router(config-if)# no switchport nonegotiate	(Optional) Configures the trunk not to use DTP. Enables DTP on the port.

When configuring the Layer 2 trunk not to use DTP, note the following syntax information:

- Before entering the **switchport mode trunk** command, you must configure the encapsulation (see the “Configuring the Layer 2 Switching Port as an ISL or 802.1Q Trunk” section on page 7-8).
- To support the **switchport nonegotiate** command, you must enter the **switchport mode trunk** command.
- Enter the **switchport mode dynamic trunk** command. See Table 7-2 on page 7-4 for information about trunking modes.
- Before entering the **switchport nonegotiate** command, you must configure the encapsulation (see the “Configuring the Layer 2 Switching Port as an ISL or 802.1Q Trunk” section on page 7-8) and configure the port to trunk unconditionally with the **switchport mode trunk** command (see the “Configuring the Layer 2 Trunk to Use DTP” section on page 7-8).



Note Complete the steps in the “Completing Trunk Configuration” section on page 7-12 after performing the tasks in this section.

Configuring the Default VLAN



Note Complete the steps in the “Preparing a Layer 2 Switching Port for Configuration as a Trunk” section on page 7-7 before performing the tasks in this section.

To configure the default VLAN, perform this task:

Command	Purpose
Router(config-if)# switchport access vlan <i>vlan_ID</i>	(Optional) Configures the default VLAN, which is used if the interface stops trunking. The <i>vlan_ID</i> value can be 1 through 4094, except reserved VLANs (see Table 10-1 on page 10-2).
Router(config-if)# no switchport access vlan	Reverts to the default value (VLAN 1).



Note Complete the steps in the “[Completing Trunk Configuration](#)” section on page 7-12 after performing the tasks in this section.

Configuring the 802.1Q Native VLAN



Note Complete the steps in the “[Preparing a Layer 2 Switching Port for Configuration as a Trunk](#)” section on page 7-7 before performing the tasks in this section.

To configure the 802.1Q native VLAN, perform this task:

Command	Purpose
Router(config-if)# switchport trunk native vlan <i>vlan_ID</i>	(Optional) Configures the 802.1Q native VLAN.
Router(config-if)# no switchport trunk native vlan	Reverts to the default value (VLAN 1).

When configuring the native VLAN, note the following syntax information:

- The *vlan_ID* value can be 1 through 4094, except reserved VLANs (see [Table 10-1 on page 10-2](#)).
- The access VLAN is not automatically used as the native VLAN.



Note Complete the steps in the “[Completing Trunk Configuration](#)” section on page 7-12 after performing the tasks in this section.

Configuring the List of VLANs Allowed on a Trunk



Note Complete the steps in the “[Preparing a Layer 2 Switching Port for Configuration as a Trunk](#)” section on page 7-7 before performing the tasks in this section.

To configure the list of VLANs allowed on a trunk, perform this task:

Command	Purpose
Router(config-if)# switchport trunk allowed vlan {add except none remove} vlan [,vlan[,vlan[,...]]]	(Optional) Configures the list of VLANs allowed on the trunk.
Router(config-if)# no switchport trunk allowed vlan	Reverts to the default value (all VLANs allowed).

When configuring the list of VLANs allowed on a trunk, note the following syntax information:

- The *vlan* parameter is either a single VLAN number from 1 through 4094, except reserved VLANs (see [Table 10-1 on page 10-2](#)), 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 *vlan* parameters or in dash-specified ranges.
- All VLANs are allowed by default.

- You can remove the default VLANs (1002–1005) from a trunk.
- You can remove VLAN 1. If you remove VLAN 1 from a trunk, the trunk interface continues to send and receive management traffic, for example, Cisco Discovery Protocol (CDP), VLAN Trunking Protocol (VTP), Port Aggregation Protocol (PAgP), and DTP in VLAN 1.

**Note**

Complete the steps in the “[Completing Trunk Configuration](#)” section on page 7-12 after performing the tasks in this section.

Configuring the List of Prune-Eligible VLANs

**Note**

Complete the steps in the “[Preparing a Layer 2 Switching Port for Configuration as a Trunk](#)” section on page 7-7 before performing the tasks in this section.

To configure the list of prune-eligible VLANs on the Layer 2 trunk, perform this task:

Command	Purpose
<code>Router(config-if)# switchport trunk pruning vlan {none {{add except remove} vlan[,vlan[,vlan[,...]]]}}</code>	(Optional) Configures the list of prune-eligible VLANs on the trunk (see the “ Understanding VTP Pruning ” section on page 9-3).
<code>Router(config-if)# no switchport trunk pruning vlan</code>	Reverts to the default value (all VLANs prune-eligible).

When configuring the list of prune-eligible VLANs on a trunk, note the following syntax information:

- The *vlan* parameter is either a single VLAN number from 1 through 4094, except reserved VLANs (see [Table 10-1 on page 10-2](#)), 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 *vlan* parameters or in dash-specified ranges.
- The default list of VLANs allowed to be pruned contains all VLANs.
- Network devices in VTP transparent mode do not send VTP Join messages. On Catalyst 6500 series switches with trunk connections to network devices in VTP transparent mode, configure the VLANs used by the transparent-mode network devices or that need to be carried across the transparent-mode network devices as pruning ineligible.

**Note**

Complete the steps in the “[Completing Trunk Configuration](#)” section on page 7-12 after performing the tasks in this section.

Completing Trunk Configuration

To complete Layer 2 trunk configuration, perform this task:

	Command	Purpose
Step 1	Router(config-if)# no shutdown	Activates the interface. (Required only if you shut down the interface.)
Step 2	Router(config-if)# end	Exits configuration mode.

Verifying Layer 2 Trunk Configuration

To verify Layer 2 trunk configuration, perform this task:

	Command	Purpose
Step 1	Router# show running-config interface type¹ slot/port	Displays the running configuration of the interface.
Step 2	Router# show interfaces [type¹ slot/port] switchport	Displays the switch port configuration of the interface.
Step 3	Router# show interfaces [type¹ slot/port] trunk	Displays the trunk configuration of the interface.

1. *type* = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

Configuration and Verification Examples

This example shows how to configure the Fast Ethernet port 5/8 as an 802.1Q trunk. This example assumes that the neighbor port is configured to support 802.1Q trunking:

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

This example shows how to verify the configuration:

```
Router# show running-config interface fastethernet 5/8
Building configuration...
Current configuration:
!
interface FastEthernet5/8
  no ip address
  switchport
    switchport trunk encapsulation dot1q
  end

Router# 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: ALL

Router# 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

Router#

```

Configuring a LAN Interface as a Layer 2 Access Port



Note If you assign a LAN port to a VLAN that does not exist, the port is shut down until you create the VLAN in the VLAN database (see the “[Creating or Modifying an Ethernet VLAN](#)” section on page 10-10).

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

Command	Purpose
Step 1 Router(config)# interface type¹ slot/port	Selects the LAN port to configure.
Step 2 Router(config-if)# shutdown	(Optional) Shuts down the interface to prevent traffic flow until configuration is complete.
Step 3 Router(config-if)# switchport	Configures the LAN port for Layer 2 switching. Note You must enter the switchport command once without any keywords to configure the LAN port as a Layer 2 port before you can enter additional switchport commands with keywords.
Step 4 Router(config-if)# no switchport	Clears Layer 2 LAN port configuration.
Step 5 Router(config-if)# switchport mode access Router(config-if)# no switchport mode	Configures the LAN port as a Layer 2 access port. Reverts to the default switchport mode (switchport mode dynamic desirable).
Step 6 Router(config-if)# switchport access vlan vlan_ID Router(config-if)# no switchport access vlan	Places the LAN port in a VLAN. The <i>vlan_ID</i> value can be 1 through 4094, except reserved VLANs (see Table 10-1 on page 10-2). Reverts to the default VLAN (VLAN 1).

Configuring LAN Interfaces for Layer 2 Switching

Command	Purpose
Step 7 Router(config-if)# no shutdown	Activates the interface. (Required only if you shut down the interface.)
Step 8 Router(config-if)# end	Exits configuration mode.
Step 9 Router# show running-config interface [type¹ slot/port]	Displays the running configuration of the interface.
Step 10 Router# show interfaces [type¹ slot/port] switchport	Displays the switch port configuration of the interface.

1. *type* = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

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

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

This example shows how to verify the configuration:

```
Router# show running-config interface fastethernet 5/6
Building configuration...
!
Current configuration:
interface FastEthernet5/6
  no ip address
  switchport access vlan 200
  switchport mode access
end

Router# show interfaces fastethernet 5/6 switchport
Name: Fa5/6
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Enabled
Access Mode VLAN: 200 (VLAN0200)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: ALL

Router#
```



CHAPTER

8

Configuring EtherChannels

This chapter describes how to configure EtherChannels on the Catalyst 6500 series switch Layer 2 or Layer 3 LAN ports.

**Note**

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication.

This chapter consists of these sections:

- [Understanding How EtherChannels Work, page 8-1](#)
- [EtherChannel Feature Configuration Guidelines and Restrictions, page 8-5](#)
- [Configuring EtherChannels, page 8-6](#)

**Note**

The commands in the following sections can be used on all LAN ports in Catalyst 6500 series switches, including the ports on the supervisor engine and a redundant supervisor engine.

Understanding How EtherChannels Work

These sections describe how EtherChannels work:

- [EtherChannel Feature Overview, page 8-1](#)
- [Understanding How EtherChannels Are Configured, page 8-2](#)
- [Understanding Port Channel Interfaces, page 8-4](#)
- [Understanding Load Balancing, page 8-4](#)

EtherChannel Feature Overview

An EtherChannel bundles individual Ethernet links into a single logical link that provides the aggregate bandwidth of up to eight physical links.

A Catalyst 6500 series switch supports a maximum of 64 EtherChannels. You can form an EtherChannel with up to eight compatibly configured LAN ports on any module in a Catalyst 6500 series switch. All LAN ports in each EtherChannel must be the same speed and must all be configured as either Layer 2 or Layer 3 LAN ports.



Note The network device to which a Catalyst 6500 series switch is connected may impose its own limits on the number of ports 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. When a failure occurs, the EtherChannel feature sends a trap that identifies 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.

Understanding How EtherChannels Are Configured

These sections describe how EtherChannels are configured:

- [EtherChannel Configuration Overview, page 8-2](#)
- [Understanding Manual EtherChannel Configuration, page 8-3](#)
- [Understanding PAgP EtherChannel Configuration, page 8-3](#)
- [Understanding IEEE 802.3ad LACP EtherChannel Configuration, page 8-3](#)

EtherChannel Configuration Overview

You can configure EtherChannels manually or you can use the Port Aggregation Control Protocol (PAgP) or 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. Ports configured to use LACP cannot form EtherChannels with ports configured to use PAgP.

[Table 8-1](#) lists the user-configurable EtherChannel modes.

Table 8-1 EtherChannel Modes

Mode	Description
on	Mode that forces the LAN port to channel unconditionally. In the on mode, a usable EtherChannel exists only when a LAN port group in the on mode is connected to another LAN port group in the on mode. Because ports configured in the on mode do not negotiate, there is no negotiation traffic between the ports. You cannot configure the on mode with an EtherChannel protocol.
auto	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. (Default)
desirable	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.
passive	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. (Default)
active	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

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 must 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 8-9](#)). 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 Channel Groups” section on page 8-7](#)). LACP uses the port priority with the port number to form the port identifier. LACP uses the port priority to decide which ports should be put in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.
- 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

On ports configured to use LACP, LACP tries to configure the maximum number of compatible ports in an EtherChannel, up to the maximum allowed by the hardware (eight ports). If LACP cannot aggregate all the ports that are compatible (for example, the remote system might have more restrictive hardware limitations), then all the ports that cannot be actively included in the channel are put in hot standby state and are used only if one of the channeled ports fails. You can configure an additional 8 standby ports (total of 16 ports associated with the EtherChannel).

Understanding Port Channel Interfaces

Each EtherChannel has a numbered port channel interface. You can configure a maximum of 64 port channel interfaces, numbered from 1 to 256.

The configuration that you apply to the port channel interface affects all LAN ports assigned to the port channel interface.

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 LAN ports affects only the LAN port where you apply the configuration. To change the parameters of all ports in an EtherChannel, apply the configuration commands to the port channel interface, for example, Spanning Tree Protocol (STP) commands or commands to configure a Layer 2 EtherChannel as a trunk.

Understanding Load Balancing

An EtherChannel balances the traffic load across the links in an EtherChannel by reducing part of the binary pattern formed from the addresses in the frame to a numerical value that selects one of the links in the channel.

EtherChannel load balancing can use MAC addresses or IP addresses. With a PFC2, EtherChannel load balancing can also use Layer 4 port numbers. EtherChannel load balancing can use either source or destination or both source and destination addresses or ports. The selected mode applies to all EtherChannels configured on the switch.

Use the option that provides the balance criteria with the greatest variety in your configuration. For example, if the traffic on an EtherChannel is going only to a single MAC address and you use the destination MAC address as the basis of EtherChannel load balancing, the EtherChannel always chooses the same link in the EtherChannel; using source addresses or IP addresses might result in better load balancing.

EtherChannel Feature Configuration Guidelines and Restrictions

When EtherChannel interfaces are configured improperly, they are disabled automatically to avoid network loops and other problems. To avoid configuration problems, observe these guidelines and restrictions:

- All Ethernet LAN ports on all modules, including those on a redundant supervisor engine, support EtherChannels (maximum of eight LAN ports) with no requirement that the LAN ports be physically contiguous or on the same module.
- Configure all LAN ports in an EtherChannel to use the same EtherChannel protocol; you cannot run two EtherChannel protocols in one EtherChannel.
- Configure all LAN ports in an EtherChannel to operate at the same speed and in the same duplex mode.
- LACP does not support half-duplex. Half-duplex ports in an LACP EtherChannel are put in the suspended state.
- Enable all LAN ports in an EtherChannel. If you shut down a LAN port in an EtherChannel, it is treated as a link failure and its traffic is transferred to one of the remaining ports in the EtherChannel.
- An EtherChannel will not form if one of the LAN ports 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 LAN ports in the channel.
- For Layer 2 EtherChannels:
 - Assign all LAN ports in the EtherChannel to the same VLAN or configure them as trunks.
 - If you configure an EtherChannel from trunking LAN ports, verify that the trunking mode is the same on all the trunks. LAN ports in an EtherChannel with different trunk modes can operate unpredictably.
 - An EtherChannel supports the same allowed range of VLANs on all the LAN ports in a trunking Layer 2 EtherChannel. If the allowed range of VLANs is not the same, the LAN ports do not form an EtherChannel.
 - LAN ports with different STP port path costs can form an EtherChannel as long they are compatibly configured with each other. If you set different STP port path costs, the LAN ports are not incompatible for the formation of an EtherChannel.
 - An EtherChannel will not form if protocol filtering is set differently on the LAN ports.

- 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 LAN ports affects only the LAN port where you apply the configuration.
- When QoS is enabled, enter the **no mls qos channel-consistency** port-channel interface command to support EtherChannels that have ports with and without strict-priority queues.

Configuring EtherChannels

These sections describe how to configure EtherChannels:

- [Configuring Port Channel Logical Interfaces for Layer 3 EtherChannels, page 8-6](#)
- [Configuring Channel Groups, page 8-7](#)
- [Configuring EtherChannel Load Balancing, page 8-10](#)



Note Make sure that the LAN ports are configured correctly (see the “EtherChannel Feature Configuration Guidelines and Restrictions” section on [page 8-5](#)).

Configuring Port Channel Logical Interfaces for Layer 3 EtherChannels



- Note**
- When configuring Layer 2 EtherChannels, you cannot put Layer 2 LAN ports into manually created port channel logical interfaces. If you are configuring a Layer 2 EtherChannel, do not perform the procedures in this section (see the “[Configuring Channel Groups](#)” section on [page 8-7](#)).
 - When configuring Layer 3 EtherChannels, you must manually create the port channel logical interface as described in this section, and then put the Layer 3 LAN ports into the channel group (see the “[Configuring Channel Groups](#)” section on [page 8-7](#)).
 - To move an IP address from a Layer 3 LAN port to an EtherChannel, you must delete the IP address from the Layer 3 LAN port before configuring it on the port channel logical interface.

To create a port channel interface for a Layer 3 EtherChannel, perform this task:

	Command	Purpose
Step 1	<code>Router(config)# interface port-channel number</code>	Creates the port channel interface.
	<code>Router(config)# no interface port-channel number</code>	Deletes the port channel interface.
Step 2	<code>Router(config-if)# ip address ip_address mask</code>	Assigns an IP address and subnet mask to the EtherChannel.
Step 3	<code>Router(config-if)# end</code>	Exits configuration mode.
Step 4	<code>Router# show running-config interface port-channel number</code>	Verifies the configuration.

The *group* number can be 1 through 256, up to a maximum of 64 port channel interfaces.

This example shows how to create port channel interface 1:

```
Router# configure terminal
Router(config)# interface port-channel 1
Router(config-if)# ip address 172.32.52.10 255.255.255.0
Router(config-if)# end
```

This example shows how to verify the configuration of port channel interface 1:

```
Router# 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
Router#
```

Configuring Channel Groups



Note

- When configuring Layer 3 EtherChannels, you must manually create the port channel logical interface first (see the “[Configuring Port Channel Logical Interfaces for Layer 3 EtherChannels](#)” section on page 8-6), and then put the Layer 3 LAN ports into the channel group as described in this section.
- When configuring Layer 2 EtherChannels, configure the LAN ports with the **channel-group** command as described in this section, which automatically creates the port channel logical interface. You cannot put Layer 2 LAN ports into a manually created port channel interface.
- For Cisco IOS to create port channel interfaces for Layer 2 EtherChannels, the Layer 2 LAN ports must be connected and functioning.

To configure channel groups, perform this task for each LAN port:

Command	Purpose
Step 1 Router(config)# interface type ¹ <i>slot/port</i>	Selects a LAN port to configure.
Step 2 Router(config-if)# no ip address	Ensures that there is no IP address assigned to the LAN port.
Step 3 Router(config-if)# channel-protocol { lacp pagp } Router(config-if)# no channel-protocol	(Optional) On the selected LAN port, restricts the channel-group command to the EtherChannel protocol configured with the channel-protocol command. Removes the restriction.
Step 4 Router(config-if)# channel-group <i>number mode</i> { active auto desirable on passive }	Configures the LAN port in a port channel and specifies the mode (see Table 8-1 on page 8-2). PAgP supports only the auto and desirable modes. LACP supports only the active and passive modes.
Router(config-if)# no channel-group	Removes the LAN port from the channel group.

Configuring EtherChannels

Command	Purpose
Step 5 Router(config-if)# lacp port-priority <i>priority_value</i>	(Optional for LACP) Valid values are 1 through 65535. Higher numbers have lower priority. The default is 32768.
	Reverts to the default.
Step 6 Router(config-if)# end	Exits configuration mode.
Step 7 Router# show running-config interface type¹ <i>slot/port</i> Router# show interfaces type¹ <i>slot/port</i> etherchannel	Verifies the configuration.

1. *type* = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

This example shows how to configure Fast Ethernet ports 5/6 and 5/7 into port channel 2 with PAgP mode **desirable**:

```
Router# configure terminal
Router(config)# interface range fastethernet 5/6 -7
Router(config-if)# channel-group 2 mode desirable
Router(config-if)# end
```



Note See the “Configuring a Range of Interfaces” section on page 5-4 for information about the **range** keyword.

This example shows how to verify the configuration of port channel interface 2:

```
Router# show running-config interface port-channel 2
Building configuration...
```

```
Current configuration:
!
interface Port-channel2
no ip address
switchport
switchport access vlan 10
switchport mode access
end
Router#
```

This example shows how to verify the configuration of Fast Ethernet port 5/6:

```
Router# show running-config interface fastethernet 5/6
Building configuration...

Current configuration:
!
interface FastEthernet5/6
no ip address
switchport
switchport access vlan 10
switchport mode access
channel-group 2 mode desirable
end
```

```

Router# show interfaces fastethernet 5/6 etherchannel
Port state      = Down Not-in-Bndl
Channel group  = 12          Mode = Desirable-Sl      Gcchange = 0
Port-channel   = null        GC   = 0x00000000      Pseudo port-channel = Po1
2
Port index     = 0           Load = 0x00          Protocol = PAgP

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.
        d - PAgP is down.

Timers: H - Hello timer is running.       Q - Quit timer is running.
        S - Switching timer is running.    I - Interface timer is running.

Local information:
               Hello      Partner    PAgP      Learning  Group
Port      Flags State  Timers Interval Count Priority Method Ifindex
Fa5/2    d      U1/S1          1s        0      128      Any      0

Age of the port in the current state: 04d:18h:57m:19s

```

This example shows how to verify the configuration of port channel interface 2 after the LAN ports have been configured:

```

Router# show etherchannel 12 port-channel
  Port-channels in the group:
  -----
  Port-channel: Po12
  -----
  Age of the Port-channel = 04d:18h:58m:50s
  Logical slot/port = 14/1          Number of ports = 0
  GC                = 0x00000000      HotStandBy port = null
  Port state        = Port-channel Ag-Not-Inuse
  Protocol          = PAgP

Router#

```

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.

Configuring EtherChannels

To configure the LACP system priority and system ID, perform this task:

	Command	Purpose
Step 1	Router(config)# lacp system-priority <i>priority_value</i>	(Optional for LACP) Valid values are 1 through 65535. Higher numbers have lower priority. The default is 32768.
	Router(config)# no lacp system-priority	Reverts to the default.
Step 2	Router(config)# end	Exits configuration mode.
Step 3	Router# show lacp sys-id	Verifies the configuration.

This example shows how to configure the LACP system priority:

```
Router# configure terminal
Router(config)# lacp system-priority 23456
Router(config)# end
Router(config)#
```

This example shows how to verify the configuration:

```
Router# show lacp sys-id
23456,0050.3e8d.6400
Router#
```

The system priority is displayed first, followed by the MAC address of the switch.

Configuring EtherChannel Load Balancing

To configure EtherChannel load balancing, perform this task:

	Command	Purpose
Step 1	Router(config)# 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.
	Router(config)# no port-channel load-balance	Reverts to default EtherChannel load balancing.
Step 2	Router(config)# end	Exits configuration mode.
Step 3	Router# show etherchannel load-balance	Verifies the configuration.

The load-balancing keywords indicate the following information:

- **src-port**—Source Layer 4 port
- **dst-port**—Destination Layer 4 port
- **src-dst-port**—Source and destination Layer 4 port
- **src-ip**—Source IP addresses
- **dst-ip**—Destination IP addresses
- **src-dst-ip**—Source and destination IP addresses
- **src-mac**—Source MAC addresses
- **dst-mac**—Destination MAC addresses
- **src-dst-mac**—Source and destination MAC addresses

This example shows how to configure EtherChannel to use source and destination IP addresses:

```
Router# configure terminal  
Router(config)# port-channel load-balance src-dst-ip  
Router(config)# end  
Router(config)#
```

This example shows how to verify the configuration:

```
Router# show etherchannel load-balance  
Source XOR Destination IP address  
Router#
```




Configuring VTP

This chapter describes how to configure the VLAN Trunking Protocol (VTP) on the Catalyst 6500 series switches.

**Note**

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication.

This chapter consists of these sections:

- [Understanding How VTP Works, page 9-1](#)
- [VTP Default Configuration, page 9-5](#)
- [VTP Configuration Guidelines and Restrictions, page 9-5](#)
- [Configuring VTP, page 9-6](#)

Understanding How VTP Works

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 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 10, “Configuring VLANs.”](#)

These sections describe how VTP works:

- [Understanding the VTP Domain, page 9-2](#)
- [Understanding VTP Modes, page 9-2](#)
- [Understanding VTP Advertisements, page 9-2](#)
- [Understanding VTP Version 2, page 9-3](#)
- [Understanding VTP Pruning, page 9-3](#)

Understanding the VTP Domain

A VTP domain (also called a VLAN management 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 one and 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 6500 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.

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 trunk connections.

VTP maps VLANs dynamically across multiple LAN types with unique names and internal index associations. Mapping eliminates excessive device administration required from network administrators.

Understanding VTP Modes

You can configure a Catalyst 6500 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 out their trunking LAN ports.



Note

Catalyst 6500 series switches 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 port 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**

If you are using VTP in a Token Ring environment, you must use version 2.

VTP version 2 supports the following features not supported in version 1:

- Token Ring support—VTP version 2 supports Token Ring LAN switching and VLANs (Token Ring Bridge Relay Function [TrBRF] and Token Ring Concentrator Relay Function [TrCRF]). For more information about Token Ring VLANs, see the “[Understanding How VLANs Work](#)” section on [page 10-1](#).
- 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, unknown, and flooded 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 support VTP pruning. On devices that do not support VTP pruning, you must manually configure the VLANs allowed on trunks.

■ Understanding How VTP Works

Figure 9-1 shows a switched network without VTP pruning enabled. Interface 1 on network Switch 1 and port 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 ports in the Red VLAN.

You enable pruning globally on the Catalyst 6500 series switch (see the “Enabling VTP Pruning” section on page 9-7). You configure pruning on Layer 2 trunking LAN ports (see the “Configuring a Layer 2 Switching Port as a Trunk” section on page 7-7).

Figure 9-1 Flooding Traffic without VTP Pruning

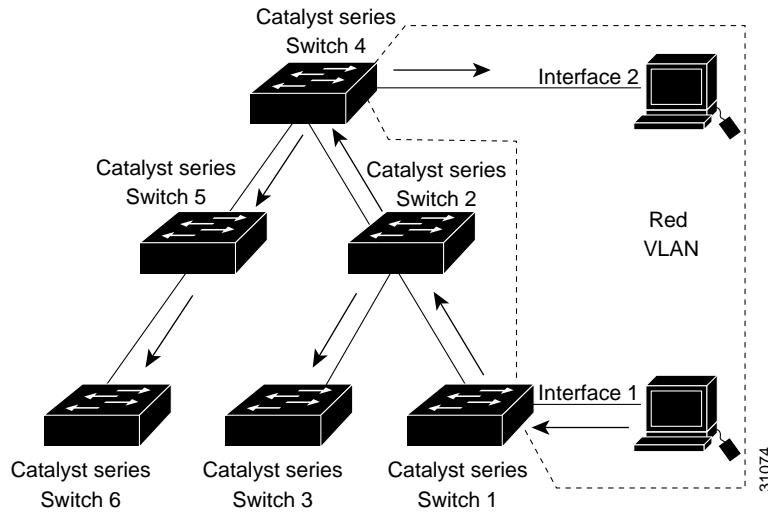
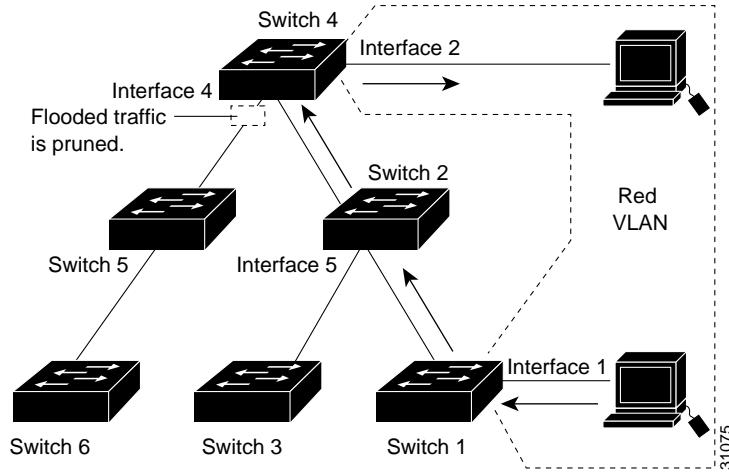


Figure 9-2 shows the same switched network with VTP pruning enabled. The broadcast traffic from Switch 1 is not forwarded to Switches 3, 5, and 6 because traffic for the Red VLAN has been pruned on the links indicated (port 5 on Switch 2 and port 4 on Switch 4).

Figure 9-2 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 pruning eligible. VTP pruning does not prune traffic from pruning-ineligible VLANs. VLAN 1 is always pruning ineligible; traffic from VLAN 1 cannot be pruned.

To configure VTP pruning on a trunking LAN port, use the **switchport trunk pruning vlan** command (see the “[Configuring a Layer 2 Switching Port as a Trunk](#)” section on page 7-7). VTP pruning operates when a LAN port is trunking. You can set VLAN pruning eligibility when VTP pruning is enabled or disabled for the VTP domain, when any given VLAN exists or not, and when the LAN port is currently trunking or not.

VTP Default Configuration

[Table 9-1](#) shows the default VTP configuration.

Table 9-1 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

VTP Configuration Guidelines and Restrictions

Follow these guidelines and restrictions when implementing VTP in your network:

- Supervisor engine redundancy does not support nondefault VLAN data file names or locations. Do not enter the **vtp file file_name** command on a switch that has a redundant supervisor engine.
- Before installing a redundant supervisor engine, enter the **no vtp file** command to return to the default configuration.
- 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 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 provided 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 network device, all of the version 2-capable network devices in the domain enable VTP version 2.
- In a Token Ring environment, you must enable VTP version 2 for Token Ring VLAN switching to function properly.

- When you enable or disable VTP pruning on a VTP server, VTP pruning for the entire management domain is enabled or disabled.
- The pruning-eligibility configuration applies globally to all trunks on the switch. You cannot configure pruning-eligibility separately for each trunk.
- When you configure VLANs as pruning eligible or pruning ineligible on a Catalyst 6500 series switch, pruning eligibility for those VLANs is affected on that switch only, not on all network devices in the VTP domain.
- If there is insufficient DRAM available for use by VTP, the VTP mode changes to transparent.
- Network devices in VTP transparent mode do not send VTP Join messages. On Catalyst 6500 series switches with trunk connections to network devices in VTP transparent mode, configure the VLANs that are used by the transparent-mode network devices or that need to be carried across trunks as pruning ineligible. For information about configuring prune eligibility, see the “[Configuring the List of Prune-Eligible VLANs](#)” section on page 7-11.

Configuring VTP

These sections describe how to configure VTP:

- [Configuring VTP Global Parameters, page 9-6](#)
- [Configuring the VTP Mode, page 9-9](#)
- [Displaying VTP Statistics, page 9-11](#)

Configuring VTP Global Parameters

These sections describe configuring the VTP global parameters:

- [Configuring a VTP Password, page 9-6](#)
- [Enabling VTP Pruning, page 9-7](#)
- [Enabling VTP Version 2, page 9-7](#)



Note You can enter the VTP global parameters in either global configuration mode or in EXEC mode.

Configuring a VTP Password

To configure the VTP global parameters, perform this task:

Command	Purpose
Router(config)# vtp password <i>password_string</i>	Sets a password, which can be from 8 to 64 characters long, for the VTP domain.
Router(config)# no vtp password	Clears the password.

This example shows one way to configure a VTP password in global configuration mode:

```
Router# configure terminal
Router(config)# vtp password WATER
Setting device VLAN database password to WATER.
Router#
```

This example shows how to configure a VTP password in EXEC mode:

```
Router# vtp password WATER
Setting device VLAN database password to WATER.
Router#
```



Note The password is not stored in the running-config file.

Enabling VTP Pruning

To enable VTP pruning in the management domain, perform this task:

	Command	Purpose
Step 1	Router(config)# vtp pruning	Enables VTP pruning in the management domain.
	Router(config)# no vtp pruning	Disables VTP pruning in the management domain.
Step 2	Router# show vtp status	Verifies the configuration.

This example shows one way to enable VTP pruning in the management domain with Release 12.2(14)SX and later releases:

```
Router# configure terminal
Router(config)# vtp pruning
Pruning switched ON
```

This example shows how to enable VTP pruning in the management domain with any release:

```
Router# vtp pruning
Pruning switched ON
```

This example shows how to verify the configuration:

```
Router# show vtp status | include Pruning
VTP Pruning Mode: Enabled
Router#
```

For information about configuring prune eligibility, see the “[Configuring the List of Prune-Eligible VLANs](#)” section on page 7-11.

Enabling VTP Version 2

VTP version 2 is disabled by default on VTP version 2-capable network devices. When you enable VTP version 2 on a network device, 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.

**Note**

In a Token Ring environment, you must enable VTP version 2 for Token Ring VLAN switching to function properly on devices that support Token Ring interfaces.

To enable VTP version 2, perform this task:

Command	Purpose
Step 1 Router(config)# vtp version {1 2} Router(config)# no vtp version	Enables VTP version 2. Reverts to the default (VTP version 1).
Step 2 Router# show vtp status	Verifies the configuration.

This example shows one way to enable VTP version 2 with Release 12.2(14)SX and later releases:

```
Router# configure terminal
Router(config)# vtp version 2
V2 mode enabled.
Router(config)#

```

This example shows how to enable VTP version 2 with any release:

```
Router# vtp version 2
V2 mode enabled.
Router#

```

This example shows how to verify the configuration:

```
Router# show vtp status | include V2
VTP V2 Mode: Enabled
Router#

```

Configuring the VTP Mode

To configure the VTP mode, perform this task:

Command	Purpose
Step 1 Router(config)# vtp mode {client server transparent} Router(config)# no vtp mode	Configures the VTP mode. Reverts to the default VTP mode (server).
Step 2 Router(config)# vtp domain domain_name	(Optional for server mode) Defines the VTP domain name, which can be up to 32 characters long. VTP server mode requires a domain name. If the switch has a trunk connection to a VTP domain, the switch learns the domain name from the VTP server in the domain. Note You cannot clear the domain name.
Step 3 Router(config)# end	Exits VLAN configuration mode.
Step 4 Router# show vtp status	Verifies the configuration.



Note

When VTP is disabled, you can enter VLAN configuration commands in configuration mode instead of the VLAN database mode and the VLAN configuration is stored in the startup configuration file.

Configuring VTP

This example shows how to configure the switch as a VTP server:

```
Router# configuration terminal
Router(config)# vtp mode server
Setting device to VTP SERVER mode.
Router(config)# vtp domain Lab_Network
Setting VTP domain name to Lab_Network
Router(config)# end
Router#
```

This example shows how to verify the configuration:

```
Router# 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)
Router#
```

This example shows how to configure the switch as a VTP client:

```
Router# configuration terminal
Router(config)# vtp mode client
Setting device to VTP CLIENT mode.
Router(config)# exit
Router#
```

This example shows how to verify the configuration:

```
Router# 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
Router#
```

This example shows how to disable VTP on the switch:

```
Router# configuration terminal
Router(config)# vtp transparent
Setting device to VTP TRANSPARENT mode.
Router(config)# end
Router#
```

This example shows how to verify the configuration:

```
Router# 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
Router#

```

Displaying VTP Statistics

To display VTP statistics, including VTP advertisements sent and received and VTP errors, perform this task:

Command	Purpose
Router# show vtp counters	Displays VTP statistics.

This example shows how to display VTP statistics:

```

Router# 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
                                         non-pruning-capable device
-----
Fa5/8        43071           42766            5

```

■ Configuring VTP



CHAPTER

10

Configuring VLANs

This chapter describes how to configure VLANs on the Catalyst 6500 series switches.



Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication.

This chapter consists of these sections:

- [Understanding How VLANs Work, page 10-1](#)
- [VLAN Default Configuration, page 10-6](#)
- [VLAN Configuration Guidelines and Restrictions, page 10-8](#)
- [Configuring VLANs, page 10-9](#)

Understanding How VLANs Work

The following sections describe how VLANs work:

- [VLAN Overview, page 10-1](#)
- [VLAN Ranges, page 10-2](#)
- [Configurable VLAN Parameters, page 10-3](#)
- [Understanding Token Ring VLANs, page 10-3](#)

VLAN Overview

A VLAN is a group of end stations with a common set of requirements, independent of physical location. VLANs have the same attributes as a physical LAN but allow you to group end stations even if they are not located physically on the same LAN segment.

VLANs are usually associated with IP subnetworks. For example, all the end stations in a particular IP subnet belong to the same VLAN. Traffic between VLANs must be routed. LAN port VLAN membership is assigned manually on a port-by-port basis.

VLAN Ranges



Note You must enable the extended system ID to use 4096 VLANs (see the “[Understanding the Bridge ID](#)” section on page 14-2).

Catalyst 6500 series switches support 4096 VLANs in accordance with the IEEE 802.1Q standard. These VLANs are organized into several ranges; you use each range slightly differently. 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 10-1](#) describes the VLAN ranges.

Table 10-1 VLAN Ranges

VLANs	Range	Usage	Propagated by VTP
0, 4095	Reserved	For system use only. You cannot see or use these VLANs.	—
1	Normal	Cisco default. You can use this VLAN but you cannot delete it.	Yes
2–1001	Normal	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.	No

The following information applies to VLAN ranges:

- Layer 3 LAN ports, WAN interfaces and subinterfaces, and some software features use internal VLANs in the extended range. You cannot use an extended range VLAN that has been allocated for internal use.
- To display the VLANs used internally, enter the **show vlan internal usage** command. With earlier releases, enter the **show vlan internal usage** and **show cwan vlans** commands.
- You can configure ascending internal VLAN allocation (from 1006 and up) or descending internal VLAN allocation (from 4094 and down).
- Switches running the Catalyst operating system 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 software.
- You must enable the extended system ID to use extended range VLANs (see the “[Understanding the Bridge ID](#)” section on page 14-2).

Configurable VLAN Parameters

**Note**

- Ethernet VLAN 1 uses only default values.
- Except for the VLAN name, Ethernet VLANs 1006 through 4094 use only default values.
- You can configure the VLAN name for Ethernet VLANs 1006 through 4094.

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

- VLAN name
- VLAN type (Ethernet, FDDI, FDDI network entity title [NET], TrBRF, or TrCRF)
- VLAN state (active or suspended)
- Security Association Identifier (SAID)
- Bridge identification number for TrBRF VLANs
- Ring number for FDDI and TrCRF VLANs
- Parent VLAN number for TrCRF VLANs
- Spanning Tree Protocol (STP) type for TrCRF VLANs

Understanding Token Ring VLANs

The following section describes the two Token Ring VLAN types supported on network devices running VTP version 2:

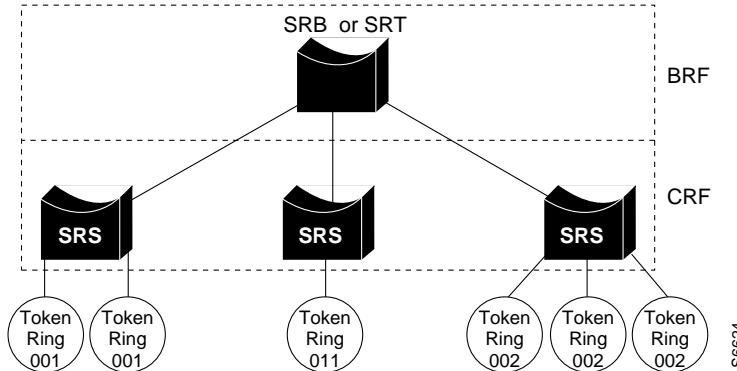
- [Token Ring TrBRF VLANs, page 10-3](#)
- [Token Ring TrCRF VLANs, page 10-4](#)

**Note**

Catalyst 6500 series switches do not support Inter-Switch Link (ISL)-encapsulated Token Ring frames. When a Catalyst 6500 series switch is configured as a VTP server, you can configure Token Ring VLANs from the switch.

Token Ring TrBRF VLANs

Token Ring Bridge Relay Function (TrBRF) VLANs interconnect multiple Token Ring Concentrator Relay Function (TrCRF) VLANs in a switched Token Ring network (see [Figure 10-1](#)). The TrBRF can be extended across a network devices interconnected via trunk links. The connection between the TrCRF and the TrBRF is referred to as a *logical port*.

Figure 10-1 Interconnected Token Ring TrBRF and TrCRF VLANs

For source routing, the Catalyst 6500 series switch appears as a single bridge between the logical rings. The TrBRF can function as a source-route bridge (SRB) or a source-route transparent (SRT) bridge running either the IBM or IEEE STP. If an SRB is used, you can define duplicate MAC addresses on different logical rings.

The Token Ring software runs an instance of STP for each TrBRF VLAN and each TrCRF VLAN. For TrCRF VLANs, STP removes loops in the logical ring. For TrBRF VLANs, STP interacts with external bridges to remove loops from the bridge topology, similar to STP operation on Ethernet VLANs.

**Caution**

Certain parent TrBRF STP and TrCRF bridge mode configurations can place the logical ports (the connection between the TrBRF and the TrCRF) of the TrBRF in a blocked state. For more information, see the “[VLAN Configuration Guidelines and Restrictions](#)” section on page 10-8.

To accommodate IBM System Network Architecture (SNA) traffic, you can use a combination of SRT and SRB modes. In a mixed mode, the TrBRF determines that some ports (logical ports connected to TrCRFs) operate in SRB mode while other ports operate in SRT mode.

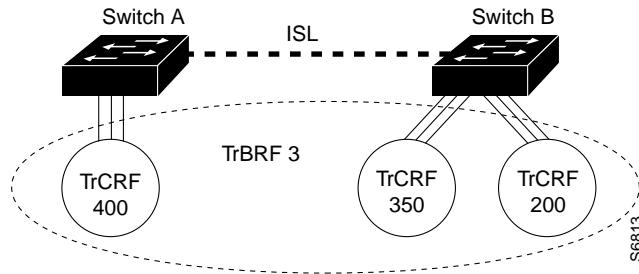
Token Ring TrCRF VLANs

Token Ring Concentrator Relay Function (TrCRF) VLANs define port groups with the same logical ring number. You can configure two types of TrCRFs in your network: undistributed and backup.

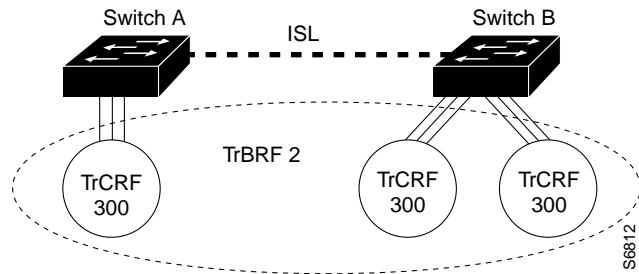
TrCRFs typically are undistributed, which means each TrCRF is limited to the ports on a single network device. Multiple undistributed TrCRFs on the same or separate network devices can be associated with a single parent TrBRF (see [Figure 10-2](#)). The parent TrBRF acts as a multiport bridge, forwarding traffic between the undistributed TrCRFs.

**Note**

To pass data between rings located on separate network devices, you can associate the rings to the same TrBRF and configure the TrBRF for an SRB.

Figure 10-2 Undistributed TrCRFs

By default, Token Ring ports are associated with the default TrCRF (VLAN 1003, `trcrf-default`), which has the default TrBRF (VLAN 1005, `trbrf-default`) as its parent. In this configuration, a distributed TrCRF is possible (see [Figure 10-3](#)), and traffic is passed between the default TrCRFs located on separate network devices if the network devices are connected through an ISL trunk.

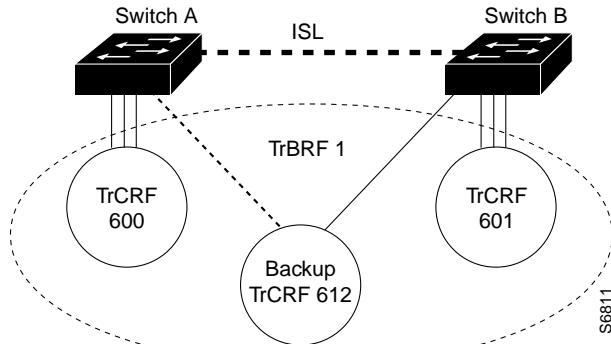
Figure 10-3 Distributed TrCRF

Within a TrCRF, source-route switching forwards frames based on either MAC addresses or route descriptors. The entire VLAN can operate as a single ring, with frames switched between ports within a single TrCRF.

You can specify the maximum hop count for All-Routes and Spanning Tree Explorer frames for each TrCRF. When you specify the maximum hop count, you limit the maximum number of hops an explorer is allowed to traverse. If a port determines that the explorer frame it is receiving has traversed more than the number of hops specified, it does not forward the frame. The TrCRF determines the number of hops an explorer has traversed by the number of bridge hops in the route information field.

If the ISL connection between network devices fails, you can use a backup TrCRF to configure an alternate route for traffic between undistributed TrCRFs. Only one backup TrCRF for a TrBRF is allowed, and only one port per network device can belong to a backup TrCRF.

If the ISL connection between the network devices fails, the port in the backup TrCRF on each affected network device automatically becomes active, rerouting traffic between the undistributed TrCRFs through the backup TrCRF. When the ISL connection is reestablished, all but one port in the backup TrCRF is disabled. [Figure 10-4](#) illustrates the backup TrCRF.

Figure 10-4 Backup TrCRF

VLAN Default Configuration

Tables 10-2 through 10-6 show the default configurations for the different VLAN media types.

Table 10-2 Ethernet VLAN Defaults and Ranges

Parameter	Default	Range
VLAN ID	1	1–4094
VLAN name	“default” for VLAN 1 “VLAN <i>vlan_ID</i> ” for other Ethernet VLANs	—
802.10 SAID	10 <i>vlan_ID</i>	100001–104094
MTU size	1500	1500–18190
Translational bridge 1	0	0–1005
Translational bridge 2	0	0–1005
VLAN state	active	active, suspend
Pruning eligibility	VLANs 2–1001 are pruning eligible; VLANs 1006–4094 are not pruning eligible.	—

Table 10-3 FDDI VLAN Defaults and Ranges

Parameter	Default	Range
VLAN ID	1002	1–1005
VLAN name	“fddi-default”	—
802.10 SAID	101002	1–4294967294
MTU size	1500	1500–18190
Ring number	0	1–4095
Parent VLAN	0	0–1005
Translational bridge 1	0	0–1005

Table 10-3 FDDI VLAN Defaults and Ranges (continued)

Parameter	Default	Range
Translational bridge 2	0	0–1005
VLAN state	active	active, suspend

Table 10-4 Token Ring (TrCRF) VLAN Defaults and Ranges

Parameter	Default	Range
VLAN ID	1003	1–1005
VLAN name	“token-ring-default”	—
802.10 SAID	101003	1–4294967294
Ring Number	0	1–4095
MTU size	VTPv1 default 1500 VTPv2 default 4472	1500–18190
Translational bridge 1	0	0–1005
Translational bridge 2	0	0–1005
VLAN state	active	active, suspend
Bridge mode	srb	srb, srt
ARE max hops	7	0–13
STE max hops	7	0–13
Backup CRF	disabled	disable; enable

Table 10-5 FDDI-Net VLAN Defaults and Ranges

Parameter	Default	Range
VLAN ID	1004	1–1005
VLAN name	“fddinet-default”	—
802.10 SAID	101004	1–4294967294
MTU size	1500	1500–18190
Bridge number	1	0–15
STP type	ieee	auto, ibm, ieee
VLAN state	active	active, suspend

Table 10-6 Token Ring (TrBRF) VLAN Defaults and Ranges

Parameter	Default	Range
VLAN ID	1005	1–1005
VLAN name	“trnet-default”	—
802.10 SAID	101005	1–4294967294

Table 10-6 Token Ring (TrBRF) VLAN Defaults and Ranges (continued)

Parameter	Default	Range
MTU size	VTPv1 1500; VTPv2 4472	1500–18190
Bridge number	1	0–15
STP type	ibm	auto, ibm, ieee
VLAN state	active	active, suspend

VLAN Configuration Guidelines and Restrictions

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

- Supervisor engine redundancy does not support nondefault VLAN data file names or locations. Do not enter the **vtp file file_name** command on a switch that has a redundant supervisor engine.
- Before installing a redundant supervisor engine, enter the **no vtp file** command to return to the default configuration.
- RPR+ redundancy (see [Chapter 6, “Configuring RPR and RPR+ Supervisor Engine Redundancy”](#)) does not support a configuration entered in VLAN database mode. Use global configuration mode with RPR+ redundancy.
- You can configure extended-range VLANs only in global configuration mode. You cannot configure extended-range VLANs in VLAN database mode. See the [“VLAN Configuration Options” section on page 10-9](#).
- Before you can create a VLAN, the Catalyst 6500 series switch must be in VTP server mode or VTP transparent mode. For information on configuring VTP, see [Chapter 9, “Configuring VTP.”](#)
- 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 this guide and in the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication.
- To do a complete backup of your configuration, include the *vlan.dat* file in the backup.
- The Cisco IOS **end** command is not supported in VLAN database mode.
- You cannot enter **Ctrl-Z** to exit VLAN database mode.
- Catalyst 6500 series switches do not support Token Ring or FDDI media. The switch does not forward FDDI, FDDI-Net, TrCRF, or TrBRF traffic, but it can propagate the VLAN configuration through VTP.
- When a Catalyst 6500 series switch is configured as a VTP server, you can configure FDDI and Token Ring VLANs from the switch.
- You must configure a TrBRF before you configure the TrCRF (the parent TrBRF VLAN you specify must exist).
- In a Token Ring environment, the logical interfaces (the connection between the TrBRF and the TrCRF) of the TrBRF are placed in a blocked state if either of these conditions exists:
 - The TrBRF is running the IBM STP, and the TrCRF is in SRT mode.
 - The TrBRF is running the IEEE STP, and the TrCRF is in SRB mode.

Configuring VLANs

These sections describe how to configure VLANs:

- [VLAN Configuration Options, page 10-9](#)
- [Creating or Modifying an Ethernet VLAN, page 10-10](#)
- [Assigning a Layer 2 LAN Interface to a VLAN, page 10-12](#)
- [Configuring the Internal VLAN Allocation Policy, page 10-12](#)
- [Mapping 802.1Q VLANs to ISL VLANs, page 10-12](#)

**Note**

VLANs support a number of parameters that are not discussed in detail in this section. For complete information, refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication.

VLAN Configuration Options

These sections describe the VLAN configuration options:

- [VLAN Configuration in Global Configuration Mode, page 10-9](#)
- [VLAN Configuration in VLAN Database Mode, page 10-9](#)

VLAN Configuration in Global Configuration Mode

If the switch is in VTP server or transparent mode (see the “[Configuring VTP](#)” section on page 9-6), you can configure VLANs in global and config-vlan configuration modes. When you configure VLANs in global and config-vlan configuration modes, the VLAN configuration is saved in the vlan.dat 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, use the **show running-config** and **show startup-config** commands to 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 can configure extended-range VLANs only in global configuration mode. You cannot configure extended-range VLANs in VLAN database mode.

VLAN Configuration in VLAN Database Mode

**Note**

You cannot configure extended-range VLANs in VLAN database mode. You can configure extended-range VLANs only in global configuration mode. RPR+ redundancy does not support configuration entered in VLAN database mode. Use global configuration mode with RPR+ redundancy.

If 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` files. To display the VLAN configuration, enter the **show vlan** command.

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 file by entering the **show running-config** command.

Creating or Modifying an Ethernet VLAN

User-configured VLANs have unique IDs from 1 to 4094, except for reserved VLANs (see [Table 10-1 on page 10-2](#)). Enter the **vlan** command with an unused ID to create a VLAN. Enter the **vlan** command for an existing VLAN to modify the VLAN (you cannot modify an existing VLAN that is being used by a Layer 3 port or a software feature).

See the “[VLAN Default Configuration](#)” section on page 10-6 for the list of default parameters that are assigned when you create a VLAN. If you do not specify the VLAN type with the **media** keyword, the VLAN is an Ethernet VLAN.

To create or modify a VLAN, perform this task:

	Command	Purpose
Step 1	Router# configure terminal OR Router# vlan database	Enters VLAN configuration mode.
Step 2	Router(config)# vlan <code>vlan_ID{ [-vlan_ID] [,vlan_ID]}</code> Router(config-vlan)# OR Router(vlan)# vlan <code>vlan_ID</code> Router(config)# no vlan <code>vlan_ID</code> Router(config-vlan)# OR Router(vlan)# no vlan <code>vlan_ID</code>	Creates or modifies an Ethernet VLAN, a range of Ethernet VLANs, or several Ethernet VLANs specified in a comma-separated list (do not enter space characters). Deletes a VLAN.
Step 3	Router(config-vlan)# end OR Router(vlan)# exit	Updates the VLAN database and returns to privileged EXEC mode.
Step 4	Router# show vlan [id name] vlan	Verifies the VLAN configuration.

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

- RPR+ redundancy does not support a configuration entered in VLAN database mode. Use global configuration mode with RPR+ redundancy.
- Because Layer 3 ports and some software features require internal VLANs allocated from 1006 and up, configure extended-range VLANs starting with 4094.
- 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.

When deleting VLANs, note the following syntax information:

- You cannot delete the default VLANs for the different media types: Ethernet VLAN 1 and FDDI or Token Ring VLANs 1002 to 1005.
- When you delete a VLAN, any LAN ports configured as access ports assigned to that VLAN become inactive. The ports remain associated with the VLAN (and inactive) until you assign them to a new VLAN.

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

```
Router# configure terminal
Router(config)# vlan 3
Router(config-vlan)# end
Router# 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
---- -----    -----           -----

```

This example shows how to create an Ethernet VLAN in VLAN database mode:

```
Router# vlan database
Router(vlan)# vlan 3
VLAN 3 added:
  Name: VLAN0003
Router(vlan)# exit
APPLY completed.
Exiting....
```

This example shows how to verify the configuration:

```
Router# 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
Router#
```

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 ports to the VLAN.



Note Make sure you assign LAN ports to a VLAN of the appropriate type. Assign Ethernet ports to Ethernet-type VLANs.

To assign one or more LAN ports to a VLAN, complete the procedures in the “[Configuring LAN Interfaces for Layer 2 Switching](#)” section on page 7-6.

Configuring the Internal VLAN Allocation Policy

For more information about VLAN allocation, see the “[VLAN Ranges](#)” section on page 10-2.



Note The internal VLAN allocation policy is applied only following a reload.

To configure the internal VLAN allocation policy, perform this task:

Command	Purpose
Step 1 Router(config)# vlan internal allocation policy {ascending descending}	Configures the internal VLAN allocation policy.
	Returns to the default (ascending).
Step 2 Router(config)# end	Exits configuration mode.
Step 3 Router# reload	Applies the new internal VLAN allocation policy.
	<p>Caution You do not need to enter the reload command immediately. Enter the reload command during a planned maintenance window.</p>

When you configure the internal VLAN allocation policy, note the following syntax information:

- Enter the **ascending** keyword to allocate internal VLANs from 1006 and up.
- Enter the **descending** keyword to allocate internal VLAN from 4094 and down.

This example shows how to configure descending as the internal VLAN allocation policy:

```
Router# configure terminal
Router(config)# vlan internal allocation policy descending
```

Mapping 802.1Q VLANs to ISL VLANs

The valid range of user-configurable ISL VLANs is 1 through 1001 and 1006 through 4094. The valid range of VLANs specified in the IEEE 802.1Q standard is 1 to 4094. You can map 802.1Q VLAN numbers to ISL VLAN numbers.

802.1Q VLANs in the range 1 through 1001 and 1006 through 4094 are automatically mapped to the corresponding ISL VLAN. 802.1Q VLAN numbers corresponding to reserved VLAN numbers must be mapped to an ISL VLAN in order to be recognized and forwarded by Cisco network devices.

These restrictions apply when mapping 802.1Q VLANs to ISL VLANs:

- You can configure up to eight 802.1Q-to-ISL VLAN mappings on the Catalyst 6500 series switch.
- You can only map 802.1Q VLANs to Ethernet-type ISL VLANs.
- Do not enter the native VLAN of any 802.1Q trunk in the mapping table.
- When you map an 802.1Q VLAN to an ISL VLAN, traffic on the 802.1Q VLAN corresponding to the mapped ISL VLAN is blocked. For example, if you map 802.1Q VLAN 1007 to ISL VLAN 200, traffic on 802.1Q VLAN 200 is blocked.
- VLAN mappings are local to each Catalyst 6500 series switch. Make sure you configure the same VLAN mappings on all appropriate network devices.

To map an 802.1Q VLAN to an ISL VLAN, perform this task:

Command	Purpose
Step 1 Router(config)# vlan mapping dot1q dot1q_vlan isl_isl_vlan	Maps an 802.1Q VLAN to an ISL Ethernet VLAN. The valid range for <i>dot1q_vlan</i> is 1001 to 4094. The valid range for <i>isl_vlan</i> is the same.
	Router(config)# no vlan mapping dot1q {all dot1q_vlan}
Step 2 Router(config)# end	Exits configuration mode.
Step 3 Router# show vlan	Verifies the VLAN mapping.

This example shows how to map 802.1Q VLAN 1003 to ISL VLAN 200:

```
Router# configure terminal
Router(config)# vlan mapping dot1q 1003 isl 200
Router(config)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show vlan
<...output truncated...>
802.1Q Trunk Remapped VLANs:
802.1Q VLAN      ISL VLAN
-----  -----
          1003        200
```

■ Configuring VLANs



Configuring Private VLANs

This chapter describes how to configure private VLANs on the Catalyst 6500 series switches.

**Note**

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication.

This chapter consists of these sections:

- [Understanding How Private VLANs Work, page 11-1](#)
- [Private VLAN Configuration Guidelines, page 11-2](#)
- [Configuring Private VLANs, page 11-4](#)

Understanding How Private VLANs Work

**Note**

To configure private VLANs, the switch must be in VTP transparent mode.

Private VLANs provide Layer 2 isolation between ports within the same private VLAN. There are three types of private VLAN ports:

- Promiscuous—A promiscuous port can communicate with all interfaces, including the community and isolated ports within a private VLAN.
- Isolated—An isolated port has complete Layer 2 separation from other ports within the same private VLAN except for the promiscuous port. Private VLANs block all traffic to isolated ports except traffic from promiscuous ports. Traffic received from an isolated port is forwarded only to promiscuous ports.
- Community—Community ports communicate among themselves and with their promiscuous ports. These interfaces are isolated at Layer 2 from all other interfaces in other communities or isolated ports within their private VLAN.

**Note**

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.

■ Private VLAN Configuration Guidelines

Private VLAN ports are associated with a set of supporting VLANs that are used to create the private VLAN structure. A private VLAN uses VLANs three ways:

- Primary VLAN—Carries traffic from promiscuous ports to isolated, community, and other promiscuous ports.
- Isolated VLAN—Carries traffic from isolated ports to promiscuous ports.
- Community VLAN—Carries traffic between community ports and to promiscuous ports. You can configure multiple community VLANs in a private VLAN.



Note Isolated and community VLANs are both called secondary VLANs.

You can extend private VLANs across multiple devices by trunking the primary, isolated, and community VLANs to other devices that support private VLANs.

In a switched environment, you can assign an individual private VLAN and associated IP subnet to each individual or common group of end stations. The end stations only need to communicate with a default gateway to gain access outside the private VLAN. With end stations in a private VLAN, you can do the following:

- Designate selected ports connected to end stations (for example, interfaces connected to servers) as isolated to prevent any communication at Layer 2. (For example, if the end stations were servers, this configuration would prevent 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 to allow all end stations access.
- Reduce VLAN and IP subnet consumption by preventing traffic between end stations even though they are in the same VLAN and IP subnet.

A promiscuous port can serve only one primary VLAN.

A promiscuous port can serve as many isolated or community VLANs as desired.

With a promiscuous port, you can connect a wide range of devices as “access points” to a private VLAN. For example, you can connect a promiscuous port to the “server port” of LocalDirector to connect an isolated VLAN or a number of community VLANs to the server so that 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 private VLAN servers from an administration workstation.

Private VLAN Configuration Guidelines

Follow these guidelines to configure private VLANs:

- Set VTP to transparent mode. After you configure a private VLAN, you cannot change the VTP mode to client or server. See [Chapter 9, “Configuring VTP.”](#)
- You cannot include VLAN 1 or VLANs 1002 to 1005 in the private VLAN configuration.
- Use only the private VLAN configuration commands to assign ports to primary, isolated, or community VLANs. Layer 2 access ports assigned to the VLANs that you configure as primary, isolated, or community VLANs are inactive while the VLAN is part of the private VLAN configuration. Layer 2 trunk interfaces remain in the STP forwarding state.
- Configure Layer 3 VLAN interfaces only for primary VLANs. Layer 3 VLAN interfaces for isolated and community VLANs are inactive while the VLAN is configured as an isolated or community VLAN.

- Do not configure private VLAN ports as EtherChannels. While a port is part of the private VLAN configuration, any EtherChannel configuration for it is inactive.
- Destination SPAN configuration supersedes private VLAN configuration. While a port is a destination SPAN port, any private VLAN configuration for it is inactive.
- Private VLANs support the following SPAN features:
 - You can configure a private VLAN port as a SPAN source port.
 - 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.

For more information about SPAN, see [Chapter 33, “Configuring Local SPAN and RSPAN.”](#)

- A primary VLAN can have one isolated VLAN and multiple community VLANs associated with it.
- An isolated or community VLAN can have only one primary VLAN associated with it.
- Enable PortFast and BPDU guard on isolated and community ports to prevent STP loops due to misconfigurations and to speed up STP convergence (see [Chapter 15, “Configuring Optional STP Features”](#)). When enabled, STP applies the BPDU guard feature to all PortFast-configured Layer 2 LAN ports.
- If you delete a VLAN used in the private VLAN configuration, the private VLAN ports associated with the VLAN become inactive.
- For Ethernet 10 Mb, 10/100 Mb, and 100 Mb modules, within groups of 12 ports (1–12, 13–24, 25–36, and 37–48), do not configure ports as isolated or community VLAN ports when one port within the 12 ports is a trunk or a SPAN destination or a promiscuous private VLAN port. While one port within the 12 ports is a trunk or a SPAN destination or a promiscuous private VLAN port, any isolated or community VLAN configuration for other ports within the 12 ports is inactive. To reactivate the ports, remove the isolated or community VLAN port configuration and enter **shutdown** and **no shutdown** commands.
- Private VLAN ports can be on different network devices as long as the devices are trunk connected and the primary and secondary VLANs have not been removed from the trunk.
- VTP does not support private VLANs. You must configure private VLANs on each device where you want private VLAN ports.
- To maintain the security of your private VLAN configuration and avoid other use of the VLANs configured as private VLANs, configure private VLANs on all intermediate devices, including devices that have no private VLAN ports.
- We recommend that you prune the private VLANs from the trunks on devices that carry no traffic in the private VLANs.
- In networks with some devices using MAC address reduction, and others not using MAC address reduction, STP parameters do not necessarily propagate to ensure that the spanning tree topologies match. You should manually check the STP configuration to ensure that the primary, isolated, and community VLANs’ spanning tree topologies match.
- If you enable MAC address reduction on the switch, we recommend that you enable MAC address reduction on all the devices in your network to ensure that the STP topologies of the private VLANs match.
- In a network where private VLANs are configured, if you enable MAC address reduction on some devices and disable it on others (mixed environment), use the default bridge priorities to make sure that the root bridge is common to the primary VLAN and to all its associated isolated and community VLANs. Be consistent with the ranges employed by the MAC address reduction feature regardless of whether it is enabled on the system. MAC address reduction allows only discrete levels

and uses all intermediate values internally as a range. You should disable a root bridge with private VLANs and MAC address reduction, and configure the root bridge with any priority higher than the highest priority range used by any nonroot bridge.

- You can apply different quality of service (QoS) configuration to primary, isolated, and community VLANs (see Chapter 24, “Configuring PFC QoS”).
- You cannot apply VACLs to secondary VLANs (see the Chapter 23, “Configuring VLAN ACLs”).
- To apply Cisco IOS output ACLs to all outgoing private VLAN traffic, configure them on the Layer 3 VLAN interface of the primary VLAN (see Chapter 21, “Configuring Network Security”).
- Cisco IOS ACLs applied to the Layer 3 VLAN interface of a primary VLAN automatically apply to the associated isolated and community VLANs.
- 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 private VLAN 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 are part of the private VLAN configuration.
- ARP entries learned on Layer 3 private VLAN interfaces are sticky ARP entries (we recommend that you display and verify private VLAN interface ARP entries).
- For security reasons, private VLAN port sticky ARP entries do not age out. Connecting a device with a different MAC address but with the same IP address generates a message and the ARP entry is not created.
- Because the private VLAN port sticky ARP entries do not age out, you must manually remove private VLAN port ARP entries if a MAC address changes. You can add or remove private VLAN ARP entries manually as follows:

```
Router(config)# no arp 11.1.3.30
IP ARP:Deleting Sticky ARP entry 11.1.3.30

Router(config)# arp 11.1.3.30 0000.5403.2356 arpa
IP ARP:Overwriting Sticky ARP entry 11.1.3.30, hw:00d0.bb09.266e by hw:0000.5403.2356
```

Configuring Private VLANs

These sections describe how to configure private VLANs:

- [Configuring a VLAN as a Private VLAN, page 11-5](#)
- [Associating Secondary VLANs with a Primary VLAN, page 11-6](#)
- [Mapping Secondary VLANs to the Layer 3 VLAN Interface of a Primary VLAN, page 11-7](#)
- [Configuring a Layer 2 Interface as a Private VLAN Host Port, page 11-8](#)
- [Configuring a Layer 2 Interface as a Private VLAN Promiscuous Port, page 11-9](#)



Note If the VLAN is not defined already, the private VLAN configuration process defines it.

Configuring a VLAN as a Private VLAN

To configure a VLAN as a private VLAN, perform this task:

Command	Purpose
Step 1 Router(config)# vlan <i>vlan_ID</i>	Enters VLAN configuration submode.
Step 2 Router(config-vlan)# private-vlan { community isolated primary }	Configures a VLAN as a private VLAN.
Router(config-vlan)# no private-vlan { community isolated primary }	Clears the private VLAN configuration. Note These commands do not take effect until you exit VLAN configuration submode.
Step 3 Router(config-vlan)# end	Exits configuration mode.
Step 4 Router# show vlan private-vlan [<i>type</i>]	Verifies the configuration.

This example shows how to configure VLAN 202 as a primary VLAN and verify the configuration:

```
Router# configure terminal
Router(config)# vlan 202
Router(config-vlan)# private-vlan primary
Router(config-vlan)# end
Router# show vlan private-vlan
```

Primary	Secondary	Type	Interfaces
202		primary	

This example shows how to configure VLAN 303 as a community VLAN and verify the configuration:

```
Router# configure terminal
Router(config)# vlan 303
Router(config-vlan)# private-vlan community
Router(config-vlan)# end
Router# show vlan private-vlan
```

Primary	Secondary	Type	Interfaces
202	303	primary	
		community	

This example shows how to configure VLAN 440 as an isolated VLAN and verify the configuration:

```
Router# configure terminal
Router(config)# vlan 440
Router(config-vlan)# private-vlan isolated
Router(config-vlan)# end
Router# show vlan private-vlan
```

Primary	Secondary	Type	Interfaces
202	303	primary	
		community	
440		isolated	

Associating Secondary VLANs with a Primary VLAN

To associate secondary VLANs with a primary VLAN, perform this task:

Command	Purpose
Step 1 Router(config)# vlan primary_vlan_ID	Enters VLAN configuration submode for the primary VLAN.
Step 2 Router(config-vlan)# private-vlan association {secondary_vlan_list add secondary_vlan_list remove secondary_vlan_list}	Associates the secondary VLANs with the primary VLAN. Clears all secondary VLAN associations.
Router(config-vlan)# no private-vlan association	
Step 3 Router(config-vlan)# end	Exits VLAN configuration mode.
Step 4 Router# show vlan private-vlan [type]	Verifies the configuration.

When you associate secondary VLANs with a primary VLAN, note the following syntax information:

- The *secondary_vlan_list* parameter cannot contain spaces. It can contain multiple comma-separated items. Each item can be a single private VLAN ID or a hyphenated range of private VLAN IDs.
- The *secondary_vlan_list* parameter can contain multiple community VLAN IDs.
- The *secondary_vlan_list* parameter can contain only one isolated VLAN ID.
- Enter a *secondary_vlan_list* or use the **add** keyword with a *secondary_vlan_list* to associate secondary VLANs with a primary VLAN.
- Use the **remove** keyword with a *secondary_vlan_list* to clear the association between secondary VLANs and a primary VLAN.
- The command does not take effect until you exit VLAN configuration submode.

This example shows how to associate community VLANs 303 through 307 and 309 and isolated VLAN 440 with primary VLAN 202 and verify the configuration:

```
Router# configure terminal
Router(config)# vlan 202
Router(config-vlan)# private-vlan association 303-307,309,440
Router(config-vlan)# end
Router# show vlan private-vlan
```

Primary	Secondary	Type	Interfaces
202	303	community	
202	304	community	
202	305	community	
202	306	community	
202	307	community	
202	309	community	
202	440	isolated	
	308	community	

Mapping Secondary VLANs to the Layer 3 VLAN Interface of a Primary VLAN



Note Isolated and community VLANs are both called secondary VLANs.

To map secondary VLANs to the Layer 3 VLAN interface of a primary VLAN to allow Layer 3 switching of private VLAN ingress traffic, perform this task:

Command	Purpose
Step 1 Router(config)# interface vlan <i>primary_vlan_ID</i>	Enters interface configuration mode for the primary VLAN.
Step 2 Router(config-if)# private-vlan mapping {<i>secondary_vlan_list</i> add <i>secondary_vlan_list</i> remove <i>secondary_vlan_list</i>}	Maps the secondary VLANs to the Layer 3 VLAN interface of a primary VLAN to allow Layer 3 switching of private VLAN ingress traffic.
Router(config-if)# [no] private-vlan mapping	Clears the mapping between the secondary VLANs and the primary VLAN.
Step 3 Router(config-if)# end	Exits configuration mode.
Step 4 Router# show interface private-vlan mapping	Verifies the configuration.

When you map secondary VLANs to the Layer 3 VLAN interface of a primary VLAN, note the following syntax information:

- The **private-vlan mapping** interface configuration command only affects private VLAN ingress traffic that is Layer 3 switched.
- The *secondary_vlan_list* parameter cannot contain spaces. It can contain multiple comma-separated items. Each item can be a single private VLAN ID or a hyphenated range of private VLAN IDs.
- Enter a *secondary_vlan_list* parameter or use the **add** keyword with a *secondary_vlan_list* parameter to map the secondary VLANs to the primary VLAN.
- Use the **remove** keyword with a *secondary_vlan_list* parameter to clear the mapping between secondary VLANs and the primary VLAN.

This example shows how to permit routing of secondary VLAN ingress traffic from private VLANs 303 through 307, 309, and 440 and verify the configuration:

```
Router# configure terminal
Router(config)# interface vlan 202
Router(config-if)# private-vlan mapping add 303-307,309,440
Router(config-if)# end
Router# show interfaces private-vlan mapping
Interface Secondary VLAN Type
-----
vlan202    303        community
vlan202    304        community
vlan202    305        community
vlan202    306        community
vlan202    307        community
vlan202    309        community
vlan202    440        isolated

Router#
```

Configuring a Layer 2 Interface as a Private VLAN Host Port

To configure a Layer 2 interface as a private VLAN host port, perform this task:

Command	Purpose
Step 1 Router(config)# interface type¹ slot/port	Selects the LAN port to configure.
Step 2 Router(config-if)# switchport	Configures the LAN port for Layer 2 switching: <ul style="list-style-type: none"> You must enter the switchport command once without any keywords to configure the LAN port as a Layer 2 interface before you can enter additional switchport commands with keywords. Required only if you have not entered the switchport command already for the interface.
Step 3 Router(config-if)# switchport mode private-vlan {host promiscuous} Router(config-if)# no switchport mode private-vlan	Configures the Layer 2 port as a private VLAN host port. Clears private VLAN port configuration.
Step 4 Router(config-if)# switchport private-vlan host-association primary_vlan_ID secondary_vlan_ID Router(config-if)# no switchport private-vlan host-association	Associates the Layer 2 port with a private VLAN. Clears the association.
Step 5 Router(config-if)# end	Exits configuration mode.
Step 6 Router# show interfaces [type¹ slot/port] switchport	Verifies the configuration.

1. *type* = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

This example shows how to configure interface FastEthernet 5/1 as a private VLAN host port and verify the configuration:

```

Router# configure terminal
Router(config)# interface fastethernet 5/1
Router(config-if)# switchport mode private-vlan host
Router(config-if)# switchport private-vlan host-association 202 303
Router(config-if)# end
Router# show interfaces fastethernet 5/1 switchport
Name: Fa5/1
Switchport: Enabled
→ Administrative Mode: private-vlan host
  Operational Mode: down
  Administrative Trunking Encapsulation: negotiate
  Negotiation of Trunking: On
  Access Mode VLAN: 1 (default)
  Trunking Native Mode VLAN: 1 (default)
→ Administrative private-vlan host-association: 202 (VLAN0202) 303 (VLAN0303)
  Administrative private-vlan mapping: none
→ Operational private-vlan: none
  Trunking VLANs Enabled: ALL
  Pruning VLANs Enabled: 2-1001
  Capture Mode Disabled

```

Configuring a Layer 2 Interface as a Private VLAN Promiscuous Port

To configure a Layer 2 interface as a private VLAN promiscuous port, perform this task:

Command	Purpose
Step 1 Router(config)# interface type¹ slot/port	Selects the LAN interface to configure.
Step 2 Router(config-if)# switchport	Configures the LAN interface for Layer 2 switching: <ul style="list-style-type: none"> You must enter the switchport command once without any keywords to configure the LAN interface as a Layer 2 interface before you can enter additional switchport commands with keywords. Required only if you have not entered the switchport command already for the interface.
Step 3 Router(config-if)# switchport mode private-vlan {host promiscuous} Router(config-if)# no switchport mode private-vlan	Configures the Layer 2 port as a private VLAN promiscuous port. Clears the private VLAN port configuration.
Step 4 Router(config-if)# switchport private-vlan mapping primary_vlan_ID {secondary_vlan_list add secondary_vlan_list remove secondary_vlan_list} Router(config-if)# no switchport private-vlan mapping	Maps the private VLAN promiscuous port to a primary VLAN and to selected secondary VLANs. Clears all mapping between the private VLAN promiscuous port and the primary VLAN and any secondary VLANs.
Step 5 Router(config-if)# end	Exits configuration mode.
Step 6 Router# show interfaces [type¹ slot/port] switchport	Verifies the configuration.

1. *type* = **ethernet**, **fastethernet**, **gigabitetherent**, or **tengigabitetherent**

When you configure a Layer 2 interface as a private VLAN promiscuous port, note the following syntax information:

- The *secondary_vlan_list* parameter cannot contain spaces. It can contain multiple comma-separated items. Each item can be a single private VLAN ID or a hyphenated range of private VLAN IDs.
- Enter a *secondary_vlan_list* value or use the **add** keyword with a *secondary_vlan_list* value to map the secondary VLANs to the private VLAN promiscuous port.
- Use the **remove** keyword with a *secondary_vlan_list* value to clear the mapping between secondary VLANs and the private VLAN promiscuous port.

This example shows how to configure interface FastEthernet 5/2 as a private VLAN promiscuous port and map it to a private VLAN:

```
Router# configure terminal
Router(config)# interface fastethernet 5/2
Router(config-if)# switchport mode private-vlan promiscuous
Router(config-if)# switchport private-vlan mapping 202 303,440
Router(config-if)# end
```

This example shows how to verify the configuration:

```
Router# show interfaces fastethernet 5/2 switchport
Name: Fa5/2
Switchport: Enabled
→ Administrative Mode: private-vlan promiscuous
Operational Mode: down
Administrative Trunking Encapsulation: negotiate
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative private-vlan host-association: none ((Inactive))
→ Administrative private-vlan mapping: 202 (VLAN0202) 303 (VLAN0303) 440 (VLAN0440)
→ Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
```



CHAPTER

12

Configuring Cisco IP Phone Support

This chapter describes how to configure support for Cisco IP Phones on the Catalyst 6500 series switches.



Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication for this release.

This chapter consists of these sections:

- [Understanding Cisco IP Phone Support, page 12-1](#)
- [Default Cisco IP Phone Support Configuration, page 12-4](#)
- [Cisco IP Phone Support Configuration Guidelines and Restrictions, page 12-4](#)
- [Configuring Cisco IP Phone Support, page 12-5](#)

Understanding Cisco IP Phone Support

These sections describe Cisco IP Phone support:

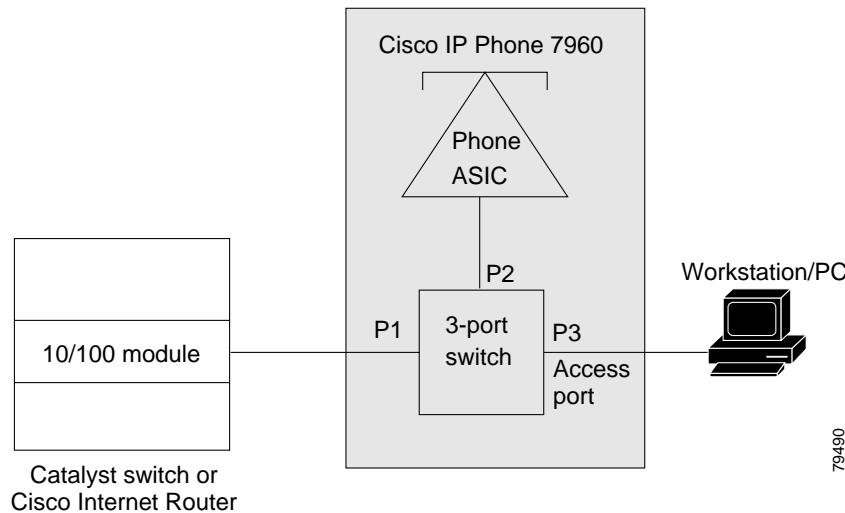
- [Cisco IP Phone Connections, page 12-1](#)
- [Cisco IP Phone Voice Traffic, page 12-2](#)
- [Cisco IP Phone Data Traffic, page 12-3](#)
- [Cisco IP Phone Power Configurations, page 12-3](#)

Cisco IP Phone Connections

The Cisco IP Phone contains an integrated 3-port 10/100 switch. The ports are dedicated connections to these devices:

- Port 1 connects to the switch.
- Port 2 is an internal 10/100 interface that carries the Cisco IP Phone traffic.
- Port 3 connects to a PC or other device.

[Figure 12-1](#) shows a Cisco IP Phone connected between a switch and a PC.

Figure 12-1 Cisco IP Phone Connected to a Switch

79490

Cisco IP Phone Voice Traffic

The Cisco IP Phone transmits voice traffic with Layer 3 IP precedence and Layer 2 CoS values, which are both set to 5 by default. The sound quality of a Cisco IP Phone call can deteriorate if the voice traffic is transmitted unevenly. To provide more predictable voice traffic flow, you can configure QoS to trust the Layer 3 IP precedence or Layer 2 CoS value in the voice traffic (refer to [Chapter 24, “Configuring PFC QoS”](#)).



Note You can configure the ports on WS-X6548-RJ-45 and WS-X6548-RJ-21 switching modules to trust received Layer 2 CoS values (QoS port architecture 1p1q0t/1p3q1t). The WS-X6548-RJ-45 and WS-X6548-RJ-21 switching modules cannot supply power to Cisco IP Phones. Configure QoS policies that use the Layer 3 IP precedence value on other switching modules.

You can configure a Layer 2 access port with an attached Cisco IP Phone to use one VLAN for voice traffic and another VLAN for data traffic from a device attached to the Cisco IP Phone.

You can configure Layer 2 access ports on the switch to send Cisco Discovery Protocol (CDP) packets that instruct an attached Cisco IP Phone to transmit voice traffic to the switch in any of the following ways:

- In the voice VLAN, tagged with a Layer 2 CoS priority value
- In the access VLAN, tagged with a Layer 2 CoS priority value
- In the access VLAN, untagged (no Layer 2 CoS priority value)



Note In all configurations, the voice traffic carries a Layer 3 IP precedence value (the default is 5 for voice traffic and 3 for voice control traffic).

You cannot use Cisco IOS software commands to configure the frame type used by data traffic sent from a device attached to the access port on the Cisco IP Phone.

Cisco IP Phone Data Traffic

**Note**

Untagged traffic from the device attached to the Cisco IP Phone passes through the Cisco IP Phone unchanged, regardless of the trust state of the access port on the Cisco IP Phone.

To process tagged data traffic (traffic in 802.1Q or 802.1p frame types) from the device attached to the access port on the Cisco IP Phone (see [Figure 12-1](#)), you can configure Layer 2 access ports on the switch to send CDP packets that instruct an attached Cisco IP Phone to configure the access port on the Cisco IP Phone to either of these two modes:

- Trusted mode—All traffic received through the access port on the Cisco IP Phone passes through the Cisco IP Phone unchanged.
- Untrusted mode—All traffic in 802.1Q or 802.1p frames received through the access port on the Cisco IP Phone is marked with a configured Layer 2 CoS value. The default Layer 2 CoS value is 0. Untrusted mode is the default.

Cisco IP Phone Power Configurations

These sections describe Cisco IP Phone power configurations:

- [Locally Powered Cisco IP Phones, page 12-3](#)
- [Inline-Powered Cisco IP Phones, page 12-3](#)

Locally Powered Cisco IP Phones

There are two varieties of local power:

- From a power supply connected to the Cisco IP Phone
- From a power supply through a patch panel over the twisted-pair Ethernet cable to the Cisco IP Phone

When a locally powered Cisco IP Phone is present on a switching module port, the switching module cannot detect its presence. The supervisor engine discovers the Cisco IP Phone through CDP messaging with the Cisco IP Phone.

If a locally powered Cisco IP Phone loses local power and the mode is set to **auto**, the switching module discovers the Cisco IP Phone and informs the supervisor engine, which then supplies inline power to the Cisco IP Phone.

Inline-Powered Cisco IP Phones

Inline power is from switching modules that support an inline power daughter card. Inline power is sent over the twisted-pair Ethernet cable to the Cisco IP Phone.

**Note**

For information about switching modules that support inline power, refer to the *Release Notes for Cisco IOS Release 12.2(14)SX on the Catalyst 6000 and Cisco 7600 Supervisor Engine and MSFC* publication at this URL:
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/ol_4164.htm

■ Default Cisco IP Phone Support Configuration

When a switching module port detects an unpowered Cisco IP Phone, the switching module reports to the supervisor engine that an unpowered Cisco IP Phone is present and on which module and port. If the port is configured in **auto** mode, the supervisor engine determines if there is enough system power available to power up the Cisco IP Phone. If there is sufficient power available, the supervisor engine removes the default-allocated power required by a Cisco IP Phone from the total available system power and sends a message to the switching module instructing it to provide power to the port. If there is not enough available power for the Cisco IP Phone, the supervisor engine sends a message to the switching module indicating that power is denied to the port.

Cisco IP Phones may have different power requirements. The supervisor engine initially allocates the configured default of 7 W (167 mA at 42 V) to the Cisco IP Phone. When the correct amount of power is determined from the CDP messaging with the Cisco IP Phone, the supervisor engine reduces or increases the allocated power.

For example, the default allocated power is 7 W. A Cisco IP Phone requiring 6.3 W is plugged into a port. The supervisor engine allocates 7 W for the Cisco IP Phone and powers it up. Once the Cisco IP Phone is operational, it sends a CDP message with the actual power requirement to the supervisor engine. The supervisor engine then decreases the allocated power to the required amount.

When you power off the Cisco IP Phone through the CLI or SNMP or remove it, the supervisor engine sends a message to the switching module to turn off the power on the port. That power is then returned to the available system power.



Caution

When a Cisco IP Phone cable is plugged into a port and the power is turned on, the supervisor engine has a 4-second timeout waiting for the link to go up on the line. During those 4 seconds, if the Cisco IP Phone cable is unplugged and a network device is plugged in, the network device could be damaged. We recommend that you wait at least 10 seconds between unplugging a network device and plugging in another network device.

Default Cisco IP Phone Support Configuration

Cisco IP Phone support is disabled by default.

When the voice VLAN feature is enabled, all untagged traffic is sent with the default CoS priority of the port.

The CoS is not trusted for 802.1P or 802.1Q tagged traffic.

Cisco IP Phone Support Configuration Guidelines and Restrictions

- You must enable the Cisco Discovery Protocol (CDP) on the Catalyst 6500 series switch port connected to the Cisco IP Phone to send configuration information to the Cisco IP Phone.
- You can configure a voice VLAN only on a Layer 2 LAN port.
- You can configure the ports on WS-X6548-RJ-45 and WS-X6548-RJ-21 switching modules to trust received Layer 2 CoS values (QoS port architecture 1p1q0t/1p3q1t). The WS-X6548-RJ-45 and WS-X6548-RJ-21 switching modules cannot supply power to Cisco IP Phones.

- You cannot configure 10/100 Mbps ports with QoS port architecture 1p4t/2q2t to trust received Layer 2 CoS values. Configure policies to trust the Layer 3 IP precedence value on switching modules with QoS port architecture 1p4t/2q2t.
- The following conditions indicate that the Cisco IP Phone and a device attached to the Cisco IP Phone are in the same VLAN and must be in the same IP subnet:
 - If they both use 802.1p or untagged frames
 - If the Cisco IP Phone uses 802.1p frames and the device uses untagged frames
 - If the Cisco IP Phone uses untagged frames and the device uses 802.1p frames
 - If the Cisco IP Phone uses 802.1Q frames and the voice VLAN is the same as the access VLAN
- The Cisco IP Phone and a device attached to the Cisco IP Phone cannot communicate if they are in the same VLAN and subnet but use different frame types, because traffic between devices in the same subnet is not routed (routing would eliminate the frame type difference).
- You cannot use Cisco IOS software commands to configure the frame type used by traffic sent from a device attached to the access port on the Cisco IP Phone.
- If you enable port security on a port configured with a voice VLAN and if there is a PC connected to the Cisco IP Phone, set the maximum allowed secure addresses on the port to at least 3.
- You cannot configure static secure MAC addresses in the voice VLAN.
- Ports configured with a voice VLAN can be secure ports (refer to [Chapter 28, “Configuring Port Security”](#)).
- In all configurations, the voice traffic carries a Layer 3 IP precedence value (the default is 5 for voice traffic and 3 for voice control traffic).

Configuring Cisco IP Phone Support

These sections describe how to configure Cisco IP Phone support:

- [Configuring Voice Traffic Support, page 12-5](#)
- [Configuring Data Traffic Support, page 12-7](#)
- [Configuring Inline Power Support, page 12-8](#)



Note Voice VLANs are referred to as *auxiliary VLANs* in the Catalyst software publications.

Configuring Voice Traffic Support

To configure the way in which the Cisco IP Phone transmits voice traffic, perform this task:

Command	Purpose
Step 1 Router(config)# interface fastethernet slot/port	Selects the port to configure.
Step 2 Router(config-if)# switchport voice vlan {voice_vlan_ID dot1p none untagged}	Configures the way in which the Cisco IP Phone transmits voice traffic.
Router(config-if)# no switchport voice vlan	Clears the configuration.

Command	Purpose
Step 3 Router(config)# end	Exits configuration mode.
Step 4 Router# show interfaces fastethernet slot/port switchport Router# show running-config interface fastethernet slot/port	Verifies the configuration.

When configuring the way in which the Cisco IP Phone transmits voice traffic, note the following syntax information:

- Enter a voice VLAN ID to send CDP packets that configure the Cisco IP Phone to transmit voice traffic in 802.1Q frames, tagged with the voice VLAN ID and a Layer 2 CoS value (the default is 5). Valid VLAN IDs are from 1 to 4094. The switch puts the 802.1Q voice traffic into the voice VLAN.
- Enter the **dot1p** keyword to send CDP packets that configure the Cisco IP Phone to transmit voice traffic in 802.1p frames, tagged with VLAN ID 0 and a Layer 2 CoS value (the default is 5 for voice traffic and 3 for voice control traffic). The switch puts the 802.1p voice traffic into the access VLAN.
- Enter the **untagged** keyword to send CDP packets that configure the Cisco IP Phone to transmit untagged voice traffic. The switch puts the untagged voice traffic into the access VLAN.
- Enter the **none** keyword to allow the Cisco IP Phone to use its own configuration and transmit untagged voice traffic. The switch puts the untagged voice traffic into the access VLAN.
- In all configurations, the voice traffic carries a Layer 3 IP precedence value (the default is 5).
- Refer to [Chapter 24, “Configuring PFC QoS,”](#) for information about how to configure QoS.
- Refer to the [“Configuring a LAN Interface as a Layer 2 Access Port” section on page 7-13](#) for information about how to configure the port as a Layer 2 access port and configure the access VLAN.

This example shows how to configure Fast Ethernet port 5/1 to send CDP packets that tell the Cisco IP Phone to use VLAN 101 as the voice VLAN:

```
Router# configure terminal
Router(config)# interface fastethernet 5/1
Router(config-if)# switchport voice vlan 101
Router(config-if)# exit
```

This example shows how to verify the configuration of Fast Ethernet port 5/1:

```
Router# show interfaces fastethernet 5/1 switchport
Name: Fa5/1
Switchport: Enabled
Administrative Mode: access
Operational Mode: access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: off
Access Mode VLAN: 100
Voice VLAN: 101
Trunking Native Mode VLAN: 1 (default)
Administrative private-vlan host-association: none
Administrative private-vlan mapping: 900 ((Inactive)) 901 ((Inactive))
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
```

Configuring Data Traffic Support

To configure the way in which the Cisco IP Phone transmits data traffic, perform this task:

Command	Purpose
Step 1 Router(config)# interface fastethernet slot/port	Selects the port to configure.
Step 2 Router(config-if)# mls qos trust extend [cos cos_value]	Configures the way in which the Cisco IP Phone transmits data traffic.
Router(config-if)# no mls qos trust extend	Clears the configuration.
Step 3 Router(config)# end	Exits configuration mode.
Step 4 Router# show interfaces fastethernet slot/port switchport Router# show running-config interface fastethernet slot/port	Verifies the configuration.

When configuring the way in which the Cisco IP Phone transmits data traffic, note the following syntax information:

- To send CDP packets that configure the Cisco IP Phone to trust tagged traffic received from a device connected to the access port on the Cisco IP Phone, do not enter the **cos** keyword and CoS value.
- To send CDP packets that configure the Cisco IP Phone to mark tagged ingress traffic received from a device connected to the access port on the Cisco IP Phone, enter the **cos** keyword and CoS value (valid values are 0 through 7).
- You cannot use Cisco IOS software commands to configure whether or not traffic sent from a device attached to the access port on the Cisco IP Phone is tagged.

This example shows how to configure Fast Ethernet port 5/1 to send CDP packets that tell the Cisco IP Phone to configure its access port as untrusted and to mark all tagged traffic received from a device connected to the access port on the Cisco IP Phone with CoS 3:

```
Router# configure terminal
Router# interface fastethernet 5/1
Router(config-if)# mls qos trust extend cos 3
```

This example shows how to configure Fast Ethernet port 5/1 to send CDP packets that tell the Cisco IP Phone to configure its access port as trusted:

```
Router# configure terminal
Router(config)# interface fastethernet 5/1
Router(config-if)# mls qos trust extend
```

This example shows how to verify the configuration on Fast Ethernet port 5/1:

```
Router# show queueing interface fastethernet 5/1 | include Extend
Extend trust state: trusted
```

Configuring Inline Power Support

To configure inline power support, perform this task:

Command	Purpose
Step 1 Router(config)# interface fastethernet slot/port	Selects the port to configure.
Step 2 Router(config-if)# power inline {auto never}	Configures inline power support.
Router(config-if)# no power inline	Clears the configuration.
Step 3 Router(config)# end	Exits configuration mode.
Step 4 Router# show power inline [fastethernet slot/port]	Verifies the configuration.

When configuring inline power support, note the following syntax information:

- To configure auto-detection of a Cisco IP Phone, enter the **auto** keyword.
- To disable auto-detection of a Cisco IP Phone, enter the **never** keyword.

This example shows how to disable inline power on Fast Ethernet port 5/1:

```
Router# configure terminal
Router(config)# interface fastethernet 5/1
Router(config-if)# power inline never
```

This example shows how to enable inline power on Fast Ethernet port 5/1:

```
Router# configure terminal
Router(config)# interface fastethernet 5/1
Router(config-if)# power inline auto
```

This example shows how to verify the inline power configuration on Fast Ethernet port 5/1:

```
Router# show power inline fastethernet 5/1
Interface Admin Oper Power Device
(Watts)
-----
Fa5/1 auto on 6.3 cisco phone device
```



CHAPTER

13

Configuring IEEE 802.1Q Tunneling and Layer 2 Protocol Tunneling

This chapter describes how to configure IEEE 802.1Q tunneling and Layer 2 protocol tunneling on the Catalyst 6500 series switches.



Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication.

This chapter consists of these sections:

- [Understanding How 802.1Q Tunneling Works, page 13-1](#)
- [802.1Q Tunneling Configuration Guidelines and Restrictions, page 13-3](#)
- [Configuring 802.1Q Tunneling, page 13-5](#)
- [Understanding How Layer 2 Protocol Tunneling Works, page 13-6](#)
- [Configuring Support for Layer 2 Protocol Tunneling, page 13-7](#)

Understanding How 802.1Q Tunneling Works

802.1Q tunneling enables service providers to use a single VLAN to support customers who have multiple VLANs, while preserving customer VLAN IDs and keeping traffic in different customer VLANs segregated.

A port configured to support 802.1Q tunneling is called a tunnel port. When you configure tunneling, you assign a tunnel port to a VLAN that you dedicate to tunneling. To keep customer traffic segregated, each customer requires a separate VLAN, but that one VLAN supports all of the customer's VLANs.

With 802.1Q tunneling, tagged customer traffic comes from an 802.1Q trunk port on a customer device and enters the service-provider edge switch through a tunnel port. The link between the 802.1Q trunk port on a customer device and the tunnel port is called an asymmetrical link because one end is configured as an 802.1Q trunk port and the other end is configured as a tunnel port. You assign the tunnel port to an access VLAN ID unique to each customer. See [Figure 13-1 on page 13-2](#) and [Figure 13-2 on page 13-2](#).

■ Understanding How 802.1Q Tunneling Works

Figure 13-1 IEEE 802.1Q Tunnel Ports in a Service-Provider Network

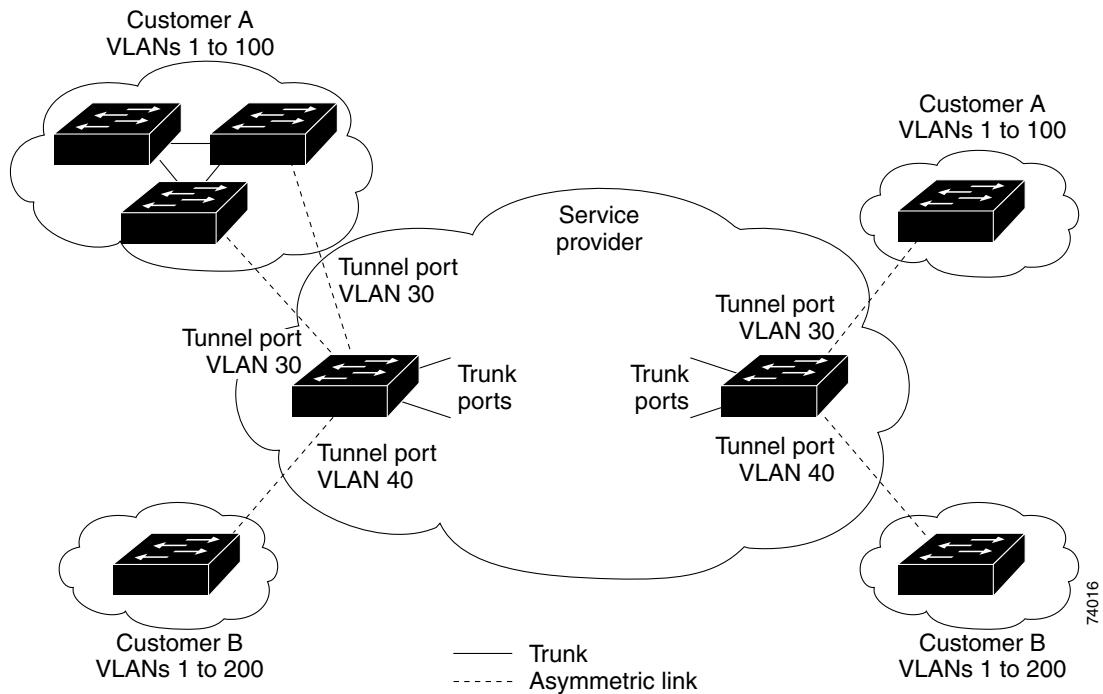
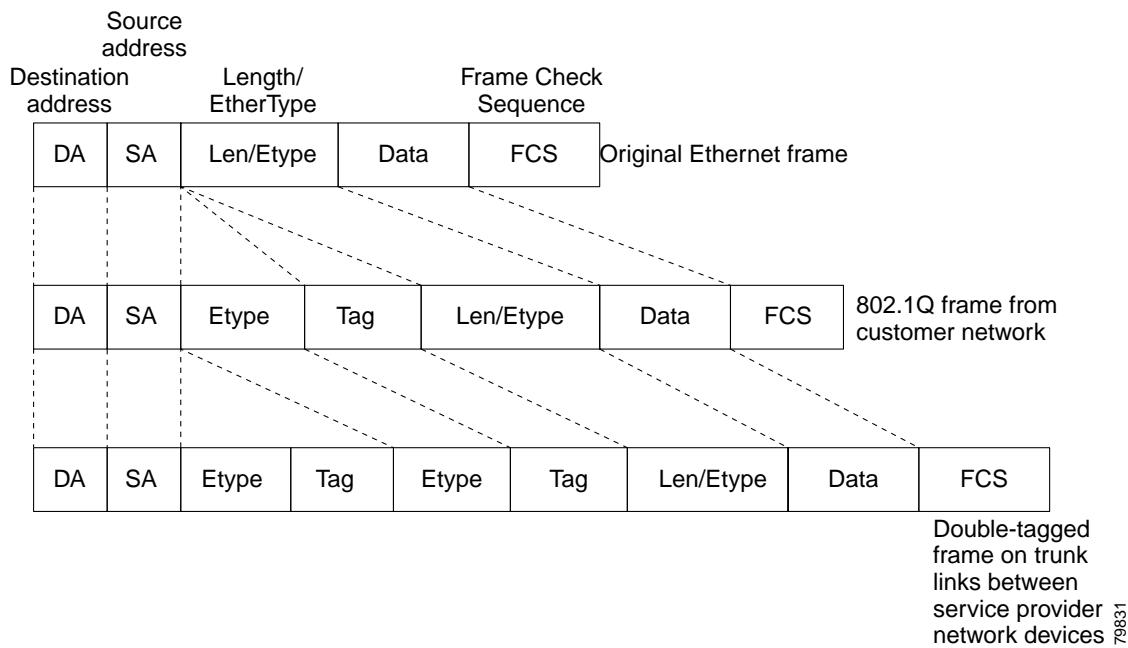


Figure 13-2 Untagged, 802.1Q-Tagged, and Double-Tagged Ethernet Frames



When a tunnel port receives tagged customer traffic from an 802.1Q trunk port, it does not strip the received 802.1Q tag from the frame header; instead, the tunnel port leaves the 802.1Q tag intact, adds a 2-byte Ethertype field (0x8100) followed by a 2-byte field containing the priority (CoS) and the VLAN. The received customer traffic is then put into the VLAN to which the tunnel port is assigned. This Ethertype 0x8100 traffic, with the received 802.1Q tag intact, is called tunnel traffic.

A VLAN carrying tunnel traffic is an 802.1Q tunnel. The tunnel ports in the VLAN are the tunnel's ingress and egress points.

The tunnel ports do not have to be on the same network device. The tunnel can cross other network links and other network devices before reaching the egress tunnel port. A tunnel can have as many tunnel ports as required to support the customer devices that need to communicate through the tunnel.

An egress tunnel port strips the 2-byte Ethertype field (0x8100) and the 2-byte length field and transmits the traffic with the 802.1Q tag still intact to an 802.1Q trunk port on a customer device. The 802.1Q trunk port on the customer device strips the 802.1Q tag and puts the traffic into the appropriate customer VLAN.

**Note**

Tunnel traffic carries a second 802.1Q tag only when it is on a trunk link between service-provider network devices, with the outer tag containing the service-provider-assigned VLAN ID and the inner tag containing the customer-assigned VLAN IDs.

802.1Q Tunneling Configuration Guidelines and Restrictions

Follow these guidelines when configuring 802.1Q tunneling in your network:

- Use asymmetrical links to put traffic into a tunnel or to remove traffic from a tunnel.
- Configure tunnel ports only to form an asymmetrical link.
- Dedicate one VLAN for each tunnel.
- Assign only tunnel ports to VLANs used for tunneling.
- Trunks require no special configuration to carry tunnel VLANs.
- We recommend that you use ISL trunks to carry tunnel traffic between devices that do not have tunnel ports. Because of the 802.1Q native VLAN feature, using 802.1Q trunks requires that you be very careful when you configure tunneling: a mistake might direct tunnel traffic to a non-tunnel port.
- Ensure that the native VLAN of the 802.1Q trunk port in an asymmetrical link carries no traffic. Because traffic in the native VLAN is untagged, it cannot be tunneled correctly. Alternatively, you can enter the global **vlan dot1q tag native** command to tag native VLAN egress traffic and drop untagged native VLAN ingress traffic.
- Because tunnel traffic has the added ethertype and length field and retains the 802.1Q tag within the switch, the following restrictions exist:
 - The Layer 3 packet within the Layer 2 frame cannot be identified in tunnel traffic.
 - Layer 3 and higher parameters cannot be identified in tunnel traffic (for example, Layer 3 destination and source addresses).
 - Because the Layer 3 addresses cannot be identified within the packet, tunnel traffic cannot be routed.
 - The switch can provide only MAC-layer filtering for tunnel traffic (VLAN IDs and source and destination MAC addresses).

- The switch can provide only MAC-layer access control and QoS for tunnel traffic.
- QoS cannot detect the received CoS value in the 802.1Q 2-byte Tag Control Information field.
- On an asymmetrical link, the Cisco Discovery Protocol (CDP) reports a native VLAN mismatch if the VLAN of the tunnel port does not match the native VLAN of the 802.1Q trunk. The 802.1Q tunnel feature does not require that the VLANs match. Ignore the messages if your configuration requires nonmatching VLANs.
- Asymmetrical links do not support the Dynamic Trunking Protocol (DTP), because only one port on the link is a trunk. Configure the 802.1Q trunk port on an asymmetrical link to trunk unconditionally.
- Jumbo frames can be tunneled as long as the jumbo frame length combined with the 802.1Q tag does not exceed the maximum frame size.
- The 802.1Q tunneling feature cannot be configured on ports configured to support private VLANs.
- The following Layer 2 protocols work between devices connected by an asymmetrical link:
 - CDP
 - UniDirectional Link Detection (UDLD)
 - Port Aggregation Protocol (PAgP)
 - Link Aggregation Control Protocol (LACP)
- PortFast BPDU filtering is enabled automatically on tunnel ports.
- CDP is automatically disabled on tunnel ports.
- VLAN Trunk Protocol (VTP) does not work between the following devices:
 - Devices connected by an asymmetrical link
 - Devices communicating through a tunnel



Note VTP works between tunneled devices if Layer 2 protocol tunneling is enabled. See the “Configuring Support for Layer 2 Protocol Tunneling” section on page 13-7 for configuration details.

- To configure an EtherChannel as an asymmetrical link, all ports in the EtherChannel must have the same tunneling configuration. Because the Layer 3 packet within the Layer 2 frame cannot be identified, you must configure the EtherChannel to use MAC-address-based frame distribution.

The following configuration guidelines are *required* for your Layer 2 protocol tunneling configuration:

- On all the service provider edge switches, PortFast BPDU filtering must be enabled on the 802.1Q tunnel ports as follows:

```
Router(config-if)# spanning-tree bpdufilter enable
Router(config-if)# spanning-tree portfast
```



Note PortFast BPDU filtering is enabled automatically on tunnel ports.

- At least one VLAN must be available for Native VLAN tagging (**vlan dot1q tag native** option). If you use all the available VLANs and then try to enable the **vlan dot1q tag native** option, the option will not be enabled.

- On all the service provider core switches, tag native VLAN egress traffic and drop untagged native VLAN ingress traffic by entering the following command:

```
Router(config)# vlan dot1q tag native
```

- On all the customer switches, *either* enable or disable the global **vlan dot1q tag native** option.



Note If this option is enabled on one switch and disabled on another switch, all traffic is dropped; all customer switches must have this option configured the same on each switch.

The following configuration guidelines are *optional* for your Layer 2 protocol tunneling configuration:

- Because all the BPDUs are being dropped, spanning tree PortFast can be enabled on Layer 2 protocol tunnel ports as follows:

```
Router(config-if)# spanning-tree portfast trunk
```

- If the service provider does not want the customer to see its switches, CDP should be disabled on the 802.1Q tunnel port as follows:

```
Router(config-if)# no cdp enable
```

Configuring 802.1Q Tunneling

These sections describe 802.1Q tunneling configuration:

- [Configuring 802.1Q Tunnel Ports, page 13-5](#)
- [Configuring the Switch to Tag Native VLAN Traffic, page 13-6](#)



Caution

Ensure that only the appropriate tunnel ports are in any VLAN used for tunneling and that one VLAN is used for each tunnel. Incorrect assignment of tunnel ports to VLANs can forward traffic inappropriately.

Configuring 802.1Q Tunnel Ports

To configure 802.1Q tunneling on a port, perform this task:

Command	Purpose
Step 1 Router(config)# interface type ¹ slot/port	Selects the LAN port to configure.
Step 2 Router(config-if)# switchport	Configures the LAN port for Layer 2 switching: <ul style="list-style-type: none"> You must enter the switchport command once without any keywords to configure the LAN port as a Layer 2 interface before you can enter additional switchport commands with keywords. Required only if you have not entered the switchport command already for the interface.
Step 3 Router(config-if)# switchport mode dot1q-tunnel Router(config-if)# no switchport mode dot1q-tunnel	Configures the Layer 2 port as a tunnel port. Clears the tunnel port configuration.

■ Understanding How Layer 2 Protocol Tunneling Works

Command	Purpose
Step 4 Router(config-if)# end	Exits configuration mode.
Step 5 Router# show dot1q-tunnel [{interface type interface-number}]	Verifies the configuration.

1. *type* = **ethernet**, **fastethernet**, **gigabitether**net, or **tengigabitether**net

This example shows how to configure tunneling on port 4/1 and verify the configuration:

```
Router# configure terminal
Router(config)# interface fastethernet 4/1
Router(config-if)# switchport mode dot1q-tunnel
Router(config-if)# end
Router# show dot1q-tunnel interface
```

Configuring the Switch to Tag Native VLAN Traffic

The **vlan dot1q tag native** command is a global command that configures the switch to tag native VLAN traffic, and admit only 802.1Q tagged frames on 802.1Q trunks, dropping any untagged traffic, including untagged traffic in the native VLAN.

To configure the switch to tag traffic in the native VLAN, perform this task:

Command	Purpose
Step 1 Router(config)# vlan dot1q tag native	Configures the switch to tag native VLAN traffic.
	Router(config)# no vlan dot1q tag native Clears the configuration.
Step 2 Router(config)# end	Exits configuration mode.
Step 3 Router# show vlan dot1q tag native	Verifies the configuration.

This example shows how to configure the switch to tag native VLAN traffic and verify the configuration:

```
Router# configure terminal
Router(config)# vlan dot1q tag native
Router(config)# end
Router# show vlan dot1q tag native
```

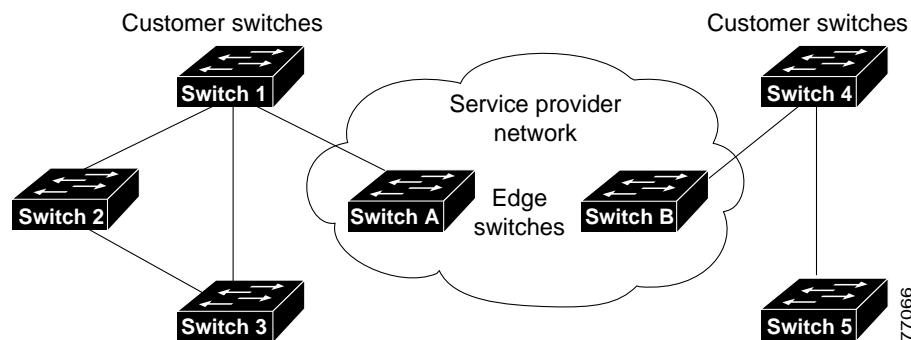
Understanding How Layer 2 Protocol Tunneling Works

Layer 2 protocol tunneling allows Layer 2 protocol data units (PDUs) (CDP, STP, and VTP) to be tunneled through a network. This section uses the following terminology:

- Edge switch—The switch connected to the customer switch and placed on the boundary of the service provider network (see [Figure 13-3](#)).
- Layer 2 protocol tunnel port—A port on the edge switch on which a specific tunneled protocol can be encapsulated or deencapsulated. The Layer 2 protocol tunnel port is configured through CLI commands.
- Tunneled PDU—A CDP, STP, or VTP PDU.

Without Layer 2 protocol tunneling, tunnel ports drop STP and VTP packets and process CDP packets. This handling of the PDUs creates different spanning tree domains (different spanning tree roots) for the customer switches. For example, STP for a VLAN on switch 1 (see [Figure 13-3](#)) builds a spanning tree topology on switches 1, 2, and 3 without considering convergence parameters based on switches 4 and 5. To provide a single spanning tree domain for the customer, a generic scheme to tunnel BPDUs was created for control protocol PDUs (CDP, STP, and VTP). This process is referred to as Generic Bridge PDU Tunneling (GBPT).

Figure 13-3 Layer 2 Protocol Tunneling Network Configuration



GBPT provides a scalable approach to PDU tunneling by software encapsulating the PDUs in the ingress edge switches and then multicasting them in hardware. All switches inside the service provider network treat these encapsulated frames as data packets and forward them to the other end. The egress edge switch listens for these special encapsulated frames and deencapsulates them; they are then forwarded out of the tunnel.

The encapsulation involves rewriting the destination media access control (MAC) address in the PDU. An ingress edge switch rewrites the destination MAC address of the PDUs received on a Layer 2 tunnel port with the Cisco proprietary multicast address (01-00-0c-cd-cd-d0). The PDU is then flooded to the native VLAN of the Layer 2 tunnel port. If you enable Layer 2 protocol tunneling on a port, PDUs of an enabled protocol are not sent out. If you disable Layer 2 protocol tunneling on a port, the disabled protocols behave the same way they were behaving before Layer 2 protocol tunneling was disabled on the port.

Configuring Support for Layer 2 Protocol Tunneling



Note Encapsulated PDUs received by an 802.1Q tunnel port are transmitted from other tunnel ports in the same vlan on the switch.

■ Configuring Support for Layer 2 Protocol Tunneling

To configure Layer 2 protocol tunneling on a port, perform this task:

Command	Purpose
Step 1 Router(config)# interface type¹ slot/port	Selects the LAN port to configure.
Step 2 Router(config-if)# switchport	Configures the LAN port for Layer 2 switching: <ul style="list-style-type: none"> You must enter the switchport command once without any keywords to configure the LAN port as a Layer 2 interface before you can enter additional switchport commands with keywords. Required only if you have not entered the switchport command already for the interface.
Step 3 Router(config-if)# l2protocol-tunnel [cdp drop-threshold [packets] shutdown-threshold [packets] stp vtp] Router(config-if)# no l2protocol-tunnel [cdp drop-threshold shutdown-threshold stp vtp]	Configures the Layer 2 port as a Layer 2 protocol tunnel port for the protocol(s) specified. Clears the configuration.
Step 4 Router(config)# end	Exits configuration mode.
Step 5 Router# show l2protocol-tunnel [interface type¹ slot/port summary]	Verifies the configuration.

1. *type* = **ethernet**, **fastethernet**, **gigabitether**net, or **tengigabitether**net

When you configure a Layer 2 port as a Layer 2 protocol tunnel port, note the following syntax information:

- Optionally, you may specify a drop-threshold for the port. The drop-threshold value, from 1 to 4096, determines the number of packets to be processed for that protocol on that interface in one second. When the drop threshold is exceeded, PDUs for the specified protocol are dropped for the remainder of the 1-second period. If a shutdown threshold is not specified, the value is 0 (shutdown threshold disabled).
- Optionally, you may specify a shutdown-threshold for the port. The drop-threshold value, from 1 to 4096, determines the number of packets to be processed for that protocol on that interface in one second. When the shutdown threshold is exceeded, the port is put in errdisable state. If a shutdown threshold is not specified, the value is 0 (shutdown threshold disabled).



Note Refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication for more information about the **l2ptguard** keyword for the following commands:

- **errdisable detect cause**
- **errdisable recovery cause**

This example shows how to configure Layer 2 protocol tunneling and shutdown thresholds on port 5/1 for CDP, STP, and VTP, and verify the configuration:

```
Router# configure terminal
Router(config)# interface fastethernet 5/1
Router(config-if)# switchport
Router(config-if)# l2protocol-tunnel shutdown-threshold cdp 10
Router(config-if)# l2protocol-tunnel shutdown-threshold stp 10
Router(config-if)# l2protocol-tunnel shutdown-threshold vtp 10
Router(config-if)# end
Router# show l2protocol-tunnel summary
```

```
Port      Protocol      Threshold  
          (cos/cdp/stp/vtp)  
-----  
Fa5/1    cdp stp vtp   0/10  /10  /10           down trunk  
Router#
```

This example shows how to display counter information for port 5/1:

```
Router# show l2protocol-tunnel interface fastethernet 5/1  
Port      Protocol      Threshold      Counters  
          (cos/cdp/stp/vtp)  (cdp/stp/vtp/decap)  
-----  
Router#
```

This example shows how to clear the Layer 2 protocol tunneling configuration from port 5/1:

```
Router(config-if)# no l2protocol-tunnel shutdown-threshold cdp 10  
Router(config-if)# no l2protocol-tunnel shutdown-threshold stp 10  
Router(config-if)# no l2protocol-tunnel shutdown-threshold vtp 10  
Router(config-if)# no l2protocol-tunnel cdp  
Router(config-if)# no l2protocol-tunnel stp  
Router(config-if)# no l2protocol-tunnel vtp  
Router(config-if)# end  
Router# show l2protocol-tunnel summary  
Port      Protocol      Threshold  
          (cos/cdp/stp/vtp)  
-----  
Router#
```

This example shows how to clear Layer 2 protocol tunneling port counters:

```
Router# clear l2protocol-tunnel counters  
Router#
```

■ Configuring Support for Layer 2 Protocol Tunneling



CHAPTER

14

Configuring STP and IEEE 802.1s MST

This chapter describes how to configure the Spanning Tree Protocol (STP) and the IEEE 802.1s Multiple Spanning Tree (MST) protocol on Catalyst 6500 series switches.



Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication.

This chapter consists of these sections:

- [Understanding How STP Works, page 14-1](#)
- [Understanding How IEEE 802.1w RSTP Works, page 14-12](#)
- [Understanding How IEEE 802.1s MST Works, page 14-13](#)
- [Default STP Configuration, page 14-19](#)
- [STP and MST Configuration Guidelines and Restrictions, page 14-20](#)
- [Configuring STP, page 14-20](#)
- [Configuring IEEE 802.1s MST, page 14-32](#)



Note

For information on configuring the PortFast, UplinkFast, and BackboneFast STP enhancements, see [Chapter 15, “Configuring Optional STP Features.”](#)

Understanding How STP Works

These sections describe how STP works:

- [STP Overview, page 14-2](#)
- [Understanding the Bridge ID, page 14-2](#)
- [Understanding Bridge Protocol Data Units, page 14-3](#)
- [Election of the Root Bridge, page 14-4](#)
- [STP Protocol Timers, page 14-4](#)
- [Creating the Spanning Tree Topology, page 14-5](#)
- [STP Port States, page 14-5](#)
- [STP and IEEE 802.1Q Trunks, page 14-11](#)

STP Overview

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. STP operation is transparent to end stations, which cannot detect whether they are connected to a single LAN segment or a switched LAN of multiple segments.

Catalyst 6500 series switches use STP (the IEEE 802.1D bridge protocol) on all VLANs. By default, a single instance of STP runs on each configured VLAN (provided you do not manually disable STP). You can enable and disable STP 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 STP algorithm calculates the best loop-free path throughout a switched Layer 2 network. Layer 2 LAN ports send and receive STP frames at regular intervals. Network devices 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 network devices might learn end station MAC addresses on multiple Layer 2 LAN ports. These conditions result in an unstable network.

STP defines a tree with a root bridge and a loop-free path from the root to all network devices in the Layer 2 network. STP forces redundant data paths into a standby (blocked) state. If a network segment in the spanning tree fails and a redundant path exists, the STP algorithm recalculates the spanning tree topology and activates the standby path.

When two Layer 2 LAN ports on a network device are part of a loop, the STP 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 STP port priority value represents the location of a port in the network topology and how well located it is to pass traffic. The STP 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.

This section contains these topics:

- [Bridge Priority Value, page 14-2](#)
- [Extended System ID, page 14-2](#)
- [STP MAC Address Allocation, page 14-3](#)

Bridge Priority Value

The bridge priority is a 4-bit value when the extended system ID is enabled (see [Table 14-2 on page 14-3](#) and the “[Configuring the Bridge Priority of a VLAN](#)” section on page [14-28](#)).

Extended System ID

A 12-bit extended system ID field is part of the bridge ID (see [Table 14-2 on page 14-3](#)). 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 [14-22](#).

Table 14-1 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 14-2 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	2048	1024	512	256	128	64	32	16	8	4	2	1

STP MAC Address Allocation

Catalyst 6500 series switch chassis have either 64 or 1024 MAC addresses available to support software features such as STP. To view the MAC address range on your chassis, enter the **show catalyst6000 chassis-mac-address** command.

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.

If you have a network device in your network with MAC address reduction enabled, you should also enable MAC address reduction on all other Layer-2 connected network devices to avoid undesirable root bridge election and spanning tree topology issues.

When MAC address reduction is enabled, the root bridge priority becomes a multiple of 4096 plus the VLAN ID. With MAC address reduction enabled, a switch bridge ID (used by the spanning-tree algorithm to determine the identity of the root bridge, the lowest being preferred) can only be specified as a multiple of 4096. Only the following values are possible: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440.

If another bridge in the same spanning-tree domain does not run the MAC address reduction feature, it could win root bridge ownership because of the finer granularity in the selection of its bridge ID.

Understanding Bridge Protocol Data Units

Bridge protocol data units (BPDUs) are transmitted in one direction from the root bridge. Each network device sends configuration BPDUs to communicate and compute the spanning tree topology. Each configuration BPDU contains the following minimal information:

- The unique bridge ID of the network device that the transmitting network device believes to be the root bridge
- The STP path cost to the root
- The bridge ID of the transmitting bridge
- Message age

- The identifier of the transmitting port
- Values for the hello, forward delay, and max-age protocol timers

When a network device transmits a BPDU frame, all network devices connected to the LAN on which the frame is transmitted receive the BPDU. When a network device 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 network device is elected as the root bridge.
- The shortest distance to the root bridge is calculated for each network device based on the path cost.
- A designated bridge for each LAN segment is selected. This is the network device 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 network device with the highest bridge ID (the lowest numerical ID value) is elected as the root bridge. If all network devices are configured with the default priority (32768), the network device with the lowest MAC address in the VLAN becomes the root bridge. The bridge priority value occupies the most significant bits of the bridge ID.

When you change the bridge priority value, you change the probability that the switch will be elected as the root bridge. Configuring a higher value increases the probability; a lower value decreases the probability.

The STP root bridge is the logical center of the spanning tree topology in a Layer 2 network. All paths that are not needed to reach the root bridge from anywhere in the Layer 2 network are placed in STP blocking mode.

BPDUs contain information about the transmitting bridge and its ports, including bridge and MAC addresses, bridge priority, port priority, and path cost. STP uses this information to elect the root bridge for the Layer 2 network, to elect the root port leading to the root bridge, and to determine the designated port for each Layer 2 segment.

STP Protocol Timers

[Table 14-3](#) describes the STP protocol timers that affect STP performance.

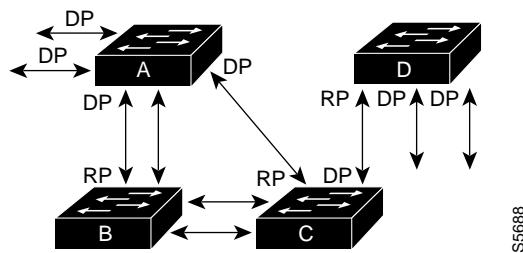
Table 14-3 STP Protocol Timers

Variable	Description
Hello timer	Determines how often the network device broadcasts hello messages to other network devices.
Forward delay timer	Determines how long each of the listening and learning states last before the port begins forwarding.
Maximum age timer	Determines the amount of time protocol information received on a port is stored by the network device.

Creating the Spanning Tree Topology

In Figure 14-1, Switch A is elected as the root bridge because the bridge priority of all the network devices is set to the default (32768) and Switch A has the lowest MAC address. However, due to traffic patterns, number of forwarding ports, or link types, Switch A might not be the ideal root bridge. By increasing the priority (lowering the numerical value) of the ideal network device so that it becomes the root bridge, you force an STP recalculation to form a new spanning tree topology with the ideal network device as the root.

Figure 14-1 Spanning Tree Topology



RP = Root Port
DP = Designated 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 ideal. 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. The goal is to make the fastest link the root 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 STP port priority on the fiber-optic port to a higher priority (lower numerical value) than the root port, the fiber-optic port becomes the new root port.

STP Port States

These sections describe the STP port states:

- [STP Port State Overview, page 14-5](#)
- [Blocking State, page 14-7](#)
- [Listening State, page 14-8](#)
- [Learning State, page 14-9](#)
- [Forwarding State, page 14-10](#)
- [Disabled State, page 14-11](#)

STP Port State Overview

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 LAN port transitions directly from nonparticipation in the spanning tree topology to the

■ Understanding How STP Works

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 using the old topology.

Each Layer 2 LAN port on a Catalyst 6500 series switch using STP exists in one of the following five states:

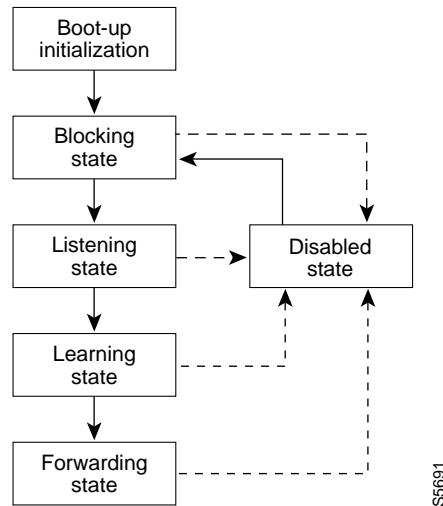
- Blocking—The Layer 2 LAN port does not participate in frame forwarding.
- Listening—First transitional state after the blocking state when STP determines that the Layer 2 LAN port should participate in frame forwarding.
- Learning—The Layer 2 LAN port prepares to participate in frame forwarding.
- Forwarding—The Layer 2 LAN port forwards frames.
- Disabled—The Layer 2 LAN port does not participate in STP and is not forwarding frames.

A Layer 2 LAN port moves through these five states as follows:

- From initialization to blocking
- From blocking to listening or to disabled
- From listening to learning or to disabled
- From learning to forwarding or to disabled
- From forwarding to disabled

[Figure 14-2](#) illustrates how a Layer 2 LAN port moves through the five states.

Figure 14-2 STP Layer 2 LAN Interface States



S5691

When you enable STP, every port in the Catalyst 6500 series switch, VLAN, and network goes through the blocking state and the transitory states of listening and learning at power up. If properly configured, each Layer 2 LAN port stabilizes to the forwarding or blocking state.

When the STP algorithm places a Layer 2 LAN port in the forwarding state, the following process occurs:

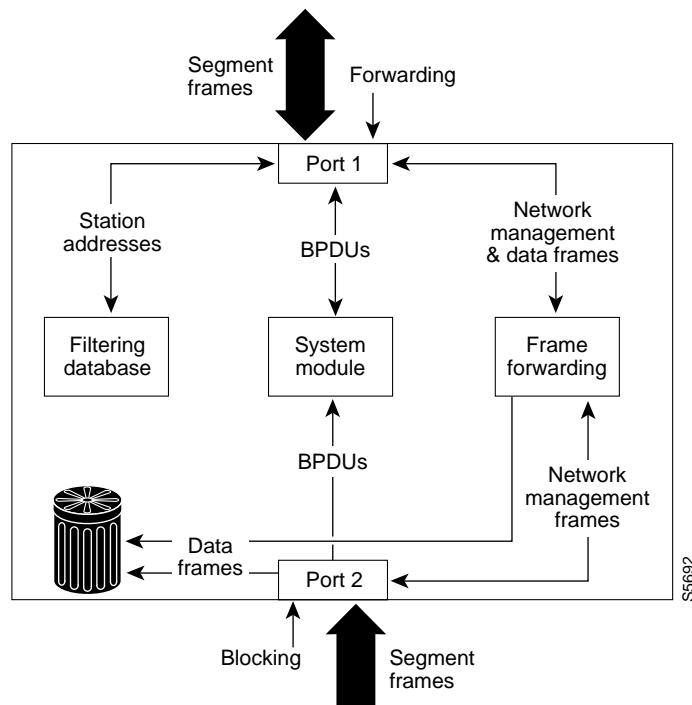
1. The Layer 2 LAN port is put into the listening state while it waits for protocol information that suggests it should go to the blocking state.

2. The Layer 2 LAN port waits for the forward delay timer to expire, moves the Layer 2 LAN port to the learning state, and resets the forward delay timer.
3. In the learning state, the Layer 2 LAN port continues to block frame forwarding as it learns end station location information for the forwarding database.
4. The Layer 2 LAN port waits for the forward delay timer to expire and then moves the Layer 2 LAN port to the forwarding state, where both learning and frame forwarding are enabled.

Blocking State

A Layer 2 LAN port in the blocking state does not participate in frame forwarding, as shown in [Figure 14-3](#). After initialization, a BPDU is sent out to each Layer 2 LAN port. A network device initially assumes it is the root until it exchanges PDUs with other network devices. This exchange establishes which network device in the network is the root or root bridge. If only one network device is in the network, no exchange occurs, the forward delay timer expires, and the ports move to the listening state. A port always enters the blocking state following initialization.

Figure 14-3 Interface 2 in Blocking State



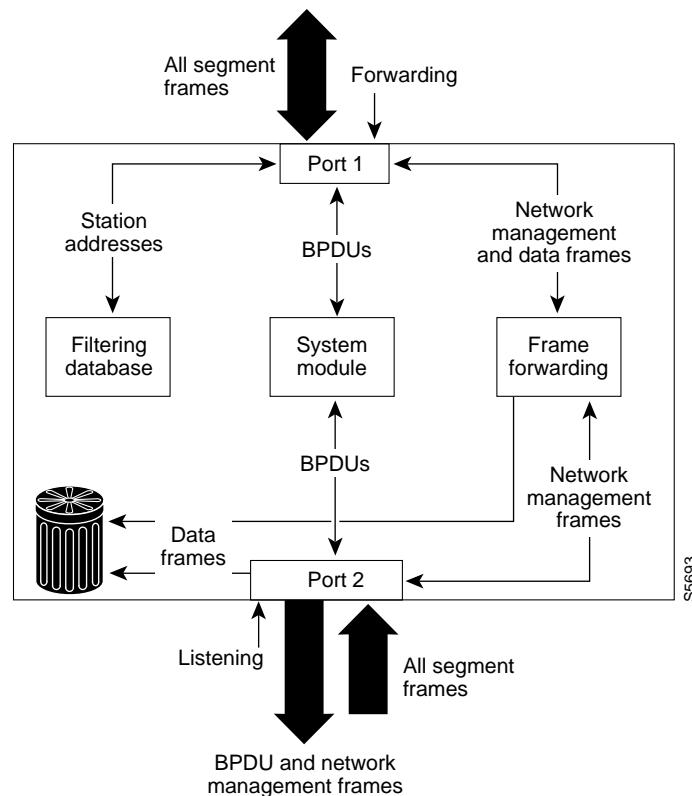
A Layer 2 LAN port in the blocking state performs as follows:

- Discards frames received from the attached segment.
- Discards frames switched from another port for forwarding.
- Does not incorporate end station location into its address database. (There is no learning on a blocking Layer 2 LAN port, so there is no address database update.)
- Receives BPDUs and directs them to the system module.
- Does not transmit BPDUs received from the system module.
- Receives and responds to network management messages.

Listening State

The listening state is the first transitional state a Layer 2 LAN port enters after the blocking state. The Layer 2 LAN port enters this state when STP determines that the Layer 2 LAN port should participate in frame forwarding. [Figure 14-4](#) shows a Layer 2 LAN port in the listening state.

Figure 14-4 Interface 2 in Listening State



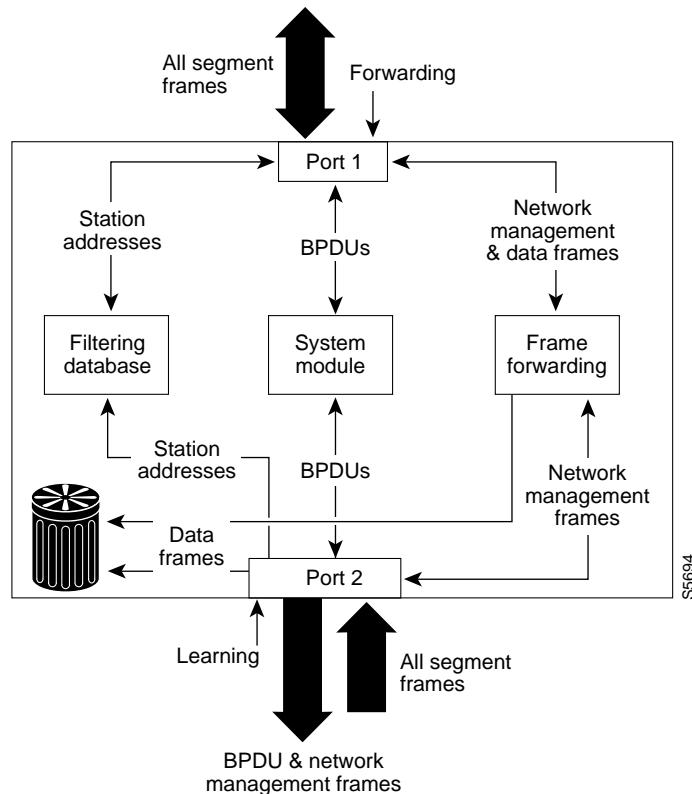
A Layer 2 LAN port in the listening state performs as follows:

- Discards frames received from the attached segment.
- Discards frames switched from another LAN port for forwarding.
- Does not incorporate end station location into its address database. (There is no learning at this point, so there is no address database update.)
- Receives BPDUs and directs them to the system module.
- Receives, processes, and transmits BPDUs received from the system module.
- Receives and responds to network management messages.

Learning State

A Layer 2 LAN port in the learning state prepares to participate in frame forwarding. The Layer 2 LAN port enters the learning state from the listening state. [Figure 14-5](#) shows a Layer 2 LAN port in the learning state.

Figure 14-5 Interface 2 in Learning State



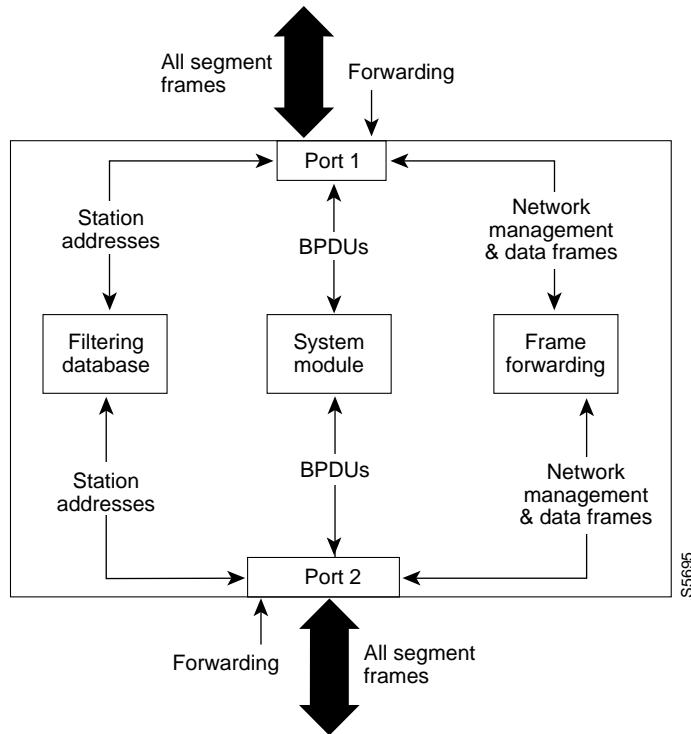
A Layer 2 LAN port in the learning state performs as follows:

- Discards frames received from the attached segment.
- Discards frames switched from another port for forwarding.
- Incorporates end station location into its address database.
- Receives BPDUs and directs them to the system module.
- Receives, processes, and transmits BPDUs received from the system module.
- Receives and responds to network management messages.

Forwarding State

A Layer 2 LAN port in the forwarding state forwards frames, as shown in [Figure 14-6](#). The Layer 2 LAN port enters the forwarding state from the learning state.

Figure 14-6 Interface 2 in Forwarding State



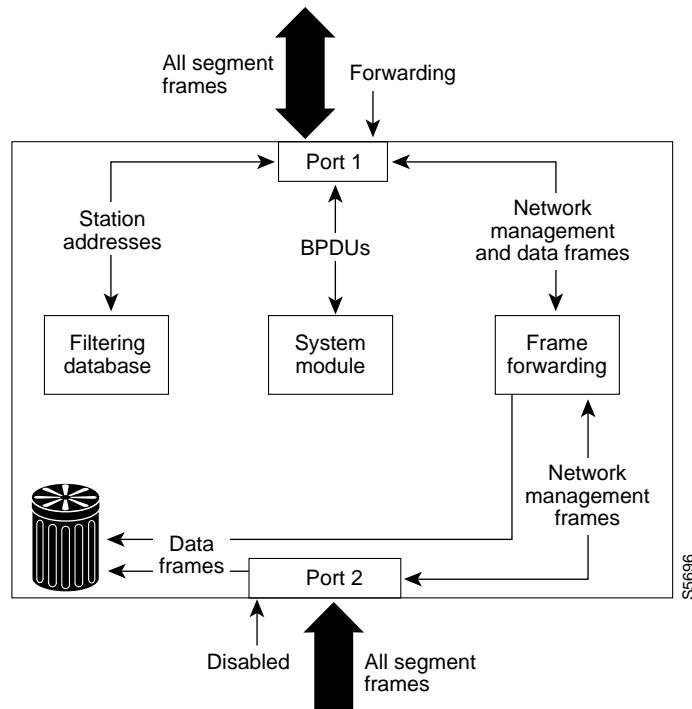
A Layer 2 LAN port in the forwarding state performs as follows:

- Forwards frames received from the attached segment.
- Forwards frames switched from another port for forwarding.
- Incorporates end station location information into its address database.
- Receives BPDUs and directs them to the system module.
- Processes BPDUs received from the system module.
- Receives and responds to network management messages.

Disabled State

A Layer 2 LAN port in the disabled state does not participate in frame forwarding or STP, as shown in Figure 14-7. A Layer 2 LAN port in the disabled state is virtually nonoperational.

Figure 14-7 Interface 2 in Disabled State



A disabled Layer 2 LAN port performs as follows:

- Discards frames received from the attached segment.
- Discards frames switched from another port for forwarding.
- Does not incorporate end station location into its address database. (There is no learning, so there is no address database update.)
- Does not receive BPDUs.
- Does not receive BPDUs for transmission from the system module.

STP and IEEE 802.1Q Trunks

802.1Q trunks impose some limitations on the STP strategy for a network. In a network of Cisco network devices connected through 802.1Q trunks, the network devices maintain one instance of STP for each VLAN allowed on the trunks. However, non-Cisco 802.1Q network devices maintain only one instance of STP for all VLANs allowed on the trunks.

When you connect a Cisco network device to a non-Cisco device through an 802.1Q trunk, the Cisco network device combines the STP instance of the 802.1Q VLAN of the trunk with the STP instance of the non-Cisco 802.1Q network device. However, all per-VLAN STP information is maintained by Cisco network devices separated by a cloud of non-Cisco 802.1Q network devices. The non-Cisco 802.1Q cloud separating the Cisco network devices is treated as a single trunk link between the network devices.

For more information on 802.1Q trunks, see [Chapter 7, “Configuring LAN Ports for Layer 2 Switching.”](#)



Note RSTP is available as a standalone protocol in Rapid-Per-VLAN-Spanning Tree (Rapid-PVST) mode. In this mode, the switch runs an RSTP instance on each VLAN, which follows the usual PVST+ approach.

These sections describe Rapid Spanning Tree Protocol (RSTP):

- [IEEE 802.1w RSTP Overview, page 14-12](#)
- [RSTP Port Roles, page 14-12](#)
- [RSTP Port States, page 14-13](#)
- [Rapid-PVST, page 14-13](#)

IEEE 802.1w RSTP Overview

RSTP significantly reduces the time to reconfigure the active topology of the network when changes occur to the physical topology or its configuration parameters. 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 forwarding using an explicit handshake between them. RSTP allows switch port configuration so that the ports can transition to forwarding directly when the switch reinitializes.

RSTP as specified in 802.1w supersedes STP specified in 802.1D, but remains compatible with STP.

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

RSTP uses the following definitions for port roles:

- 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 by a point-to-point link 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.

Port roles are assigned 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 14-4](#) provides a comparison between STP port states and RSTP port states.

Table 14-4 Comparison Between STP and RSTP Port States

Operational Status	STP Port State	RSTP Port State	Port Included in Active Topology
Enabled	Blocking ¹	Discarding ²	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 RSTP and MST.

In a stable topology, RSTP ensures that every root port and designated port transition to forwarding, and ensures that all alternate ports and backup ports are always in the discarding state.

Rapid-PVST

Rapid-PVST uses the existing configuration for PVST+; however, Rapid-PVST uses RSTP to provide faster convergence. Independent VLANs run their own RSTP instance.

Dynamic entries are flushed immediately on a per-port basis upon receiving a topology change.

UplinkFast and BackboneFast configurations are ignored in Rapid-PVST mode; both features are included in RSTP.

Understanding How IEEE 802.1s MST Works

These sections describe Multiple Spanning Tree (MST):

- [IEEE 802.1s MST Overview, page 14-14](#)
- [MST-to-PVST Interoperability, page 14-15](#)
- [Common Spanning Tree, page 14-16](#)
- [MST Instances, page 14-17](#)
- [MST Configuration Parameters, page 14-17](#)
- [MST Regions, page 14-17](#)

- [Message Age and Hop Count, page 14-19](#)
- [Default STP Configuration, page 14-19](#)

IEEE 802.1s MST Overview

MST in this release is based on the draft version of the IEEE standard. 802.1s for MST is an amendment to 802.1Q. 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 PVST+. MST 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 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).

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 version called the Multiple Spanning Tree Protocol (MSTP). The MST feature has these characteristics:

- MST runs a variant of spanning tree called internal spanning tree (IST). IST augments the 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 single spanning tree bridges as follows:
 - MST bridges run IST, which augments the common spanning tree (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 ISTs in each MST region, the CST that interconnects the MST regions, and the SST bridges. CIST is the same as an IST inside an MST region and the same as 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 referred to as 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 that 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).

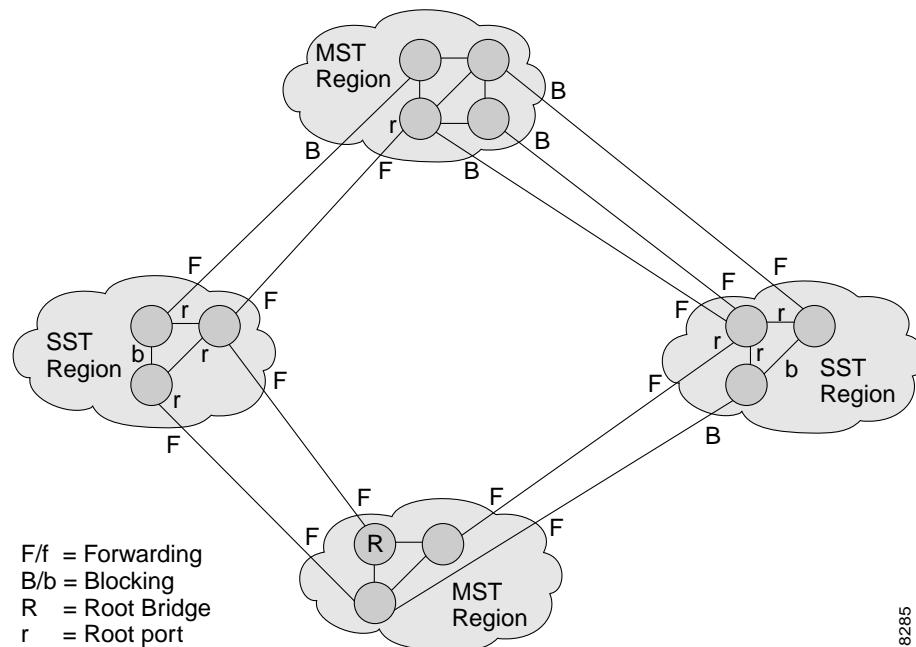
M-records are always encapsulated within MST BPDUs (MST BPDUs). The original spanning trees computed by MSTP are called M-trees. M-trees are active only within the MST region. M-trees merge with the IST at the boundary of the MST region and form the CST.
- MST provides interoperability with PVST+ by 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 included in RSTP.
 - PortFast is supported.
 - BPDUs 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), secondary VLANs must be mapped to the same instance as the primary.

MST-to-PVST Interoperability

A virtual bridged LAN may contain interconnected regions of single spanning tree (SST) and MST bridges. Figure 14-8 shows this relationship.

Figure 14-8 Network with Interconnected SST and MST Regions



An MST region appears as an SST or pseudobridge to STP running in the SST region. Pseudobridges operate as follows:

- The same values for root identifiers and root path costs are sent in all BPDUs of all the pseudobridge ports. Pseudobridges differ 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 1 second for each hop, the difference in the message age is in the order of seconds.

■ Understanding How IEEE 802.1s MST Works

- 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 may follow different paths within the MST regions established by MST.
- Loop prevention is achieved by 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.
- A pseudobridge differs from a single SST bridge because the BPDUs sent from the pseudobridge's ports have different bridge identifiers. The root identifier and root cost are the same for both bridges.

These guidelines apply in a topology where you configure MST switches (all in the same region) to interact with PVST+ switches:

- Configure the root for all VLANs inside the MST region as shown in this example:

```
Router# 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 Vlans 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 reenable 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. Do not designate switches with a slower CPU running PVST+ as a switch running MST.

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 this case, the topology changes are only propagated in the instance to which the VLAN is mapped. The topology change stays local to the first MST region and the 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.

Common Spanning Tree

CST (802.1Q) is a single spanning tree for all the VLANs. In a Catalyst 6500 series switch running PVST+, the VLAN 1 spanning tree corresponds to CST. In a Catalyst 6500 series 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 includes these three parts:

- Name—A 32-character string (null padded) identifying 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 BPDU only if the MST BPDU configuration ID and the checksum match its own MST region configuration ID and checksum. If one value is different, the MST BPDU is considered to be an SST BPDU.

MST Regions

These sections describe MST regions:

- [MST Region Overview, page 14-17](#)
- [Boundary Ports, page 14-18](#)
- [IST Master, page 14-18](#)
- [Edge Ports, page 14-18](#)
- [Link Type, page 14-19](#)

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 process assigns a port role to the boundary and assigns the same state as the state 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. To display the information about the IST master, path cost, and remaining hops for the bridge, enter the **show spanning-tree mst** command.

Edge Ports

An edge port is a port that is a port that is connected to a nonbridging device (for example, a host or a router). A port that connects to a hub is also an edge port if the hub or any LAN that is connected by it does not have a bridge. An edge port can start forwarding as soon as the link is up.

MST requires that you configure all ports for each host or router. To establish rapid connectivity after a failure, you need to block the nonedge 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 routers as edge ports while using MST.

To prevent a misconfiguration, the PortFast operation is turned off if the port receives a BPDU. To display the configured and operational status of PortFast, enter 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 router. 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 process that is very similar to the IP TTL process. 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.

Default STP Configuration

[Table 14-5](#) shows the default STP configuration.

Table 14-5 STP Default Configuration

Feature	Default Value
Enable state	STP enabled for all VLANs
Bridge priority	32768
STP port priority (configurable on a per-port basis—used on LAN ports configured as Layer 2 access ports)	128
STP port cost (configurable on a per-port basis—used on LAN ports configured as Layer 2 access ports)	<ul style="list-style-type: none"> • 10-Gigabit Ethernet: 2 • Gigabit Ethernet: 4 • Fast Ethernet: 19 • Ethernet: 100
STP VLAN port priority (configurable on a per-VLAN basis—used on LAN ports configured as Layer 2 trunk ports)	128
STP VLAN port cost (configurable on a per-VLAN basis—used on LAN ports configured as Layer 2 trunk ports)	<ul style="list-style-type: none"> • 10-Gigabit Ethernet: 2 • Gigabit Ethernet: 4 • Fast Ethernet: 19 • Ethernet: 100

Table 14-5 STP Default Configuration (continued)

Feature	Default Value
Hello time	2 seconds
Forward delay time	15 seconds
Maximum aging time	20 seconds
Mode	PVST

STP and MST Configuration Guidelines and Restrictions

Follow these guidelines and restrictions when configuring MST:

- Do not disable spanning tree on any VLAN in any of the PVST bridges.
- Do not use PVST bridges as the root of CST.
- Ensure that all PVST spanning tree 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.
- Do not connect switches with access links because access links may partition a VLAN.
- Any MST configuration involving a large number of either existing or new logical VLAN ports should be completed 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 STP

These sections describe how to configure STP on VLANs:

- [Enabling STP, page 14-21](#)
- [Enabling the Extended System ID, page 14-22](#)
- [Configuring the Root Bridge, page 14-23](#)
- [Configuring a Secondary Root Bridge, page 14-24](#)
- [Configuring STP Port Priority, page 14-25](#)
- [Configuring STP Port Cost, page 14-27](#)
- [Configuring the Bridge Priority of a VLAN, page 14-28](#)
- [Configuring the Hello Time, page 14-30](#)
- [Configuring the Forward-Delay Time for a VLAN, page 14-30](#)
- [Configuring the Maximum Aging Time for a VLAN, page 14-31](#)
- [Enabling Rapid-PVST, page 14-31](#)



Note The STP commands described in this chapter can be configured on any LAN port, but they are in effect only on LAN ports configured with the **switchport** keyword.

**Caution**

We do not recommend disabling spanning tree, even in a topology that is free of physical loops. Spanning tree serves as a safeguard against misconfigurations and cabling errors. Do not disable spanning tree in a VLAN without ensuring that there are no physical loops present in the VLAN.

Enabling STP

**Note**

STP is enabled by default on VLAN 1 and on all newly created VLANs.

You can enable STP on a per-VLAN basis. The Catalyst 6500 series switch maintains a separate instance of STP for each VLAN (except on VLANs on which you disable STP).

To enable STP on a per-VLAN basis, perform this task:

Command	Purpose
Step 1 Router(config)# spanning-tree vlan <i>vlan_ID</i>	Enables STP on a per-VLAN basis. The <i>vlan_ID</i> value can be 1 through 4094, except reserved VLANs (see Table 14-5 on page 14-19).
Router(config)# default spanning-tree vlan <i>vlan_ID</i>	Reverts all STP parameters to default values for the specified VLAN.
Router(config)# no spanning-tree vlan <i>vlan_ID</i>	Disables STP on the specified VLAN; see the following Cautions for information regarding this command.
Step 2 Router(config)# end	Exits configuration mode.
Step 3 Router# show spanning-tree vlan <i>vlan_ID</i>	Verifies that STP is enabled.

**Caution**

Do not disable spanning tree on a VLAN unless all switches and bridges in the VLAN have spanning tree disabled. You cannot disable spanning tree on some switches and bridges in a VLAN and leave it enabled on other switches and bridges in the VLAN. This action can have unexpected results because switches and bridges with spanning tree enabled will have incomplete information regarding the physical topology of the network.

**Note**

We do not recommend disabling spanning tree, even in a topology that is free of physical loops. Spanning tree serves as a safeguard against misconfigurations and cabling errors. Do not disable spanning tree in a VLAN without ensuring that there are no physical loops present in the VLAN.

This example shows how to enable STP on VLAN 200:

```
Router# configure terminal
Router(config)# spanning-tree vlan 200
Router(config)# end
Router#
```

**Note**

Because STP is enabled by default, entering a **show running** command to view the resulting configuration does not display the command you entered to enable STP.

This example shows how to verify the configuration:

```
Router# show spanning-tree vlan 200

VLAN0200
  Spanning tree enabled protocol ieee
  Root ID    Priority    32768
              Address     00d0.00b8.14c8
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32768
              Address     00d0.00b8.14c8
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300

  Interface      Role Sts Cost      Prio.Nbr Status
  -----  -----
  Fa4/4          Desg FWD 200000    128.196  P2p
  Fa4/5          Back BLK 200000    128.197  P2p
```

Router#



Note

You must have at least one interface that is active in VLAN 200 to create a VLAN 200 spanning tree. In this example, two interfaces are active in VLAN 200.

Enabling the Extended System ID



Note

The extended system ID is enabled permanently on chassis that support 64 MAC addresses.

You can enable the extended system ID on chassis that support 1024 MAC addresses (see the “[Understanding the Bridge ID](#)” section on page 14-2).

To enable the extended system ID, perform this task:

	Command	Purpose
Step 1	Router(config)# spanning-tree extend system-id	Enables the extended system ID.
	Router(config)# no spanning-tree extend system-id	Disables the extended system ID.
		Note You cannot disable the extended system ID on chassis that support 64 MAC addresses or when you have configured extended range VLANs (see “ STP Default Configuration ” section on page 14-19).
Step 2	Router(config)# end	Exits configuration mode.
Step 3	Router# show spanning-tree vlan vlan_ID	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:

```
Router# configure terminal
Router(config)# spanning-tree extend system-id
Router(config)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show spanning-tree summary | include Extended
Extended system ID is enabled.
```

Configuring the Root Bridge

Catalyst 6500 series switches maintain a separate instance of STP for each active VLAN. A bridge ID, consisting of the bridge priority and the bridge MAC address, is associated with each instance. For each VLAN, the network device with the lowest bridge ID becomes the root bridge for that VLAN.

To configure a VLAN instance to become the root bridge, enter the **spanning-tree vlan *vlan_ID* root** command to modify the bridge priority from the default value (32768) to a significantly lower value.

When you enter the **spanning-tree vlan *vlan_ID* root** command, the switch checks the bridge priority of the current root bridges for each VLAN. When the extended system ID is disabled, the switch sets the bridge priority for the specified VLANs to 8192 if this value will cause the switch to become the root for the specified VLANs. When the extended system ID is enabled, the switch sets the bridge priority for the specified VLANs to 24576 if this value will cause the switch to become the root for the specified VLANs.

If the extended system ID is disabled and if any root bridge for the specified VLANs has a bridge priority lower than 8192, the switch sets the bridge priority for the specified VLANs to 1 less than the lowest bridge priority.

If the extended system ID is enabled and if any root bridge for the specified VLANs has a bridge priority lower than 24576, the switch sets the bridge priority for the specified VLANs to 4096 less than the lowest bridge priority. (4096 is the value of the least significant bit of a 4-bit bridge priority value; see [Table 14-2 on page 14-3](#).)



Note

The **spanning-tree vlan *vlan_ID* root** command fails if the value required to be the root bridge is less than 1.

The **spanning-tree vlan *vlan_ID* root** command can cause the following effects:

- If the extended system ID is disabled, and if all network devices in VLAN 100 have the default priority of 32768, entering the **spanning-tree vlan 100 root primary** command on the switch sets the bridge priority for VLAN 100 to 8192, which causes the switch to become the root bridge for VLAN 100.
- If the extended system ID is enabled, and if all network devices in VLAN 20 have the default priority of 32768, entering the **spanning-tree vlan 20 root primary** command on the switch sets the bridge priority to 24576, which causes the switch to become the root bridge for VLAN 20.



Caution

The root bridge for each instance of STP should be a backbone or distribution switch. Do not configure an access switch as the STP primary root.

Use the **diameter** keyword to specify the Layer 2 network diameter (that is, the maximum number of bridge hops between any two end stations in the Layer 2 network). When you specify the network diameter, the Catalyst 6500 series switch automatically selects an optimal hello time, forward delay time, and maximum age time for a network of that diameter, which can significantly reduce the STP convergence time. You can use the **hello** keyword to override the automatically calculated hello time.



- Note** To preserve a stable STP topology, we recommend that you avoid configuring the hello time, forward delay time, and maximum age time manually after configuring the Catalyst 6500 series switch as the root bridge.

To configure a Catalyst 6500 series switch as the root bridge, perform this task:

Command	Purpose
Step 1 Router(config)# spanning-tree vlan <i>vlan_ID</i> root primary [diameter <i>hops</i> [hello-time <i>seconds</i>]]	Configures a Catalyst 6500 series switch as the root bridge. The <i>vlan_ID</i> value can be 1 through 4094, except reserved VLANs (see Table 14-5 on page 14-19).
Router(config)# no spanning-tree vlan <i>vlan_ID</i> root	Clears the root bridge configuration.
Step 2 Router(config)# end	Exits configuration mode.

This example shows how to configure the Catalyst 6500 series switch as the root bridge for VLAN 10, with a network diameter of 4:

```
Router# configure terminal
Router(config)# spanning-tree vlan 10 root primary diameter 4
Router(config)# end
Router#
```

Configuring a Secondary Root Bridge

When you configure a Catalyst 6500 series switch as the secondary root, the STP bridge priority is modified from the default value (32768) so that the switch is likely to become the root bridge for the specified VLANs if the primary root bridge fails (assuming the other network devices in the network use the default bridge priority of 32768).

If the extended system ID is enabled, STP sets the bridge priority to 28672. If the extended system ID is disabled, STP sets the bridge priority to 16384.

You can run this command on more than one Catalyst 6500 series switch to configure multiple backup root bridges. Use the same network diameter and hello time values as you used when configuring the primary root bridge.

To configure a Catalyst 6500 series switch as the secondary root bridge, perform this task:

Command	Purpose
Step 1 Router(config)# [no] spanning-tree vlan <i>vlan_ID</i> root secondary [diameter <i>hops</i> [hello-time seconds]]	Configures a Catalyst 6500 series switch as the secondary root bridge. The <i>vlan_ID</i> value can be 1 through 4094, except reserved VLANs (see Table 10-1 on page 10-2).
Router(config)# no spanning-tree vlan <i>vlan_ID</i> root	Clears the root bridge configuring.
Step 2 Router(config)# end	Exits configuration mode.

This example shows how to configure the Catalyst 6500 series switch as the secondary root bridge for VLAN 10, with a network diameter of 4:

```
Router# configure terminal
Router(config)# spanning-tree vlan 10 root secondary diameter 4
Router(config)# end
Router#
```

Configuring STP Port Priority

If a loop occurs, STP considers port priority when selecting a LAN port to put into the forwarding state. You can assign higher priority values to LAN ports that you want STP to select first and lower priority values to LAN ports that you want STP to select last. If all LAN ports have the same priority value, STP puts the LAN port with the lowest LAN port number in the forwarding state and blocks other LAN ports. The possible priority range is 0 through 240 (default 128), configurable in increments of 16.

Cisco IOS uses the port priority value when the LAN port is configured as an access port and uses VLAN port priority values when the LAN port is configured as a trunk port.

To configure the STP port priority of a Layer 2 LAN interface, perform this task:

Command	Purpose
Step 1 Router(config)# interface {{type ¹ slot/port} {port-channel <i>port_channel_number</i> }}	Selects an interface to configure.
Step 2 Router(config-if)# spanning-tree port-priority <i>port_priority</i>	Configures the port priority for the LAN interface. The <i>port_priority</i> value can be from 1 to 252 in increments of 4.
Router(config-if)# no spanning-tree port-priority	Reverts to the default port priority value.
Step 3 Router(config-if)# spanning-tree vlan <i>vlan_ID</i> port-priority <i>port_priority</i>	Configures the VLAN port priority for the LAN interface. The <i>port_priority</i> value can be from 1 to 252 in increments of 4. The <i>vlan_ID</i> value can be 1 through 4094, except reserved VLANs (see Table 10-1 on page 10-2).
Router(config-if)# [no] spanning-tree vlan <i>vlan_ID</i> port-priority	Reverts to the default VLAN port priority value.
Step 4 Router(config-if)# end	Exits configuration mode.

Configuring STP

Command	Purpose
Step 5 Router# show spanning-tree interface {type ¹ slot/port} {port-channel port_channel_number} Router# show spanning-tree vlan vlan_ID	Verifies the configuration.

1. type = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

This example shows how to configure the STP port priority of Fast Ethernet port 4/4:

```
Router# configure terminal
Router(config)# interface fastethernet 4/4
Router(config-if)# spanning-tree port-priority 160
Router(config-if)# end
Router#
```

This example shows how to verify the configuration of Fast Ethernet port 4/4:

```
Router# show spanning-tree interface fastethernet 4/4
Vlan      Role Sts Cost      Prio.Nbr Status
-----  -----
VLAN0001    Back BLK 200000    160.196  P2p
VLAN0006    Back BLK 200000    160.196  P2p
...
VLAN0198    Back BLK 200000    160.196  P2p
VLAN0199    Back BLK 200000    160.196  P2p
VLAN0200    Back BLK 200000    160.196  P2p
Router#
```

Fastethernet 4/4 is a trunk. Several VLANs are configured and active as shown in the example. The port priority configuration applies to all VLANs on this interface.



Note The **show spanning-tree interface** command only displays information if the port is connected and operating. If this condition is not met, enter a **show running-config interface** command to verify the configuration.

This example shows how to configure the VLAN port priority of Fast Ethernet port 4/4:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fastEthernet 4/4
Router(config-if)# spanning-tree vlan 200 port-priority 64
Router(config-if)# ^Z
Router#
```

The configuration entered in the example only applies to VLAN 200. All VLANs other than 200 still have a port priority of 160.

This example shows how to verify the configuration:

```
Router# show spanning-tree interface fastethernet 4/4
Vlan      Role Sts Cost      Prio.Nbr Status
-----  -----
VLAN0001    Back BLK 200000    160.196  P2p
VLAN0006    Back BLK 200000    160.196  P2p
...
VLAN0199    Back BLK 200000    160.196  P2p
VLAN0200    Desg FWD 200000    64.196  P2p
Router#
```

You also can display spanning tree information for VLAN 200 using the following command:

```
Router# show spanning-tree vlan 200 interface fastEthernet 4/4
Interface      Role Sts Cost      Prio.Nbr Status
-----        Desg Lrn 200000      64.196   P2p
Fa4/4
```

Configuring STP Port Cost

The STP port path cost default value is determined from the media speed of a LAN interface. If a loop occurs, STP considers port cost when selecting a LAN interface to put into the forwarding state. You can assign lower cost values to LAN interfaces that you want STP to select first and higher cost values to LAN interfaces that you want STP to select last. If all LAN interfaces have the same cost value, STP puts the LAN interface with the lowest LAN interface number in the forwarding state and blocks other LAN interfaces. The possible cost range is 0 through 200000000 (the default is media specific).

STP uses the port cost value when the LAN interface is configured as an access port and uses VLAN port cost values when the LAN interface is configured as a trunk port.

To configure the STP port cost of a Layer 2 LAN interface, perform this task:

Command	Purpose
Step 1 Router(config)# interface {{type¹ slot/port} {port-channel port_channel_number}}	Selects an interface to configure.
Step 2 Router(config-if)# spanning-tree cost port_cost	Configures the port cost for the LAN interface. The <i>port_cost</i> value can be from 1 to 200000000 (1 to 65535 in Release 12.1(2)E and earlier releases).
Router(config-if)# no spanning-tree cost	Reverts to the default port cost.
Step 3 Router(config-if)# [no] spanning-tree vlan vlan_ID cost port_cost	Configures the VLAN port cost for the LAN interface. The <i>port_cost</i> value can be from 1 to 200000000. The <i>vlan_ID</i> value can be 1 through 4094, except reserved VLANs (see Table 10-1 on page 10-2).
Step 4 Router(config-if)# no spanning-tree vlan vlan_ID cost	Reverts to the default VLAN port cost.
Step 5 Router(config-if)# end	Exits configuration mode.
Step 6 Router# show spanning-tree interface {type¹ slot/port} {port-channel port_channel_number} Router# show spanning-tree vlan vlan_ID	Verifies the configuration.

1. *type* = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

This example shows how to change the STP port cost of Fast Ethernet port 4/4:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fastEthernet 4/4
Router(config-if)# spanning-tree cost 1000
Router(config-if)# ^Z
Router#
```

This example shows how to verify the configuration:

```
Router# show spanning-tree interface fastEthernet 4/4
Vlan      Role Sts Cost      Prio.Nbr Status
-----        Desg Lrn 200000      64.196   P2p
VLAN0001    Back BLK 1000      160.196   P2p
```

Configuring STP

```
VLAN0006      Back BLK 1000    160.196  P2p
VLAN0007      Back BLK 1000    160.196  P2p
VLAN0008      Back BLK 1000    160.196  P2p
VLAN0009      Back BLK 1000    160.196  P2p
VLAN0010      Back BLK 1000    160.196  P2p
Router#
```

This example shows how to configure the port priority at an individual port VLAN cost for VLAN 200:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fastEthernet 4/4
Router(config-if)# spanning-tree vlan 200 cost 2000
Router(config-if)# ^Z
Router#
```

This example shows how to verify the configuration:

```
Router# show spanning-tree vlan 200 interface fastEthernet 4/4
Interface      Role Sts Cost      Prio.Nbr Status
-----        -----
Fa4/4          Desg FWD 2000    64.196  P2p
```



Note In the following output other VLANs (VLAN 1 for example) have not been affected by this configuration.

```
Router# show spanning-tree vlan 1 interface fastEthernet 4/4
Interface      Role Sts Cost      Prio.Nbr Status
-----        -----
Fa4/4          Back BLK 1000    160.196  P2p
Router#
```



Note The **show spanning-tree** command only displays information for ports that are in link-up operative state and are appropriately configured for DTP. If these conditions are not met, you can enter a **show running-config** command to confirm the configuration.

Configuring the Bridge Priority of a VLAN



Note Be careful when using this command. For most situations, 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 STP bridge priority of a VLAN when the extended system ID is disabled, perform this task:

Command	Purpose
Step 1 Router(config)# spanning-tree vlan <i>vlan_ID</i> priority <i>bridge_priority</i>	Configures the bridge priority of a VLAN when the extended system ID is disabled. The <i>bridge_priority</i> value can be from 1 to 65535. The <i>vlan_ID</i> value can be 1 through 4094, except reserved VLANs (see Table 10-1 on page 10-2).
Router(config)# no spanning-tree vlan <i>vlan_ID</i> priority	Reverts to the default bridge priority value.
Step 2 Router(config)# end	Exits configuration mode.
Step 3 Router# show spanning-tree vlan <i>vlan_ID</i> bridge [detail]	Verifies the configuration.

To configure the STP bridge priority of a VLAN when the extended system ID is enabled, perform this task:

Command	Purpose
Step 1 Router(config)# [no] spanning-tree vlan <i>vlan_ID</i> priority {0 4096 8192 12288 16384 20480 24576 28672 32768 36864 40960 45056 49152 53248 57344 61440}	Configures the bridge priority of a VLAN when the extended system ID is enabled. The <i>vlan_ID</i> value can be 1 through 4094, except reserved VLANs (see Table 10-1 on page 10-2).
Router(config)# no spanning-tree vlan <i>vlan_ID</i> priority	Reverts to the default bridge priority value.
Step 2 Router(config)# end	Exits configuration mode.
Step 3 Router# show spanning-tree vlan <i>vlan_ID</i> bridge [detail]	Verifies the configuration.

This example shows how to configure the bridge priority of VLAN 200 to 33792 when the extended system ID is disabled:

```
Router# configure terminal
Router(config)# spanning-tree vlan 200 priority 33792
Router(config)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show spanning-tree vlan 200 bridge
          Hello Max Fwd
          Bridge ID      Time  Age Delay Protocol
Vlan
-----  -----
VLAN200      33792 0050.3e8d.64c8    2   20   15  ieee
Router#
```

Configuring the Hello Time



Note Be careful when using this command. For most situations, we recommend that you use the **spanning-tree vlan *vlan_ID* root primary** and **spanning-tree vlan *vlan_ID* root secondary** commands to modify the hello time.

To configure the STP hello time of a VLAN, perform this task:

Command	Purpose
Step 1 Router(config)# spanning-tree vlan <i>vlan_ID</i> hello-time <i>hello_time</i>	Configures the hello time of a VLAN. The <i>hello_time</i> value can be from 1 to 10 seconds. The <i>vlan_ID</i> value can be 1 through 4094, except reserved VLANs (see Table 10-1 on page 10-2).
	Reverts to the default hello time.
Step 2 Router(config)# end	Exits configuration mode.
Step 3 Router# show spanning-tree vlan <i>vlan_ID</i> bridge [detail]	Verifies the configuration.

This example shows how to configure the hello time for VLAN 200 to 7 seconds:

```
Router# configure terminal
Router(config)# spanning-tree vlan 200 hello-time 7
Router(config)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show spanning-tree vlan 200 bridge
          Hello Max Fwd
Vlan      Bridge ID      Time Age Delay Protocol
-----  -----
VLAN200   49152 0050.3e8d.64c8    7  20    15  ieee
Router#
```

Configuring the Forward-Delay Time for a VLAN

To configure the STP forward delay time for a VLAN, perform this task:

Command	Purpose
Step 1 Router(config)# spanning-tree vlan <i>vlan_ID</i> forward-time <i>forward_time</i>	Configures the forward time of a VLAN. The <i>forward_time</i> value can be from 4 to 30 seconds. The <i>vlan_ID</i> value can be 1 through 4094, except reserved VLANs (see Table 10-1 on page 10-2).
	Reverts to the default forward time.
Step 2 Router(config)# end	Exits configuration mode.
Step 3 Router# show spanning-tree vlan <i>vlan_ID</i> bridge [detail]	Verifies the configuration.

This example shows how to configure the forward delay time for VLAN 200 to 21 seconds:

```
Router# configure terminal
Router(config)# spanning-tree vlan 200 forward-time 21
Router(config)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show spanning-tree vlan 200 bridge
          Hello Max Fwd
Vlan      Bridge ID     Time Age Delay Protocol
-----  -----
VLAN200    49152 0050.3e8d.64c8   2   20   21  ieee
Router#
```

Configuring the Maximum Aging Time for a VLAN

To configure the STP maximum aging time for a VLAN, perform this task:

	Command	Purpose
Step 1	Router(config)# spanning-tree vlan <i>vlan_ID</i> max-age <i>max_age</i>	Configures the maximum aging time of a VLAN. The <i>max_age</i> value can be from 6 to 40 seconds. The <i>vlan_ID</i> value can be 1 through 4094, except reserved VLANs (see Table 10-1 on page 10-2).
	Router(config)# no spanning-tree vlan <i>vlan_ID</i> max-age	Reverts to the default maximum aging time.
Step 2	Router(config)# end	Exits configuration mode.
Step 3	Router# show spanning-tree vlan <i>vlan_ID</i> bridge [detail]	Verifies the configuration.

This example shows how to configure the maximum aging time for VLAN 200 to 36 seconds:

```
Router# configure terminal
Router(config)# spanning-tree vlan 200 max-age 36
Router(config)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show spanning-tree vlan 200 bridge
          Hello Max Fwd
Vlan      Bridge ID     Time Age Delay Protocol
-----  -----
VLAN200    49152 0050.3e8d.64c8   2   36   15  ieee
Router#
```

Enabling Rapid-PVST

Rapid-PVST uses the existing PVST+ framework for configuration and interaction with other features. It also supports some of the PVST+ extensions.

To enable Rapid-PVST mode on the switch, enter the **spanning-tree mode rapid-pvst** command in privileged mode. To configure the switch in Rapid-PVST mode, see the [“Configuring STP” section on page 14-20](#).

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, enter 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. An MSTP switch can also detect that a port is at the boundary of a region when it receives a legacy BPDU, or an MST BPDU (version 3) associated with a different region, or an RST BPDU (version 2).

However, the switch does not automatically revert to the MSTP mode if it no longer receives 802.1D BPDUs because it cannot determine whether 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 (force the renegotiation with neighboring switches) on the entire switch, you can use the **clear spanning-tree detected-protocols** privileged EXEC command. To restart the protocol migration process on a specific interface, enter the **clear spanning-tree detected-protocols interface *interface-id*** privileged EXEC command.

Configuring IEEE 802.1s MST

Release 12.2(14)SX and later releases support MST. These sections describe how to configure MST:

- [Enabling MST, page 14-32](#)
- [Displaying MST Configurations, page 14-34](#)
- [Configuring MST Instance Parameters, page 14-37](#)
- [Configuring MST Instance Port Parameters, page 14-38](#)
- [Restarting Protocol Migration, page 14-38](#)

Enabling MST

To enable and configure MST on the switch, perform these tasks in privileged mode:

Command	Purpose
Step 1 Router# show spanning-tree mst configuration	Displays the current MST configuration.
Step 2 Router(config)# spanning-tree mode mst	Configures MST mode.
Step 3 Router(config)# spanning-tree mst configuration Router(config)# no spanning-tree mst configuration	Configures the MST region by entering the MST configuration submode. Clears the MST configuration.

Command	Purpose
Step 4 Router(config-mst)# show current	Displays the current MST configuration from within the MST configuration submode
Step 5 Router(config-mst)# name name revision revision_number instance instance_number vlan vlan_range	Enters the MST configuration.
Step 6 Router(config-mst)# no instance instance_number	(Optional) Unmaps all VLANs that were mapped to an instance.
Step 7 Router(config-mst)# no instance instance_number vlan vlan_number	(Optional) Unmaps a VLAN from an instance.
Step 8 Router(config-mst)# end	Applies the configuration and exit configuration mode.
Step 9 Router# show spanning-tree mst config	Shows the MST configuration from the global configuration mode.

These examples show how to enable MST:

```

Router# show spanning-tree mst configuration
% Switch is not in mst mode
Name      []
Revision   0
Instance  Vlans mapped
-----  -----
0          1-4094
-----
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# spanning-tree mode mst

Router(config)# spanning-tree mst configuration

Router(config-mst)# show current
Current MST configuration
Name      []
Revision   0
Instance  Vlans mapped
-----  -----
0          1-4094
-----
Router(config-mst)# name cisco
Router(config-mst)# revision 2
Router(config-mst)# instance 1 vlan 1
Router(config-mst)# instance 2 vlan 1-1000
Router(config-mst)# show pending
Pending MST configuration
Name      [cisco]
Revision  2
Instance  Vlans mapped
-----  -----
0          1001-4094
2          1-1000
-----
Router(config-mst)# no instance 2
Router(config-mst)# show pending
Pending MST configuration
Name      [cisco]
Revision  2
Instance  Vlans mapped
-----  -----
0          1-4094
-----
```

■ Configuring IEEE 802.1s MST

```

Router(config-mst)# instance 1 vlan 2000-3000
Router(config-mst)# no instance 1 vlan 1500
Router(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
-----
Router(config)# exit
Router(config)# no spanning-tree mst configuration
Router(config)# do show spanning-tree mst configuration
Name      []
Revision  0
Instance  Vlans mapped
-----
0        1-4094
-----

```

Displaying MST Configurations

To display MST configurations, perform these tasks in MST mode:

	Command	Purpose
Step 1	Router# show spanning-tree mst configuration	Displays the active configuration.
Step 2	Router# show spanning-tree mst [detail]	Displays information about the MST instances currently running.
Step 3	Router# show spanning-tree mst instance-id [detail]	Displays information about a specific MST instance.
Step 4	Router# show spanning-tree mst interface interface name [detail]	Displays information for a given port.
Step 5	Router# show spanning-tree mst number interface interface name [detail]	Displays MST information for a given port and a given instance.
Step 6	Router# show spanning-tree mst [x] [interface Y] detail	Displays detailed MST information.
Step 7	Router# show spanning-tree vlan vlan_ID	Displays VLAN information in MST mode.

These examples show how to display spanning tree VLAN configurations in MST mode:

```

Router(config)# spanning-tree mst configuration
Router(config-mst)# instance 1 vlan 1-10
Router(config-mst)# name cisco
Router(config-mst)# revision 1
Router(config-mst)# ^Z

Router# show spanning-tree mst configuration
Name      [cisco]
Revision  1
Instance  Vlans mapped
-----
0        11-4094
1        1-10
-----

```

```
Router# 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	160.196	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	160.196	P2p
Fa4/5	Desg	FWD	200000	128.197	P2p
Fa4/48	Boun	FWD	200000	128.240	P2p Bound(STP)

```
Router# 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	160.196	P2p
Fa4/5	Desg	FWD	200000	128.197	P2p
Fa4/48	Boun	FWD	200000	128.240	P2p Bound(STP)

```
Router# 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	160.196	11-4094
1	Back	BLK	1000	160.196	1-10

```
Router# 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	160.196	1-10

Configuring IEEE 802.1s MST

```

Router# 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       160.196 priority   160 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

Router# 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     160.196  P2p
  Fa4/5          Desg FWD 200000   128.197  P2p

Router# 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
Router#

```

Configuring MST Instance Parameters

To configure MST instance parameters, perform these tasks:

Command	Purpose
Step 1 Router(config)# spanning-tree mst X priority Y	Configures the priority for an MST instance.
Step 2 Router(config)# spanning-tree mst X root [primary secondary]	Configures the bridge as root for an MST instance.
Step 3 Router# show spanning-tree mst	Verifies the configuration.

This example shows how to configure MST instance parameters:

```

Router(config)# spanning-tree mst 1 priority ?
<0-61440> bridge priority in increments of 4096

Router(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

Router(config)# spanning-tree mst 1 priority 49152
Router(config)#

Router(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
Router(config)# ^z
Router#


Router# 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     160.196  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)

Router#

```

Configuring MST Instance Port Parameters

To configure MST instance port parameters, perform these tasks:

Command	Purpose
Step 1 Router(config-if)# spanning-tree mst x cost y	Configures the MST instance port cost.
Step 2 Router(config-if)# spanning-tree mst x port-priority y	Configures the MST instance port priority.
Step 3 Router# show spanning-tree mst x interface y	Verifies the configuration.

This example shows how to configure MST instance port parameters:

```
Router(config)# interface fastEthernet 4/4
Router(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

Router(config-if)# spanning-tree mst 1 cost 1234567
Router(config-if)# spanning-tree mst 1 port-priority 240
Router(config-if)# ^z

Router# 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

Router#
```

Restarting Protocol Migration

A switch running both MSTP and RSTP supports a built-in protocol migration mechanism 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. An MSTP switch can also detect that a port is at the boundary of a region when it receives a legacy BPDU, an MST BPDU (version 3) associated with a different region, or an RST BPDU (version 2).

However, the switch does not automatically revert to the MSTP mode if it no longer receives 802.1D BPDUs because it cannot determine whether 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 (force the renegotiation with neighboring switches) on the entire switch, you can use the **clear spanning-tree detected-protocols** privileged EXEC command. Use the **clear spanning-tree detected-protocols interface *interface-id*** privileged EXEC command to restart the protocol migration process on a specific interface.

This example shows how to restart protocol migration:

```
Router# clear spanning-tree detected-protocols interface fastEthernet 4/4
Router#
```




CHAPTER

15

Configuring Optional STP Features

This chapter describes how to configure optional STP features.



Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication.

This chapter consists of these sections:

- [Understanding How PortFast Works, page 15-2](#)
- [Understanding How BPDU Guard Works, page 15-2](#)
- [Understanding How PortFast BPDU Filtering Works, page 15-2](#)
- [Understanding How UplinkFast Works, page 15-3](#)
- [Understanding How BackboneFast Works, page 15-4](#)
- [Understanding How EtherChannel Guard Works, page 15-6](#)
- [Understanding How Root Guard Works, page 15-6](#)
- [Understanding How Loop Guard Works, page 15-6](#)
- [Enabling PortFast, page 15-8](#)
- [Enabling PortFast BPDU Filtering, page 15-10](#)
- [Enabling BPDU Guard, page 15-11](#)
- [Enabling UplinkFast, page 15-12](#)
- [Enabling BackboneFast, page 15-13](#)
- [Enabling EtherChannel Guard, page 15-14](#)
- [Enabling Root Guard, page 15-14](#)
- [Enabling Loop Guard, page 15-15](#)



Note

For information on configuring the spanning tree protocol (STP), see [Chapter 14, “Configuring STP and IEEE 802.1s MST.”](#)

Understanding How PortFast Works

STP PortFast causes a Layer 2 LAN interface configured as an 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, instead of waiting for STP to converge. Interfaces connected to a single workstation or server should not receive bridge protocol data units (BPDUs). When configured for PortFast, a port is still running the spanning tree protocol. A PortFast enabled port can immediately transition to the blocking state if necessary (this could happen on receipt of a superior BPDU). PortFast can be enabled on trunk ports. PortFast can have an operational value that is different from the configured value.

**Caution**

Because the purpose of PortFast is to minimize the time that access ports must wait for STP to converge, it should only be used on access ports. If you enable PortFast on a port connected to a switch, you might create a temporary bridging loop.

Understanding How BPDU Guard Works

When enabled on a port, BPDU Guard shuts down a port that receives a BPDU. When configured globally, BPDU Guard is only effective on ports in the operational PortFast state. In a valid configuration, PortFast Layer 2 LAN interfaces do not receive BPDUs. Reception of a BPDU by a PortFast Layer 2 LAN 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 Layer 2 LAN interface back in service. BPDU Guard can be configured at the interface level. When configured at the interface level, BPDU Guard shuts the port down as soon as the port receives a BPDU, regardless of the PortFast configuration.

**Note**

When enabled globally, BPDU Guard applies to all interfaces that are in an operational PortFast state.

Understanding How PortFast BPDU Filtering Works

PortFast BPDU filtering 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 as the port will ignore any BPDU it receives and go to forwarding.

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 15-10), then 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 15-1](#) 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 15-1 PortFast BPDU Filtering Port Configurations

Per-Port Configuration	Global Configuration	PortFast State	PortFast BPDU Filtering State
Default	Enable	Enable	Enable ¹
Default	Enable	Disable	Disable
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.

Understanding How UplinkFast Works

UplinkFast provides fast convergence after a direct link failure and achieves load balancing between redundant Layer 2 links using uplink groups. An uplink group is a set of Layer 2 LAN 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.

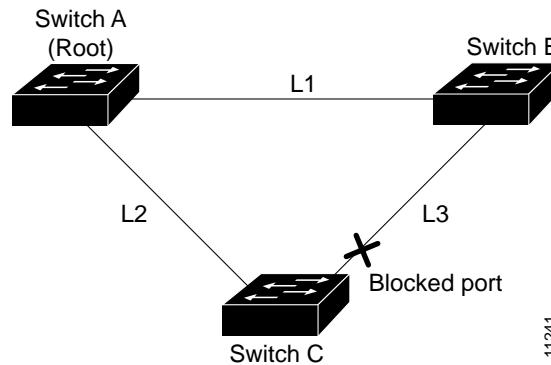


Note

UplinkFast is most useful in wiring-closet switches. This feature may not be useful for other types of applications.

[Figure 15-1](#) shows an example topology with no link failures. Switch A, the root bridge, is connected directly to Switch B over link L1 and to Switch C over link L2. The Layer 2 LAN interface on Switch C that is connected directly to Switch B is in the blocking state.

Figure 15-1 UplinkFast Example Before Direct Link Failure

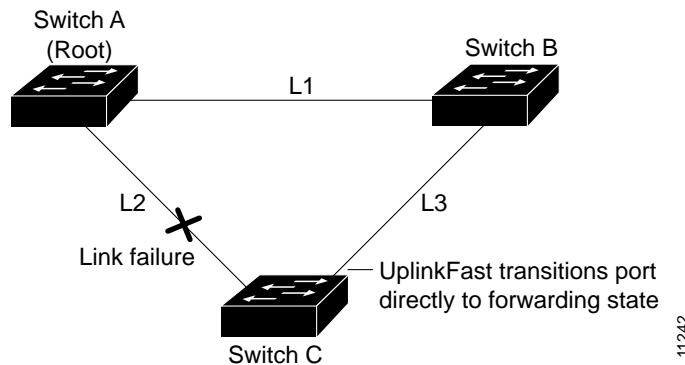


11241

■ Understanding How BackboneFast Works

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 15-2](#). This switchover takes approximately one to five seconds.

Figure 15-2 UplinkFast Example After Direct Link Failure



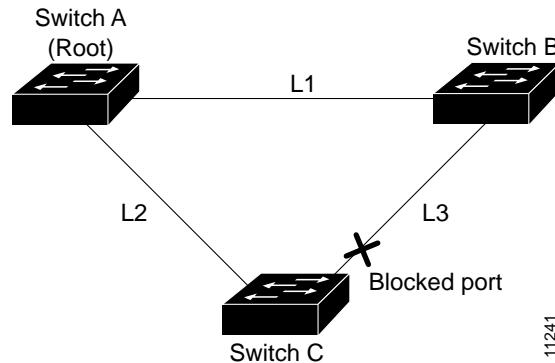
Understanding How BackboneFast Works

BackboneFast is initiated when a root port or blocked port on a network device receives inferior BPDUs from its designated bridge. An inferior BPDU identifies one network device as both the root bridge and the designated bridge. When a network device receives an inferior BPDU, it indicates that a link to which the network device is not directly connected (an *indirect* link) has failed (that is, the designated bridge has lost its connection to the root bridge). Under normal STP rules, the network device ignores inferior BPDUs for the configured maximum aging time, as specified by the STP **max-age** command.

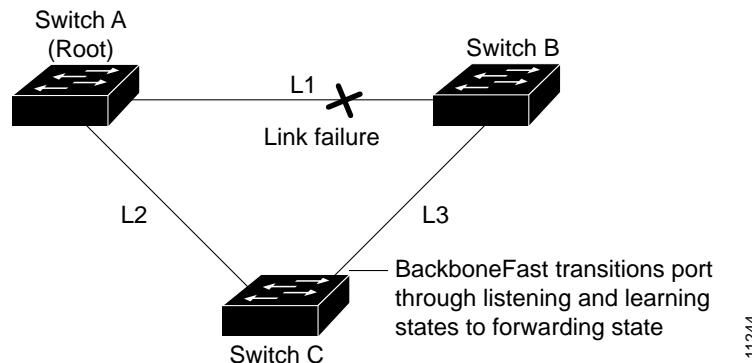
The network device tries to determine if it has an alternate path to the root bridge. If the inferior BPDU arrives on a blocked port, the root port and other blocked ports on the network device become alternate paths to the root bridge. (Self-looped ports are not considered alternate paths to the root bridge.) If the inferior BPDU arrives on the root port, all blocked ports become alternate paths to the root bridge. If the inferior BPDU arrives on the root port and there are no blocked ports, the network device assumes that it has lost connectivity to the root bridge, causes the maximum aging time on the root to expire, and becomes the root bridge according to normal STP rules.

If the network device has alternate paths to the root bridge, it uses these alternate paths to transmit a new kind of Protocol Data Unit (PDU) called the Root Link Query PDU. The network device sends the Root Link Query PDU out all alternate paths to the root bridge. If the network device determines that it still has an alternate path to the root, it causes the maximum aging time to expire on the ports on which it received the inferior BPDU. If all the alternate paths to the root bridge indicate that the network device has lost connectivity to the root bridge, the network device causes the maximum aging times on the ports on which it received an inferior BPDU to expire. If one or more alternate paths can still connect to the root bridge, the network device makes all ports on which it received an inferior BPDU its designated ports and moves them out of the blocking state (if they were in the blocking state), through the listening and learning states, and into the forwarding state.

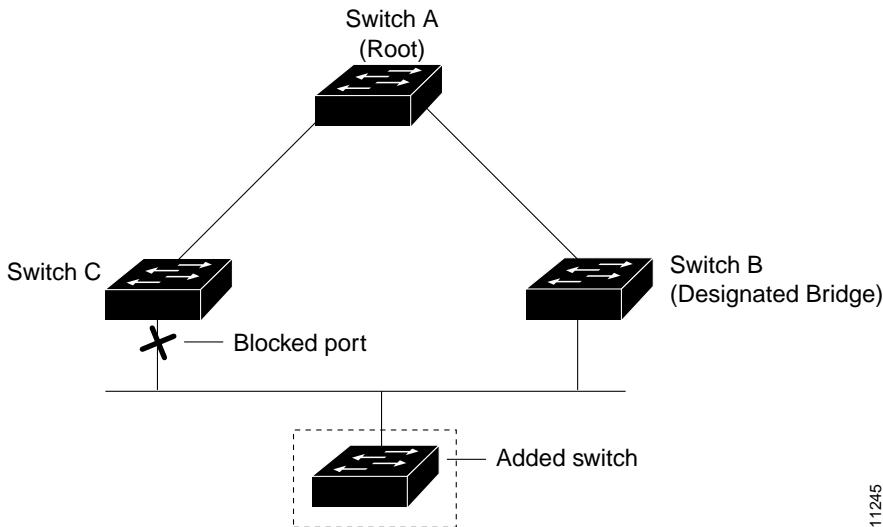
[Figure 15-3](#) shows an example topology with no link failures. Switch A, the root bridge, connects directly to Switch B over link L1 and to Switch C over link L2. The Layer 2 LAN interface on Switch C that connects directly to Switch B is in the blocking state.

Figure 15-3 BackboneFast Example Before Indirect Link Failure

If link L1 fails, 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 bridge over L1, it detects the failure and elects itself the root and begins sending BPDUs to Switch C indicating itself as the root. When Switch C receives the inferior BPDUs from Switch B, Switch C infers that an indirect failure has occurred. At that point, BackboneFast allows the blocked port on Switch C to move immediately to the listening state without waiting for the maximum aging time for the port to expire. BackboneFast then transitions the Layer 2 LAN 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 15-4](#) shows how BackboneFast reconfigures the topology to account for the failure of link L1.

Figure 15-4 BackboneFast Example After Indirect Link Failure

If a new network device is introduced into a shared-medium topology as shown in [Figure 15-5](#), BackboneFast is not activated because the inferior BPDUs did not come from the recognized designated bridge (Switch B). The new network device begins sending inferior BPDUs that indicate that it is the root bridge. However, the other network devices ignore these inferior BPDUs and the new network device learns that Switch B is the designated bridge to Switch A, the root bridge.

Figure 15-5 Adding a Network Device in a Shared-Medium Topology

11245

Understanding How EtherChannel Guard Works

EtherChannel guard detects a misconfigured EtherChannel where interfaces on the Catalyst 6500 series switch are configured as an EtherChannel while interfaces on the other device are not or not all the interfaces on the other device are in the same EtherChannel.

In response to misconfiguration detected on the other device, EtherChannel guard puts interfaces on the Catalyst 6500 series switch into the errdisabled state.

Understanding How Root Guard Works

The STP root guard feature prevents a port from becoming root port or blocked port. If a port configured for root guard receives a superior BPDU, the port immediately goes to the root-inconsistent (blocked) state.

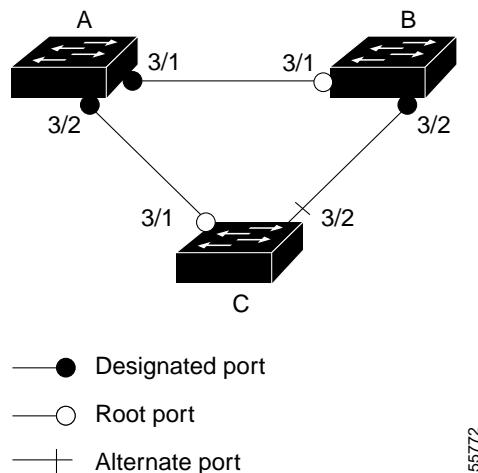
Understanding How Loop Guard Works

Loop guard helps prevent bridging loops that could occur because of a uni-directional link failure on a point-to-point link. When enabled globally, the 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 loop-inconsistent blocking state, assuming there is a physical link error on this port. The port recovers from this loop-inconsistent 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 15-6](#) shows loop guard in a triangle switch configuration.

Figure 15-6 Triangle Switch Configuration with Loop Guard



55772

[Figure 15-6](#) 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:

- You cannot enable loop guard on PortFast-enabled or dynamic VLAN ports.
- You cannot 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 be always designated as 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.

Enabling PortFast

- 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.

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, perform this task:

	Command	Purpose
Step 1	Router(config)# interface {type ¹ slot/port} {port-channel port_channel_number}	Selects an interface to configure.
Step 2	Router(config-if)# spanning-tree portfast	Enables PortFast on a Layer 2 access port connected to a single workstation or server.
Step 3	Router(config-if)# spanning-tree portfast default	Disables PortFast.
Step 4	Router(config-if)# end	Exits configuration mode.
Step 5	Router# show running interface {type ¹ slot/port} {port-channel port_channel_number}	Verifies the configuration.

1. type = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

This example shows how to enable PortFast on Fast Ethernet interface 5/8:

```
Router# configure terminal
Router(config)# interface fastethernet 5/8
Router(config-if)# spanning-tree portfast
Router(config-if)# end
Router#
```

This example shows how to verify the configuration:

```
Router# 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

Router#
```

To enable the default PortFast configuration, perform this task:

Command	Purpose
Step 1 Router(config)# spanning-tree portfast default	Configures the PortFast default.
Step 2 Router(config)# show spanning-tree summary totals	Verifies the global configuration.
Step 3 Router(config)# show spanning-tree interface x detail	Verifies the effect on a specific port.
Step 4 Router(config-if)# spanning-tree portfast trunk	Enables the PortFast trunk on a port
Step 5 Router# show spanning-tree interface fastEthernet x detail	Verifies the configuration.

This example shows how to enable the default PortFast configuration:

```

Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# spanning-tree portfast default
Router(config)# ^Z

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 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
-----  -----  -----  -----  -----  -----
VLAN0001          0        0        0        1        1
VLAN0010          0        0        0        2        2
-----  -----  -----  -----  -----  -----
2 vlans           0        0        0        3        3
Router#
Router# 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 default
  Link type is point-to-point by default
  BPDU:sent 10, received 0

Router(config-if)# spanning-tree portfast trunk
%Warning:portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

Router(config-if)# ^Z

```

■ Enabling PortFast BPDU Filtering

```
Router# 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:sent 30, received 0
Router#
```

Enabling PortFast BPDU Filtering

These sections describe how to configure PortFast BPDU filtering on the switch:

To enable PortFast BPDU filtering globally, perform this task:

	Command	Purpose
Step 1	Router(config)# spanning-tree portfast bpdulfILTER default	Enables BPDU filtering globally on the switch.
Step 2	Router# show spanning-tree summary totals	Verifies the configuration.

BPDU filtering is set to default on each port. This example shows how to enable PortFast BPDU filtering on the port and verify the configuration in PVST+ mode:



Note For PVST+ information, see [Chapter 14, “Configuring STP and IEEE 802.1s MST.”](#)

```
Router(config)# spanning-tree portfast bpdulfILTER default
Router(config)# ^z

Router# 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
Router#
```

To enable PortFast BPDU filtering on a nontrunking port, perform this task:

Command	Purpose
Step 1 Router(config)# interface fastEthernet 4/4	Selects the interface to configure.
Step 2 Router(config-if)# spanning-tree bpdufilter enable	Enables BPDU filtering.
Step 3 Router# show spanning-tree interface fastEthernet 4/4	Verifies the configuration.

This example shows how to enable PortFast BPDU filtering on a nontrunking port:

```
Router(config)# interface fastEthernet 4/4
Router(config-if)# spanning-tree bpdufilter enable
Router(config-if)# ^Z

Router# show spanning-tree interface fastEthernet 4/4

Vlan          Role Sts Cost      Prio.Nbr Status
-----  -----
VLAN0010      Desg FWD 1000    160.196  Edge P2p
Router# show spanning-tree interface fastEthernet 4/4 detail
Router# 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
Router#
```

Enabling BPDU Guard

To enable BPDU Guard globally, perform this task:

Command	Purpose
Step 1 Router(config)# spanning-tree portfast bpduguard default	Enables BPDU Guard globally.
Router(config)# no spanning-tree portfast bpduguard default	Disables BPDU Guard globally.
Step 2 Router(config)# end	Exits configuration mode.
Step 3 Router# show spanning-tree summary totals	Verifies the configuration.

This example shows how to enable BPDU Guard:

```
Router# configure terminal
Router(config)# spanning-tree portfast bpduguard
Router(config)# end
Router#
```

■ Enabling UplinkFast

This example shows how to verify the configuration:

```
Router# show spanning-tree summary totals default
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
Router#
```

Enabling UplinkFast

UplinkFast increases the bridge priority to 49152 and adds 3000 to the STP port cost of all Layer 2 LAN interfaces on the Catalyst 6500 series switch, decreasing the probability that the switch will become the root bridge. The *max_update_rate* value represents the number of multicast packets transmitted per second (the default is 150 packets per second). 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 Catalyst 6500 series switch. You cannot configure UplinkFast on an individual VLAN.

To enable UplinkFast, perform this task:

	Command	Purpose
Step 1	Router(config)# spanning-tree uplinkfast [max-update-rate <i>max_update_rate</i>]	Enables UplinkFast.
	Router(config)# no spanning-tree uplinkfast max-update-rate	Reverts to the default rate.
	Router(config)# no spanning-tree uplinkfast	Disables UplinkFast.
Step 2	Router(config)# end	Exits configuration mode.
Step 3	Router# show spanning-tree vlan <i>vlan_ID</i>	Verifies that UplinkFast is enabled.

This example shows how to enable UplinkFast with an update rate of 400 packets per second:

```
Router# configure terminal
Router(config)# spanning-tree uplinkfast max-update-rate 400
Router(config)# exit
Router#
```

This example shows how to verify that UplinkFast is enabled:

```
Router# show spanning-tree uplinkfast
UplinkFast is enabled
Router#
```

Enabling BackboneFast


Note

BackboneFast operates correctly only when enabled on all network devices in the network. BackboneFast is not supported on Token Ring VLANs. This feature is supported for use with third-party network devices.

To enable BackboneFast, perform this task:

Command	Purpose
Step 1 Router(config)# spanning-tree backbonefast	Enables BackboneFast.
	Router(config)# no spanning-tree backbonefast
Step 2 Router(config)# end	Exits configuration mode.
Step 3 Router# show spanning-tree vlan vlan_ID	Verifies that UplinkFast is enabled.

This example shows how to enable BackboneFast:

```
Router# configure terminal
Router(config)# spanning-tree backbonefast
Router(config)# end
Router#
```

This example shows how to verify that BackboneFast is enabled:

```
Router# 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
Router#
```

■ Enabling EtherChannel Guard

Enabling EtherChannel Guard

To enable EtherChannel guard, perform this task:

Command	Purpose
Step 1 Router(config)# spanning-tree etherchannel guard misconfig	Enables EtherChannel guard.
	Router(config)# no spanning-tree etherchannel guard misconfig Disables EtherChannel guard.
Step 2 Router(config)# end	Exits configuration mode.
Step 3 Router# show spanning-tree summary include EtherChannel	Verifies that EtherChannel guard is enabled.

This example shows how to enable EtherChannel guard:

```
Router# configure terminal
Router(config)# spanning-tree etherchannel guard misconfig
Router(config)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show spanning-tree summary | include EtherChannel
EtherChannel misconfiguration guard is enabled
```

Enter the **show interface status err-disable** command to display interfaces in the errdisable state.

After the misconfiguration has been cleared, interfaces in the errdisable state might automatically recover. To manually return an interface to service, enter a **shutdown** and then a **no shutdown** command for the interface.

Enabling Root Guard

To enable root guard, perform this task:

Command	Purpose
Step 1 Router(config)# interface {type¹ slot/port} port-channel port_channel_number}	Selects an interface to configure.
Step 2 Router(config-if)# spanning-tree guard root	Enables root guard.
	Router(config-if)# no spanning-tree guard root Disables root guard.
Step 3 Router(config-if)# end	Exits configuration mode.
Step 4 Router# show spanning-tree Router# show running interface {type¹ slot/port} port-channel port_channel_number	Verifies the configuration.

1. type = ethernet, fastethernet, gigabitethernet, or tengigabitethernet

Enter the **show spanning-tree inconsistentports** command to display ports that are in the root-inconsistent state.

Enabling Loop Guard

Use the **set spanning-tree guard** command to enable or disable the spanning tree loop guard feature on a per-port basis.

To enable loop guard globally on the switch, perform this task:

Command	Purpose
Step 1 Router(config)# spanning-tree loopguard default	Enables loop guard globally on the switch.
Step 2 Router(config)# end	Exits configuration mode.
Step 3 Router# show spanning tree interface 4/4 detail	Verifies the configuration impact on a port.

This example shows how to enable loop guard globally:

```
Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# spanning-tree loopguard default
Router(config)# ^Z

Router# 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 Router(config)# interface {type¹ slot/port} {port-channel port_channel_number}	Selects an interface to configure.
Step 2 Router(config-if)# spanning-tree guard loop	Configures loop guard.
Step 3 Router(config)# end	Exits configuration mode.
Step 4 Router# show spanning tree interface 4/4 detail	Verifies the configuration impact on that port.

1. *type* = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

This example shows how to enable loop guard:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fastEthernet 4/4
Router(config-if)# spanning-tree guard loop
Router(config-if)# ^Z
```

■ Enabling Loop Guard

This example shows how to verify the configuration:

```
Router# 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
Router#
```



Configuring Layer 3 Interfaces

This chapter contains information about how to configure Layer 3 interfaces on the Catalyst 6500 series switches, which supplements the information and procedures in the Release 12.2 publications at this URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/index.htm>

This chapter consists of these sections:

- [Configuring IP Routing and Addresses, page 16-1](#)
- [Configuring IPX Routing and Network Numbers, page 16-4](#)
- [Configuring AppleTalk Routing, Cable Ranges, and Zones, page 16-5](#)
- [Configuring Other Protocols on Layer 3 Interfaces, page 16-6](#)



Note

- For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication and the Release 12.2 publications at this URL:
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/index.htm>
- We recommend that you configure no more than 2,000 Layer 3 VLAN interfaces on an MSFC3.
- To support VLAN interfaces, create and configure VLANs and assign VLAN membership to Layer 2 LAN ports. For more information, see [Chapter 10, “Configuring VLANs”](#) and [Chapter 9, “Configuring VTP.”](#)

Configuring IP Routing and Addresses

For complete information and procedures, refer to these publications:

- *Cisco IOS IP and IP Routing Configuration Guide*, Release 12.2, at this URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/index.htm
- *Cisco IOS IP and IP Routing Command Reference*, Release 12.2, at these URLs:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipras_r/index.htm
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fiprrp_r/index.htm

**Note**

- For information about the **maximum paths** command, refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication.
- The Policy Feature Card 3 (PFC3) and any Distributed Feature Card 3s (DFC3s) provide hardware support for policy-based routing (PBR) for route-map sequences that use the **match ip address**, **set ip next-hop**, and **ip default next-hop** PBR keywords.

To configure PBR, refer to the *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.2, “Classification,” “Configuring Policy-Based Routing,” at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_c/fqcprr1/qcfpbr.htm

To configure IP routing and an IP address on a Layer 3 interface, perform this task:

	Command	Purpose
Step 1	Router(config)# ip routing	Enables IP routing. (Required only if IP routing is disabled.)
Step 2	Router(config)# router ip_routing_protocol	Specifies an IP routing protocol.
Step 3	Router(config)# interface {vlan vlan_ID} {type¹ slot/port} {port-channel port_channel_number}	Selects an interface to configure.
Step 4	Router(config-if)# ip address ip_address subnet_mask	Configures the IP address and IP subnet.
Step 5	Router(config-if)# no shutdown	Enables the interface.
Step 6	Router(config-if)# end	Exits configuration mode.
Step 7	Router# show interfaces [{vlan vlan_ID} {type¹ slot/port} {port-channel port_channel_number}] Router# show ip interfaces [{vlan vlan_ID} {type¹ slot/port} {port-channel port_channel_number}] Router# show running-config interfaces [{vlan vlan_ID} {type¹ slot/port} {port-channel port_channel_number}]	Verifies the configuration.

1. *type* = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

This example shows how to enable IP Routing Information Protocol (RIP) routing:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip routing
Router(config)# router rip
Router(config-router)# network 10.0.0.0
Router(config-router)# end
Router#
```

This example shows how to configure an IP address on Fast Ethernet port 5/4:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fastethernet 5/4
Router(config-if)# ip address 172.20.52.106 255.255.255.248
Router(config-if)# no shutdown
Router(config-if)#
```

```
Router(config-if)# end
Router#
```

This example uses the **show interfaces** command to display the interface IP address configuration and status of Fast Ethernet port 5/4:

```
Router# show interfaces fastethernet 5/4
FastEthernet5/4 is up, line protocol is up
    Hardware is Cat6K 100Mb Ethernet, address is 0050.f0ac.3058 (bia 0050.f0ac.3058)
    Internet address is 172.20.52.106/29
    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 00:00:01, output never, output hang never
    Last clearing of "show interface" counters never
    Queueing strategy: fifo
    Output queue 0/40, 0 drops; input queue 0/75, 0 drops
    5 minute input rate 0 bits/sec, 0 packets/sec
    5 minute output rate 0 bits/sec, 0 packets/sec
        7 packets input, 871 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
        8 packets output, 1658 bytes, 0 underruns
        0 output errors, 0 collisions, 4 interface resets
        0 babbles, 0 late collision, 0 deferred
        0 lost carrier, 0 no carrier
        0 output buffer failures, 0 output buffers swapped out
Router#
```

This example uses the **show ip interface** command to display the detailed configuration and status of Fast Ethernet port 5/4:

```
Router# show ip interface fastethernet 5/4
FastEthernet5/4 is up, line protocol is up
    Internet address is 172.20.52.106/29
    Broadcast address is 255.255.255.255
    Address determined by setup command
    MTU is 1500 bytes
    Helper address is not set
    Directed broadcast forwarding is disabled
    Multicast reserved groups joined: 224.0.0.10
    Outgoing access list is not set
    Inbound access list is not set
    Proxy ARP is enabled
    Security level is default
    Split horizon is enabled
    ICMP redirects are always sent
    ICMP unreachables are always sent
    ICMP mask replies are never sent
    IP fast switching is enabled
    IP fast switching on the same interface is disabled
    IP Flow switching is disabled
    IP CEF switching is enabled
    IP Fast switching turbo vector
    IP Normal CEF switching turbo vector
    IP multicast fast switching is enabled
    IP multicast distributed fast switching is disabled
    Router Discovery is disabled
    IP output packet accounting is disabled
    IP access violation accounting is disabled
```

■ Configuring IPX Routing and Network Numbers

```

TCP/IP header compression is disabled
RTP/IP header compression is disabled
Probe proxy name replies are disabled
Policy routing is disabled
Network address translation is disabled
WCCP Redirect outbound is disabled
WCCP Redirect exclude is disabled
BGP Policy Mapping is disabled
IP multicast multilayer switching is disabled
IP mls switching is enabled
Router#

```

This example uses the **show running-config** command to display the interface IP address configuration of Fast Ethernet port 5/4:

```

Router# show running-config interfaces fastethernet 5/4
Building configuration...

Current configuration:
!
interface FastEthernet5/4
  description "Router port"
  ip address 172.20.52.106 255.255.255.248
  no ip directed-broadcast
!

```

Configuring IPX Routing and Network Numbers

For complete information and procedures, refer to these publications:

- *Cisco IOS AppleTalk and Novell IPX Configuration Guide*, Release 12.2, at this URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fatipx_c/index.htm
- *Cisco IOS AppleTalk and Novell IPX Command Reference*, Release 12.2, at this URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fatipx_r/index.htm

To configure routing for Internetwork Packet Exchange (IPX) and configure IPX on a Layer 3 interface, perform this task:

	Command	Purpose
Step 1	Router(config)# ipx routing	Enables IPX routing.
Step 2	Router(config)# router ipx_routing_protocol	Specifies an IP routing protocol. This step might include other commands, such as specifying the networks to route with the network command.
Step 3	Router(config)# interface {vian vlan_ID} {type¹ slot/port} {port-channel port_channel_number}	Selects an interface to configure.
Step 4	Router(config-if)# ipx network [network unnumbered] encapsulation encapsulation_type	Configures the IPX network number. This enables IPX routing on the interface. When you enable IPX routing on the interface, you can also specify an encapsulation type.
Step 5	Router(config-if)# no shutdown	Enables the interface.

Command	Purpose
Step 6 Router(config-if)# end	Exits configuration mode.
Step 7 Router# show interfaces [{vian vlan_ID} {type ¹ slot/port} {port-channel port_channel_number}] Router# show ipx interfaces [{vian vlan_ID} {type ¹ slot/port} {port-channel port_channel_number}] Router# show running-config interfaces [{vian vlan_ID} {type ¹ slot/port} {port-channel port_channel_number}]	Verifies the configuration.

1. type = ethernet, fastethernet, gigabitethernet, or tengigabitethernet

This example shows how to enable IPX routing and assign an IPX network address to interface VLAN 100:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ipx routing
Router(config)# ipx router rip
Router(config-ipx-router)# network all
Router(config-ipx-router)# interface vlan 100
Router(config-if)# ipx network 100 encapsulation snap
Router(config-if)# no shutdown
Router(config-if)# end
Router# copy running-config startup-config
```

Configuring AppleTalk Routing, Cable Ranges, and Zones

For complete information and procedures, refer to these publications:

- *Cisco IOS AppleTalk and Novell IPX Configuration Guide*, Release 12.2, at this URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fatipx_c/index.htm
- *Cisco IOS AppleTalk and Novell IPX Command Reference*, Release 12.2, at this URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fatipx_r/index.htm

Configuring Other Protocols on Layer 3 Interfaces

To configure routing for AppleTalk, perform this task beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# appletalk routing	Enables AppleTalk routing.
Step 2	Router(config)# interface {vIan vlan_ID} {type ¹ slot/port} {port-channel port_channel_number}	Selects an interface to configure.
Step 3	Router(config-if)# appletalk cable-range cable_range	Assigns a cable range to the interface.
Step 4	Router(config-if)# appletalk zone zone_name	Assigns a zone name to the interface.
Step 5	Router(config-if)# no shutdown	Enables the interface.
Step 6	Router(config-if)# end	Exits configuration mode.
Step 7	Router# show interfaces [{vIan vlan_ID} {type ¹ slot/port} {port-channel port_channel_number}] Router# show appletalk interfaces [{vIan vlan_ID} {type ¹ slot/port} {port-channel port_channel_number}] Router# show running-config interfaces [{vIan vlan_ID} {type ¹ slot/port} {port-channel port_channel_number}]	Verifies the configuration.

1. type = ethernet, fastethernet, gigabitethernet, or tengigabitethernet

This example shows how to enable AppleTalk routing and assign an AppleTalk cable-range and zone name to interface VLAN 100:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# appletalk routing
Router(config)# interface vIan 100
Router(config-if)# appletalk cable-range 100-100
Router(config-if)# appletalk zone Engineering
Router(config-if)# no shutdown
Router(config-if)# end
Router# copy running-config startup-config
```

Configuring Other Protocols on Layer 3 Interfaces

Refer to these publications for information about configuring other protocols on Layer 3 interfaces:

- *Cisco IOS Apollo Domain, VINES, DECnet, ISO CLNS, and XNS Configuration Guide*, Release 12.2, at this URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fapolo_c/index.htm
- *Cisco IOS Apollo Domain, VINES, DECnet, ISO CLNS, and XNS Command Reference*, Release 12.2, at this URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fapolo_r/index.htm



CHAPTER

17

Configuring IP Unicast Layer 3 Switching on Supervisor Engine 720

This chapter describes how to configure IP unicast Layer 3 switching for Policy Feature Card 3 (PFC3), Distributed Forwarding Card 3 (DFC3), and Multilayer Switch Feature Card 3 (MSFC3).



Note

- DFC3 naming and numbering aligns with the PFC3 naming and numbering scheme. A DFC2 is not available.
- For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication and the publications at this URL:
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/index.htm>

This chapter consists of these sections:

- [Understanding How Layer 3 Switching Works](#), page 17-2
- [Default Hardware Layer 3 Switching Configuration](#), page 17-4
- [Configuration Guidelines and Restrictions](#), page 17-5
- [Configuring Hardware Layer 3 Switching](#), page 17-5
- [Displaying Hardware Layer 3 Switching Statistics](#), page 17-6



Note

- Supervisor Engine 720, PFC3, and MSFC3 support IPX with fast switching on the MSFC3. For more information, refer to this URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fatipx_c/index.htm
- For information about IP multicast Layer 3 switching, see [Chapter 18, “Configuring IP Multicast Layer 3 Switching on Supervisor Engine 720.”](#)

Understanding How Layer 3 Switching Works

These sections describe Layer 3 switching with PFC3 and DFC3s:

- [Understanding Hardware Layer 3 Switching on PFC3 and DFC3s, page 17-2](#)
- [Understanding Layer 3-Switched Packet Rewrite, page 17-2](#)

Understanding Hardware Layer 3 Switching on PFC3 and DFC3s

Hardware Layer 3 switching allows the PFC3 and DFC3s, instead of the MSFC3, to forward IP unicast traffic between subnets. Hardware Layer 3 switching provides wire-speed forwarding on the PFC3 and DFC3s, instead of in software on the MSFC3. Hardware Layer 3 switching requires minimal support from the MSFC3. The MSFC3 routes any traffic that cannot be hardware Layer 3 switched.

Hardware Layer 3 switching supports the routing protocols configured on the MSFC3. Hardware Layer 3 switching does not replace the routing protocols configured on the MSFC3.

Hardware Layer 3 switching runs equally on the PFC3 and DFC3s to provide IP unicast Layer 3 switching locally on each module. Hardware Layer 3 switching provides the following functions:

- Hardware access control list (ACL) switching for policy-based routing (PBR)
- Hardware NetFlow switching for TCP intercept, reflexive ACL forwarding decisions, Web Cache Communication Protocol (WCCP), and server load balancing (SLB)



Note With PFC3 and DFC3, SLB Network Address Translation (NAT) is performed by the hardware; SLB NAT was previously performed by the software.

- Hardware Cisco Express Forwarding (CEF) switching for all other IP unicast traffic

Hardware Layer 3 switching on the PFC3 supports modules that do not have a DFC3. The MSFC3 forwards traffic that cannot be Layer 3 switched.

Traffic is hardware Layer 3 switched after being processed by access lists and quality of service (QoS).

Hardware Layer 3 switching makes a forwarding decision locally on the ingress-port module for each packet and sends the rewrite information for each packet to the egress port, where the rewrite occurs when the packet is transmitted from the Catalyst 6500 series switch.

Hardware Layer 3 switching generates flow statistics for Layer 3-switched traffic. Hardware Layer 3 flow statistics can be used for NetFlow Data Export (NDE). (See [Chapter 32, “Configuring NetFlow and NDE”](#).)

Understanding Layer 3-Switched Packet Rewrite

When a packet is Layer 3 switched from a source in one subnet to a destination in another subnet, the Catalyst 6500 series switch performs a packet rewrite at the egress port based on information learned from the MSFC3 so that the packets appear to have been routed by the MSFC3.

Packet rewrite alters five fields:

- Layer 2 (MAC) destination address
- Layer 2 (MAC) source address
- Layer 3 IP Time to Live (TTL)
- Layer 3 checksum
- Layer 2 (MAC) checksum (also called the frame checksum or FCS)


Note

Packets are rewritten with the encapsulation appropriate for the next-hop subnet.

If Source A and Destination B are in different subnets and Source A sends a packet to the MSFC3 to be routed to Destination B, the switch recognizes that the packet was sent to the Layer 2 (MAC) address of the MSFC3.

To perform Layer 3 switching, the switch rewrites the Layer 2 frame header, changing the Layer 2 destination address to the Layer 2 address of Destination B and the Layer 2 source address to the Layer 2 address of the MSFC3. The Layer 3 addresses remain the same.

In IP unicast and IP multicast traffic, the switch decrements the Layer 3 TTL value by 1 and recomputes the Layer 3 packet checksum. The switch recomputes the Layer 2 frame checksum and forwards (or, for multicast packets, replicates as necessary) the rewritten packet to Destination B's subnet.

A received IP unicast packet is formatted (conceptually) as follows:

Layer 2 Frame Header		Layer 3 IP Header					Data	FCS
Destination	Source	Destination	Source	TTL	Checksum			
<i>MSFC3 MAC</i>	<i>Source A MAC</i>	<i>Destination B IP</i>	<i>Source A IP</i>	<i>n</i>	<i>calculation1</i>			

After the switch rewrites an IP unicast packet, it is formatted (conceptually) as follows:

Layer 2 Frame Header		Layer 3 IP Header					Data	FCS
Destination	Source	Destination	Source	TTL	Checksum			
<i>Destination B MAC</i>	<i>MSFC3 MAC</i>	<i>Destination B IP</i>	<i>Source A IP</i>	<i>n-1</i>	<i>calculation2</i>			

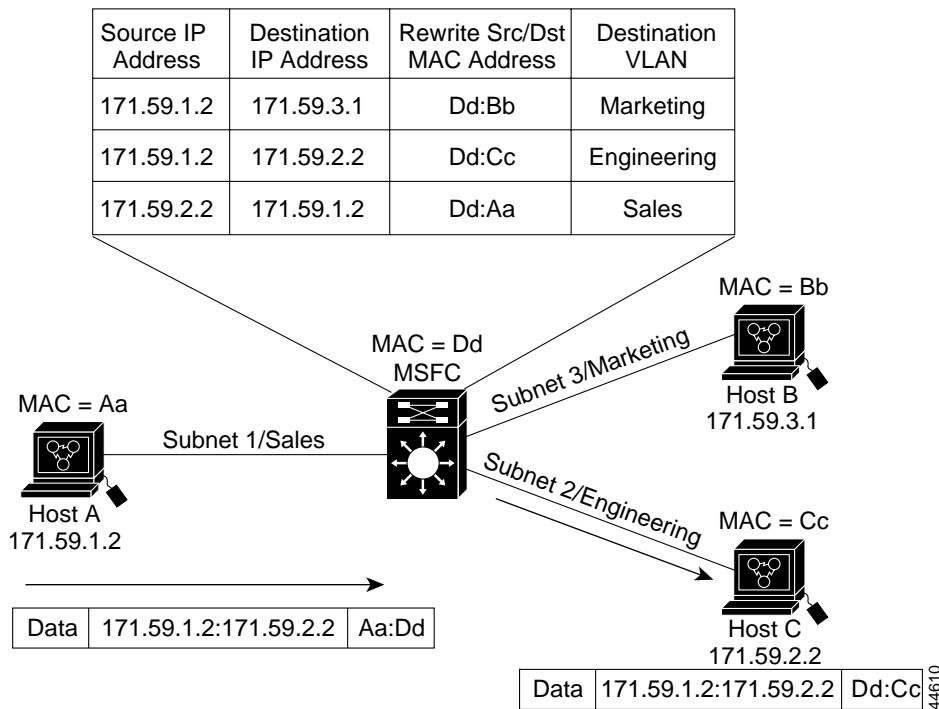
Hardware Layer 3 Switching Examples

Figure 17-1 on page 17-4 shows a simple network topology. In this example, Host A is on the Sales VLAN (IP subnet 171.59.1.0), Host B is on the Marketing VLAN (IP subnet 171.59.3.0), and Host C is on the Engineering VLAN (IP subnet 171.59.2.0).

When Host A initiates an HTTP file transfer to Host C, Hardware Layer 3 switching uses the information in the local forwarding information base (FIB) and adjacency table to forward packets from Host A to Host C.

■ Default Hardware Layer 3 Switching Configuration

Figure 17-1 Hardware Layer 3 Switching Example Topology



Default Hardware Layer 3 Switching Configuration

Table 17-1 shows the default hardware Layer 3 switching configuration.

Table 17-1 Default Hardware Layer 3 Switching Configuration

Feature	Default Value
Hardware Layer 3 switching enable state	Enabled (cannot be disabled)
Cisco IOS CEF enable state on MSFC3	Enabled (cannot be disabled)
Cisco IOS dCEF ¹ enable state on MSFC3	Enabled (cannot be disabled)
IGMP ² snooping	Enabled
Multicast routing on MSFC3	Disabled globally
PIM ³ routing on MSFC3	Disabled on all Layer 3 interfaces
IP multicast Layer 3 switching threshold	Unconfigured—no default value
IP multicast Layer 3 switching	Enabled when multicast routing is enabled and IP PIM is enabled on the interface

1. dCEF = Distributed Cisco Express Forwarding

2. IGMP = Internet Group Management Protocol

3. PIM = Protocol Independent Multicast

Configuration Guidelines and Restrictions

Follow these guidelines and restrictions when configuring hardware Layer 3 switching:

- Hardware Layer 3 switching supports the following ingress and egress encapsulations:
 - Ethernet V2.0 (ARPA)
 - 802.3 with 802.2 with 1 byte control (SAP1)
 - 802.3 with 802.2 and SNAP


Note

When you are in configuration mode you can enter EXEC mode-level commands by entering the **do** keyword before the EXEC mode-level command.

Configuring Hardware Layer 3 Switching


Note

For information on configuring unicast routing on the MSFC3, see [Chapter 16, “Configuring Layer 3 Interfaces.”](#)

Hardware Layer 3 switching is permanently enabled on Supervisor Engine 720 with PFC3, MSFC3, and DFC3s. No configuration is required.

To display information about Layer 3-switched traffic, perform this task:

Command	Purpose
<code>Router# show interface {{type¹ slot/port} {port-channel number}} begin L3</code>	Displays a summary of Layer 3-switched traffic.

1. *type* = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

This example shows how to display information about hardware Layer 3-switched traffic on Fast Ethernet port 3/3:

```
Router# 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...
Router#
```


Note

The Layer 3 switching packet count is updated approximately every five seconds.

Cisco IOS CEF and dCEF are permanently enabled on the MSFC3. No configuration is required to support hardware Layer 3 switching.

With PFC3 (and DFC3s, if present), hardware Layer 3 switching uses per-flow load balancing based on IP source and destination addresses. Per-flow load balancing avoids the packet reordering that can be necessary with per-packet load balancing. For any given flow, all PFC3- and DFC3-equipped switches make exactly the same load-balancing decision, which can result in nonrandom load balancing.

■ Displaying Hardware Layer 3 Switching Statistics

The Cisco IOS CEF **ip load-sharing per-packet**, **ip cef accounting per-prefix**, and **ip cef accounting non-recursive** commands on the MSFC3 apply only to traffic that is CEF-switched in software on the MSFC3. The commands do not affect traffic that is hardware Layer 3 switched on the PFC3 or on DFC3-equipped switching modules.

For information about Cisco IOS CEF and dCEF on the MSFC3, refer to these publications:

- The “Cisco Express Forwarding” sections at this URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fswitch_c/swprt1/index.htm
- The *Cisco IOS Switching Services Command Reference* publication at this URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fswitch_r/index.htm

Displaying Hardware Layer 3 Switching Statistics

Hardware Layer 3 switching statistics are obtained on a per-VLAN basis.

To display hardware Layer 3 switching statistics, perform this task:

Command	Purpose
Router# show interfaces {{type¹ slot/port} {port-channel number}}	Displays hardware Layer 3 switching statistics.

1. *type* = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

This example shows how to display hardware Layer 3 switching statistics:

```
Router# show interfaces gigabitethernet 9/5 | include Switched
L2 Switched: ucast: 8199 pkt, 1362060 bytes - mcast: 6980 pkt, 371952 bytes
L3 in Switched: ucast: 0 pkt, 0 bytes - mcast: 0 pkt, 0 bytes mcast
L3 out Switched: ucast: 0 pkt, 0 bytes - mcast: 0 pkt, 0 bytes
```

To display adjacency table information, perform this task:

Command	Purpose
Router# show adjacency [{{type¹ slot/port} {port-channel number}} detail internal summary]	Displays adjacency table information. The optional detail keyword displays detailed adjacency information, including Layer 2 information.

1. *type* = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

This example shows how to display adjacency statistics:

```
Router# show adjacency gigabitethernet 9/5 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 60 seconds.



CHAPTER

18

Configuring IP Multicast Layer 3 Switching on Supervisor Engine 720

This chapter describes how to configure IP multicast Layer 3 switching on the Catalyst 6500 series switches.



Note

For more information on the syntax and usage for the commands used in this chapter, refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference* and to the Release 12.2 publications at this URL: <http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/index.htm>

This chapter consists of these sections:

- Understanding How IP Multicast Layer 3 Switching Works, page 18-1
- Understanding How Bidirectional PIM Works, page 18-6
- Default IP Multicast Layer 3 Switching Configuration, page 18-6
- IP Multicast Layer 3 Switching Configuration Guidelines and Restrictions, page 18-7
- Configuring IP Multicast Layer 3 Switching, page 18-8
- Configuring Bidirectional PIM, page 18-19

Understanding How IP Multicast Layer 3 Switching Works

These sections describe how IP multicast Layer 3 switching works:

- IP Multicast Layer 3 Switching Overview, page 18-2
- Multicast Layer 3 Switching Cache, page 18-2
- Layer 3-Switched Multicast Packet Rewrite, page 18-3
- Partially and Completely Switched Flows, page 18-3
- Non-RPF Traffic Processing, page 18-5
- Understanding How Bidirectional PIM Works, page 18-6

IP Multicast Layer 3 Switching Overview

The Policy Feature Card 3 (PFC3) provides Layer 3 switching for IP multicast flows using the hardware replication table and hardware Cisco Express Forwarding (CEF), which uses the forwarding information base (FIB) and the adjacency table on the PFC3. In systems with Distributed Forwarding Cards (DFCs), IP multicast flows are Layer 3 switched locally using Multicast Distributed Hardware Switching (MDHS). MDHS uses local hardware CEF and replication tables on each DFC to perform Layer 3 switching and rate limiting of reverse path forwarding (RPF) failures locally on each DFC-equipped switching module.

The PFC3 and the DFCs support hardware switching of (*,G) state flows. The PFC3 and the DFCs support rate limiting of non-RPF traffic.

Multicast Layer 3 switching forwards IP multicast data packet flows between IP subnets using advanced application-specific integrated circuit (ASIC) switching hardware, which offloads processor-intensive multicast forwarding and replication from network routers.

Layer 3 flows that cannot be hardware switched are still forwarded in the software by routers. Protocol Independent Multicast (PIM) is used for route determination.

The PFC3 and the DFCs all use the Layer 2 multicast forwarding table to determine on which ports Layer 2 multicast traffic should be forwarded (if any). The multicast forwarding table entries are populated in conjunction with Internet Group Management Protocol (IGMP) snooping (see [Chapter 19, “Configuring IGMP Snooping”](#)).

Multicast Layer 3 Switching Cache

The PFC3 and the DFCs maintain Layer 3 switching information in one or more hardware tables as follows:

The PFC3 and DFC populate the (S,G) or (*,G) flows in the hardware FIB table with the appropriate masks; for example, (S/32, G/32) and (*0, G/32). The RPF interface and the adjacency pointer information is also stored in each entry. The adjacency table contains the rewrite and a pointer to the replication entries. If a flow matches a FIB entry, the RPF check compares the incoming interface/VLAN with the entry. A mismatch is an RPF failure, which can be rate limited if this feature is enabled.

The MSFC updates its multicast routing table and forwards the new information to the PFC whenever it receives traffic for a new flow. In addition, if an entry in the multicast routing table on the MSFC ages out, the MSFC deletes the entry and forwards the updated information to the PFC. In systems with DFCs, flows are populated symmetrically on all DFCs and on the PFC3.

The Layer 3 switching cache contains flow information for all active Layer 3-switched flows. After the switching cache is populated, multicast packets identified as belonging to an existing flow can be Layer 3 switched based on the cache entry for that flow. For each cache entry, the PFC maintains a list of outgoing interfaces for the IP multicast group. From this list, the PFC determines onto which VLANs traffic from a given multicast flow should be replicated.

These commands affect the Layer 3 switching cache entries:

- Clearing the multicast routing table (using the **clear ip mroute** command) clears all multicast Layer 3 switching cache entries.
- Disabling IP multicast routing on the MSFC (using the **no ip multicast-routing** command) purges all multicast Layer 3 switching cache entries on the PFC.
- Disabling multicast Layer 3 switching on an individual interface basis (using the **no mls ip multicast** command) causes flows that use this interface as the RPF interface to be routed only by the MSFC in software.

Layer 3-Switched Multicast Packet Rewrite

When a multicast packet is Layer 3 switched from a multicast source to a destination multicast group, the PFC3 and the DFCs perform a packet rewrite that is based on information learned from the MSFC and stored in the adjacency table.

For example, Server A sends a multicast packet addressed to IP multicast group G1. If there are members of group G1 on VLANs other than the source VLAN, the PFC3 must perform a packet rewrite when it replicates the traffic to the other VLANs (the switch also bridges the packet in the source VLAN).

When the PFC3 receives the multicast packet, it is (conceptually) formatted as follows:

Layer 2 Frame Header		Layer 3 IP Header				Data	FCS
Destination	Source	Destination	Source	TTL	Checksum		
<i>Group G1 MAC¹</i>	<i>Source A MAC</i>	<i>Group G1 IP</i>	<i>Source A IP</i>	<i>n</i>	<i>calculation1</i>		

1. In this example, Destination B is a member of Group G1.

The PFC3 rewrites the packet as follows:

- Changes the source MAC address in the Layer 2 frame header from the MAC address of the host to the MAC address of the MSFC (This is the burned-in MAC address of the system. This MAC address will be the same for all outgoing interfaces and cannot be modified. This MAC address can be displayed using the **show mls multicast statistics** command.)
- Decrements the IP header Time to Live (TTL) by one and recalculates the IP header checksum

The result is a rewritten IP multicast packet that appears to have been routed. The PFC3 replicates the rewritten packet onto the appropriate destination VLANs, where it is forwarded to members of IP multicast group G1.

After the PFC3 performs the packet rewrite, the packet is (conceptually) formatted as follows:

Frame Header		IP Header				Data	FCS
Destination	Source	Destination	Source	TTL	Checksum		
<i>Group G1 MAC</i>	<i>MSFC3 MAC</i>	<i>Group G1 IP</i>	<i>Source A IP</i>	<i>n-1</i>	<i>calculation2</i>		

Partially and Completely Switched Flows

When at least one outgoing Layer 3 interface for a given flow is multilayer switched and at least one outgoing interface is not multilayer switched, that flow is considered partially switched. When a partially switched flow is created, all multicast traffic belonging to that flow still reaches the MSFC and is forwarded by software on those outgoing interfaces that are not multilayer switched.

These sections describe partially and completely switched flow:

- [Partially Switched Flows, page 18-4](#)
- [Completely Switched Flows, page 18-4](#)

Partially Switched Flows

A flow might be partially switched instead of completely switched in these situations:

- The switch is configured as a member of the IP multicast group (using the **ip igmp join-group** command) on the RPF interface of the multicast source.
- During the registering state if the switch is the first-hop router to the source in PIM sparse mode (in this case, the switch must send PIM-register messages to the rendezvous point [RP]).
- The multicast TTL threshold is configured on an outgoing interface for the flow (using the **ip multicast ttl-threshold** command).
- The multicast helper is configured on the RPF interface for the flow, and multicast to broadcast translation is required.
- The outgoing interface is a generic routing encapsulation (GRE) Distance Vector Multicast Routing Protocol (DVMRP) tunnel interface.
- If Network Address Translation (NAT) is configured on an interface and source address translation is required for the outgoing interface.
- Flows are partially switched if any of the outgoing interfaces for a given flow are not Layer 3 switched.

(S,G) flows are partially switched instead of completely switched in these situations:

- (S,G) flows are partially switched if the (S,G) entry has RPT-bit (R bit) set.
- (S,G) flows are partially switched if the (S,G) entry does not have the SPT bit (T flag) set and the Prune bit (P flag) set.

(*,G) flows are partially switched instead of completely switched in these situations:

- (*,G) flows are partially switched on the last-hop leaf router if the shared-tree to shortest-path-tree (SPT) threshold is not equal to infinity. This allows the flow to transition from SPT.
- (*,G) flows are partially switched if at least one (S,G) entry has the same RPF as (*,g) entry but does not have RPT flag (R bit) OR SPT flag(T bit) OR Prune-flag (P bit) is not set.
- (*,G) flows are partially switched if DVMRP neighbor is detected on the input interface of (*,G) entry
- (*,G) flows are partially switched if interface/mask entry is not installed for RPF-interface of (*,G) entry rpf interface is not P2P interface.

Completely Switched Flows

When all the outgoing interfaces for a given flow are Layer 3 switched, and none of the above situations apply to the flow, that flow is considered completely switched. When a completely switched flow is created, the PFC3 prevents multicast traffic bridged on the source VLAN for that flow from reaching the MSFC interface in that VLAN, freeing the MSFC of the forwarding and replication load for that flow.

One consequence of a completely switched flow is that multicast statistics on a per-packet basis for that flow cannot be recorded. Therefore, the PFC3 periodically sends multicast packet and byte count statistics for all completely switched flows to the MSFC. The MSFC updates the corresponding multicast routing table entry and resets the expiration timer for that multicast route.



Note

A (*,G) state is created on the PIM-RP or for PIM-dense mode but is not used for forwarding the flows, and Layer 3 switching entries are not created for these flows.

Non-RPF Traffic Processing

These sections describe non-RPF traffic processing:

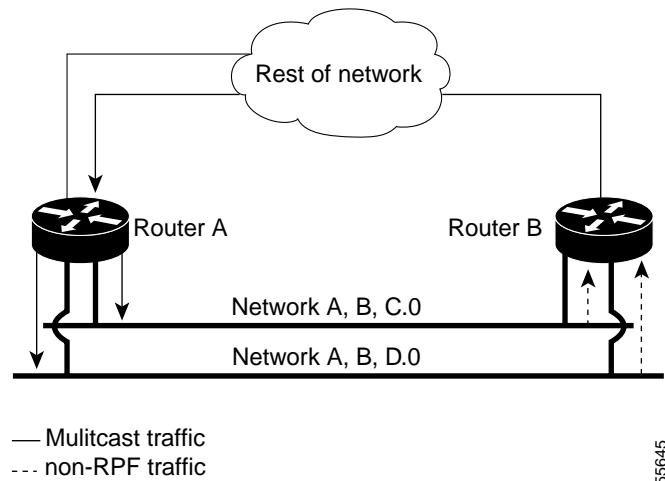
- [Non-RPF Traffic Overview, page 18-5](#)
- [Filtering of RPF Failures for Stub Networks, page 18-5](#)
- [Rate Limiting of RPF Failure Traffic, page 18-6](#)

Non-RPF Traffic Overview

In a redundant configuration where multiple routers connect to the same LAN segment, only one router forwards the multicast traffic from the source to the receivers on the outgoing interfaces (see [Figure 18-1](#)). In this kind of topology, only the PIM designated router (PIM DR) forwards the data in the common VLAN, but the non-PIM DR receives the forwarded multicast traffic. The redundant router (non-PIM DR) 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.

The Catalyst 6500 series switch processes non-RPF traffic in hardware on the PFC3 by filtering (dropping) or rate limiting the non-RPF traffic.

Figure 18-1 Redundant Multicast Router Configuration in a Stub Network



Filtering of RPF Failures for Stub Networks

The PFC3 and the DFCs support ACL-based filtering of RPF failures for sparse mode stub networks. When you enable the ACL-based method of filtering RPF failures by entering the **mls ip multicast stub** command on the redundant router, the following ACLs automatically download to the PFC3 and are applied to the interface you specify:

```
access-list 100 permit ip A.B.C.0 0.0.0.255 any
access-list 100 permit ip A.B.D.0 0.0.0.255 any
access-list 100 permit ip any 224.0.0.0 0.0.0.255
access-list 100 permit ip any 224.0.1.0 0.0.0.255
access-list 100 deny ip any 224.0.0.0 15.255.255.255
```

The ACLs filter RPF failures and drop them in hardware so that they are not forwarded to the router.

■ Understanding How Bidirectional PIM Works

Use the ACL-based method of filtering RPF failures only in sparse mode stub networks where there are no downstream routers. For dense mode groups, RPF failure packets have to be seen on the router for the PIM assert mechanism to function properly. Use CEF-based or NetFlow-based rate limiting to limit the rate of RPF failures in dense mode networks and sparse mode transit networks.

For information on configuring ACL-based filtering of RPF failures, see the “[Configuring ACL-Based Filtering of RPF Failures](#)” section on page 18-14.

Rate Limiting of RPF Failure Traffic

When you enable rate limiting of packets that fail the RPF check (non-RPF packets), most non-RPF packets are dropped in hardware. According to the multicast protocol specification, the router needs to receive the non-RPF packets for the PIM assert mechanism to function properly, so all non-RPF packets cannot be dropped in hardware.

When a non-RPF packet is received, a NetFlow entry is created for each non-RPF flow.

When the first non-RPF packet arrives, the PFC3 bridges the packet to the MSFC3 and to any bridged ports and creates a NetFlow entry that contains source, group, and ingress interface information, after which the NetFlow entry handles all packets for that source and group, sending packets only to bridged ports and not to the MSFC3.

To support the PIM assert mechanism, the PFC3 periodically forwards a percentage of the non-RPF flow packets to the MSFC.

The first packets for directly connected sources in PIM sparse mode are also rate-limited and are processed by the CPU.

Rate limiting of RPF failures is enabled by default.

Understanding How Bidirectional PIM Works

Supervisor Engine 720 supports hardware forwarding of bidirectional PIM groups. To support bidirectional PIM groups, the Supervisor Engine 720 implements a new mode called designated forwarder (DF) mode. The designated forwarder is the router elected to forward packets to and from a segment for a bidirectional PIM group. In DF mode, the supervisor engine accepts packets from the RPF and from the DF interfaces.

When the supervisor engine is forwarding bidirectional PIM groups, the RPF interface is always included in the outgoing interface list of (*,G) entry, and the DF interfaces are included depending on IGMP/PIM joins.

If the route to the RP becomes unavailable, the group is changed to dense mode. Should the RPF link to the RP become unavailable, the bidirectional flow is removed from the hardware FIB.

For information on configuring bidirectional PIM, see the “[Configuring Bidirectional PIM](#)” section on page 18-19.

Default IP Multicast Layer 3 Switching Configuration

[Table 18-1](#) shows the default IP multicast Layer 3 switching configuration.

Table 18-1 Default IP Multicast Layer 3 Switching Configuration

Feature	Default Value
ACL for stub networks	Disabled on all interfaces
Installing of directly connected subnet entries	Enabled globally
Multicast routing	Disabled globally
PIM routing	Disabled on all interfaces
IP multicast Layer 3 switching	Enabled when multicast routing is enabled and PIM is enabled on the interface
Shortcut consistency checking	Enabled

Internet Group Management Protocol (IGMP) snooping is enabled by default on all VLAN interfaces. If you disable IGMP snooping on an interface, multicast Layer 3 flows are still switched by the hardware. Bridging of the flow on an interface with IGMP snooping disabled causes flooding to all forwarding interfaces of the VLAN. For details on configuring IGMP snooping, see [Chapter 19, “Configuring IGMP Snooping.”](#)

IP Multicast Layer 3 Switching Configuration Guidelines and Restrictions

These sections describe IP Multicast Layer 3 switching configuration restrictions:

- [Restrictions, page 18-7](#)
- [Unsupported Features, page 18-8](#)

Restrictions

IP multicast Layer 3 switching is not provided for an IP multicast flow in the following situations:

- For IP multicast groups that fall into the range 224.0.0.* (where * is in the range 0 to 255), which is used by routing protocols. Layer 3 switching is supported for groups 225.0.0.* through 239.0.0.* and 224.128.0.* through 239.128.0.*.



Note Groups in the 224.0.0.* range are reserved for routing control packets and must be flooded to all forwarding ports of the VLAN. These addresses map to the multicast MAC address range 01-00-5E-00-00-xx, where xx is in the range 0–0xFF.

- For PIM auto-RP multicast groups (IP multicast group addresses 224.0.1.39 and 224.0.1.40).
- For packets with IP options. However, packets in the flow that do not specify IP options are hardware switched.
- For source traffic received on tunnel interfaces (such as MBONE traffic).
- If a (S,G) entry for sparse mode does not have the SPT-bit, RPT-bit, or Pruned flag set.
- A (*,G) entry is not hardware switched if at least one (S,G) entry has an RPF different from the (*,G) entry's RPF and the (S,G) is not hardware switched.

■ Configuring IP Multicast Layer 3 Switching

- If the ingress interface of a (S,G) or (*,G) entry is null, except if the (*,G) entry is a bidirectional PIM entry and the switch is the RP for the group.
- For bidirectional PIM entries when a DF interface or RPF interface is a tunnel.
- NAT translations and GRE tunnel encapsulation and de-encapsulation for multicast packets is handled in software.

Unsupported Features

If you enable IP multicast Layer 3 switching, IP accounting for Layer 3 interfaces does not report accurate values. The **show ip accounting** command is not supported.

Configuring IP Multicast Layer 3 Switching

These sections describe how to configure IP multicast Layer 3 switching:

- [Source-Specific Multicast with IGMPv3, IGMP v3lite, and URD](#), page 18-9
- [Enabling IP Multicast Routing Globally](#), page 18-9
- [Enabling IP PIM on Layer 3 Interfaces](#), page 18-9
- [Enabling IP Multicast Layer 3 Switching on Layer 3 Interfaces](#), page 18-10
- [Enabling Ingress Replication Mode](#), page 18-11
- [Specifying the Maximum Number of Multicast Routes](#), page 18-11
- [Configuring the Layer 3 Switching Global Threshold](#), page 18-12
- [Enabling Installation of Directly Connected Subnets](#), page 18-12
- [Specifying the Flow Statistics Message Interval](#), page 18-13
- [Configuring Bidirectional PIM](#), page 18-19
- [Setting the Bidirectional PIM Scan Interval](#), page 18-21
- [Enabling Shortcut-Consistency Checking](#), page 18-13
- [Configuring ACL-Based Filtering of RPF Failures](#), page 18-14
- [Displaying RPF Failure Rate-Limiting Information](#), page 18-14
- [Displaying IP Multicast Layer 3 Hardware Switching Summary](#), page 18-14
- [Displaying the IP Multicast Routing Table](#), page 18-17
- [Displaying IP Multicast Layer 3 Switching Statistics](#), page 18-18
- [Displaying Bidirectional PIM Information](#), page 18-21
- [Using Debug Commands](#), page 18-23
- [Clearing IP Multicast Layer 3 Switching Statistics](#), page 18-23



Note When you are in configuration mode you can enter EXEC mode commands by entering the **do** keyword before the EXEC mode command.

Source-Specific Multicast with IGMPv3, IGMP v3lite, and URD

For complete information and procedures about source-specific multicast with IGMPv3, IGMP v3lite, and URL Rendezvous Directory (URD), refer to this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/pcpt3/1cfssm.htm

Enabling IP Multicast Routing Globally

You must enable IP multicast routing globally before you can enable IP multicast Layer 3 switching on Layer 3 interfaces.

For complete information and procedures, refer to these publications:

- *Cisco IOS IP and IP Routing Configuration Guide*, Release 12.2, at this URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/pcpt2/index.htm
- *Cisco IOS IP and IP Routing Command Reference*, Release 12.1, at this URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipras_r/index.htm

To enable IP multicast routing globally, perform this task:

Command	Purpose
Router(config)# ip multicast-routing	Enables IP multicast routing globally.
Router(config)# no ip multicast-routing	Disables IP multicast routing globally.

This example shows how to enable multicast routing globally:

```
Router(config)# ip multicast-routing
Router(config) #
```

Enabling IP PIM on Layer 3 Interfaces

You must enable PIM on the Layer 3 interfaces before IP multicast Layer 3 switching functions on those interfaces.

To enable IP PIM on a Layer 3 interface, perform this task:

Step	Command	Purpose
Step 1	Router(config)# interface {{vlan vlan_ID} {type ¹ slot/port}}	Selects an interface to configure.
Step 2	Router(config-if)# ip pim {dense-mode sparse-mode sparse-dense-mode}	Enables IP PIM on a Layer 3 interface.

1. type = ethernet, fastethernet, gigabitethernet, or tengigabitethernet

■ Configuring IP Multicast Layer 3 Switching

This example shows how to enable PIM on an interface using the default mode (**sparse-dense-mode**):

```
Router(config-if)# ip pim
Router(config-if)#

```

This example shows how to enable PIM sparse mode on an interface:

```
Router(config-if)# ip pim sparse-mode
Router(config-if)#

```

Enabling IP Multicast Layer 3 Switching Globally

To globally enable hardware switching of multicast routes globally on your system, perform this task:

Command	Purpose
Step 1 Router(config)# no mls ip multicast	Globally enables hardware switching of multicast routes.
Step 2 Router(config)# show mls ip multicast	Displays MLS IP multicast configuration.

This example shows how to globally enable hardware switching of multicast routes:

```
Router(config)# mls ip multicast
Router(config)#

```

Enabling IP Multicast Layer 3 Switching on Layer 3 Interfaces

IP multicast Layer 3 switching is enabled by default on the Layer 3 interface when you enable PIM on the interface. Perform this task only if you disabled IP multicast Layer 3 switching on the interface and you want to reenable it.

PIM can be enabled on any Layer 3 interface, including VLAN interfaces.



Note You must enable PIM on all participating Layer 3 interfaces before IP multicast Layer 3 switching will function. For information on configuring PIM on Layer 3 interfaces, see the “[Enabling IP PIM on Layer 3 Interfaces](#)” section on page 18-9.

To enable IP multicast Layer 3 switching on a Layer 3 interface, perform this task:

Command	Purpose
Step 1 Router(config)# interface {vlan vlan_ID} {type ¹ slot/port}	Selects an interface to configure.
Step 2 Router(config-if)# mls ip multicast	Enables IP multicast Layer 3 switching on a Layer 3 interface.
Step 3 Router(config-if)# no mls ip multicast	Disables IP multicast Layer 3 switching on a Layer 3 interface.

1. type = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

This example shows how to enable IP multicast Layer 3 switching on a Layer 3 interface:

```
Router(config-if)# mls ip multicast
Router(config-if)#

```

Enabling Ingress Replication Mode

By default, a Supervisor Engine 720 will automatically detect the replication mode based on the module types installed in the system. If all modules are capable of egress replication, the system will use egress-replication mode. If the supervisor engine detects modules that are not capable of egress replication, the replication mode will automatically switch to ingress replication.

If the system is functioning in automatic detection egress mode, and you install a module cannot perform egress replication, the following occurs:

- The system reverts to ingress mode
- A system log is generated
- A system reload occurs to revert to the old configuration

During the change from egress- to ingress-replication mode, traffic interruptions may occur because the shortcuts will be purged and reinstalled. To avoid interruptions in traffic forwarding, enter the **mls ip multicast replication-mode ingress** command in global configuration mode. The **no** form of the command restores the system to auomatic detection mode.

To enable IP multicast Layer 3 switching on a Layer 3 interface, perform this task:

Command	Purpose
Step 1 Router(config)# mls ip multicast replication-mode ingress	Specifies the replication mode.
Step 1 Router(config)# show mls ip multicast summary	Displays the replication mode and if automatic detection is enabled or disabled.

This example shows how to enable the ingress replication mode:

```
Router (config)# mls ip multicast replication-mode
Router (config)# showm mls ip multicast summary
4 MMLS entries using 656 bytes of memory
Number of partial hardware-switched flows:2
Number of complete hardware-switched flows:2

Directly connected subnet entry install is enabled
Current mode of replication is Ingress
Auto-detection of replication mode is enabled
Consistency checker is enabled
Router (config)#

```

Specifying the Maximum Number of Multicast Routes

By default, a Supervisor Engine 720 supports 32,000 multicast routes in sparse mode. The following default settings apply for maximum number of multicast routes:

- 32,000 for PIM-SM/DM/SSM for ingress- or egress-replication mode
- 32,000 for bidirectional PIM ingress-replication mode
- 10,700 for bidirectional PIM egress-replication mode

By entering the **mls ip multicast max-routes** command, you can increase the maximum number of multicast routes to 64,000 for PIM-SM/DM/SSM with either ingress- and egress-replication mode.

Configuring IP Multicast Layer 3 Switching**Note**

Rate limiting of directly connected sources is not available if you increase the maximum number of multicast routes above the default values.

To change the maximum number of multicast routes supported for PIM-SM/DM/SSM, perform this task:

Step	Command	Purpose
Step 1	<code>Router(config)# mls ip multicast max-routes</code>	Specifies the maximum number of multicast routes.
Step 1	<code>Router(config)# show mls ip multicast</code>	Displays the multicast route configuration.

Configuring the Layer 3 Switching Global Threshold

You can configure a global multicast rate threshold, specified in packets per second, below which all multicast traffic is routed by the MSFC, which prevents creation of switching cache entries for low-rate Layer 3 flows.

**Note**

This command does not affect flows that are already being routed. To apply the threshold to existing routes, clear the route and let it reestablish.

To configure the Layer 3 switching threshold, perform this task:

Command	Purpose
<code>Router(config)# mls ip multicast threshold ppsec</code>	Configures the IP MMLS threshold.
<code>Router(config)# no mls ip multicast threshold</code>	Reverts to the default IP MMLS threshold.

This example shows how to configure the Layer 3 switching threshold to 10 packets per second:

```
Router(config)# mls ip multicast threshold 10
Router(config)#

```

Enabling Installation of Directly Connected Subnets

In PIM sparse mode, a first-hop router that is the designated router for the interface may need to encapsulate the source traffic in a PIM register message and unicast it to the rendezvous point. To prevent new sources for the group from being learned in the routing table, the (*,G) flows should remain as completely hardware-switched flows. (subnet/mask, 224/4) entries installed in the hardware FIB allows both (*,G) flows to remain completely hardware-switched flows, and new, directly connected sources to be learned correctly. Installing of directly connected subnets is enabled globally by default. One (subnet/mask, 224/4) is installed per PIM-enabled interface.

To view FIB entries, enter the **show mls ip multicast connected** command.

To enable installation of directly connected subnets, perform this task:

Command	Purpose
Router(config)# mls ip multicast connected	Enables installation of directly connected subnets.
Router(config)# no mls ip multicast connected	Disables installation of directly connected subnets.

This example shows how to enable installation of directly connected subnets:

```
Router(config)# mls ip multicast connected
Router(config)#

```

Specifying the Flow Statistics Message Interval

By default, the Supervisor Engine forwards flow statistics messages to the MSFC every 25 seconds. The messages are forwarded in batches, and each batch of messages contains statistics for 25 percent of all flows. If you leave the interval at the default of 25 seconds, it will take 100 seconds to forward statistics for all flows to the MSFC.

To specify how often flow statistics messages forwarded from the Supervisor Engine to the MSFC, perform this task:

Command	Purpose
Router(config)# mls ip multicast flow-stat-timer num	Specifies how the Supervisor Engine forwards flow statistics messages to the MSFC.
Router(config)# no mls ip multicast flow-stat-timer num	Restores the default.

This example shows how to configure the Supervisor Engine to forward flow statistics messages to the MSFC every 10 seconds:

```
Router(config)# mls ip multicast flow-stat-timer 10
Router(config)#

```

Enabling Shortcut-Consistency Checking

When you enable the shortcut-consistency checking feature, the multicast route table and the multicast-hardware entries are checked for consistency, and any inconsistencies are corrected. You can view inconsistencies by entering the **show mls ip multicast consistency-check** command.

If consistency checking is enabled, the multicast route table will be scanned every two seconds and a full scan is completed within 4 minutes.

To enable shortcut-consistency checking, perform this task:

Command	Purpose
Router(config)# mls ip multicast consistency-check	Enables shortcut-consistency checking.
Router(config)# no mls ip multicast consistency-check num	Restores the default.

This example shows how to enable the hardware shortcut-consistency checker:

```
Router (config)# mls ip multicast consistency-check
Router (config)#
```

Configuring ACL-Based Filtering of RPF Failures

When you configure ACL-based filtering of RPF failures, ACLs that filter RPF failures in hardware are downloaded to the hardware-based ACL engine and applied on the interface you specify.

To enable ACL-based filtering of RPF failures on an interface, perform this task:

	Command	Purpose
Step 1	Router(config)# interface {{vlan <i>vlan_ID</i> } {type ¹ <i>slot/port</i> } {port-channel <i>number</i> }}	Selects an interface to configure.
Step 2	Router(config-if)# mls ip multicast stub Router(config-if)# no mls ip multicast stub	Enables ACL-based filtering of RPF failures on an interface. Disables ACL-based filtering of RPF failures on an interface.

1. *type* = ethernet, fastethernet, gigabitethernet, or tengigabitethernet

Displaying RPF Failure Rate-Limiting Information

To display RPF failure rate-limiting information, perform this task:

Command	Purpose
Router# show mls ip multicast summary	Displays RPF failure rate-limiting information.

This example shows how to display RPF failure rate-limiting information:

```
Router# show mls ip multicast summary
10004 MMLS entries using 1280464 bytes of memory
Number of partial hardware-switched flows:4
Number of complete hardware-switched flows:10000
Router#
```

Displaying IP Multicast Layer 3 Hardware Switching Summary



Note The **show interface statistics** command does not display hardware-switched packets, only packets switched by software.

The **show ip pim interface count** command displays the IP multicast Layer 3 switching enable state on IP PIM interfaces and the number of packets received and sent on the interface.

To display IP multicast Layer 3 switching information for an IP PIM Layer 3 interface, perform one of these tasks:

Command	Purpose
Router# show ip pim interface [{{vlan vlan_ID} {type ¹ slot/port} {port-channel number}}] count	Displays IP multicast Layer 3 switching enable state information for all MSFC IP PIM Layer 3 interfaces.
Router# show ip interface	Displays the IP multicast Layer 3 switching enable state on the Layer 3 interfaces.

1. type = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

These examples show how to display the IP PIM configuration of the interfaces:

```
Router# show ip pim interface count

State: * - Fast Switched, D - Distributed Fast Switched
      H - Hardware Switching Enabled
Address          Interface      FS  Mpackets In/Out
10.15.1.20      GigabitEthernet4/8 * H 952/4237130770
10.20.1.7       GigabitEthernet4/9 * H 1385673757/34
10.25.1.7       GigabitEthernet4/10* H 0/34
10.11.1.30      FastEthernet6/26   * H 0/0
10.37.1.1       FastEthernet6/37   * H 0/0
1.22.33.44      FastEthernet6/47   * H 514/68
```

The “*”flag indicates that this interface can be fast switched and the “H” flag indicates that this interface is hardware switched. The “In”flag indicates the number of multicast packet bytes that have been received on the interface. The “Out”flag indicates the number of multicast packet bytes that have been forwarded from this interface.

```
Router# show ip mroute count
IP Multicast Statistics
56 routes using 28552 bytes of memory
13 groups, 3.30 average sources per group
Forwarding Counts:Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts:Total/RPF failed/Other drops(OIF-null, rate-limit etc)

Group:224.2.136.89, Source count:1, Group pkt count:29051
  Source:132.206.72.28/32, Forwarding:29051/-278/1186/0, Other:85724/8/56665
Router#
```



Note The “*” counter means that the outgoing interface list of the corresponding entry is NULL, and this indicates that this flow is still active.

This example shows how to display the IP multicast Layer 3 switching configuration of interface VLAN 10:

```
Router# show ip interface vlan 10
Vlan10 is up, line protocol is up
  Internet address is 10.0.0.6/8
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.1 224.0.0.2 224.0.0.13 224.0.0.10
  Outgoing access list is not set
  Inbound access list is not set
```

Configuring IP Multicast Layer 3 Switching

```

Proxy ARP is enabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachables are never sent
ICMP mask replies are never sent
IP fast switching is enabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP CEF switching is enabled
IP Fast switching turbo vector
IP Normal CEF switching turbo vector
IP multicast fast switching is enabled
IP multicast distributed fast switching is disabled
IP route-cache flags are Fast, CEF
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Probe proxy name replies are disabled
Policy routing is disabled
Network address translation is disabled
WCCP Redirect outbound is disabled
WCCP Redirect exclude is disabled
BGP Policy Mapping is disabled
IP multicast multilayer switching is enabled
IP mls switching is enabled
Router#

```

This example shows how to display the IP multicast Layer 3 switching configuration of Gigabit Ethernet interface 1/2:

```

Router# show interfaces gigabitEthernet 1/2
GigabitEthernet1/2 is up, line protocol is up (connected)
  Hardware is C6k 1000Mb 802.3, address is 0001.c9db.2441 (bia 0001.c9db.2441)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
  Last clearing of "show interface" counters 00:05:13
...
  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 10000 bits/sec, 1 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    284 packets input, 113104 bytes, 0 no buffer
    Received 284 broadcasts (284 multicast) <<<<<<<<<<<< ( 1 )
    0 runts, 41 giants, 0 throttles <<<<<<<<<<<< ( 2 )
    41 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored <<<<<<< ( 3 )
    0 input packets with dribble condition detected
    198 packets output, 14732 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
Cat6k-B#

```

Displaying the IP Multicast Routing Table

The **show ip mroute** command displays the IP multicast routing table.

To display the IP multicast routing table, perform this task:

Command	Purpose
Router# show ip mroute partical-sc [hostname group_number]	Displays the IP multicast routing table and the hardware-switched interfaces.

This example shows how to display the IP multicast routing table:

```
Router# show ip mroute 230.13.13.1
IP Multicast Routing Table
Flags:D - Dense, S - Sparse, s - SSM Group, C - Connected, L - Local,
P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
J - Join SPT, M - MSDP created entry, X - Proxy Join Timer Running
A - Advertised via MSDP, U - URD, I - Received Source Specific Host
Report
Outgoing interface flags:H - Hardware switched
Timers:Uptime/Expires
Interface state:Interface, Next-Hop or VCD, State/Mode

(*, 230.13.13.1), 00:16:41/00:00:00, RP 10.15.1.20, flags:SJC
  Incoming interface:GigabitEthernet4/8, RPF nbr 10.15.1.20
  Outgoing interface list:
    GigabitEthernet4/9, Forward/Sparse-Dense, 00:16:41/00:00:00, H

(*, 230.13.13.2), 00:16:41/00:00:00, RP 10.15.1.20, flags:SJC
  Incoming interface:GigabitEthernet4/8, RPF nbr 10.15.1.20, RPF-MFD
  Outgoing interface list:
    GigabitEthernet4/9, Forward/Sparse-Dense, 00:16:41/00:00:00, H

(10.20.1.15, 230.13.13.1), 00:14:31/00:01:40, flags:CJT
  Incoming interface:GigabitEthernet4/8, RPF nbr 10.15.1.20, RPF-MFD
  Outgoing interface list:
    GigabitEthernet4/9, Forward/Sparse-Dense, 00:14:31/00:00:00, H
(132.206.72.28, 224.2.136.89), 00:14:31/00:01:40, flags:CJT
  Incoming interface:GigabitEthernet4/8, RPF nbr 10.15.1.20, RPF-MFD
  Outgoing interface list:Null
Router#
```



The RPF-MFD flag indicates the flow is completely switched by the hardware. The H flag indicates the flow is switched by the hardware on the outgoing interface.

Displaying IP Multicast Layer 3 Switching Statistics

The **show mls ip multicast** command displays detailed information about IP multicast Layer 3 switching.

To display detailed IP multicast Layer 3 switching information, perform these tasks:

Command	Purpose
Router# show mls ip multicast group ip_address [interface type slot/port statistics]	Displays IP multicast Layer 3 switching group information.
Router# show mls ip multicast interface {{vlan vlan_ID} {type¹ slot/port} {port-channel number}} [statistics summary]	Displays IP multicast Layer 3 switching details for all interfaces.
Router# show mls ip multicast source ip_address [interface {{vlan vlan_ID} {type¹ slot/port} {port-channel number}} statistics]	Displays IP multicast Layer 3 switching source information.
Router# show mls ip multicast summary	Displays a summary of IP multicast Layer 3 switching information.
Router# show mls ip multicast statistics	Displays IP multicast Layer 3 switching statistics.

1. *type* = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

This example shows how to display information on a specific IP multicast Layer 3 switching entry:

```
Router# show mls ip multicast group 10.1.0.11
Multicast hardware switched flows:
Total shortcut installed: 0
```

This example shows how to display IP multicast group information:

```
Router# show mls ip multicast group 230.13.13.1 source 10.20.1.15
Multicast hardware switched flows:
(10.20.1.15, 230.13.13.1) Incoming interface:Gi4/8, Packets switched:0
Hardware switched outgoing interfaces:Gi4/9
RPF-MFD installed

Total hardware switched flows :1
Router#
```

This example shows how to display IP multicast Layer 3 switching information for VLAN 10:

```
Router# show mls ip multicast interface vlan 10
Multicast hardware switched flows:
(10.1.0.15, 224.2.2.15) Incoming interface: Vlan10, Packets switched: 0
Hardware switched outgoing interfaces:
MFD installed: Vlan10

(10.1.0.19, 224.2.2.19) Incoming interface: Vlan10, Packets switched: 1970
Hardware switched outgoing interfaces:
MFD installed: Vlan10

(10.1.0.11, 224.2.2.11) Incoming interface: Vlan10, Packets switched: 0
Hardware switched outgoing interfaces:
MFD installed: Vlan10

(10.1.0.10, 224.2.2.10) Incoming interface: Vlan10, Packets switched: 2744
Hardware switched outgoing interfaces:
MFD installed: Vlan10
```

```
(10.1.0.17, 224.2.2.17) Incoming interface: Vlan10, Packets switched: 3340
Hardware switched outgoing interfaces:
MFD installed: Vlan10
```

```
(10.1.0.13, 224.2.2.13) Incoming interface: Vlan10, Packets switched: 0
Hardware switched outgoing interfaces:
```

This example shows how to display the IP multicast Layer 3 switching statistics:

```
Router# show mls ip multicast statistics
```

```
MLS Multicast Operation Status:
MLS Multicast configuration and state:
  Router Mac: 00e0.b0ff.7b00, Router IP: 33.0.33.24
  MLS multicast operating state: ACTIVE
  Shortcut Request Queue size 4
  Maximum number of allowed outstanding messages: 1
  Maximum size reached from feQ: 3096
  Feature Notification sent: 1
  Feature Notification Ack received: 1
  Unsolicited Feature Notification received: 0
  MSM sent: 205170
  MSM ACK received: 205170
  Delete notifications received: 0
  Flow Statistics messages received: 35211

MLS Multicast statistics:
  Flow install Ack: 996508
  Flow install Nack: 1
  Flow update Ack: 1415959
  Flow update Nack: 0
  Flow delete Ack: 774953
  Complete flow install Ack: 958469
```

```
Router#
```

Configuring Bidirectional PIM

To configure bidirectional PIM, you must do the following:

-
- | | |
|---------------|---|
| Step 1 | Enable bidirectional PIM globally. |
| Step 2 | Configure the rendezvous point for the bidirectional group. |
-

These sections show how to configure bidirectional PIM and display bidirectional PIM configuration information and statistics:

- [Enabling Bidirectional PIM Globally, page 18-20](#)
- [Configuring the Rendezvous Point for Bidirectional Groups, page 18-20](#)
- [Setting the Bidirectional PIM Scan Interval, page 18-21](#)
- [Displaying Bidirectional PIM Information, page 18-21](#)

Enabling Bidirectional PIM Globally

To enable bidirectional Protocol Independent Multicast (PIM), perform this task:

Command	Purpose
Router(config)# ip pim bidir-enable	Enables bidirectional PIM globally on the switch.
Router(config)# [no] ip pim bidir-enable	Disables bidirectional PIM globally on the switch.

This example shows how to enable bidirectional PIM on the switch:

```
Router(config)# ip pim bidir-enable
Router(config)#

```

Configuring the Rendezvous Point for Bidirectional Groups

To statically configure the rendezvous point for a bidirectional group, perform this task:

Command	Purpose
Step 1 Router(config)# ip pim rp-address <i>ip_address</i> access-list [<i>override</i>]	Statically configures the IP address of the rendezvous point for the group. When you specify the override option, the static rendezvous point is used.
Step 2 Router(config)# access-list <i>access-list</i> permit deny <i>ip_address</i>	Configures an access-list.
Step 3 Router(config)# ip pim send-rp-announce type number <i>scope ttl-value [group-list access-list] [interval seconds] [bidir]</i>	Configures the system to use Auto-RP to configure groups for which the router will act as a rendezvous point (RP).
Step 4 Router(config)# ip access-list standard <i>access-list-name</i> permit deny <i>ip_address</i>	Configures a standard IP access-list.
Step 5 Router(config)# mls ip multicast	Enables MLS IP multicast.

This example shows how to configure a static rendezvous point for a bidirectional group:

```
Router(config)# ip pim rp-address 10.0.0.1 10 bidir override
Router(config)# access-list 10 permit 224.1.0.0 0.0.255.255
Router(config)# ip pim send-rp-announce Loopback0 scope 16 group-list c21-rp-list-0 bidir
Router(config)# ip access-list standard c21-rp-list-0 permit 230.31.31.1 0.0.255.255

```

Setting the Bidirectional PIM Scan Interval

You can specify the interval between the bidirectional PIM RP Reverse Path Forwarding (RPF) scans.

To set the bidirectional RP RPF scan interval, perform this task:

Command	Purpose
Router(config)# mls ip multicast bidir gm-scan-interval <i>interval</i>	Specifies the bidirectional RP RPF scan interval; valid values are from 1 to 1000 seconds. The default is 10 seconds.
Router(config)# no mls ip multicast bidir gm-scan-interval	Restores the default.

This example shows how to set the bidirectional RP RPF scan interval:

```
Router(config)# mls ip multicast bidir gm-scan-interval 30
Router(config)#
```

Displaying Bidirectional PIM Information

To display bidirectional PIM information, perform this task:

Command	Purpose
Router# show ip pim rp mapping [in-use]	Displays mappings between PIM groups and rendezvous points and shows learned rendezvous points in use.
Router# show mls ip multicast rp-mapping [rp-address]	Displays PIM group to active rendezvous points mappings.
Router# show mls ip multicast rp-mapping gm-cache	Displays information based on the group/mask ranges in the RP mapping cache.
Router# show mls ip multicast rp-mapping df-cache	Displays information based on the DF list in RP mapping cache
Router# show mls ip multicast bidir	Displays bidirectional PIM information.
Router# show ip mroute	Displays information about the multicast routing table.

This example shows how to display information about the PIM group and rendezvous point mappings:

```
Router# show ip pim rp mapping
PIM Group-to-RP Mappings
This system is an RP (Auto-RP)
This system is an RP-mapping agent
Group(s) 230.31.0.0/16
    RP 60.0.0.60 (?), v2v1, bidir
        Info source:60.0.0.60 (?), elected via Auto-RP
        Uptime:00:03:47, expires:00:02:11
    RP 50.0.0.50 (?), v2v1, bidir
        Info source:50.0.0.50 (?), via Auto-RP
        Uptime:00:03:04, expires:00:02:55
    RP 40.0.0.40 (?), v2v1, bidir
        Info source:40.0.0.40 (?), via Auto-RP
        Uptime:00:04:19, expires:00:02:38
```

Configuring Bidirectional PIM

This example shows how to display information in the IP multicast routing table that is related to bidirectional PIM :

```
Router# show ip mroute bidirectional
(*, 225.1.3.0), 00:00:02/00:02:57, RP 3.3.3.3, flags:BC
  Bidir-Upstream:GigabitEthernet2/1, RPF nbr 10.53.1.7, RPF-MFD
  Outgoing interface list:
    GigabitEthernet2/1, Bidir-Upstream/Sparse-Dense, 00:00:02/00:00:00,H
    Vlan30, Forward/Sparse-Dense, 00:00:02/00:02:57, H

(*, 225.1.2.0), 00:00:04/00:02:55, RP 3.3.3.3, flags:BC
  Bidir-Upstream:GigabitEthernet2/1, RPF nbr 10.53.1.7, RPF-MFD
  Outgoing interface list:
    GigabitEthernet2/1, Bidir-Upstream/Sparse-Dense, 00:00:04/00:00:00,H
    Vlan30, Forward/Sparse-Dense, 00:00:04/00:02:55, H

(*, 225.1.4.1), 00:00:00/00:02:59, RP 3.3.3.3, flags:BC
  Bidir-Upstream:GigabitEthernet2/1, RPF nbr 10.53.1.7, RPF-MFD
  Outgoing interface list:
    GigabitEthernet2/1, Bidir-Upstream/Sparse-Dense, 00:00:00/00:00:00,H
    Vlan30, Forward/Sparse-Dense, 00:00:00/00:02:59, H
```

This example show how to display information related to a specific multicast route. In the output below, the arrow in the margin points to information about a partical short cut:

```
Router# show ip mroute 239.1.1.2 4.4.4.4
IP Multicast Routing Table
Flags:D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
      L - Local, P - Pruned, R - RP-bit set, F - Register flag,
      T - SPT-bit set, J - Join SPT, M - MSDP created entry,
      X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
      U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel
      Y - Joined MDT-data group, y - Sending to MDT-data group
Outgoing interface flags:H - Hardware switched
Timers:Uptime/Expires
Interface state:Interface, Next-Hop or VCD, State/Mode

(4.4.4.4, 239.1.1.2), 1d02h/00:03:20, flags:FTZ
  Incoming interface:Loopback0, RPF nbr 0.0.0.0, Partial-SC
  Outgoing interface list:
    Vlan10, Forward/Sparse-Dense, 1d02h/00:02:39 (ttl-threshold 5)
```

This example shows how to display the entries for a specific multicast group address:

```
Router# show mls ip multicast group 230.31.31.1
Multicast hardware switched flows:
(*, 230.31.31.1) Incoming interface:Vlan611, Packets switched:1778
Hardware switched outgoing interfaces:Vlan131 Vlan151 Vlan415 Gi4/16 Vlan611
RPF-MFD installed
```

This example shows how to display PIM group to active rendezvous points mappings:

```
Router# show mls ip multicast rp-mapping
State:H - Hardware Switched, I - Install Pending, D - Delete Pending, Z - Zombie

RP Address      State       RPF          DF-count      GM-count
60.0.0.60       H           Vl611          4             1
```

This example shows how to display information based on the group/mask ranges in the RP mapping cache:

```
Router# show mls ip multicast rp-mapping gm-cache
State:H - Hardware Switched, I - Install Pending, D - Delete Pending,
      Z - Zombie
```

RP Address	State	Group	Mask	State	Packet/Byte-count
60.0.0.60	H	230.31.0.0	255.255.0.0	H	100/6400

This example shows how to display information about specific MLS IP multicasting groups:

```
Router# show mls ip multicast rp-mapping df-cache
State:H - Hardware Switched, I - Install Pending, D - Delete Pending, Z - Zombie

RP Address      State       DF          State
60.0.0.60       H          Vl131      H
60.0.0.60       H          Vl151      H
60.0.0.60       H          Vl415      H
60.0.0.60       H          Gi4/16    H
```

Using Debug Commands

Table 18-2 describes IP multicast Layer 3 switching debug commands that you can use to troubleshoot IP multicast Layer 3 switching problems.

Table 18-2 IP Multicast Layer 3 Switching Debug Commands

Command	Description
[no] debug mls ip multicast events	Displays IP multicast Layer 3 switching events.
[no] debug mls ip multicast errors	Turns on debug messages for multicast MLS-related errors.
[no] debug mls ip multicast group group_id group_mask	Turns on debugging for a subset of flows.
[no] debug mls ip multicast messages	Displays IP multicast Layer 3 switching messages from and to hardware switching engine.
[no] debug mls ip multicast all	Turns on all IP multicast Layer 3 switching messages.
[no] debug mdss errors	Turns on MDSS ¹ error messages.
[no] debug mdss events	Displays MDSS-related events for debugging.
[no] debug mdss events mrouting-bidir	Displays bidirectional PIM MDSS events for debugging.
[no] debug mdss all	Displays all MDSS messages.
[no] debug ip pim df ip_address	Displays the DF election for a given rendezvous point for debug purposes.

1. MDSS = Multicast Distributed Switching Services

Clearing IP Multicast Layer 3 Switching Statistics

To clear IP multicast Layer 3 switching statistics, perform this task:

Command	Purpose
Router# clear mls ip multicast statistics	Clears IP multicast Layer 3 switching statistics.

This example shows how to clear IP multicast Layer 3 switching statistics:

```
Router# clear mls ip multicast statistics
```

The **show mls multicast statistics** command displays a variety of information about the multicast flows being handled by the PFC3. You can display entries based on any combination of the participating MSFC, the VLAN, the multicast group address, or the multicast traffic source. For an example of the **show mls ip multicast statistics** command, see the “[Displaying IP Multicast Layer 3 Switching Statistics](#)” section on page 18-18.



CHAPTER

19

Configuring IGMP Snooping

This chapter describes how to configure Internet Group Management Protocol (IGMP) snooping on the Catalyst 6500 series switches.



Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication.

This chapter consists of these sections:

- [Understanding How IGMP Snooping Works, page 19-1](#)
- [Default IGMP Snooping Configuration, page 19-7](#)
- [IGMP Snooping Configuration Guidelines and Restrictions, page 19-7](#)
- [IGMP Snooping Querier Configuration Guidelines and Restrictions, page 19-7](#)
- [Enabling the IGMP Snooping Querier, page 19-8](#)
- [Configuring IGMP Snooping, page 19-8](#)



Note

- To support Cisco Group Management Protocol (CGMP) client devices, configure the Multilayer Switch Feature Card (MSFC) as a CGMP server. Refer to the *Cisco IOS IP and IP Routing Configuration Guide*, Release 12.2, “IP Multicast,” “Configuring IP Multicast Routing,” at this URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/pcpt3/1cfmulti.htm
- For more information on IP multicast and IGMP, refer to RFC 1112 and RFC 2236.

Understanding How IGMP Snooping Works

These sections describe IGMP snooping:

- [IGMP Snooping Overview, page 19-2](#)
- [Joining a Multicast Group, page 19-2](#)
- [Leaving a Multicast Group, page 19-4](#)
- [Understanding IGMP Version 3 Support, page 19-5](#)

IGMP Snooping Overview

You can configure the switch to use IGMP snooping in subnets that receive IGMP queries from either IGMP or the IGMP snooping querier. IGMP snooping constrains multicast traffic at Layer 2 by configuring Layer 2 LAN ports dynamically to forward multicast traffic only to those ports that want to receive it.

IGMP, which runs at Layer 3 on a multicast router, generates Layer 3 IGMP queries in subnets where the multicast traffic needs to be routed. For information about IGMP, see [Chapter 18, “Configuring IP Multicast Layer 3 Switching on Supervisor Engine 720.”](#)

You can configure the IGMP snooping querier on the switch to support IGMP snooping in subnets that do not have any multicast router interfaces because the multicast traffic does not need to be routed. For more information about the IGMP snooping querier, see the “[Enabling the IGMP Snooping Querier](#)” section on page 19-8.

IGMP (on a multicast router) or the IGMP snooping querier (on the supervisor engine) sends out periodic general IGMP queries that the switch forwards through all ports in the VLAN and to which hosts respond. IGMP snooping monitors the Layer 3 IGMP traffic.



Note

If a multicast group has only sources and no receivers in a VLAN, IGMP snooping constrains the multicast traffic to only the multicast router ports.

Joining a Multicast Group

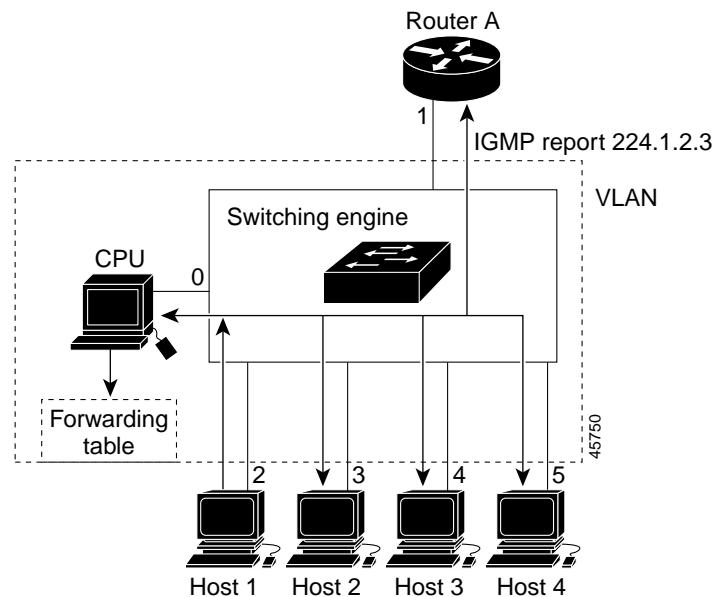
Hosts join multicast groups either by sending an unsolicited IGMP join message or by sending an IGMP join message in response to a general query from a multicast router (the switch forwards general queries from multicast routers to all ports in a VLAN).

In response to an IGMP join request, the switch creates an entry in its Layer 2 forwarding table for the VLAN on which the join request was received. When other hosts that are interested in this multicast traffic send IGMP join requests, the switch adds them to the existing Layer 2 forwarding table entry. The switch creates only one entry per VLAN in the Layer 2 forwarding table for each multicast group for which it receives an IGMP join request.

IGMP snooping suppresses all but one of the host join messages per multicast group and forwards this one join message to the multicast router.

The switch forwards multicast traffic for the multicast group specified in the join message to the interfaces where join messages were received. See [Figure 19-1](#).

Layer 2 multicast groups learned through IGMP snooping are dynamic. However, you can statically configure Layer 2 multicast groups using the **mac-address-table static** command. When you specify group membership for a multicast group address statically, the static setting supersedes any IGMP snooping learning. Multicast group membership lists can consist of both static and IGMP snooping-learned settings.

Figure 19-1 Initial IGMP Join Message

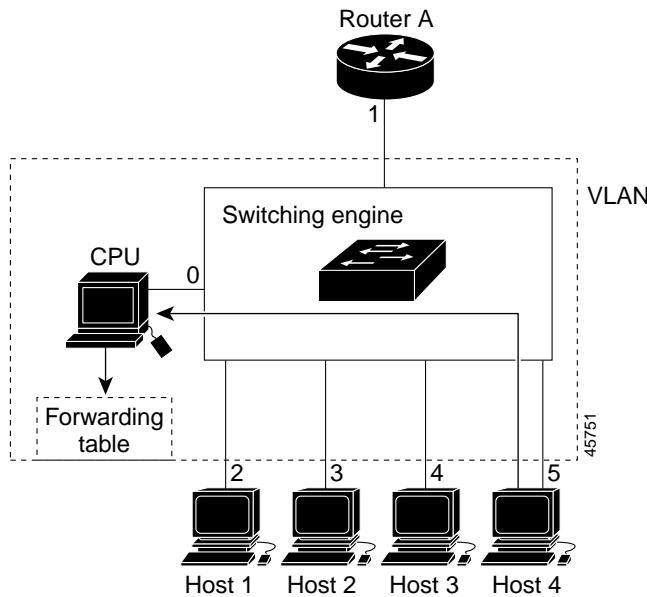
Multicast router A sends a general query to the switch, which forwards the query to ports 2 through 5 (all members of the same VLAN). Host 1 wants to join multicast group 224.1.2.3 and multicasts an IGMP membership report (IGMP join message) to the group with the equivalent MAC destination address of 0x0100.5E01.0203. When the CPU receives the IGMP report multicast by Host 1, the CPU uses the information in the IGMP report to set up a forwarding-table entry, as shown in [Table 19-1](#), that includes the port numbers of Host 1, the multicast router, and the switch internal CPU.

Table 19-1 IGMP Snooping Forwarding Table

Destination Address	Type of Packet	Ports
0100.5exx.xxxx	IGMP	0
0100.5e01.0203	!IGMP	1, 2

The switch hardware can distinguish IGMP information packets from other packets for the multicast group. The first entry in the table tells the switching engine to send only IGMP packets to the CPU. This prevents the CPU from becoming overloaded with multicast frames. The second entry tells the switching engine to send frames addressed to the 0x0100.5E01.0203 multicast MAC address that are not IGMP packets (!IGMP) to the multicast router and to the host that has joined the group.

If another host (for example, Host 4) sends an unsolicited IGMP join message for the same group ([Figure 19-2](#)), the CPU receives that message and adds the port number of Host 4 to the forwarding table as shown in [Table 19-2](#). Because the forwarding table directs IGMP messages only to the CPU, the message is not flooded to other ports. Any known multicast traffic is forwarded to the group and not to the CPU.

Figure 19-2 Second Host Joining a Multicast Group**Table 19-2 Updated IGMP Snooping Forwarding Table**

Destination Address	Type of Packet	Ports
0100.5exx.xxxx	IGMP	0
0100.5e01.0203	!IGMP	1, 2, 5

Leaving a Multicast Group

These sections describe leaving a multicast group:

- [Normal Leave Processing, page 19-4](#)
- [Fast-Leave Processing, page 19-5](#)

Normal Leave Processing

Interested hosts must continue to respond to the periodic general IGMP queries. As long as at least one host in the VLAN responds to the periodic general IGMP queries, the multicast router continues forwarding the multicast traffic to the VLAN. When hosts want to leave a multicast group, they can either ignore the periodic general IGMP queries (called a “silent leave”), or they can send a group-specific IGMPv2 leave message.

When IGMP snooping receives a group-specific IGMPv2 leave message from a host, it sends out a MAC-based general query to determine if any other devices connected to that interface are interested in traffic for the specific multicast group. If IGMP snooping does not receive an IGMP Join message in response to the general query, it assumes that no other devices connected to the interface are interested in receiving traffic for this multicast group, and it removes the interface from its Layer 2 forwarding table entry for that multicast group. If the leave message was from the only remaining interface with hosts interested in the group and IGMP snooping does not receive an IGMP Join in response to the general

query, it removes the group entry and relays the IGMP leave to the multicast router. If the multicast router receives no reports from a VLAN, the multicast router removes the group for the VLAN from its IGMP cache.

The interval for which the switch waits before updating the table entry is called the “last member query interval.” Enter the **ip igmp snooping last-member-query-interval *interval*** command to configure the interval.

Fast-Leave Processing

IGMP snooping fast-leave processing allows IGMP snooping to remove a Layer 2 LAN interface from the forwarding-table entry without first sending out IGMP group-specific queries to the interface. Upon receiving a group-specific IGMPv2 leave message, IGMP snooping immediately removes the interface from the Layer 2 forwarding table entry for that multicast group, unless a multicast router was learned on the port. Fast-leave processing improves bandwidth management for all hosts on a switched network.



Note Use fast-leave processing only on VLANs where only one host is connected to each Layer 2 LAN port. If fast-leave is enabled in VLANs where more than one host is connected to a Layer 2 LAN port, some hosts might be dropped inadvertently. Fast-leave processing is supported only with IGMP version 2 hosts.

Understanding IGMP Version 3 Support

IGMP snooping supports IGMP version 3. IGMP version 3 uses source-based filtering, which enables hosts and routers to specify which source addresses should be allowed or blocked for a specific multicast group. When you enable IGMP version 3 snooping on a Catalyst 6500 series switch, the system maintains IGMP version 3 states based on messages it receives for a particular group in a particular VLAN and either allows or blocks traffic based on the following information in these messages:

- Source lists
- Allow (include) or block (exclude) filtering options

Because the Layer 2 table is (MAC-group, VLAN) based, with IGMPv3 hosts it is preferable to have only a single multicast source per MAC-group.



Note Source-based filtering for IGMP version 3 reports is not supported in hardware. The states are maintained only in software and used for explicit host tracking and statistics collection.

IGMPv3 Fast-Leave Processing

IGMP version 3 fast-leave processing is enabled by default. To disable IGMP version 3 fast-leave processing you must turn off explicit-host tracking.

Fast-leave processing with IGMPv3 is implemented by maintaining source-group based membership information in software while also allocating LTL indexes on a MAC GDA basis.

When fast-leave processing is enabled, hosts send BLOCK_OLD_SOURCES{src-list} messages for a specific group when they no longer want to receive traffic from that source. When the switch receives such a message from a host, it parses the list of sources for that host for the given group. If this source list is exactly the same as the source list received in the leave message, the switch removes the host from the LTL index and stops forwarding this multicast group traffic to this host.

■ Understanding How IGMP Snooping Works

If the source lists do not match, the switch does not remove the host from the LTL index until the host is no longer interested in receiving traffic from any source.

Proxy Reporting

Because IGMPv3 does not have report suppression, all the hosts send their complete membership information to the router in response to queries. The switch receives these responses, updates the database and forwards the reports to the router. To prevent the router from becoming overloaded with reports, you can configure the switch for proxy-reporting mode. In proxy reporting mode, the switch forwards only the first report for a channel to the router and suppresses all other reports for the same channel.

With IGMPv3 proxy reporting, the switch does proxy reporting for unsolicited reports, as well as for reports received in the general query interval. Proxy reporting is turned on by default. When you disable proxy reporting, the switch works in transparent mode and updates the IGMP snooping database as it receives reports and forwards this information to the upstream router, which can then explicitly track all reporting hosts.

To support a mix of IGMPv2 and IGMPv3 hosts, the switch converts the IGMPv2 report into a EXCLUDE mode report. You must configure the switch to support both IGMPv2 and IGMPv3 hosts.



Note Source-based filtering for IGMP version 3 reports is not supported in hardware. The states are maintained only in software and used for explicit host tracking and statistics collection.



Note Turning off explicit host tracking will disable fast-leave processing and proxy reporting.

Explicit Host Tracking

IGMPv3 supports explicit tracking of membership information on any port. The explicit-tracking database is used for fast-leave processing for IGMPv3 hosts, proxy reporting, and statistics collection. When explicit tracking is enabled on a VLAN, the IGMP snooping software processes the IGMPv3 report it receives from a host and builds an explicit-tracking database that contains the following information:

- The port connected to the host
- The channels reported by the host
- The filter mode for each group reported by the host
- The list of sources for each group reported by the hosts
- The router filter mode of each group
- For each group, the list of hosts requesting the source



Note Turning off explicit host tracking will disable fast-leave processing and proxy reporting.



Note When explicit tracking is enabled and the switch is working in proxy-reporting mode, the router may not be able to track all the hosts behind a VLAN interface.

Default IGMP Snooping Configuration

[Table 19-3](#) shows the default IGMP snooping configuration.

Table 19-3 IGMP Snooping Default Configuration

Feature	Default Values
IGMP snooping querier	Disabled
IGMP snooping	Enabled
Multicast routers	None configured
IGMPv3 proxy reporting	Enabled
IGMP snooping router learning method	Learned automatically through PIM or IGMP packets
Fast-Leave Processing	Disabled
IGMPv3 Explicit Host Tracking	Enabled
IGMPv3 SSM Safe Reporting	Disabled

IGMP Snooping Configuration Guidelines and Restrictions

Follow these guidelines and restrictions when configuring the IGMP snooping:

- IGMP snooping supports private VLANs. Private VLANs do not impose any restrictions on IGMP snooping.
- IGMP snooping constrains traffic in MAC multicast groups 0100.5e00.0001 to 0100.5eff.ffff.
- IGMP snooping does not constrain Layer 2 multicasts generated by routing protocols.

IGMP Snooping Querier Configuration Guidelines and Restrictions

Follow these guidelines and restrictions when configuring the IGMP snooping querier:

- Configure the VLAN in global configuration mode (see [Chapter 10, “Configuring VLANs”](#)).
- Configure an IP address on the VLAN interface (see [Chapter 16, “Configuring Layer 3 Interfaces”](#)). When enabled, the IGMP snooping querier uses the IP address as the query source address.
- If there is no IP address configured on the VLAN interface, the IGMP snooping querier does not start. The IGMP snooping querier disables itself if the IP address is cleared. When enabled, the IGMP snooping querier restarts if you configure an IP address.
- The IGMP snooping querier supports IGMP version 2.
- When enabled, the IGMP snooping querier does not start if it detects IGMP traffic from a multicast router.
- When enabled, the IGMP snooping querier starts after 60 seconds with no IGMP traffic detected from a multicast router.

■ Enabling the IGMP Snooping Querier

- When enabled, the IGMP snooping querier disables itself if it detects IGMP traffic from a multicast router.
- QoS does not support IGMP packets when IGMP snooping is enabled.
- You can enable the IGMP snooping querier on all the Catalyst 6500 series switches in the VLAN. One switch is elected as the querier.



Note When you are in configuration mode you can enter EXEC mode commands by entering the **do** keyword before the EXEC mode command.

Enabling the IGMP Snooping Querier

Use the IGMP snooping querier to support IGMP snooping in a VLAN where PIM and IGMP are not configured because the multicast traffic does not need to be routed.

To enable the IGMP snooping querier in a VLAN, perform this task:

	Command	Purpose
Step 1	Router(config)# interface vlan <i>vlan_ID</i>	Selects the VLAN interface.
Step 2	Router(config-if)# ip igmp snooping querier	Enables the IGMP snooping querier.
	Router(config-if)# no ip igmp snooping querier	Disables the IGMP snooping querier.
Step 3	Router(config-if)# end	Exits configuration mode.
Step 4	Router# show ip igmp interface vlan <i>vlan_ID</i> include querier	Verifies the configuration.

This example shows how to enable the IGMP snooping querier on VLAN 200 and verify the configuration:

```
Router# interface vlan 200
Router(config-if)# igmp snooping querier
Router(config-if)# end
Router# show ip igmp interface vlan 200 | include querier
IGMP snooping querier is enabled on this interface
Router#
```

Configuring IGMP Snooping



Note To use IGMP snooping, configure a Layer 3 interface in the subnet for multicast routing (see [Chapter 18, “Configuring IP Multicast Layer 3 Switching on Supervisor Engine 720”](#)) or enable the IGMP snooping querier in the subnet (see the “Enabling the IGMP Snooping Querier” section on page 19-8).

IGMP snooping allows Catalyst 6500 series switches to examine IGMP packets and make forwarding decisions based on their content.

These sections describe how to configure IGMP snooping:

- [Enabling IGMP Snooping, page 19-9](#)

- Configuring a Member Port Statically, page 19-10
- Configuring a Multicast Router Port Statically, page 19-10
- Configuring the IGMP Query Interval, page 19-11
- Enabling IGMP Fast-Leave Processing, page 19-11
- Enabling SSM Safe Reporting, page 19-12
- Configuring IGMPv3 Explicit Host Tracking, page 19-12
- Displaying IGMP Snooping Information, page 19-13



Note Except for the global enable command, all IGMP snooping commands are supported only on VLAN interfaces.

Enabling IGMP Snooping

To enable IGMP snooping globally, perform this task:

Command	Purpose
Step 1 Router(config)# ip igmp snooping	Enables IGMP snooping.
Router(config)# no ip igmp snooping	Disables IGMP snooping.
Step 2 Router(config)# end	Exits configuration mode.
Step 3 Router# show ip igmp interface vlan <i>vlan_ID</i> include globally	Verifies the configuration.

This example shows how to enable IGMP snooping globally and verify the configuration:

```
Router(config)# ip igmp snooping
Router(config)# end
Router# show ip igmp interface vlan 200 | include globally
    IGMP snooping is globally enabled
Router#
```

To enable IGMP snooping in a VLAN, perform this task:

Command	Purpose
Step 1 Router(config)# interface vlan <i>vlan_ID</i>	Selects a VLAN interface.
Step 2 Router(config-if)# ip igmp snooping	Enables IGMP snooping.
Router(config-if)# no ip igmp snooping	Disables IGMP snooping.
Step 3 Router(config-if)# end	Exits configuration mode.
Step 4 Router# show ip igmp interface vlan <i>vlan_ID</i> include snooping	Verifies the configuration.

This example shows how to enable IGMP snooping on VLAN 25 and verify the configuration:

```
Router# interface vlan 25
Router(config-if)# ip igmp snooping
Router(config-if)# end
Router# show ip igmp interface v125 | include snooping
```

■ Configuring IGMP Snooping

```

IGMP snooping is globally enabled
IGMP snooping is enabled on this interface
IGMP snooping fast-leave is disabled and querier is disabled
IGMP snooping explicit-tracking is enabled on this interface
IGMP snooping last member query interval on this interface is 1000 ms
Router#

```

Configuring a Member Port Statically

To configure a static connection to a member port, perform this task:

	Command	Purpose
Step 1	Router(config)# mac-address-table static mac_addr vlan vlan_id interface type ¹ slot/port [disable-snooping]	Configures a static connection to a multicast router.
	Router(config)# no mac-address-table static mac_addr vlan vlan_id	Clears a static connection to a multicast router.
Step 2	Router(config-if)# end	Exits configuration mode.
Step 3	Router# show mac-address-table address mac_addr	Verifies the configuration.

1. *type* = ethernet, fastethernet, gigabitethernet, or tengigabitethernet

When you configure a static connection, enter the **disable-snooping** keyword to prevent multicast traffic addressed to the statically configured multicast MAC address from also being sent to other multicast router ports in the same VLAN.

This example shows how to configure a static connection to a multicast router:

```
Router(config)# mac-address-table static 0050.3e8d.6400 vlan 12 interface fastethernet 5/7
```

Configuring a Multicast Router Port Statically

To configure a static connection to a multicast router, perform this task:

	Command	Purpose
Step 1	Router(config)# ip igmp snooping mrouter interface type ¹ slot/port	Configures a static connection to a multicast router.
Step 2	Router(config-if)# end	Exits configuration mode.
Step 3	Router# show ip igmp snooping mrouter	Verifies the configuration.

1. *type* = ethernet, fastethernet, gigabitethernet, or tengigabitethernet

The interface to the router must be in the VLAN where you are entering the command, the interface must be administratively up, and the line protocol must be up.

This example shows how to configure a static connection to a multicast router:

```
Router(config-if)# ip igmp snooping mrouter interface fastethernet 5/6
Router(config-if)#

```

Configuring the IGMP Query Interval

You can configure the interval for which the switch waits after sending a group-specific query to determine if hosts are still interested in a specific multicast group.



- Note** When both IGMP fast-leave processing and the IGMP query interval are configured, fast-leave processing takes precedence.

To configure the interval for the IGMP queries sent by the switch, perform this task:

Command	Purpose
Step 1 Router(config)# interface vlan <i>vlan_ID</i>	Selects a VLAN interface.
Step 2 Router(config-if)# ip igmp snooping last-member-query-interval <i>interval</i>	Configures the interval for the IGMP queries sent by the switch. Default is 1 second. Valid range is 100 to 999 milliseconds.
Router(config-if)# no ip igmp snooping last-member-query-interval	Reverts to the default value.

This example shows how to configure the IGMP query interval:

```
Router(config-if)# ip igmp snooping last-member-query-interval 200
Router(config-if)# exit
Router# show ip igmp interface vlan 200 | include last-member-query-interval
IGMP snooping last member query interval on this interface is 200 ms
```

Enabling IGMP Fast-Leave Processing

To enable IGMP fast-leave processing in a VLAN, perform this task:

Command	Purpose
Step 1 Router(config)# interface vlan <i>vlan_ID</i>	Selects a VLAN interface.
Step 2 Router(config-if)# ip igmp snooping fast-leave	Enables IGMP fast-leave processing in the VLAN.
Router(config-if)# no ip igmp snooping fast-leave	Disables IGMP fast-leave processing in the VLAN.

This example shows how to enable IGMP fast-leave processing on the VLAN 200 interface and verify the configuration:

```
Router# interface vlan 200
Router(config-if)# ip igmp snooping fast-leave
Configuring fast leave on vlan 200
Router(config-if)# end
Router# show ip igmp interface vlan 200 | include fast-leave
IGMP snooping fast-leave is enabled on this interface
Router(config-if)#

```

Enabling SSM Safe Reporting

When you configure source-specific multicast (SSM) safe reporting, the group mode in switch and the router will be IGMPv3 even in the presence of IGMPv1 and IGMPv2 hosts.

To make sure the switch is able to support both IGMPv1, IGMPv2, and IGMPv3 hosts in the same VLAN, perform this task:

Command	Purpose
Step 1 Router(config)# interface vlan <i>vlan_ID</i>	Selects a VLAN interface.
Step 2 Router(config-if)# ip igmp snooping ssm-safe-reporting	Enables support for both IGMPv2 and IGMPv3 hosts.
Router(config-if)# no ip igmp snooping ssm-safe-reporting	Clears the configuration.

This example shows how to configure the switch to support both IGMPv2 and IGMPv3 hosts:

```
Router(config)# interface vlan 10
Router(config-if)# ip igmp snooping ssm-safe-reporting
```

Configuring IGMPv3 Explicit Host Tracking

To enable explicit host tracking on a VLAN, perform this task:

Command	Purpose
Step 1 Router(config)# interface vlan <i>vlan_ID</i>	Selects a VLAN interface.
Step 2 Router(config-if)# ip igmp snooping explicit-tracking	Enables explicit host tracking.
Router(config-if)# no ip igmp snooping explicit-tracking	Clears the explicit host tracking configuration.
Step 3 Router# show ip igmp snooping explicit-tracking { <i>vlan vlan-id</i> }	Displays information about the explicit host tracking status for IGMPv3 hosts.

This example shows how to enable explicit host tracking:

```
Router(config)# interface vlan 25
Router(config-if)# ip igmp snooping explicit-tracking
Router(config-if)# end
Router# show ip igmp snooping explicit-tracking vlan 25
```

Source/Group	Interface	Reporter	Filter_mode
10.1.1.1/226.2.2.2	Vl25:1/2	16.27.2.3	INCLUDE
10.2.2.2/226.2.2.2	Vl25:1/2	16.27.2.3	INCLUDE

Displaying IGMP Snooping Information

These sections describe displaying IGMP snooping information:

- [Displaying Multicast Router Interfaces, page 19-13](#)
- [Displaying MAC Address Multicast Entries, page 19-13](#)
- [Displaying IGMP Snooping Information for a VLAN Interface, page 19-14](#)
- [Displaying IGMP Snooping Statistics, page 19-14](#)

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
<code>Router# show ip igmp snooping mrouter interface vlan_ID</code>	Displays multicast router interfaces.

This example shows how to display the multicast router interfaces in VLAN 1:

```
Router# show ip igmp snooping mrouter interface vlan 1
vlan      ports
-----+
 1        Gi1/1,Gi2/1,Fa3/48,Router
Router#
```

Displaying MAC Address Multicast Entries

To display MAC address multicast entries for a VLAN, perform this task:

Command	Purpose
<code>Router# show mac-address-table multicast vlan_ID [count]</code>	Displays MAC address multicast entries for a VLAN.

This example shows how to display MAC address multicast entries for VLAN 1:

```
Router# show mac-address-table multicast vlan 1
vlan  mac address   type    qos      ports
-----+-----+-----+-----+
 1  0100.5e02.0203  static   --  Gi1/1,Gi2/1,Fa3/48,Router
 1  0100.5e00.0127  static   --  Gi1/1,Gi2/1,Fa3/48,Router
 1  0100.5e00.0128  static   --  Gi1/1,Gi2/1,Fa3/48,Router
 1  0100.5e00.0001  static   --  Gi1/1,Gi2/1,Fa3/48,Router,Switch
Router#
```

This example shows how to display a total count of MAC address entries for a VLAN:

```
Router# show mac-address-table multicast 1 count

Multicast MAC Entries for vlan 1:      4
Router#
```

Displaying IGMP Snooping Information for a VLAN Interface

To display IGMP snooping information for a VLAN interface, perform this task:

Command	Purpose
Router# show ip igmp interface vlan_ID	Displays IGMP snooping information on a VLAN interface.

This example shows how to display IGMP snooping information on the VLAN 200 interface:

```
Router# show ip igmp interface vlan 43
Vlan43 is up, line protocol is up
  Internet address is 43.0.0.1/24
  IGMP is enabled on interface
  Current IGMP host version is 2
  Current IGMP router version is 2
  IGMP query interval is 60 seconds
  IGMP querier timeout is 120 seconds
  IGMP max query response time is 10 seconds
  Last member query count is 2
  Last member query response interval is 1000 ms
  Inbound IGMP access group is not set
  IGMP activity:1 joins, 0 leaves
  Multicast routing is enabled on interface
  Multicast TTL threshold is 0
  Multicast designated router (DR) is 43.0.0.1 (this system)
  IGMP querying router is 43.0.0.1 (this system)
  Multicast groups joined by this system (number of users):
    224.0.1.40(1)
  IGMP snooping is globally enabled
  IGMP snooping is enabled on this interface
  IGMP snooping fast-leave is disabled and querier is disabled
  IGMP snooping explicit-tracking is enabled on this interface
  IGMP snooping last member query interval on this interface is 1000 ms
Router#
```

Displaying IGMP Snooping Statistics

The **show ip igmp snooping statistics interface vlan_ID** command displays the following information:

- The list of ports that are members of a group
- The filter mode
- The reporter-address behind the port
- The last-join and last-leave information collected since the last time a **clear ip igmp snooping statistics** command was entered

To display IGMP snooping statistics, perform this task:

Command	Purpose
Router# show ip igmp snooping statistics interface vlan_ID	Displays IGMP snooping information on a VLAN interface.

This example shows IGMP snooping statistics information for interface VLAN 25:

```
Router# show ip igmp snooping statistics interface vlan 25

Snooping staticstics for Vlan25
#channels:2
#hosts   :1

Source/Group          Interface    Reporter      Uptime      Last-Join  Last-Leave
10.1.1.1/226.2.2.2   Gi1/2:Vl25  16.27.2.3   00:01:47   00:00:50   -
10.2.2.2/226.2.2.2   Gi1/2:Vl25  16.27.2.3   00:01:47   00:00:50   -
Router#
```

■ Configuring IGMP Snooping



Configuring RGMP

This chapter supplements the information and procedures about Router-Port Group Management Protocol (RGMP) in the Release 12.2 publication at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/pcpt3/1cfrgmp.htm

This chapter consists of these sections:

- [Understanding How RGMP Works, page 20-1](#)
- [Default RGMP Configuration, page 20-2](#)
- [RGMP Configuration Guidelines and Restrictions, page 20-2](#)
- [Enabling RGMP on Layer 3 Interfaces, page 20-3](#)

**Note**

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication and to the Release 12.2 publications at this URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/index.htm>

Understanding How RGMP Works

RGMP constrains multicast traffic that exits the Catalyst 6500 series switch through ports to which only disinterested multicast routers are connected. RGMP reduces network congestion by forwarding multicast traffic to only those routers that are configured to receive it.

**Note**

To use RGMP, you must enable IGMP snooping on the Catalyst 6500 series switch. IGMP snooping constrains multicast traffic that exits through LAN ports to which hosts are connected. IGMP snooping does not constrain traffic that exits through LAN ports to which one or more multicast routers are connected.

**Note**

You must enable Protocol Independent Multicast (PIM) on all routers and switches for RGMP to work. Only PIM sparse mode is currently supported.

■ Default RGMP Configuration

All routers on the network must be RGMP-capable. RGMP-capable routers send RGMP hello messages periodically. The RGMP hello message tells the Catalyst 6500 series switch not to send multicast data to the router unless an RGMP join message has also been sent to the Catalyst 6500 series switch from that router. When an RGMP join message is sent, the router is able to receive multicast data.

To stop receiving multicast data, a router must send an RGMP leave message to the Catalyst 6500 series switch. To disable RGMP on a router, the router must send an RGMP bye message to the Catalyst 6500 series switch.

[Table 20-1](#) provides a summary of the RGMP packet types.

Table 20-1 RGMP Packet Types

Description	Action
Hello	When RGMP is enabled on the router, no multicast data traffic is sent to the router by the Catalyst 6500 series switch unless an RGMP join is specifically sent for a group.
Bye	When RGMP is disabled on the router, all multicast data traffic is sent to the router by the Catalyst 6500 series switch.
Join	Multicast data traffic for a multicast MAC address from the Layer 3 group address G is sent to the router. These packets have group G in the Group Address field of the RGMP packet.
Leave	Multicast data traffic for the group G is not sent to the router. These packets have group G in the group address field of the RGMP packet.

Default RGMP Configuration

RGMP is permanently enabled on Layer 2 LAN ports. RGMP is disabled by default on Layer 3 interfaces.

RGMP Configuration Guidelines and Restrictions

Follow these guidelines and restrictions when configuring RGMP:

- RGMP supports PIM sparse mode. RGMP does not support PIM dense mode. RGMP explicitly supports the two AutoRP groups in dense mode by not restricting traffic to those groups but by flooding it to all router ports. For this reason, you should configure PIM sparse-dense mode. If you configure groups other than the AutoRP groups for dense mode, their traffic will not be correctly forwarded through router ports that have been enabled for RGMP.
- To effectively constrain multicast traffic with RGMP, connect RGMP-enabled routers to separate ports on RGMP-enabled Catalyst 6500 series switches. (VLAN interfaces satisfy this restriction.)
- RGMP only constrains traffic that exits through LAN ports on which it detects an RGMP-enabled router. If a non-RGMP enabled router is detected on a LAN port, that port receives all multicast traffic.
- RGMP does not support directly connected multicast sources in the network. A directly connected multicast source will send multicast traffic into the network without signaling through RGMP or PIM. This multicast traffic will not be received by an RGMP-enabled router unless the router already requested receipt of that multicast group through RGMP. This restriction applies to hosts and to functions in routers that source multicast traffic, such as the **ping** and **mtrace** commands and multicast applications that source multicast traffic, such as UDPTRN.

- RGMP supports directly connected receivers in the network. Traffic to these receivers will be constrained by IGMP snooping, or if the receiver is a router itself, by PIM and RGMP.
- CGMP is not supported in networks where RGMP is enabled on routers. You cannot enable both RGMP and CGMP on a Layer 3 interface. If RGMP is enabled on a Layer 3 interface, CGMP is silently disabled and vice versa.
- The following properties of RGMP are the same as for IGMP snooping:
 - RGMP constrains traffic based on the multicast group, not on the sender's IP address.
 - If spanning tree topology changes occur in the network, the state is not flushed as it is with Cisco Group Management Protocol (CGMP).
 - RGMP does not constrain traffic for multicast groups 224.0.0.x (x = 0...255), which allows use of PIMv2 bootstrap router (BSR) in an RGMP-controlled network.
 - RGMP in Cisco network devices operates on MAC addresses, not on IP multicast addresses. Because multiple IP multicast addresses can map to one MAC address (see RFC 1112), RGMP cannot differentiate between the IP multicast groups that might map to a MAC address.
 - The capability of the Catalyst 6500 series switch to constrain traffic is limited by its content-addressable memory (CAM) table capacity.

Enabling RGMP on Layer 3 Interfaces

To enable RGMP on a Layer 3 interface, perform this task:

Command	Purpose
Step 1 Router(config)# interface {{vlan vlan_ID} {type¹ slot/port} {port-channel number}}	Selects an interface to configure.
Step 2 Router(config-if)# ip rgmp	Enables RGMP on the Layer 3 interface.
Router(config-if)# no ip rgmp	Disables RGMP on the Layer 3 interface.
Step 3 Router(config-if)# end	Exits configuration mode.
Step 4 Router# debug ip rgmp [name_or_group_address]	(Optional) Monitors RGMP.

1. type = **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, or **ge-wan**

This example shows how to configure RGMP on FastEthernet port 3/3:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fastethernet 3/3
Router(config-if)# ip rgmp
Router(config-if)# end
Router#
```

■ Enabling RGMP on Layer 3 Interfaces



Configuring Network Security

This chapter contains network security information unique to the Catalyst 6500 series switches, which supplements the network security information and procedures in these publications:

- *Cisco IOS Security Configuration Guide*, Release 12.2, at this URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/index.htm
- *Cisco IOS Security Command Reference*, Release 12.2, at this URL
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_r/index.htm

This chapter consists of these sections:

- [Configuring MAC Address-Based Traffic Blocking, page 21-1](#)
- [Configuring TCP Intercept, page 21-2](#)
- [Configuring Unicast Reverse Path Forwarding Check, page 21-2](#)

Configuring MAC Address-Based Traffic Blocking

To block all traffic to or from a MAC address in a specified VLAN, perform this task:

Command	Purpose
<pre>Router(config)# mac-address-table static mac_address vlan vlan_ID drop</pre>	Blocks all traffic to or from the configured MAC address in the specified VLAN.
<pre>Router(config)# no mac-address-table static mac_address vlan vlan_ID</pre>	Clears MAC address-based blocking.

This example shows how to block all 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 TCP Intercept

The PFC3 provides Netflow table hardware support for TCP intercept watch mode and intercept mode without timeout. Intercept mode with timeout is supported in software on the MSFC3.

For configuration procedures, refer to the *Cisco IOS Security Configuration Guide*, Release 12.2, “Traffic Filtering and Firewalls,” “Configuring TCP Intercept (Preventing Denial-of-Service Attacks),” at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/ftraw/ftraw.htm

Configuring Unicast Reverse Path Forwarding Check

These sections describe configuring Cisco IOS Unicast Reverse Path Forwarding check (Unicast RPF check):

- [Understanding Unicast RPF Check Support, page 21-2](#)
- [Configuring Unicast RPF Check, page 21-3](#)

Understanding Unicast RPF Check Support

For a complete explanation of how Unicast PRF check works, refer to the *Cisco IOS Security Configuration Guide*, Release 12.2, “Other Security Features,” “Configuring Unicast Reverse Path Forwarding” at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fothersf/scfrpf.htm

The PFC3 provides hardware support for RPF check of traffic from multiple interfaces.

With strict-method Unicast PRF check, the PFC3 supports two parallel paths for all prefixes in the routing table, and up to four parallel paths for prefixes reached through any of four user-configurable RPF interface groups (each interface group can contain four interfaces).

With loose-method Unicast PRF check (also known as exist-only method), the PFC3 supports up to eight reverse-path interfaces (the Cisco IOS software is limited to eight reverse paths in the routing table).

There are four methods of performing Unicast PRF check in Cisco IOS:

- Strict Unicast PRF check
- Strict Unicast PRF check with allow-default
- Loose Unicast PRF check
- Loose Unicast PRF check with allow-default

You configure Unicast PRF check on a per-interface basis, but the PFC3 supports only one Unicast PRF method for all interfaces that have Unicast PRF check enabled. When you configure an interface to use a Unicast PRF method that is different from the currently configured method, all other interfaces in the system that have Unicast PRF check enabled use the new method.

**Note**

- If you configure Unicast RPF check to filter with an ACL, the PFC3 determines whether or not traffic matches the ACL. The PFC3 sends the traffic denied by the RPF ACL to the MSFC3 for the Unicast PRF check. Packets permitted by the ACL are forwarded in hardware without a Unicast PRF check.
- Because the packets in a denial-of-service attack typically match the deny ACE and are sent to the MSFC3 for the Unicast PRF check, they can overload the MSFC3.
- The PFC3 provides hardware support for traffic that does not match the Unicast RPF check ACL, but that does match an input security ACL.
- ACL-based Unicast RPF check is processed in software on the MSFC3. (CSCdz35099)
- The PFC3 does not support Unicast RPF check for policy-based routing (PBR) traffic. (CSCea53554)

Configuring Unicast RPF Check

These sections describe how to configure Unicast RPF check:

- [Configuring the Unicast RPF Check Mode, page 21-3](#)
- [Configuring the Multiple-Path Unicast RPF Check Mode, page 21-5](#)
- [Enabling Self-Pinging, page 21-6](#)

Configuring the Unicast RPF Check Mode

There are two Unicast RPF check modes:

- Strict check mode, which verifies that the source IP address exists in the FIB table and verifies that the source IP address is reachable through the input port.
- Exist-only check mode, which only verifies that the source IP address exists in the FIB table.

**Note**

The most recently configured mode is automatically applied to all ports configured for Unicast RPF check.

To configure Unicast RPF check mode, perform this task:

Command	Purpose
Step 1 Router(config)# interface {{vian <i>vlan_ID</i> } {type ¹ <i>slot/port</i> } {port-channel <i>number</i> }}	Selects an interface to configure. Note Based on the input port, Unicast RPF check verifies the best return path before forwarding the packet on to the next destination.
Step 2 Router(config-if)# ip verify unicast source reachable-via {rx any} [allow-default] [list] Router(config-if)# no ip verify unicast	Configures the Unicast RPF check mode. Reverts to the default Unicast RPF check mode.
Step 3 Router(config-if)# exit	Exits interface configuration mode.
Step 4 Router# show mls cef ip rpf	Verifies the configuration.

■ Configuring Unicast Reverse Path Forwarding Check

- type* = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

When configuring the Unicast RPF check mode, note the following syntax information:

- Use the **rx** keyword to enable strict check mode.
- Use the **any** keyword to enable exist-only check mode.
- Use the **allow-default** keyword to allow use of the default route for RPF verification.
- Use the *list* option to identify an access list.
 - If the access list denies network access, spoofed packets are dropped at the port.
 - If the access list permits network access, spoofed packets are forwarded to the destination address. Forwarded packets are counted in the interface statistics.
 - If the access list includes the logging action, information about the spoofed packets is sent to the log server.



Note When you enter the **ip verify unicast source reachable-via** command, the Unicast RPF check mode changes on all ports in the switch.

This example shows how to enable Unicast RPF exist-only check mode on Gigabit Ethernet port 4/1:

```
Router(config)# interface gigabitethernet 4/1
Router(config-if)# ip verify unicast source reachable-via any
Router(config-if)# end
Router#
```

This example shows how to enable Unicast RPF strict check mode on Gigabit Ethernet port 4/2:

```
Router(config)# interface gigabitethernet 4/2
Router(config-if)# ip verify unicast source reachable-via rx
Router(config-if)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show running-config interface gigabitethernet 4/2
Building configuration...
Current configuration : 114 bytes
!
interface GigabitEthernet4/2
ip address 42.0.0.1 255.0.0.0
ip verify unicast reverse-path
no cdp enable
end
Router# show running-config interface gigabitethernet 4/1
Building configuration...
Current configuration : 114 bytes
!
interface GigabitEthernet4/1
ip address 41.0.0.1 255.0.0.0
→ ip verify unicast reverse-path (RPF mode on g4/1 also changed to strict-check RPF mode)
no cdp enable
end
Router#
```

Configuring the Multiple-Path Unicast RPF Check Mode

To configure the multiple-path Unicast PRF check mode, perform this task:

Command	Purpose
Step 1 Router(config)# mls ip cef rpf mpath {punt pass interface-group}	Configures the multiple path RPF check mode.
Step 2 Router(config)# no mls ip cef rpf mpath {punt interface-group}	Returns to the default (mls ip cef rpf mpath punt).
Step 3 Router(config)# end	Exits configuration mode.
Step 4 Router# show mls cef ip rpf	Verifies the configuration.

When configuring multiple path RPF check, note the following syntax information:

- **punt** (default)—The PFC3 performs the Unicast PRF check in hardware for up to two interfaces per prefix. Packets arriving on any additional interfaces are redirected (punted) to the MSFC3 for Unicast PRF check in software.
- **pass**—The PFC3 performs the Unicast PRF check in hardware for single-path and two-path prefixes. Unicast RPF check is disabled for packets coming from multipath prefixes with three or more reverse-path interfaces (these packets always pass the Unicast PRF check).
- **interface-group**—The PFC3 performs the Unicast PRF check in hardware for single-path and two-path prefixes. The PFC3 also performs the Unicast PRF check for up to four additional interfaces per prefix through user-configured multipath Unicast PRF check interface groups. Unicast RPF check is disabled for packets coming from other multipath prefixes that have three or more reverse-path interfaces (these packets always pass the Unicast PRF check).

This example shows how to configure multiple path RPF check:

```
Router(config)# mls ip cef rpf mpath punt
```

Configuring Multiple-Path Interface Groups

To configure multiple-path Unicast PRF interface groups, perform this task:

Command	Purpose
Step 1 Router(config)# mls ip cef rpf interface-group [0 1 2 3] interface1 [interface2 [interface3 [interface4]]]	Configures a multiple path RPF interface group.
Step 2 Router(config)# mls ip cef rpf interface-group group_number	Removes an interface group.
Step 3 Router(config)# end	Exits configuration mode.
Step 4 Router# show mls cef ip rpf	Verifies the configuration.

This example shows how to configure interface group 2:

```
Router(config)# mls ip cef rpf interface-group 2 fastethernet 3/3 fastethernet 3/4
fastethernet 3/5 fastethernet 3/6
```

Enabling Self-Pinging

With Unicast RPF check enabled, by default the switch cannot ping itself.

To enable self-pinging, perform this task:

	Command	Purpose
Step 1	Router(config)# interface {{vlan <i>vlan_ID</i> } {type ¹ <i>slot/port</i> } {port-channel <i>number</i> }}	Selects the interface to configure.
Step 2	Router(config-if)# ip verify unicast source reachable-via any allow-self-ping Router(config-if)# no ip verify unicast source reachable-via any allow-self-ping	Enables the switch to ping itself or a secondary address. Disables self-pinging.
Step 3	Router(config-if)# exit	Exits interface configuration mode.

1. *type* = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

This example shows how to enable self-pinging:

```
Router(config)# interface gigabitethernet 4/1
Router(config-if)# ip verify unicast source reachable-via any allow-self-ping
Router(config-if)# end
```



Understanding Cisco IOS ACL Support

This chapter describes Cisco IOS ACL support on the Catalyst 6500 series switches.

- [Cisco IOS ACL Configuration Guidelines and Restrictions, page 22-1](#)
- [Hardware and Software ACL Support, page 22-2](#)
- [Guidelines and Restrictions for Using Layer 4 Operators in ACLs, page 22-2](#)

For complete information about configuring Cisco IOS ACLs, refer to the *Cisco IOS Security Configuration Guide*, Release 12.2, “Traffic Filtering and Firewalls,” at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/ftrawf/index.htm

Cisco IOS ACL Configuration Guidelines and Restrictions

The following guidelines and restrictions apply to Cisco IOS ACL configurations:

- You can apply Cisco IOS ACLs directly to Layer 3 ports and to VLAN interfaces.
- You can apply VLAN ACLs (VACLs) to VLANs (refer to [Chapter 23, “Configuring VLAN ACLs”](#)).
- Each type of ACL (IP, IPX, and MAC) filters only traffic of the corresponding type. A Cisco IOS MAC ACL never matches IP or IPX traffic.
- The PFC3 does not provide hardware support for Cisco IOS IPX ACLs. Cisco IOS IPX ACLs are supported in software on the MSFC3.
- By default, the MSFC3 sends Internet Control Message Protocol (ICMP) unreachable messages when a packet is denied by an access group.

With the **ip unreachable** command enabled (which is the default), a Supervisor Engine 3 drops most of the denied packets in hardware and sends only a small number of packets to the MSFC3 to be dropped (10 packets per second, maximum), which generates ICMP-unreachable messages.

With the **ip unreachable** command enabled, a Supervisor Engine 1 sends all the denied packets to the MSFC3 to be dropped, which generates ICMP-unreachable messages. With a Supervisor Engine 1, to drop access list-denied packets in hardware, you must disable ICMP-unreachable messages using the **no ip unreachable** interface configuration command.

To eliminate the load imposed on the MSFC3 CPU by the task of dropping denied packets and generating ICMP-unreachable messages, you can enter the **no ip unreachable** interface configuration command to disable ICMP unreachable messages, which allows all access group-denied packets to be dropped in hardware.

- ICMP unreachable messages are not sent if a packet is denied by a VACL.

Hardware and Software ACL Support

Access control lists (ACLs) can be processed in hardware by the Policy Feature Card 3 (PFC3), a Distributed Forwarding Card 3 (DFC3), or in software by the Multilayer Switch Feature Card 3 (MSFC3). The following behavior describes software and hardware handling of ACLs:

- ACL flows that match a “deny” statement in standard and extended ACLs (input and output) are dropped in hardware if “ip unreachables” is disabled.
- ACL flows that match a “permit” statement in standard and extended ACLs (input and output) are processed in hardware.
- VLAN ACL (VACL) flows are processed in hardware. If a field specified in a VACL is not supported by hardware processing that field is ignored (for example, the **log** keyword in an ACL) or the whole configuration is rejected (for example, a VACL containing IPX ACL parameters).
- VACL logging is processed in software.
- Dynamic ACL flows are processed in the hardware; however, idle timeout is processed in software.
- IP accounting for an ACL access violation on a given port is supported by forwarding all denied packets for that port to the MSFC3 for software processing without impacting other flows.
- The PFC3 does not provide hardware support for Cisco IOS IPX ACLs. Cisco IOS IPX ACLs are supported in software on the MSFC3.
- Extended name-based MAC address ACLs are supported in hardware.
- The following ACL types are processed in software:
 - Standard XNS access list
 - Extended XNS access list
 - DECnet access list
 - Extended MAC address access list
 - Protocol type-code access list

**Note**

IP packets with a header length of less than five will not be access controlled.

- Flows that require logging are processed in software without impacting nonlogged flow processing in hardware.
- The forwarding rate for software-processed flows is substantially less than for hardware-processed flows.
- When you enter the **show ip access-list** command, the match count displayed does not include packets processed in hardware.

Guidelines and Restrictions for Using Layer 4 Operators in ACLs

These sections describe guidelines and restrictions when configuring ACLs that include Layer 4 port operations:

- [Determining Layer 4 Operation Usage, page 22-3](#)
- [Determining Logical Operation Unit Usage, page 22-3](#)

Determining Layer 4 Operation Usage

You can specify these types of operations:

- gt (greater than)
- lt (less than)
- neq (not equal)
- eq (equal)
- range (inclusive range)

We recommend that you do not specify more than *nine different* operations on the same ACL. If you exceed this number, each new operation might cause the affected ACE to be translated into more than one ACE.

Use the following two guidelines to determine Layer 4 operation usage:

- Layer 4 operations are considered different if the operator or the operand differ. For example, in this ACL there are three different Layer 4 operations (“gt 10” and “gt 11” are considered two different Layer 4 operations):

```
... gt 10 permit
... lt 9 deny
... gt 11 deny
```



Note There is no limit to the use of “eq” operators as the “eq” operator does not use a logical operator unit (LOU) or a Layer 4 operation bit. See the [“Determining Logical Operation Unit Usage” section on page 22-3](#) for a description of LOUs.

- Layer 4 operations are considered different if the same operator/operand couple applies once to a source port and once to a destination port. For example, in this ACL there are two different Layer 4 operations because one ACE applies to the source port and one applies to the destination port.

```
... Src gt 10 ...
... Dst gt 10
```

Determining Logical Operation Unit Usage

Logical operation units (LOUs) are registers that store operator-operand couples. All ACLs use LOUs. There can be up to 32 LOUs; each LOU can store two different operator-operand couples with the exception of the range operator. LOU usage per Layer 4 operation is as follows:

- gt uses 1/2 LOU
- lt uses 1/2 LOU
- neq uses 1/2 LOU
- range uses 1 LOU
- eq does not require a LOU

For example, this ACL would use a single LOU to store two different operator-operand couples:

```
... Src gt 10 ...
... Dst gt 10
```

■ Guidelines and Restrictions for Using Layer 4 Operators in ACLs

A more detailed example follows:

```
ACL1
... (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

ACL2
... (dst port) gt 20 deny
... (src port) lt 9 deny
... (src port) range 11 13 deny
... (dst port) neq 6 permit
```

The Layer 4 operations and LOU usage is as follows:

- ACL1 Layer 4 operations: 5
- ACL2 Layer 4 operations: 4
- LOUs: 4

An explanation of the LOU usage follows:

- LOU 1 stores “gt 10” and “lt 9”
- LOU 2 stores “gt 11” and “neq 6”
- LOU 3 stores “gt 20” (with space for one more)
- LOU 4 stores “range 11 13” (range needs the entire LOU)



Configuring VLAN ACLs

This chapter describes how to configure VLAN ACLs (VACLS) on Catalyst 6500 series switches:

- [Understanding VACLS, page 23-1](#)
- [Configuring VACLS, page 23-4](#)
- [Configuring VACL Logging, page 23-8](#)

Understanding VACLS

These sections describe VACLS:

- [VACL Overview, page 23-1](#)
- [Bridged Packets, page 23-2](#)
- [Routed Packets, page 23-2](#)
- [Multicast Packets, page 23-3](#)

VACL Overview

VACLS can provide access control for all packets that are bridged within a VLAN or that are routed into or out of a VLAN. Unlike regular Cisco IOS standard or extended ACLs that are configured on router interfaces only and are applied on routed packets only, VACLS apply to all packets and can be applied to any VLAN or WAN interface. VACLS are processed in hardware. VACLS use Cisco IOS ACLs. VACLS ignore any Cisco IOS ACL fields that are not supported in hardware.

You can configure VACLS for IP, IPX, and MAC-Layer traffic.

When you configure a VACL and apply it to a VLAN, all packets entering the VLAN are checked against this VACL. If you apply a VACL to the VLAN and an ACL to a routed interface in the VLAN, a packet coming in to the VLAN is first checked against the VACL and, if permitted, is then checked against the input ACL before it is handled by the routed interface. When the packet is routed to another VLAN, it is first checked against the output ACL applied to the routed interface and, if permitted, the VACL configured for the destination VLAN is applied. If a VACL is configured for a packet type and a packet of that type does not match the VACL, the default action is deny.

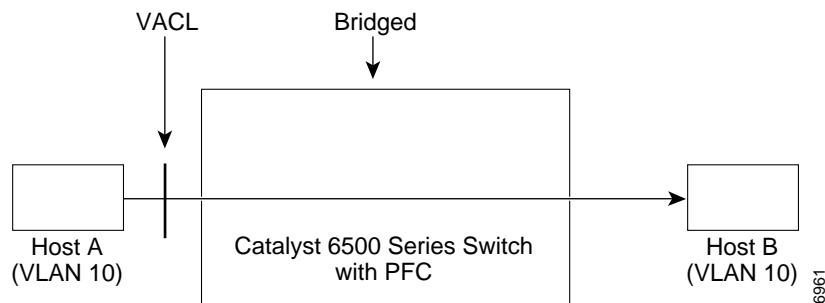


- Note**
- TCP Intercepts and Reflexive ACLs take precedence over a VACL action if these are configured on the same interface.
 - VACLs and CBAC cannot be configured on the same interface.
 - IGMP packets are not checked against VACLs.

Bridged Packets

Figure 23-1 shows a VACL applied on bridged packets.

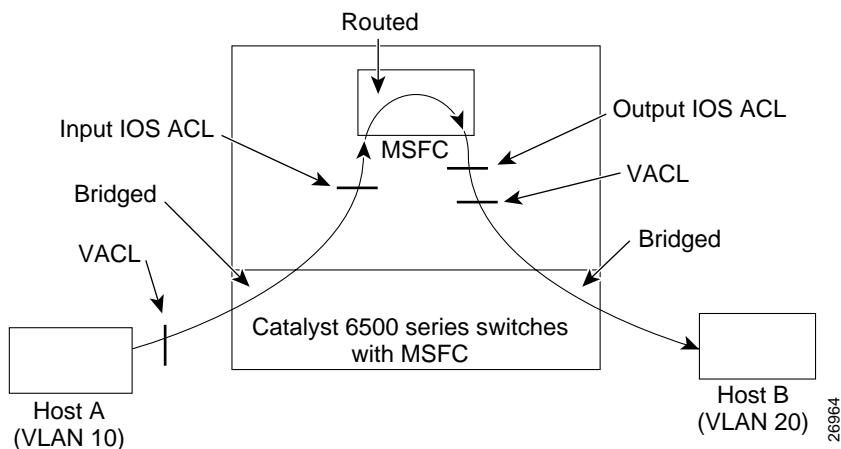
Figure 23-1 Applying VACLS on Bridged Packets



Routed Packets

Figure 23-2 shows how ACLs are applied on routed and Layer 3-switched packets. For routed or Layer 3-switched packets, the ACLs are applied in the following order:

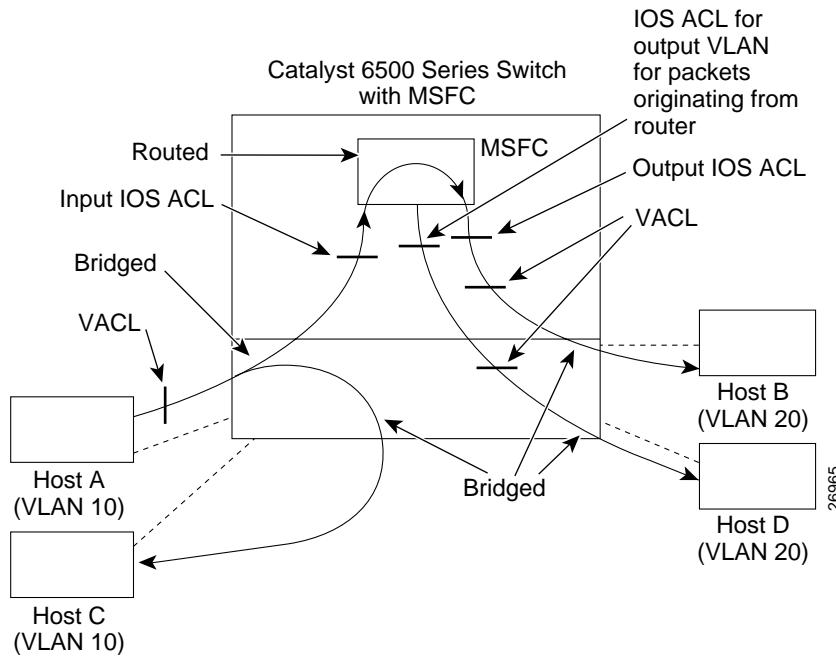
1. VACL for input VLAN
2. Input Cisco IOS ACL
3. Output Cisco IOS ACL
4. VACL for output VLAN

Figure 23-2 Applying VACLs on Routed Packets

Multicast Packets

Figure 23-3 shows how ACLs are applied on packets that need multicast expansion. For packets that need multicast expansion, the ACLs are applied in the following order:

1. Packets that need multicast expansion:
 - a. VACL for input VLAN
 - b. Input Cisco IOS ACL
2. Packets after multicast expansion:
 - a. Output Cisco IOS ACL
 - b. VACL for output VLAN
3. Packets originating from router—VACL for output VLAN

Figure 23-3 Applying VACLS on Multicast Packets

Configuring VACLS

These sections describe configuring VACLS:

- [VACL Configuration Overview, page 23-4](#)
- [Defining a VLAN Access Map, page 23-5](#)
- [Configuring a Match Clause in a VLAN Access Map Sequence, page 23-6](#)
- [Configuring an Action Clause in a VLAN Access Map Sequence, page 23-6](#)
- [Applying a VLAN Access Map, page 23-7](#)
- [Verifying VLAN Access Map Configuration, page 23-7](#)
- [VLAN Access Map Configuration and Verification Examples, page 23-7](#)

VACL Configuration Overview

VACLS use standard and extended Cisco IOS IP and IPX ACLs, and MAC-Layer named ACLs (see the “[Configuring MAC-Layer Named Access Lists \(Optional\)](#)” section on page 24-38) and VLAN access maps.

VLAN access maps can be applied to VLANs.

Each VLAN access map can consist of one or more map sequences, each sequence with a match clause and an action clause. The match clause specifies IP, IPX, or MAC ACLs for traffic filtering and the action clause specifies the action to be taken when a match occurs. When a flow matches a permit ACL entry, the associated action is taken and the flow is not checked against the remaining sequences. When a flow

matches a deny ACL entry, it will be checked against the next ACL in the same sequence or the next sequence. If a flow does not match any ACL entry and at least one ACL is configured for that packet type, the packet is denied.

To use access-control for both bridged and routed traffic, you can use VACLs alone or a combination of VACLs and ACLs. You can define ACLs on the VLAN interfaces to use access-control for both the input and output routed traffic. You can define a VACL to use access-control for the bridged traffic.

The following caveats apply to ACLs when used with VACLs:

- Packets that require logging on the outbound ACLs are not logged if they are denied by a VACL.
- VACLs are applied on packets before NAT translation. If the translated flow is not subject to access control, the flow might be subject to access control after the translation because of the VACL configuration.

The action clause in a VACL can be forward, drop, or redirect. Traffic can also be logged. VACLs applied to WAN interfaces do not support the redirect or log actions.


Note

- VACLs have an implicit deny at the end of the map; a packet is denied if it does not match any ACL entry, and at least one ACL is configured for the packet type.
- If an empty or undefined ACL is specified in a VACL, any packets will match the ACL and the associated action is taken.

Defining a VLAN Access Map

To define a VLAN access map, perform this task:

Command	Purpose
Router(config)# vlan access-map <i>map_name</i> [0-65535]	Defines the VLAN access map. Optionally, you can specify the VLAN access map sequence number.
Router(config)# no vlan access-map <i>map_name</i> 0-65535	Deletes a map sequence from the VLAN access map.
Router(config)# no vlan access-map <i>map_name</i>	Deletes the VLAN access map.

When defining a VLAN access map, note the following syntax information:

- To insert or modify an entry, specify the map sequence number.
- If you do not specify the map sequence number, a number is automatically assigned.
- You can specify only one match clause and one action clause per map sequence.
- Use the **no** keyword with a sequence number to remove a map sequence.
- Use the **no** keyword without a sequence number to remove the map.

See the “[VLAN Access Map Configuration and Verification Examples](#)” section on page 23-7.

Configuring a Match Clause in a VLAN Access Map Sequence

To configure a match clause in a VLAN access map sequence, perform this task:

Command	Purpose
Router(config-access-map)# match {ip address {1-199 1300-2699 acl_name} ipx address {800-999 acl_name} mac address acl_name}	Configures the match clause in a VLAN access map sequence.
Router(config-access-map)# no match {ip address {1-199 1300-2699 acl_name} ipx address {800-999 acl_name} mac address acl_name}	Deletes the match clause in a VLAN access map sequence.

When configuring a match clause in a VLAN access map sequence, note the following syntax information:

- You can select one or more ACLs.
- Use the **no** keyword to remove a match clause or specified ACLs in the clause.
- For information about named MAC-Layer ACLs, refer to the “[Configuring MAC-Layer Named Access Lists \(Optional\)](#)” section on page 24-38.
- For information about Cisco IOS ACLs, refer to the *Cisco IOS Security Configuration Guide*, Release 12.2, “Traffic Filtering and Firewalls,” at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/ftrawf/index.htm

See the “[VLAN Access Map Configuration and Verification Examples](#)” section on page 23-7.

Configuring an Action Clause in a VLAN Access Map Sequence

To configure an action clause in a VLAN access map sequence, perform this task:

Command	Purpose
Router(config-access-map)# action {drop [log] {forward} {redirect {{ethernet fastethernet gigabitethernet tengigabitethernet} slot/port} {port-channel channel_id}}}	Configures the action clause in a VLAN access map sequence.
Router(config-access-map)# no action {drop [log] {forward} {redirect {{ethernet fastethernet gigabitethernet tengigabitethernet} slot/port} {port-channel channel_id}}}	Deletes the action clause in from the VLAN access map sequence.

When configuring an action clause in a VLAN access map sequence, note the following syntax information:

- You can set the action to drop, forward, or redirect packets.
- Forwarded packets are still subject to any configured Cisco IOS security ACLs.
- When the **log** action is specified, dropped packets are logged in software. Only dropped IP packets can be logged.
- The **redirect** action allows you to specify up to five interfaces, which can be physical interfaces or EtherChannels. You cannot specify packets to be redirected to an EtherChannel member or a VLAN interface.

- The redirect interface must be in the VLAN for which the VACL access map is configured.
- Use the **no** keyword to remove an action clause or specified redirect interfaces.

See the “[VLAN Access Map Configuration and Verification Examples](#)” section on page 23-7.

Applying a VLAN Access Map

To apply a VLAN access map, perform this task:

Command	Purpose
Router(config)# vlan filter <i>map_name</i> { <i>vlan-list</i> <i>vlan_list</i> }	Applies the VLAN access map to the specified VLANs.
Router(config)# no vlan filter <i>map_name</i> [<i>vlan-list</i> <i>vlan_list</i>]	Removes the VLAN access map from the specified VLANs.

When applying a VLAN access map, note the following syntax information:

- You can apply the VLAN access map to one or more VLANs.
- The *vlan_list* parameter can be a single VLAN ID or a comma-separated list of VLAN IDs or VLAN ID ranges (*vlan_ID*-*vlan_ID*).
- You can apply only one VLAN access map to each VLAN.
- VACLS applied to VLANs are active only for VLANs with a Layer 3 VLAN interface configured. VACLS applied to VLANs without a Layer 3 VLAN interface are inactive. Applying a VLAN access map to a VLAN without a Layer 3 VLAN interface creates an administratively down Layer 3 VLAN interface to support the VLAN access map. If creation of the Layer 3 VLAN interface fails, the VACL is inactive.
- You cannot apply a VACL to a secondary private VLAN. VACLS applied to primary private VLANs also apply to secondary private VLANs.
- Use the **no** keyword to clear VLAN access maps from VLANs.

See the “[VLAN Access Map Configuration and Verification Examples](#)” section on page 23-7.

Verifying VLAN Access Map Configuration

To verify VLAN access map configuration, perform this task:

Command	Purpose
Router# show vlan access-map [<i>map_name</i>]	Verifies VLAN access map configuration by displaying the content of a VLAN access map.
Router# show vlan filter [<i>access-map</i> <i>map_name</i> <i>vlan</i> <i>vlan_id</i>]	Verifies VLAN access map configuration by displaying the mappings between VACLS and VLANs.

VLAN Access Map Configuration and Verification Examples

Assume IP-named ACL **net_10** and **any_host** are defined as follows:

■ Configuring VACL Logging

```
Router# show ip access-lists net_10
Extended IP access list net_10
    permit ip 10.0.0.0 0.255.255.255 any
```

```
Router# show ip access-lists any_host
Standard IP access list any_host
    permit any
```

This example shows how to define and apply a VLAN access map to forward IP packets. In this example, IP traffic matching net_10 is forwarded and all other IP packets are dropped due to the default drop action. The map is applied to VLAN 12 to 16.

```
Router(config)# vlan access-map thor 10
Router(config-access-map)# match ip address net_10
Router(config-access-map)# action forward
Router(config-access-map)# exit
Router(config)# vlan filter thor vlan-list 12-16
```

This example shows how to define and apply a VLAN access map to drop and log IP packets. In this example, IP traffic matching net_10 is dropped and logged and all other IP packets are forwarded:

```
Router(config)# vlan access-map ganymede 10
Router(config-access-map)# match ip address net_10
Router(config-access-map)# action drop log
Router(config-access-map)# exit
Router(config)# vlan access-map ganymede 20
Router(config-access-map)# match ip address any_host
Router(config-access-map)# action forward
Router(config-access-map)# exit
Router(config)# vlan filter ganymede vlan-list 7-9
```

Configuring VACL Logging

When you configure VACL logging, IP packets that are denied generate log messages in these situations:

- When the first matching packet is received
- For any matching packets received during the last 5-minute interval
- If the threshold is reached before the 5-minute interval

Log messages are generated on a per-flow basis. A flow is defined as packets with the same IP addresses and Layer 4 (UDP or TCP) port numbers. When a log message is generated, the timer and packet count is reset.

These restrictions apply to VACL logging:

- Because of the rate-limiting function for redirected packets, VACL logging counters may not be accurate.
- Only denied IP packets are logged.

To configure VACL logging, use the **action drop log** command action in VLAN access map submode (see the “[Configuring VACLS](#)” section on page 23-4 for configuration information) and perform this task in global configuration mode to specify the global VACL logging parameters:

Command	Purpose
Step 1 Router(config)# vlan access-log maxflow max_number	Sets the log table size. The content of the log table can be deleted by setting the maxflow number to 0. The default is 500 with a valid range of 0 to 2048. When the log table is full, logged packets from new flows are dropped by the software.
Step 2 Router(config)# vlan access-log ratelimit pps	Sets the maximum redirect VACL logging packet rate. The default packet rate is 2000 packets per second with a valid range of 0 to 5000. Packets exceeding the limit are dropped by the hardware.
Step 3 Router(config)# vlan access-log threshold pkt_count	Sets the logging threshold. A logging message is generated if the threshold for a flow is reached before the 5-minute interval. By default, no threshold is set.
Step 4 Router(config)# exit	Exits VLAN access map configuration mode.
Step 5 Router# show vlan access-log config	(Optional) Displays the configured VACL logging properties.
Step 6 Router# show vlan access-log flow protocol {{src_addr src_mask} any {host {hostname host_ip}}} {{dst_addr dst_mask} any {host {hostname host_ip}}} [vlan vlan_id]	(Optional) Displays the content of the VACL log table.
Step 7 Router# show vlan access-log statistics	(Optional) Displays packet and message counts and other statistics.

This example shows how to configure global VACL logging in hardware:

```
Router(config)# vlan access-log maxflow 800
Router(config)# vlan access-log ratelimit 2200
Router(config)# vlan access-log threshold 4000
```

■ Configuring VACL Logging



Configuring PFC QoS

This chapter describes how to configure quality of service (QoS) as implemented on the Policy Feature Card 3 (PFC3) on the Catalyst 6500 series switches.

**Note**

For complete syntax and usage information for the commands used in this publication, refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication.

This chapter contains these sections:

- [Understanding How PFC QoS Works, page 24-1](#)
- [PFC QoS Default Configuration, page 24-22](#)
- [PFC QoS Configuration Guidelines and Restrictions, page 24-28](#)
- [Configuring PFC QoS, page 24-30](#)

Understanding How PFC QoS Works

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 makes network performance more predictable and bandwidth utilization more effective.

**Note**

On the Catalyst 6500 series switches, queue architecture and QoS queuing features such as Weighted-Round Robin (WRR) and Weighted Random Early Detection (WRED) are implemented with a fixed configuration in Application Specific Integrated Circuits (ASICs). The queuing architecture cannot be reconfigured. For more information, see the “[Receive Queues](#)” section on page 24-10 and the “[Transmit Queues](#)” section on page 24-19.

These sections describe PFC QoS:

- [QoS Terminology, page 24-2](#)
- [PFC QoS Feature Flowcharts, page 24-4](#)
- [PFC QoS Feature Summary, page 24-8](#)

- Ingress LAN Port Features, page 24-9
- PFC3 Marking and Policing, page 24-13
- LAN Egress Port Features, page 24-19

QoS Terminology

This section defines some QoS terminology:

- *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 LAN ports configured as Layer 2 ISL trunks, all traffic is in ISL frames. On LAN ports 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 Type of Service (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 Value Maps” section on page 24-51).



Note Layer 3 IP packets can carry either an IP precedence value or a DSCP value. PFC QoS supports the use of either value, since DSCP values are backwards compatible with IP precedence values (see Table 24-1).

Table 24-1 IP Precedence and DSCP Values

3-bit IP Precedence	6 MSb ¹ of ToS						6-bit DSCP		3-bit IP Precedence	6 MSb ¹ of ToS						6-bit DSCP
	8	7	6	5	4	3				8	7	6	5	4	3	
0	0	0	0	0	0	0	0	0	4	1	0	0	0	0	0	32
	0	0	0	0	0	1	1	1		1	0	0	0	0	1	33
	0	0	0	0	1	0	2	1		1	0	0	0	1	0	34
	0	0	0	0	1	1	3	1		1	0	0	0	1	1	35
	0	0	0	1	0	0	4	1		1	0	0	1	0	0	36
	0	0	0	1	0	1	5	1		1	0	0	1	0	1	37
	0	0	0	1	1	0	6	1		1	0	0	1	1	0	38
	0	0	0	1	1	1	7	1		1	0	0	1	1	1	39
1	0	0	1	0	0	0	8	5	5	1	0	1	0	0	0	40
	0	0	1	0	0	1	9	1		1	0	1	0	0	1	41
	0	0	1	0	1	0	10	1		1	0	1	0	1	0	42
	0	0	1	0	1	1	11	1		1	0	1	0	1	1	43
	0	0	1	1	0	0	12	1		1	0	1	1	0	0	44
	0	0	1	1	0	1	13	1		1	0	1	1	0	1	45
	0	0	1	1	1	0	14	1		1	0	1	1	1	0	46
	0	0	1	1	1	1	15	1		1	0	1	1	1	1	47
2	0	1	0	0	0	0	16	6	6	1	1	0	0	0	0	48
	0	1	0	0	0	1	17	1		1	1	0	0	0	1	49
	0	1	0	0	1	0	18	1		1	1	0	0	1	0	50
	0	1	0	0	1	1	19	1		1	1	0	0	1	1	51
	0	1	0	1	0	0	20	1		1	1	0	1	0	0	52
	0	1	0	1	0	1	21	1		1	1	0	1	0	1	53
	0	1	0	1	1	0	22	1		1	1	0	1	1	0	54
	0	1	0	1	1	1	23	1		1	1	0	1	1	1	55
3	0	1	1	0	0	0	24	7	7	1	1	1	0	0	0	56
	0	1	1	0	0	1	25	1		1	1	1	0	0	1	57
	0	1	1	0	1	0	26	1		1	1	1	0	1	0	58
	0	1	1	0	1	1	27	1		1	1	1	0	1	1	59
	0	1	1	1	0	0	28	1		1	1	1	1	0	0	60
	0	1	1	1	0	1	29	1		1	1	1	1	0	1	61
	0	1	1	1	1	0	30	1		1	1	1	1	1	0	62
	0	1	1	1	1	1	31	1		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. PFC QoS assigns frames to a queue based on Layer 2 CoS values.
- *Congestion avoidance* is the process by which PFC QoS reserves ingress and egress LAN port capacity for Layer 2 frames with high-priority Layer 2 CoS values. PFC QoS implements congestion avoidance with Layer 2 CoS value-based drop thresholds. A drop threshold is the percentage of queue buffer utilization above which frames with a specified Layer 2 CoS value is dropped, leaving the buffer available for frames with higher-priority Layer 2 CoS values.

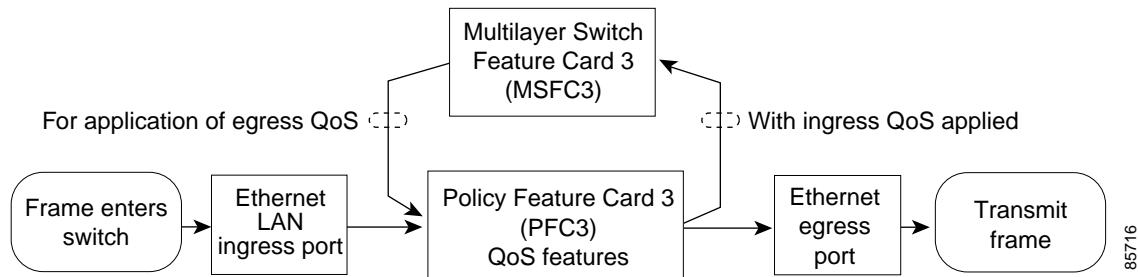
■ Understanding How PFC QoS Works

- *Policing* is limiting bandwidth used by a flow of traffic. Policing is done on the the PFC3 and Distributed Forwarding Card 3s (DFC3s). Policing can mark or drop traffic.

PFC QoS Feature Flowcharts

[Figure 24-1](#) show hows traffic flows through the components that support PFC QoS features.

Figure 24-1 Traffic Flow Through PFC QoS Features with PFC3



[Figure 24-2](#) through [Figure 24-5](#) show how the PFC QoS features are implemented on the switch components.

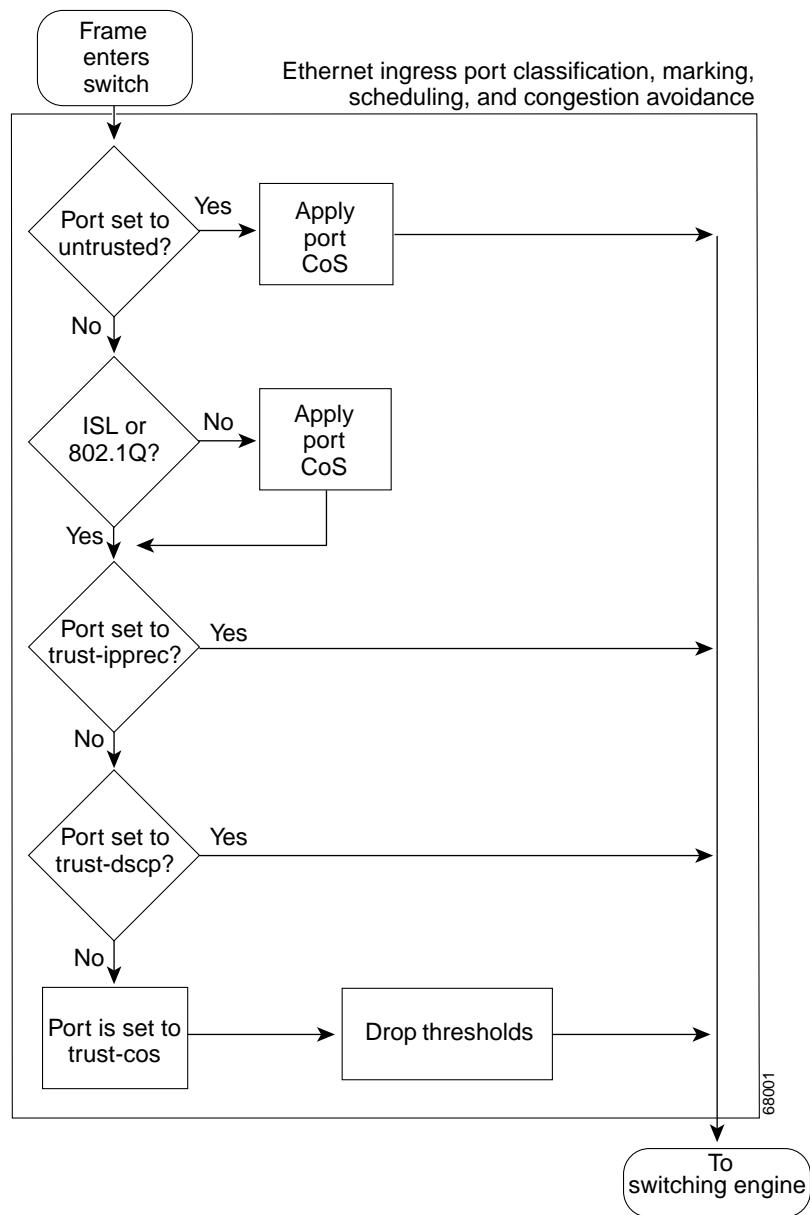
Figure 24-2 Ingress LAN Port Layer 2 PFC QoS Features

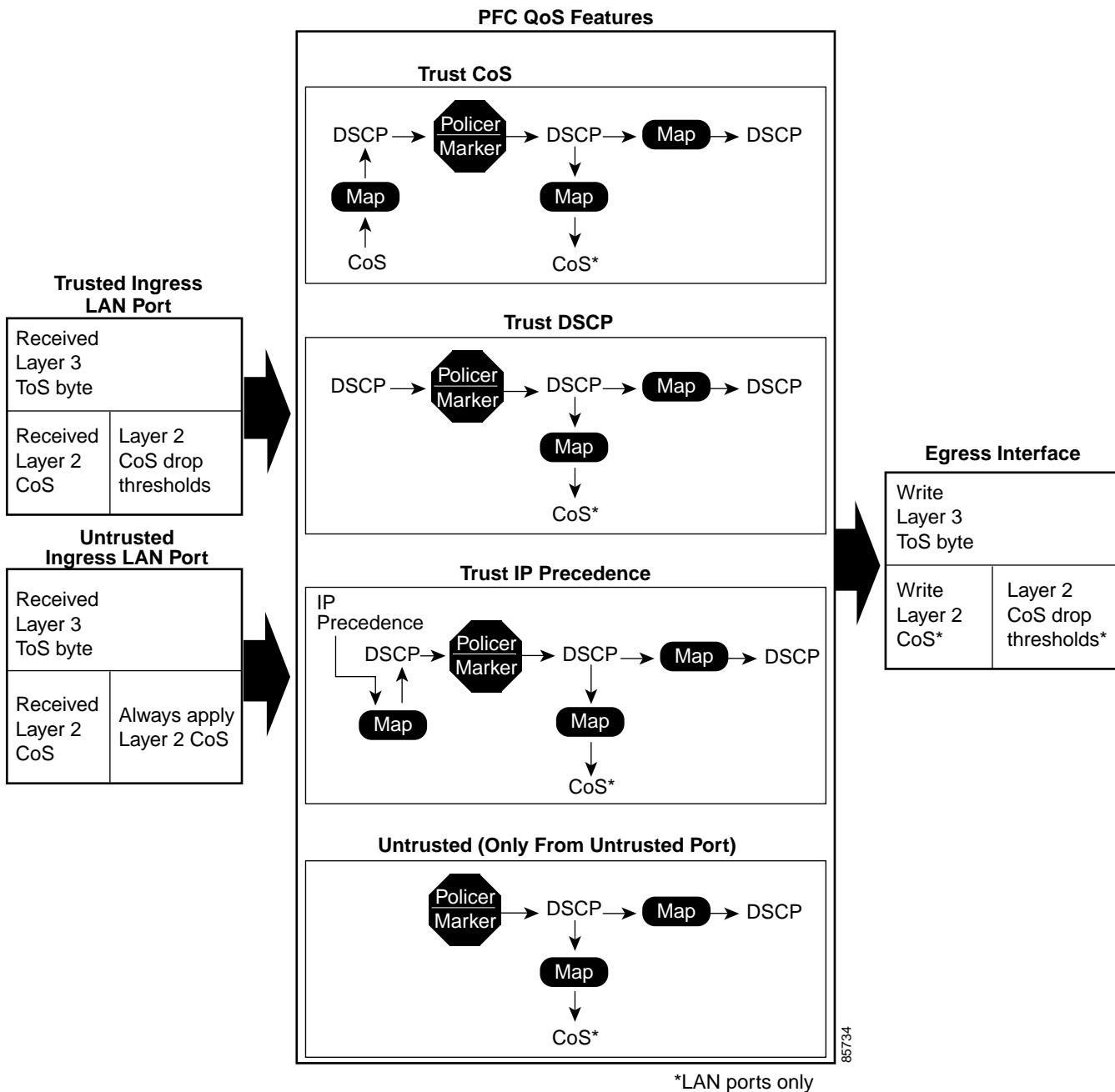
Figure 24-3 PFC3 Classification, Marking, and Policing

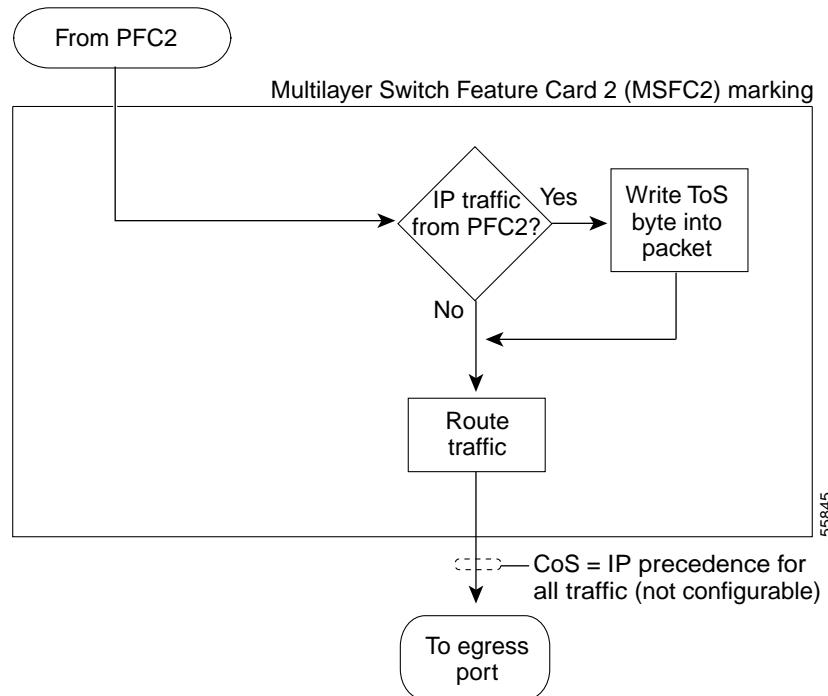
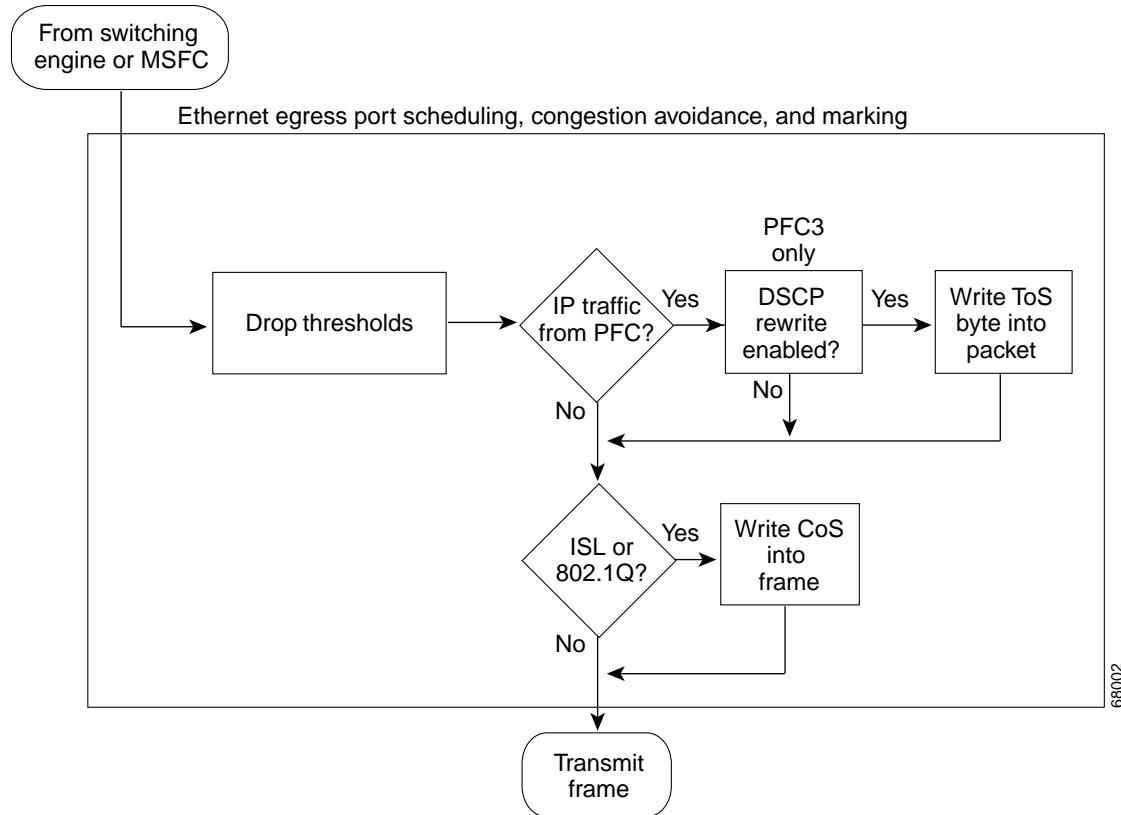
Figure 24-4 Marking with PFC3 and Multilayer Switch Feature Card 3

Figure 24-5 Egress LAN Port Scheduling, Congestion Avoidance, and Marking

PFC QoS Feature Summary

These sections summarize the PFC QoS features:

- [Ingress LAN Port Features, page 24-8](#)
- [PFC QoS Features, page 24-9](#)
- [Egress LAN Port Features, page 24-9](#)
- [MSFC3 Features, page 24-9](#)

Ingress LAN Port Features

PFC QoS supports classification, marking, scheduling, and congestion avoidance using Layer 2 CoS values at ingress LAN ports. Classification, marking, scheduling, and congestion avoidance at ingress LAN ports do not use or set Layer 3 IP precedence or DSCP values. You can configure ingress LAN port trust states that can be used by the PFC3 to set Layer 3 IP precedence or DSCP values and the Layer 2 CoS value. See [Figure 24-2](#) and the “[Ingress LAN Port Features](#)” section on page 24-9.

PFC QoS Features

On the PFC3, PFC QoS supports ingress classification, marking, and policing using policy maps. You can attach one policy map to each ingress port or EtherChannel and to VLAN interfaces for application to ingress traffic. You can attach one policy map to each VLAN interface for application to egress traffic. Each policy map can contain multiple policy-map classes. You can configure a separate policy-map class for each type of traffic handled by the interface. See the “[PFC3 Marking and Policing](#)” section on page 24-13.

Egress LAN Port Features

PFC QoS supports egress LAN port scheduling and congestion avoidance using Layer 2 CoS values. Egress LAN port marking sets Layer 2 CoS values and Layer 3 DSCP values. See the “[LAN Egress Port Features](#)” section on page 24-19.

MSFC3 Features

PFC QoS marks IP traffic transmitted to the MSFC3 with rewritten Layer 3 DSCP values. CoS is equal to IP precedence in all traffic sent from the MSFC3 to egress ports.



Note Traffic that is Layer 3 switched does not go through the MSFC3 and retains the CoS value assigned by the PFC3.

Ingress LAN Port Features

These sections describe ingress LAN port PFC QoS features:

- [Ingress LAN Port Trust States, page 24-9](#)
- [Marking at Untrusted Ingress LAN Ports, page 24-10](#)
- [Marking at Trusted Ingress LAN Ports, page 24-10](#)
- [Ingress LAN Port Scheduling and Congestion Avoidance, page 24-10](#)

Ingress LAN Port Trust States

The trust state of an ingress LAN port determines how the port marks, schedules, and classifies received Layer 2 frames, and whether or not congestion avoidance is implemented. You can configure the trust state of each ingress LAN port as follows:

- Untrusted (default)
- Trust IP precedence (not supported on **1q4t** LAN ports except Gigabit Ethernet)
- Trust DSCP (not supported on **1q4t** LAN ports except Gigabit Ethernet)
- Trust CoS (not supported on **1q4t** LAN ports except Gigabit Ethernet)

See the “[Configuring the Trust State of Ethernet LAN Ports](#)” section on page 24-56. PFC QoS implements ingress LAN port congestion avoidance only on LAN ports configured to trust CoS.



Note Ingress LAN port marking, scheduling, and congestion avoidance use Layer 2 CoS values and does not use or set Layer 3 IP precedence or DSCP values.

Marking at Untrusted Ingress LAN Ports

PFC QoS marks all frames received through untrusted ingress LAN ports with the ingress port CoS value (the default is zero). PFC QoS does not implement ingress port congestion avoidance on untrusted ingress LAN ports.



- To use the ingress port CoS value applied to untrusted traffic as the basis of egress DSCP, configure a trust-CoS policy map that matches the ingress traffic.
 - The ingress port CoS value is configurable for each ingress LAN port (see the “[Configuring the Ingress LAN Port CoS Value](#)” section on page 24-57).
-

Marking at Trusted Ingress LAN Ports

When an ISL frame enters the Catalyst 6500 series switch through a trusted ingress LAN port, PFC QoS accepts the three least significant bits in the User field as a CoS value. When an 802.1Q frame enters the switch through a trusted ingress LAN port, PFC QoS accepts the User Priority bits as a CoS value. PFC QoS marks all traffic received in untagged frames with the ingress port CoS value.



- PFC QoS uses the received CoS value in tagged trusted traffic as the basis of egress DSCP, unless there is a policy map that changes the trust state of the traffic.
 - PFC QoS uses the ingress port CoS value applied to untagged trusted traffic as the basis of egress DSCP, unless there is a policy map that changes the trust state of the traffic.
 - The ingress port CoS value is configurable for each ingress LAN port (see the “[Configuring the Ingress LAN Port CoS Value](#)” section on page 24-57).
-

Ingress LAN Port Scheduling and Congestion Avoidance

On ingress LAN ports configured to trust CoS, PFC QoS uses Layer 2 CoS-value based receive-queue drop thresholds to avoid congestion (see the “[Configuring the Trust State of Ethernet LAN Ports](#)” section on page 24-56).

Receive Queues

Enter the **show queueing interface {ethernet | fastethernet | gigabitethernet | tengigabitethernet} slot/port | include type** command to see the queue structure of a LAN port.

- **1q4t** indicates one standard queue with four configurable tail-drop thresholds (usable only on Gigabit Ethernet ports).
- **1p1q4t** indicates one strict-priority queue and one standard queue with four configurable tail-drop thresholds.

- **1p1q0t** indicates one strict-priority queue and one standard queue with no configurable threshold (effectively a tail-drop threshold at 100 percent).
- **1p1q8t** indicates one strict-priority queue and one standard queue with eight configurable WRED-drop thresholds and one non-configurable (100 percent) tail-drop threshold.

Strict-priority queues are queues that are serviced in preference to other queues. PFC QoS services traffic in a strict-priority queue before servicing the standard queue. When PFC QoS services the standard queue, after receiving a packet, it checks for traffic in the strict-priority queue. If PFC QoS detects traffic in the strict-priority queue, it suspends its service of the standard queue and completes service of all traffic in the strict-priority queue before returning to the standard queue.

Scheduling

PFC QoS schedules traffic through the receive queues based on Layer 2 CoS values. In the **1p1q4t**, **1p1q0t** and **1p1q8t** default configurations, PFC QoS assigns all traffic with CoS 5 to the strict-priority queue; PFC QoS assigns all other traffic to the standard queue. In the **1q4t** default configuration, PFC QoS assigns all traffic to the standard queue.

Congestion Avoidance

If an ingress LAN port is configured to trust CoS, PFC QoS implements Layer 2 CoS-value-based receive-queue drop thresholds to avoid congestion in received traffic.

1q4t ingress LAN ports have this default drop-threshold configuration:

- Using receive-queue tail-drop threshold 1, the switch drops incoming frames with CoS 0 or 1 when the receive-queue buffer is 50 percent or more full.
- Using receive-queue tail-drop threshold 2, the switch drops incoming frames with CoS 2 or 3 when the receive-queue buffer is 60 percent or more full.
- Using receive-queue tail-drop threshold 3, the switch drops incoming frames with CoS 4 or 5 when the receive-queue buffer is 80 percent or more full.
- Using receive-queue tail-drop threshold 4, the switch drops incoming frames with CoS 6 or 7 when the receive-queue buffer is 100 percent full.

1p1q4t ingress LAN ports have this default drop-threshold configuration:

- Frames with CoS 5 go to the strict-priority receive queue (queue 2), where the switch drops incoming frames only when the strict-priority receive-queue buffer is 100 percent full.
- Frames with CoS 0, 1, 2, 3, 4, 6, or 7 go to the standard receive queue.
 - Using standard receive-queue tail-drop threshold 1, the switch drops incoming frames with CoS 0 or 1 when the receive-queue buffer is 50 percent or more full.
 - Using standard receive-queue tail-drop threshold 2, the switch drops incoming frames with CoS 2 or 3 when the receive-queue buffer is 60 percent or more full.
 - Using standard receive-queue tail-drop threshold 3, the switch drops incoming frames with CoS 4 when the receive-queue buffer is 80 percent or more full.
 - Using standard receive-queue tail-drop threshold 4, the switch drops incoming frames with CoS 6 or 7 when the receive-queue buffer is 100 percent full.

1p1q0t ingress LAN ports have this default drop-threshold configuration:

- Frames with CoS 5 go to the strict-priority receive queue (queue 2), where the switch drops incoming frames only when the strict-priority receive-queue buffer is 100 percent full.
- Frames with CoS 0, 1, 2, 3, 4, 6, or 7 go to the standard receive queue. The switch drops incoming frames when the receive-queue buffer is 100 percent full.

1p1q8t ports have this default drop-threshold configuration:

- Frames with CoS 5 go to the strict-priority receive queue (queue 2), where the switch drops incoming frames only when the strict-priority receive-queue buffer is 100 percent full.
- Frames with CoS 0, 1, 2, 3, 4, 6, or 7 go to the standard receive queue, which uses WRED-drop thresholds:
 - Using standard receive-queue WRED-drop threshold 1 for incoming frames with CoS 0, the switch starts to drop frames when the receive-queue buffer is 40 percent full and drops all frames with CoS 0 when the receive-queue buffer is 70 percent or more full.
 - Using standard receive-queue WRED-drop threshold 2 for incoming frames with CoS 1, the switch starts to drop frames when the receive-queue buffer is 40 percent full and drops all frames with CoS 1 when the receive-queue buffer is 70 percent or more full.
 - Using standard receive-queue WRED-drop threshold 3 for incoming frames with CoS 2, the switch starts to drop frames when the receive-queue buffer is 50 percent full and drops all frames with CoS 2 when the receive-queue buffer is 80 percent or more full.
 - Using standard receive-queue WRED-drop threshold 4 for incoming frames with CoS 3, the switch starts to drop frames when the receive-queue buffer is 50 percent full and drops all frames with CoS 3 when the receive-queue buffer is 80 percent or more full.
 - Using standard receive-queue WRED-drop threshold 5 for incoming frames with CoS 4, the switch starts to drop frames when the receive-queue buffer is 60 percent full and drops all frames with CoS 4 when the receive-queue buffer is 90 percent or more full.
 - Using standard receive-queue WRED-drop threshold 6 for incoming frames with CoS 6, the switch starts to drop frames when the receive-queue buffer is 60 percent full and drops all frames with CoS 6 when the receive-queue buffer is 90 percent or more full.
 - Using standard receive-queue WRED-drop threshold 7 for incoming frames with CoS 7, the switch starts to drop frames when the receive-queue buffer is 70 percent full and drops all frames with CoS 7 when the receive-queue buffer is 100 percent or more full.

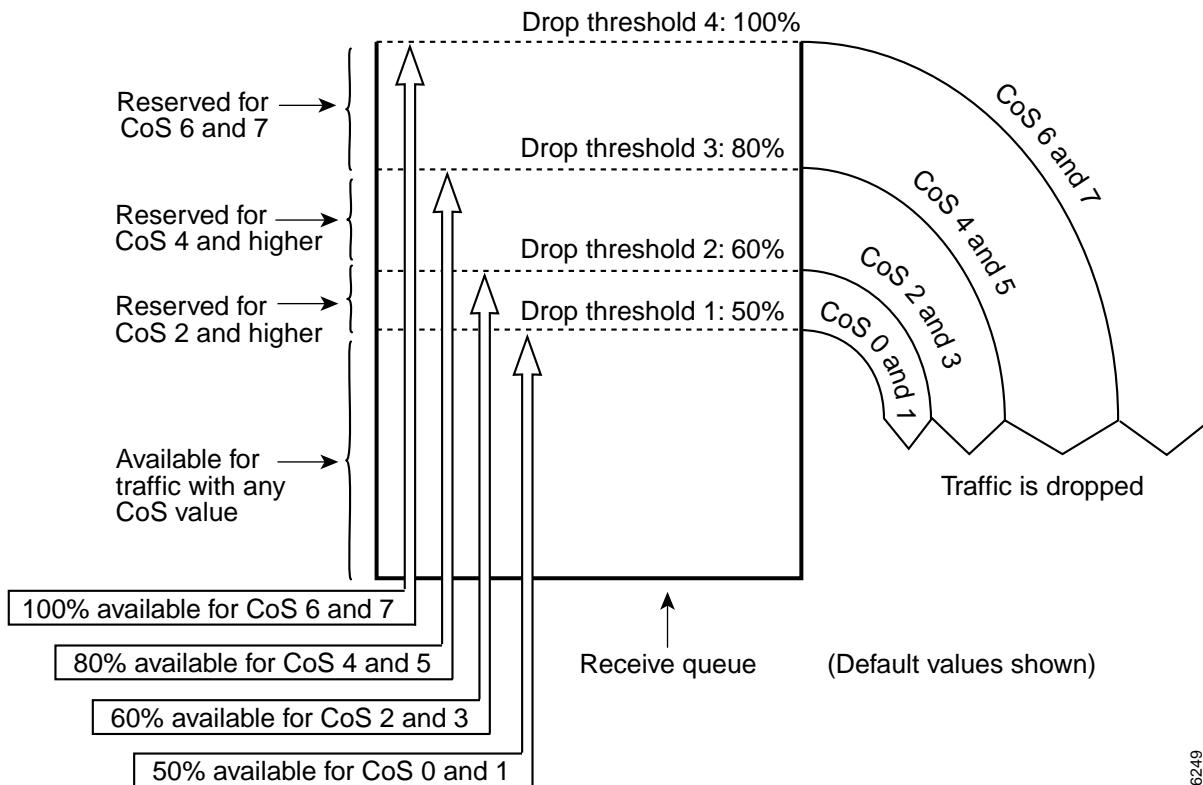


Note You can configure the standard receive queue to use both a tail-drop and a WRED-drop threshold by mapping a CoS value to the queue or to the queue and a threshold. The switch uses the tail-drop threshold for traffic carrying CoS values mapped only to the queue. The switch uses WRED-drop thresholds for traffic carrying CoS values mapped to the queue and a threshold. See the “Configuring Standard Queue WRED-Drop Thresholds” section on page 24-60.



Note The explanations in this section use default values. You can configure many of the parameters (see the “Configuring PFC QoS” section on page 24-30). All LAN ports of the same type use the same drop-threshold configuration.

Figure 24-6 illustrates the drop thresholds for a **1q4t** ingress LAN port. Drop thresholds in other configurations function similarly.

Figure 24-6 Receive Queue Drop Thresholds

26249

PFC3 Marking and Policing


Note

- To mark untrusted traffic without policing, use the `set ip dscp` or `set ip precedence` policy map class commands (see the “Configuring Policy Map Class Actions” section on page 24-43).
- Filtering for PFC QoS can use Layer 2, 3, and 4 values. Marking uses Layer 2 CoS values and Layer 3 IP precedence or DSCP values.

These sections describe PFC3 marking and policing:

- [Internal DSCP Values, page 24-14](#)
- [Policy Maps, page 24-14](#)
- [Policers, page 24-15](#)
- [Attaching Policy Maps, page 24-17](#)
- [Egress CoS Values, page 24-18](#)
- [Egress DSCP Mutation, page 24-18](#)

Internal DSCP Values

During processing, PFC QoS represents the priority of all traffic (including non-IP traffic) with an internal DSCP value. PFC QoS derives the internal DSCP value from the following:

- For trust-cos traffic, from received or ingress port Layer 2 CoS values



Note Traffic from an untrusted ingress LAN port has the ingress port CoS value and if traffic from an untrusted ingress Ethernet port matches a trust-cos policer, PFC QoS derives the internal DSCP value from the ingress port CoS value.

- For trust-iprec traffic, from received IP precedence values
- For trust-dscp traffic, from received DSCP values
- For untrusted traffic, from ingress port CoS or configured DSCP values

The trust state of traffic is the trust state of the ingress LAN port unless set otherwise by a matching ACE.



Note A **trust-cos** policer cannot restore received CoS in traffic from untrusted ingress LAN ports. Traffic from untrusted ingress LAN ports always has the ingress port CoS value.

PFC QoS uses configurable mapping tables to derive the internal 6-bit DSCP value from CoS or IP precedence, which are 3-bit values (see the “[Mapping Received CoS Values to Internal DSCP Values](#)” section on page 24-51 or the “[Mapping Received IP Precedence Values to Internal DSCP Values](#)” section on page 24-53).

Policy Maps

PFC QoS supports filtering, marking, and policing using policy maps (see the “[Configuring a Policy Map](#)” section on page 24-41). Each policy map can contain multiple policy-map classes. You can configure a separate policy-map class for each type of traffic.

Policy-map classes specify filtering with the following:

- Access control lists (optional for IP, required for MAC-Layer filtering)



Note To base microflow policing only on source or destination addresses, you must configure filtering for the policy-map class to use only source or destination addresses.

- Class-map **match** commands for Layer 3 IP precedence and DSCP values

Policy-map classes specify actions with the following:

- (Optional for ingress interfaces) Policy-map class **trust** commands. If specified, PFC QoS applies the policy-map class trust state to matched ingress traffic. Policy-map class trust states supersede ingress LAN port trust states.



Note If traffic matches a policy-map class that does not contain a **trust** command, the trust state remains as set on the ingress LAN port.

- (Optional) Aggregate and microflow policers, which can use bandwidth limits to either mark or drop both conforming and nonconforming traffic. See the “[PFC3 Marking and Policing](#)” section on page 24-13.

PFC QoS uses the trust state (set by the ingress LAN port configuration or by a **trust** policy-map class command) to select the Layer 2 and Layer 3 PFC QoS labels that the egress port writes into the packets and frames before it is transmitted:

- Trust IP precedence—Sets the internal DSCP value to a mapped value based on received IP precedence (see the “[Mapping Received IP Precedence Values to Internal DSCP Values](#)” section on page 24-53).
- Trust DSCP—Sets the internal DSCP value to the received DSCP value.
- Trust CoS—Sets the internal DSCP value to a mapped value based on received or port CoS. With trust CoS, note the following:
 - Received CoS is overwritten with port CoS in traffic received through ports not configured to trust CoS.
 - Received CoS is preserved only in traffic received through ports configured to trust CoS.
 - Port CoS is applied to all traffic received in untagged frames, regardless of the port trust state.
 - For information about mapping, see the “[Mapping Received CoS Values to Internal DSCP Values](#)” section on page 24-51.
- Untrusted—Sets the internal DSCP value to a configured DSCP value.



Note With the default values, PFC QoS applies DSCP zero to traffic from ingress LAN ports configured as untrusted.

Policers



Policing with the **conform-action transmit** keywords supersedes the ingress LAN port trust state of matched traffic with trust DSCP or with the trust state defined by a **trust** policy-map class command (see the “[Configuring the Policy Map Class Trust State](#)” section on page 24-44).

You can create policers that do the following:

- Mark traffic
- Limit bandwidth utilization and mark traffic

For more information, see the “[Creating Named Aggregate Policers](#)” section on page 24-34 and the “[Configuring Policy Map Class Actions](#)” section on page 24-43.

Policers can act on ingress traffic per-port or per-VLAN and on egress traffic per-VLAN.

Policing rates are based on the Layer 2 frame size. You specify the bandwidth utilization limit as a committed information rate (CIR). You can also specify a higher peak information rate (PIR). Packets that exceed a rate are “out of profile” or “nonconforming.”

In each policer, you specify if out-of-profile packets are to be dropped or to have a new DSCP value applied to them (applying a new DSCP value is called “markdown”). Because out-of-profile packets do not retain their original priority, they are not counted as part of the bandwidth consumed by in-profile packets.

If you configure a PIR, the PIR out-of-profile action cannot be less severe than the CIR out-of-profile action. For example, if the CIR out-of-profile action is to mark down the traffic, then the PIR out-of-profile action cannot be to transmit the traffic.

For all policers, PFC QoS uses a configurable global table that maps the internal DSCP value to a marked-down DSCP value (see the “[Configuring DSCP Markdown Values](#)” section on page 24-53). When markdown occurs, PFC QoS gets the marked-down DSCP value from the table. You cannot specify marked-down DSCP values in individual policers.


Note

- By default, the markdown table is configured so that no markdown occurs: the marked-down DSCP values are equal to the original DSCP values. To enable markdown, configure the table appropriately for your network.
- When you apply both ingress policing and egress policing to the same traffic, both the input policy and the output policy must either mark down traffic or drop traffic. PFC QoS does not support ingress markdown with egress drop or ingress drop with egress markdown.

You can create two kinds of policers: *aggregate* and *microflow*:

- PFC QoS applies the bandwidth limits specified in an aggregate policer cumulatively to all flows in matched traffic. You can create up to 1023 aggregate policers. You can create two types of aggregate policer: named and per port. Both types can be attached to more than one port:
 - You define per-interface aggregate policers in a policy map class with the **police** command. If you attach a per-interface aggregate policer to multiple ingress ports, it polices the matched traffic on each ingress port separately.
 - You create named aggregate policers with the **mls qos aggregate-policer** command. If you attach a named aggregate policer to multiple ingress ports, it polices the matched traffic from all the ingress ports to which it is attached.


Note

Aggregate policing works independently on each DFC3-equipped switching module and independently on the PFC3, which supports any non-DFC3-equipped switching modules. Aggregate policing does not combine flow statistics from different DFC3-equipped switching modules. You can display aggregate policing statistics for each DFC3-equipped switching module and for the PFC3 and any non-DFC3-equipped switching modules supported by the PFC3.

- PFC QoS applies the bandwidth limit specified in a microflow policer separately to each flow in matched traffic as follows:
 - You can create microflow policers with up to 63 different rate and burst parameter combinations.
 - You create microflow policers in a policy map class with the **police flow** command.
 - You can configure a microflow policer to use only source addresses, which applies the microflow policer to all traffic from a source address regardless of the destination addresses.
 - You can configure a microflow policer to use only destination addresses, which applies the microflow policer to all traffic to a destination address regardless of the source addresses.
 - For MAC-Layer microflow policing, PFC QoS considers MAC-Layer traffic with the same protocol and the same source and destination MAC-Layer addresses to be part of the same flow, including traffic with different ethertypes.

**Note**

You can configure MAC-Layer named access lists to filter IPX traffic (see the “Configuring MAC-Layer Named Access Lists (Optional)” section on page 24-38).

- By default, microflow policers only affect traffic routed by the MSFC3. To enable microflow policing of other traffic, including traffic in bridge groups, enter the **mls qos bridged** command (see the “Enabling Microflow Policing of Bridged Traffic” section on page 24-32).

You can include both an aggregate policer and a microflow policer in each policy map class to police a flow based on both its own bandwidth utilization and on its bandwidth utilization combined with that of other flows.

**Note**

If traffic is both aggregate and microflow policed, then the aggregate and microflow policers must both be in the same policy-map class and each must use the same **conform-action** and **exceed-action** keyword option: **drop**, **set-dscp-transmit**, **set-prec-transmit**, or **transmit**.

For example, you could create a microflow policer with a bandwidth limit suitable for individuals in a group and you could create a named aggregate policer with bandwidth limits suitable for the group as a whole. You could include both policers in policy map classes that match the group’s traffic. The combination would affect individual flows separately and the group aggregately.

For policy map classes that include both an aggregate and a microflow policer, PFC QoS responds to an out-of-profile status from either policer and, as specified by the policer, applies a new DSCP value or drops the packet. If both policers return an out-of-profile status, then if either policer specifies that the packet is to be dropped, it is dropped; otherwise PFC QoS applies a marked-down DSCP value.

**Note**

To avoid inconsistent results, ensure that all traffic policed by the same aggregate policer has the same trust state.

Attaching Policy Maps

These sections describe attaching policy maps:

- [Attaching Policy Maps to Ingress Interfaces, page 24-17](#)
- [Attaching Policy Maps to Egress Interfaces, page 24-18](#)

Attaching Policy Maps to Ingress Interfaces

You can configure each ingress LAN port for either physical port-based PFC QoS (default) or VLAN-based PFC QoS (see the “Enabling VLAN-Based PFC QoS on Layer 2 LAN Ports” section on page 24-33) and attach a policy map to the selected interface (see the “Attaching a Policy Map to an Interface” section on page 24-48).

On ports configured for port-based PFC QoS, you can attach a policy map to the ingress LAN port as follows:

- On a nontrunk ingress LAN port configured for port-based PFC QoS, all traffic received through the port is classified, marked, and policed according to the policy map attached to the port.
- On a trunking ingress LAN port configured for port-based PFC QoS, traffic in *all VLANs* received through the port is classified, marked, and policed according to the policy map attached to the port.

On a nontrunk ingress LAN port configured for VLAN-based PFC QoS, traffic received through the port is classified, marked, and policed according to the policy map attached to the *port's* VLAN.

On a trunking ingress LAN port configured for VLAN-based PFC QoS, traffic received through the port is classified, marked, and policed according to the policy map attached to the *traffic's* VLAN.

Attaching Policy Maps to Egress Interfaces

You can attach an output policy map to a Layer 3 interface (either a LAN port configured as a Layer 3 interface or a VLAN interface) to apply the policy to egress traffic (see “[Attaching a Policy Map to an Interface](#)” section on page 24-48).


Note

- Output policies do not support microflow policing.
- You cannot set a trust state in an output policy.

Egress DSCP and CoS Values

These sections describe egress DSCP and CoS values:

- [Egress CoS Values](#), page 24-18
- [Egress DSCP Mutation](#), page 24-18
- [Egress ToS Byte](#), page 24-18

Egress CoS Values

For all egress traffic, PFC QoS uses a configurable mapping table to derive a CoS value from the internal DSCP value associated with traffic (see the “[Internal DSCP Values](#)” section on page 24-14 and the “[Mapping Internal DSCP Values to Egress CoS Values](#)” section on page 24-55).

PFC QoS sends the CoS value to the egress LAN ports for use in scheduling and to be written into ISL and 802.1Q frames (see the “[LAN Egress Port Features](#)” section on page 24-19).


Note

PFC QoS derives the egress CoS value from the internal DSCP value. If you configure egress DSCP mutation, PFC QoS does not derive the egress CoS value from the mutated DSCP value.

Egress DSCP Mutation

You can configure 15 egress DSCP mutation maps to mutate the internal DSCP value before it is written as the egress DSCP value (see the “[Configuring Egress DSCP Mutation](#)” section on page 24-49). You can attach egress DSCP mutation maps to any interface that PFC QoS supports.

Egress ToS Byte

For egress IP traffic, PFC QoS creates a ToS byte from the internal or mutated DSCP value and sends it to the egress port 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 or mutated DSCP value can mimic an IP precedence value (see [Table 24-1](#) on page 24-3).

LAN Egress Port Features

These sections describe how PFC QoS schedules traffic through the transmit queues based on CoS values and uses CoS-value-based transmit-queue drop thresholds to avoid congestion in traffic transmitted from egress LAN ports:

- [Transmit Queues, page 24-19](#)
- [Scheduling and Congestion Avoidance, page 24-20](#)
- [Marking, page 24-21](#)


Note

Egress LAN port scheduling and congestion avoidance uses Layer 2 CoS values. Egress LAN port marking writes Layer 2 CoS values into trunk traffic and the Layer 3 ToS byte into all IP traffic.

Transmit Queues

Enter the **show queueing interface {ethernet | fastethernet | gigabitethernet | tengigabitethernet} slot/port | include type** command to see the queue structure of an egress LAN port.

The command displays one of the following:

- **2q2t** indicates two standard queues, each with two configurable tail-drop thresholds
- **1p2q2t** indicates one strict-priority queue and two standard queues, each with two configurable WRED-drop thresholds.
- **1p3q1t** indicates one strict-priority queue and three standard queues, each with one configurable WRED-drop threshold (on **1p3q1t** ports, each standard queue also has one nonconfigurable tail-drop threshold).
- **1p2q1t** indicates one strict-priority queue and two standard queues, each with one configurable WRED-drop threshold (on **1p2q1t** ports, each standard queue also has one nonconfigurable tail-drop threshold).

All port types have a low-priority and a high-priority standard transmit queue. **1p3q1t** ports have a medium-priority standard transmit queue. **1p2q2t**, **1p3q1t** and **1p2q1t** ports have a strict-priority transmit queue in addition to the standard queues.

On **2q2t** ports, the default PFC QoS configuration allocates a minimum of 80 percent of the total transmit queue size to the low-priority standard queue and a minimum of 20 percent to the high-priority standard queue.

On **1p2q2t**, **1p3q1t**, and **1p2q1t** ports, the switch services traffic in the strict-priority queue before servicing the standard queues. When the switch is servicing a standard queue, after transmitting a packet, it checks for traffic in the strict-priority queue. If the switch detects traffic in the strict-priority queue, it suspends its service of the standard queue and completes service of all traffic in the strict-priority queue before returning to the standard queue.

On **1p2q2t** ports, the default PFC QoS configuration allocates a minimum of 70 percent of the total transmit queue size to the low-priority standard queue, a minimum of 15 percent to the high-priority standard queue, and a minimum of 15 percent to the strict-priority queue.

On **1p3q1t** ports, the transmit queue size is not configurable and is allocated equally among all queues.

On **1p2q1t** ports, the default PFC QoS configuration allocates a minimum of 50 percent of the total transmit queue size to the low-priority standard queue, a minimum of 30 percent to the high-priority standard queue, and a minimum of 20 percent to the strict-priority queue.



Note Transmit-queue size is limited to the configured value (see the “[Setting the Receive-Queue Size Ratio on a 1p1q0t or 1p1q8t Ingress LAN Ports](#)” section on page 24-68), but any queue can use all available bandwidth (bandwidth is only available when there is no traffic in the other queues).

Scheduling and Congestion Avoidance

These sections describe scheduling and congestion avoidance:

- [2q2t Ports, page 24-20](#)
- [1p2q2t Ports, page 24-20](#)
- [1p3q1t Ports, page 24-21](#)
- [1p2q1t Ports, page 24-21](#)



Note The explanations in these sections use default values. You can configure many of the parameters (for more information, see the “[Configuring PFC QoS](#)” section on page 24-30). All ports of the same type use the same drop-threshold configuration.

2q2t Ports

For **2q2t** ports, each transmit queue has two tail-drop thresholds that function as follows:

- Frames with CoS 0, 1, 2, or 3 go to the low-priority transmit queue (queue 1):
 - Using transmit queue 1, tail-drop threshold 1, the switch drops frames with CoS 0 or 1 when the low-priority transmit-queue buffer is 80 percent full.
 - Using transmit queue 1, tail-drop threshold 2, the switch drops frames with CoS 2 or 3 when the low-priority transmit-queue buffer is 100 percent full.
- Frames with CoS 4, 5, 6, or 7 go to the high-priority transmit queue (queue 2):
 - Using transmit queue 2, tail-drop threshold 1, the switch drops frames with CoS 4 or 5 when the high-priority transmit-queue buffer is 80 percent full.
 - Using transmit queue 2, tail-drop threshold 2, the switch drops frames with CoS 6 or 7 when the high-priority transmit-queue buffer is 100 percent full.

1p2q2t Ports

1p2q2t ports have a strict-priority queue and two standard transmit queues. The two standard transmit queues each have two WRED-drop thresholds.

- Frames with CoS 5 go to the strict-priority transmit queue (queue 3), where the switch drops frames only when the buffer is 100 percent full.
- Frames with CoS 0, 1, 2, or 3 go to the low-priority standard transmit queue (queue 1):
 - Using standard transmit queue 1, WRED-drop threshold 1, the switch drops frames with CoS 0 or 1 when the low-priority transmit-queue buffer is 80 percent full.
 - Using standard transmit queue 1, WRED-drop threshold 2, the switch drops frames with CoS 2 or 3 when the low-priority transmit-queue buffer is 100 percent full.

- Frames with CoS 4, 6, or 7 go to the high-priority standard transmit queue (queue 2):
 - Using standard transmit queue 2, WRED-drop threshold 1, the switch drops frames with CoS 4 when the high-priority transmit-queue buffer is 80 percent full.
 - Using standard transmit queue 2, WRED-drop threshold 2, the switch drops frames with CoS 6 or 7 when the high-priority transmit-queue buffer is 100 percent full.

1p3q1t Ports

1p3q1t ports have a strict-priority queue and three standard transmit queues. The standard transmit queues each have one WRED-drop threshold and one nonconfigurable tail-drop threshold.

- Frames with CoS 5 go to the strict-priority transmit queue (queue 4), where the switch drops frames only when the buffer is 100 percent full.
- Frames with CoS 0 and 1 go to the low-priority standard transmit queue (queue 1).
- Frames with CoS 2, 3, or 4 go to the medium-priority standard transmit queue (queue 2).
- Frames with CoS 6 or 7 go to the high-priority standard transmit queue (queue 3).



Note

You can configure each standard transmit queue to use both a non-configurable 100 percent tail-drop threshold and a configurable WRED-drop threshold (see the “[Configuring Standard Queue WRED-Drop Thresholds](#)” section on page 24-60).

1p2q1t Ports

1p2q1t ports have a strict-priority queue and two standard transmit queues. The standard transmit queues each have one WRED-drop threshold and one nonconfigurable tail-drop threshold.

- Frames with CoS 5 go to the strict-priority transmit queue (queue 3), where the switch drops frames only when the buffer is 100 percent full.
- The standard transmit queues have WRED-drop thresholds:
 - Frames with CoS 0, 1, 2, or 3 go to the low-priority transmit queue (queue 1), where the switch starts to drop frames when the low-priority transmit-queue buffer is 70 percent full and drops all frames with CoS 0, 1, 2, or 3 when the buffer is 100 percent full.
 - Frames with CoS 4, 6, or 7 go to the high-priority transmit queue (queue 2), where the switch starts to drop frames when the high-priority transmit-queue buffer is 70 percent full and drops all frames with CoS 4, 6, or 7 when the buffer is 100 percent full.



Note

You can configure each standard transmit queue to use both the tail-drop and the WRED-drop threshold. See the “[Configuring Standard Queue WRED-Drop Thresholds](#)” section on page 24-60.

Marking

When traffic is transmitted from the switch, PFC QoS writes the ToS byte into IP packets. On LAN ports, PFC QoS also writes the CoS value that was used for scheduling and congestion avoidance into ISL and 802.1Q frames (see the “[Egress CoS Values](#)” section on page 24-18).

PFC QoS Default Configuration

Table 24-2 shows the PFC QoS default configuration.

Table 24-2 PFC QoS Default Configuration

Feature	Default Value
PFC QoS global enable state	Disabled Note With PFC QoS enabled and all other PFC QoS parameters at default values, PFC QoS sets Layer 3 DSCP to zero and Layer 2 CoS to zero in all traffic transmitted from the switch.
PFC QoS port enable state	Enabled when PFC QoS is globally enabled
Port CoS value	0
Microflow policing	Enabled
IntraVLAN microflow policing	Disabled
Port-based or VLAN-based PFC QoS	Port-based
CoS to DSCP map (DSCP set from CoS values)	CoS 0 = DSCP 0 CoS 1 = DSCP 8 CoS 2 = DSCP 16 CoS 3 = DSCP 24 CoS 4 = DSCP 32 CoS 5 = DSCP 40 CoS 6 = DSCP 48 CoS 7 = DSCP 56
IP precedence to DSCP map (DSCP set from IP precedence values)	IP precedence 0 = DSCP 0 IP precedence 1 = DSCP 8 IP precedence 2 = DSCP 16 IP precedence 3 = DSCP 24 IP precedence 4 = DSCP 32 IP precedence 5 = DSCP 40 IP precedence 6 = DSCP 48 IP precedence 7 = DSCP 56
DSCP to CoS map (CoS set from DSCP values)	DSCP 0–7 = CoS 0 DSCP 8–15 = CoS 1 DSCP 16–23 = CoS 2 DSCP 24–31 = CoS 3 DSCP 32–39 = CoS 4 DSCP 40–47 = CoS 5 DSCP 48–55 = CoS 6 DSCP 56–63 = CoS 7
Marked-down DSCP from DSCP map	Marked-down DSCP value equals original DSCP value (no markdown)
Policers	None
Policy maps	None

Table 24-2 PFC QoS Default Configuration (continued)

Feature	Default Value
With PFC QoS enabled	
Ingress LAN port trust state	Untrusted
2q2t transmit-queue size ratio	Low priority: 80%; high priority: 20%
1p1q0t receive-queue size ratio	Standard: 80%; strict priority: 20%
1p2q2t transmit-queue size ratio	Low priority: 70%; high priority: 15%; strict priority: 15%
1p2q1t transmit-queue size ratio	Low priority: 70%; high priority: 15%; strict priority: 15%
1p2q1t standard transmit-queue low:high priority bandwidth allocation ratio	100:255
2q2t , 1p2q2t , and 1p2q1t standard transmit-queue low:high priority bandwidth allocation ratio	5:255
1p3q1t standard transmit-queue low:medium:high-priority bandwidth allocation ratio	100:150:255
1q4t/2q2t receive and transmit queue CoS value/drop-threshold mapping	<ul style="list-style-type: none"> • Receive queue 1/drop threshold 1(50%) and transmit queue 1/drop threshold 1 (80%): CoS 0 and 1 • Receive queue 1/drop threshold 2 (60%) and transmit queue 1/drop threshold 2 (100%): CoS 2 and 3 • Receive queue 1/drop threshold 3 (80%) and transmit queue 2/drop threshold 1 (80%): CoS 4 and 5 • Receive queue 1/drop threshold 4 (100%) and transmit queue 2/drop threshold 2 (100%): CoS 6 and 7
1p1q4t/1p2q2t port receive and transmit queue CoS value/drop-threshold mapping and threshold percentages:	<ul style="list-style-type: none"> • Strict-priority receive queue and strict-priority transmit queue: CoS 5 • Receive queue 1/drop threshold 1 and transmit queue 1/drop threshold 1: <ul style="list-style-type: none"> – CoS 0 and 1 – Transmit queue low and high WRED-drop thresholds: 40% and 70% • Receive queue 1/drop threshold 2 and transmit queue 1/drop threshold 2: <ul style="list-style-type: none"> – CoS 2 and 3 – Transmit queue low and high WRED-drop thresholds: 70% and 100% • Receive queue 1/drop threshold 3 and transmit queue 2/drop threshold 1: <ul style="list-style-type: none"> – CoS 4 and 6 – Transmit queue low and high WRED-drop thresholds: 40% and 70% • Receive queue 1/drop threshold 4 and transmit queue 2/drop threshold 2: <ul style="list-style-type: none"> – CoS 7 – Transmit queue low and high WRED-drop thresholds: 70% and 100%

Table 24-2 PFC QoS Default Configuration (continued)

Feature	Default Value
1p1q0t receive queue CoS value mapping	<ul style="list-style-type: none"> Receive queue 1 (standard) nonconfigurable 100% tail-drop threshold: CoS 0, 1, 2, 3, 4, 6, and 7 Receive queue 2 (strict priority): CoS 5
1p3q1t transmit queue CoS value/drop-threshold mapping	<ul style="list-style-type: none"> Transmit queue 1 (standard low priority) tail-drop threshold: <ul style="list-style-type: none"> CoS 0 and 1 Low and high WRED-drop threshold: 70% and 100% Transmit queue 2 (standard medium priority) tail-drop threshold: <ul style="list-style-type: none"> CoS 2, 3, and 4 Low and high WRED-drop threshold: 70% and 100% Transmit queue 3 (standard high priority) tail-drop threshold: <ul style="list-style-type: none"> CoS 6 and 7 Low and high WRED-drop threshold: 70% and 100% Transmit queue 4 (strict priority): CoS 5
1p1q8t receive queue port CoS value/drop-threshold mapping	<ul style="list-style-type: none"> Receive queue 1 (standard) WRED-drop threshold: CoS 0, 1, 2, 3, 4, 6, and 7: <ul style="list-style-type: none"> Drop threshold 1: CoS 0 Low WRED threshold: 40% High WRED-drop threshold: 70% Drop threshold 2: CoS 1 Low WRED threshold: 40% High WRED-drop threshold: 70% Drop threshold 3: CoS 2 Low WRED threshold: 50% High WRED-drop threshold: 80% Drop threshold 4: CoS 3 Low WRED threshold: 50% High WRED-drop threshold: 80% Drop threshold 5: CoS 4 Low WRED threshold: 60% High WRED-drop threshold: 90% Drop threshold 6: CoS 6 Low WRED threshold: 60% High WRED-drop threshold: 90% Drop threshold 7: CoS 7 Low WRED threshold: 70% High WRED-drop threshold: 100% Receive queue 2 (strict priority): CoS 5

DSCP to CoS map (CoS set from DSCP values)	DSCP 0–7 = CoS 0 DSCP 8–15 = CoS 1 DSCP 16–23 = CoS 2
	DSCP 24–31 = CoS 3 DSCP 32–39 = CoS 4 DSCP 40–47 = CoS 5 DSCP 48–55 = CoS 6 DSCP 56–63 = CoS 7
Marked-down DSCP from DSCP map	Marked-down DSCP value equals original DSCP value (no markdown)
Policers	None
Policy maps	None

PFC QoS Default Configuration

1p1q4t/1p2q2t port receive and transmit queue CoS value/drop-threshold mapping and threshold percentages:

- Strict-priority receive queue and strict-priority transmit queue: CoS 5
- Receive queue 1/drop threshold 1 and transmit queue 1/drop threshold 1:
 - CoS 0 and 1
 - Transmit queue low and high WRED-drop thresholds: 40% and 70%
- Receive queue 1/drop threshold 2 and transmit queue 1/drop threshold 2:
 - CoS 2 and 3

Table 24-2 PFC QoS Default Configuration (continued)

Feature	Default Value
	<p>Transmit queue low and high WRED-drop thresholds: 70% and 100%</p> <ul style="list-style-type: none"> • Receive queue 1/drop threshold 3 and transmit queue 2/drop threshold 1: <ul style="list-style-type: none"> – CoS 4 and 6 – Transmit queue low and high WRED-drop thresholds: 40% and 70% • Receive queue 1/drop threshold 4 and transmit queue 2/drop threshold 2: <ul style="list-style-type: none"> – CoS 7 – Transmit queue low and high WRED-drop thresholds: 70% and 100%

1p1q8t receive queue port CoS value/drop-threshold mapping	<ul style="list-style-type: none"> • Receive queue 1 (standard) WRED-drop threshold: CoS 0, 1, 2, 3, 4, 6, and 7: <ul style="list-style-type: none"> – Drop threshold 1: CoS 0 Low WRED threshold: 40% High WRED-drop threshold: 70% – Drop threshold 2: CoS 1 Low WRED threshold: 40% High WRED-drop threshold: 70% – Drop threshold 3: CoS 2 Low WRED threshold: 50% High WRED-drop threshold: 80% – Drop threshold 4: CoS 3 Low WRED threshold: 50% High WRED-drop threshold: 80% – Drop threshold 5: CoS 4 Low WRED threshold: 60% High WRED-drop threshold: 90% – Drop threshold 6: CoS 6 Low WRED threshold: 60% High WRED-drop threshold: 90% – Drop threshold 7: CoS 7 Low WRED threshold: 70% High WRED-drop threshold: 100% • Receive queue 2 (strict priority): CoS 5
---	--

Table 24-2 PFC QoS Default Configuration (continued)

Feature	Default Value
	<ul style="list-style-type: none"> – Drop threshold 6: CoS 7 Low WRED threshold: 70% High WRED-drop threshold: 100% • Receive queue 2 (strict priority): CoS 5

Table 24-2 PFC QoS Default Configuration (continued)

Feature	Default Value
Transmit-queue size ratio	Low priority: 100% (other queues not used)
CoS value/drop threshold mapping	All CoS values mapped to the low-priority queue.

PFC QoS Configuration Guidelines and Restrictions

Follow these guidelines and restrictions when configuring PFC QoS:

- When you apply both ingress policing and egress policing to the same traffic, both the input policy and the output policy must either mark down traffic or drop traffic. PFC QoS does not support ingress markdown with egress drop or ingress drop with egress markdown. (CSCea23571)
- If traffic is both aggregate and microflow policed, then the aggregate and microflow policers must both be in the same policy-map class and each must use the same **conform-action** and **exceed-action** keyword option: **drop**, **set-dscp-transmit**, **set-prec-transmit**, or **transmit**.
- PFC QoS does not rewrite the payload ToS byte in tunnel traffic.
- The PFC3 does not apply egress policing to traffic that is being bridged to the MSFC3.
- The PFC3 does not apply egress policing or egress DSCP mutation to multicast traffic from the MSFC3.
- With a PFC3, PFC QoS does not rewrite the ToS byte in bridged multicast traffic.
- You cannot configure PFC QoS features on tunnel interfaces.
- PFC QoS filters only by access lists, dscp values, or IP precedence values.
- PFC QoS supports class maps that contain a *single* **match** command.
- PFC QoS does not support these class map commands:
 - **match cos**
 - **match any**
 - **match classmap**
 - **match destination-address**
 - **match input-interface**
 - **match mpls**
 - **match protocol**
 - **match qos-group**
 - **match source-address**
- PFC QoS does not support these policy map commands:
 - **class class_name destination-address**
 - **class class_name input-interface**
 - **class class_name protocol**
 - **class class_name qos-group**
 - **class class_name source-address**

- PFC QoS does not support these policy map class commands:
 - **bandwidth**
 - **priority**
 - **queue-limit**
 - **random-detect**
 - **set mpls experimental**
 - **set qos-group**
 - **service-policy**
- PFC QoS supports the **set ip dscp** and **set ip precedence** policy map class commands (see the “Configuring Policy Map Class Actions” section on page 24-43).
- PFC QoS has the following hardware granularity for CIR and PIR rate values:

CIR and PIR Rate Value Range	Granularity
32768 to 2097152 (2 Mbs)	32768 (32 Kb)
2097153 to 4194304 (4 Mbs)	65536 (64 Kb)
4194305 to 8388608 (8 Mbs)	131072 (128 Kb)
8388609 to 16777216 (16 Mbs)	262144 (256 Kb)
16777217 to 33554432 (32 Mbs)	524288 (512 Kb)
33554433 to 67108864 (64 Mbs)	1048576 (1 Mb)
67108865 to 134217728 (128 Mbs)	2097152 (2 Mb)
134217729 to 268435456 (256 Mbs)	4194304 (4 Mb)
268435457 to 536870912 (512 Mbs)	8388608 (8 Mb)
536870913 to 1073741824 (1 Gps)	16777216 (16 Mb)
1073741825 to 2147483648 (2 Gps)	33554432 (32 Mb)
2147483649 to 4294967296 (4 Gps)	67108864 (64 Mb)

Within each range, PFC QoS programs the PFC3 with rate values that are multiples of the granularity values.

- PFC QoS has the following hardware granularity for CIR and PIR token bucket (burst) sizes:

CIR and PIR Token Bucket Size Range	Granularity
1 to 32768 (32 KB)	1024 (1 KB)
32769 to 65536 (64 KB)	2048 (2 KB)
65537 to 131072 (128 KB)	4096 (4 KB)
131073 to 262144 (256 KB)	8196 (8 KB)
262145 to 524288 (512 KB)	16392 (16 KB)
524289 to 1048576 (1 MB)	32768 (32 KB)
1048577 to 2097152 (2 MB)	65536 (64 KB)
2097153 to 4194304 (4 MB)	131072 (128 KB)

CIR and PIR Token Bucket Size Range	Granularity
4194305 to 8388608 (8 MB)	262144 (256 KB)
8388609 to 16777216 (16 MB)	524288 (512 KB)
16777217 to 33554432 (32 MB)	1048576 (1 MB)

Within each range, PFC QoS programs the PFC3 with token bucket sizes that are multiples of the granularity values.

- For these commands, PFC QoS applies identical configuration to all LAN ports controlled by the same application-specific integrated circuit (ASIC):
 - `rcv-queue queue-limit`
 - `wrr-queue queue-limit`
 - `wrr-queue bandwidth` (except Gigabit Ethernet LAN ports)
 - `priority-queue cos-map`
 - `rcv-queue cos-map`
 - `wrr-queue cos-map`
 - `wrr-queue threshold`
 - `rcv-queue threshold`
 - `wrr-queue random-detect`
 - `wrr-queue random-detect min-threshold`
 - `wrr-queue random-detect max-threshold`

Configuring PFC QoS

These sections describe how to configure PFC QoS on the Catalyst 6500 series switches:

- [Enabling PFC QoS Globally](#), page 24-31
- [Enabling or Disabling Microflow Policing](#), page 24-31
- [Enabling Microflow Policing of Bridged Traffic](#), page 24-32
- [Enabling VLAN-Based PFC QoS on Layer 2 LAN Ports](#), page 24-33
- [Enabling or Disabling PFC Features on an Interface](#), page 24-33
- [Creating Named Aggregate Policers](#), page 24-34
- [Configuring a PFC QoS Policy](#), page 24-37
- [Configuring DSCP Value Maps](#), page 24-51
- [Configuring the Trust State of Ethernet LAN Ports](#), page 24-56
- [Configuring the Ingress LAN Port CoS Value](#), page 24-57
- [Configuring LAN-Port Drop Threshold Percentages](#), page 24-57
- [Enabling and Disabling WRED-Drop Thresholds](#), page 24-62
- [Mapping CoS Values to LAN-Port Drop Thresholds](#), page 24-62
- [Allocating Bandwidth Between LAN-Port Transmit Queues](#), page 24-67

- Setting the Receive-Queue Size Ratio on a 1p1q0t or 1p1q8t Ingress LAN Ports, page 24-68
- Setting the LAN-Port Transmit-Queue Size Ratio, page 24-68

**Note**

PFC QoS processes both unicast and multicast traffic.

Enabling PFC QoS Globally

To enable PFC QoS globally, perform this task:

Command	Purpose
Step 1	Router(config)# mls qos
	Router(config)# no mls qos
Step 2	Router(config)# end
Step 3	Router# show mls qos

This example shows how to enable PFC QoS globally:

```
Router# configure terminal
Router(config)# mls qos
Router(config)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show mls qos
QoS is enabled globally
Microflow QoS is enabled globally

QoS global counters:
  Total packets: 544393
  IP shortcut packets: 1410
  Packets dropped by policing: 0
  IP packets with TOS changed by policing: 467
  IP packets with COS changed by policing: 59998
  Non-IP packets with COS changed by policing: 0

Router#
```

Enabling or Disabling Microflow Policing

To enable or disable microflow policing (see the “[Policers](#)” section on page 24-15), perform this task:

Command	Purpose
Step 1	Router(config)# mls qos flow-policing
	Router(config)# no mls qos flow-policing
Step 2	Router(config)# end
Step 3	Router# show mls qos

This example shows how to disable microflow policing:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# no mls qos flow-policing
Router(config)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show mls qos | include Microflow
    Microflow QoS is disabled globally
Router#
```

Enabling Microflow Policing of Bridged Traffic



Note To apply microflow policing to multicast traffic, you must enter the **mls qos bridged** command on the Layer 3 multicast ingress interfaces.

By default, microflow policers affect only routed traffic. To enable microflow policing of bridged traffic on specified VLANs, perform this task:

	Command	Purpose
Step 1	Router(config)# interface {{vlan <i>vlan_ID</i> } {type ¹ <i>slot/port</i> }}	Selects the interface to configure.
Step 2	Router(config-if)# mls qos bridged	Enables microflow policing of bridged traffic, including bridge groups, on the VLAN.
	Router(config-if)# no mls qos bridged	Disables microflow policing of bridged traffic.
Step 3	Router(config-if)# end	Exits configuration mode.
Step 4	Router# show mls qos	Verifies the configuration.

1. *type* = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

This example shows how to enable microflow policing of bridged traffic on VLANs 3 through 5:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface range vlan 3 - 5
Router(config-if)# mls qos bridged
Router(config-if)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show mls qos | begin Bridged QoS
Bridged QoS is enabled on the following interfaces:
    Vl3 Vl4 Vl5
<...output truncated...>
Router#
```

Enabling VLAN-Based PFC QoS on Layer 2 LAN Ports



Note PFC QoS supports VLAN-based QoS with DFC3s installed.

By default, PFC QoS uses policy maps attached to LAN ports. For ports configured as Layer 2 LAN ports with the **switchport** keyword, you can configure PFC QoS to use policy maps attached to a VLAN (see the “[Attaching Policy Maps](#)” section on page 24-17). Ports not configured with the **switchport** keyword are not associated with a VLAN.

To enable VLAN-based PFC QoS on a Layer 2 LAN port, perform this task:

Command	Purpose
Step 1 Router(config)# interface {{type¹ slot/port} {port-channel number}}	Selects the interface to configure.
Step 2 Router(config-if)# mls qos vlan-based	Enables VLAN-based PFC QoS on a Layer 2 LAN port.
Router(config-if)# no mls qos vlan-based	Disables VLAN-based PFC QoS.
Step 3 Router(config-if)# end	Exits configuration mode.
Step 4 Router# show mls qos	Verifies the configuration.

1. *type* = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

This example shows how to enable VLAN-based PFC QoS on Fast Ethernet port 5/42:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fastethernet 5/42
Router(config-if)# mls qos vlan-based
Router(config-if)# end
```

This example shows how to verify the configuration:

```
Router# show mls qos | begin QoS is vlan-based
    QoS is vlan-based on the following interfaces:
        Fa5/42
    <...Output Truncated...>
```



Note Configuring a Layer 2 LAN port for VLAN-based PFC QoS preserves the policy map port configuration. The **no mls qos vlan-based** port command reenables any previously configured port commands.

Enabling or Disabling PFC Features on an Interface

You can enable or disable the PFC QoS features implemented on the PFC for traffic from an interface (see the “[PFC3 Marking and Policing](#)” section on page 24-13). Disabling the PFC QoS features on an interface leaves the configuration intact. The **mls qos** interface command reenables any previously configured PFC QoS features. The **mls qos** interface command does not affect the port queueing configuration.

To enable or disable PFC features for traffic from an interface, perform this task:

Command	Purpose
Step 1 Router(config)# interface {{type ¹ slot/port} {port-channel number}}	Selects the interface to configure.
Step 2 Router(config-if)# mls qos	Enables PFC QoS on the interface.
Router(config-if)# no mls qos	Disables PFC QoS on the interface.
Step 3 Router(config-if)# end	Exits configuration interface.
Step 4 Router# show mls qos	Verifies the configuration.

1. type = **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **ge-wan**, **pos**, or **atm**

This example shows how to disable PFC QoS on the VLAN 5 interface:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface vlan 5
Router(config-if)# no mls qos
Router(config-if)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show mls qos | begin QoS is disabled
QoS is disabled on the following interfaces:
    V15
<...Output Truncated...>
Router#
```

Creating Named Aggregate Policers

To create a named aggregate policer (see the “[Policers](#)” section on page 24-15), perform this task:

Command	Purpose
Router(config)# mls qos aggregate-policer policer_name bits_per_second normal_burst_bytes [maximum_burst_bytes] [pir peak_rate_bps] [[[conform-action { drop set-dscp-transmit ¹ dscp_value set-prec-transmit ¹ ip_precedence_value transmit }] exceed-action { drop policed-dscp transmit }]] violate-action { drop policed-dscp transmit }]]	Creates a named aggregate policer.
Router(config)# no mls qos aggregate-policer policer_name	Deletes a named aggregate policer.

1. The **set-dscp-transmit** and **set-prec-transmit** keywords are only supported for IP traffic.

**Note**

Aggregate policers can be applied to ingress interfaces on multiple modules, but aggregate policing works independently on each DFC3-equipped switching module and independently on the PFC3, which supports any non-DFC3-equipped switching modules. Aggregate policing does not combine flow statistics from different DFC3-equipped switching modules. You can display aggregate policing statistics for each DFC3-equipped switching module and for the PFC3 and any non-DFC3-equipped switching modules supported by the PFC3.

When creating a named aggregate policer, note the following:

- Policing uses the Layer 2 frame size.
- See the “[PFC QoS Configuration Guidelines and Restrictions](#)” section on page 24-28 for information about rate and burst size granularity.
- The valid range of values for the *CIR bits_per_second* parameter is as follows:
 - Minimum—32 kilobits per second, entered as 32000
 - Maximum—4 gigabits per second, entered as 4000000000
- The *normal_burst_bytes* parameter sets the CIR token bucket size.
- The *maximum_burst_bytes* parameter sets the PIR token bucket size.
- When configuring the size of a token bucket, note the following:
 - The minimum token bucket size is 1 kilobyte, entered as 1000 (the *maximum_burst_bytes* parameter must be set larger than the *normal_burst_bytes* parameter)
 - The maximum token bucket size is 32 megabytes, entered as 32000000
 - To sustain a specific rate, set the token bucket size to be at least the rate value divided by 4000, because tokens are removed from the bucket every 1/4000th of a second (0.25 ms).
 - Because the token bucket must be large enough to hold at least one frame, set the parameter larger than the maximum Layer 3 packet size of the traffic being policed.
 - For TCP traffic, configure the token bucket size as a multiple of the TCP window size, with a minimum value at least twice as large as the maximum Layer 3 packet size of the traffic being policed.
- The valid range of values for the *pir bits_per_second* parameter is as follows:
 - Minimum—32 kilobits per second, entered as 32000 (the value cannot be smaller than the *CIR bits_per_second* parameters)
 - Maximum—4 gigabits per second, entered as 4000000000
- (Optional) You can specify a conform action for matched in-profile traffic as follows:
 - The default conform action is **transmit**, which sets the policy map class trust state to *trust DSCP* unless the policy map class contains a **trust** command (see the “[Policy Maps](#)” section on page 24-14 and the “[Configuring Policy Map Class Actions](#)” section on page 24-43).
 - To set PFC QoS labels in untrusted traffic, enter the **set-dscp-transmit** keyword to mark matched untrusted traffic with a new DSCP value or enter the **set-prec-transmit** keyword to mark matched untrusted traffic with a new IP precedence value. The **set-dscp-transmit** and **set-prec-transmit** keywords are only supported for IP traffic. PFC QoS sets egress ToS and CoS from the configured value.
 - Enter the **drop** keyword to drop all matched traffic.



Note When you configure **drop** as the conform action, PFC QoS configures **drop** as the exceed action and the violate action.

- (Optional) For traffic that exceeds the CIR, you can specify an exceed action as follows:
 - The default exceed action is **drop**, except with a *maximum_burst_bytes* parameter (**drop** is not supported with a *maximum_burst_bytes* parameter).



Note When the exceed action is **drop**, PFC QoS ignores any configured violate action.

- 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 the “[Configuring DSCP Markdown Values](#)” section on page 24-53).



Note When you create a policer that does not use the **pir** keyword and the *maximum_burst_bytes* parameter is equal to the *normal_burst_bytes* parameter (which is the case if you do not enter the *maximum_burst_bytes* parameter), the **exceed-action policed-dscp-transmit** keywords cause PFC QoS to mark traffic down as defined by the **policed-dscp max-burst** markdown map.

- (Optional) For traffic that exceeds the PIR, you can specify a violate action as follows:
 - To mark traffic without policing, enter the **transmit** keyword to transmit all matched out-of-profile traffic.
 - The default violate action is equal to the exceed action.
 - 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 the “[Configuring DSCP Markdown Values](#)” section on page 24-53).
 - For marking without policing, enter the **transmit** keyword to transmit all matched out-of-profile traffic.



Note When you apply both ingress policing and egress policing to the same traffic, both the input policy and the output policy must either mark down traffic or drop traffic. PFC QoS does not support ingress markdown with egress drop or ingress drop with egress markdown.

This example shows how to create a named aggregate policer with a 1-Mbps rate limit and a 10-MB burst size that transmits conforming traffic and marks down out-of-profile traffic:

```
Router(config)# mls qos aggregate-policer aggr-1 1000000 10000000 conform-action transmit
exceed-action policed-dscp-transmit
Router(config)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show mls qos aggregate-policer aggr-1
ag1 1000000 1000000 conform-action transmit exceed-action policed-dscp-transmit AgId=0
[pol1]
Router#
```

The output displays the following:

- The **AgId** parameter displays the hardware policer ID.
- The policy maps that use the policer are listed in the square brackets ([]).

Configuring a PFC QoS Policy

These sections describe PFC QoS policy configuration:

- [PFC QoS Policy Configuration Overview, page 24-37](#)
- [Configuring MAC-Layer Named Access Lists \(Optional\), page 24-38](#)
- [Configuring a Class Map \(Optional\), page 24-40](#)
- [Verifying Class Map Configuration, page 24-41](#)
- [Configuring a Policy Map, page 24-41](#)
- [Verifying Policy Map Configuration, page 24-48](#)
- [Attaching a Policy Map to an Interface, page 24-48](#)



Note PFC QoS policies process both unicast and multicast traffic.

PFC QoS Policy Configuration Overview



To mark traffic without limiting bandwidth utilization, create a policer that uses the **transmit** keywords for both conforming and nonconforming traffic.

These commands configure traffic classes and the policies to be applied to those traffic classes and attach the policies to ports:

- **access-list** (Optional for IP traffic. You can filter IP traffic with **class-map** commands.):
 - With the PFC3, PFC QoS supports these access list types:

Protocol	Numbered Access Lists?	Extended Access Lists?	Named Access Lists?
IP	Yes: 1 to 99 1300 to 1999	Yes: 100 to 199 2000 to 2699	Yes
IPX and MAC Layer	No	No	Yes

- The PFC3 does not support IPX ACLs. With the PFC3, you can configure MAC-Layer named access lists (see the “[Configuring MAC-Layer Named Access Lists \(Optional\)](#)” section on page 24-38) to filter IPX traffic.
- Except for MAC-Layer named access lists (see the “[Configuring MAC-Layer Named Access Lists \(Optional\)](#)” section on page 24-38), refer to the *Cisco IOS Security Configuration Guide*, Release 12.2, “Traffic Filtering and Firewalls,” at this URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/ftrawf/index.htm

- See [Chapter 21, “Configuring Network Security,”](#) for additional information about ACLs on the Catalyst 6500 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 24-40).



Note You can also create class-maps during policy map creation with the **policy-map class** command (see the “[Creating a Policy Map Class and Configuring Filtering](#)” section on page 24-42).

- **policy-map**—Enter the **policy-map** command to define the following:
 - New class maps
 - Policy map class trust mode
 - Aggregate policing and marking
 - Microflow policing and marking
- **service-policy**—Enter the **service-policy** command to attach a policy map to an interface.

Configuring MAC-Layer Named Access Lists (Optional)

You can configure named access lists that filter IPX, DECnet, AppleTalk, VINES, or XNS traffic based on Layer 2 addresses.

To configure a MAC-Layer named access list, perform this task:

	Command	Purpose
Step 1	Router(config)# mac access-list extended <i>list_name</i>	Configures a MAC-Layer named access list.
	Router(config)# no mac access-list extended <i>list_name</i>	Deletes a MAC-Layer named access list.
Step 2	Router(config-ext-macl)# {permit deny} {src-mac-mask any} {dest-mac-mask any} [aarp amber appletalk diagnostic decnet-iv dec-spanning dsm etype-6000 etype-8042 ipx-arpa ipx-non-arpa lat lavc-sca mop-console mop-dump msdos mumps netbios vines-ip vines-echo xns]	Configures an access control entry (ACE) in a MAC-Layer named access list.
	Router(config-ext-macl)# no {permit deny} {src-mac-mask any} {dest-mac-mask any} [aarp amber appletalk diagnostic decnet-iv dec-spanning dsm etype-6000 etype-8042 ipx-arpa ipx-non-arpa lat lavc-sca mop-console mop-dump msdos mumps netbios vines-ip vines-echo xns]	Deletes an ACE from a MAC-Layer named access list.

When configuring an entry in a MAC-Layer access list, note the following:

- You can enter MAC addresses as three 4-byte values in dotted hexadecimal format. For example, 0030.9629.9f84.

- You can enter MAC address masks as three 4-byte values in dotted hexadecimal format. Use 1 bits as wildcards. For example, to match an address exactly, use 0000.0000.0000 (can be entered as 0.0.0).
- Entries without a protocol parameter match any protocol.
- Access lists entries are scanned in the order you enter them. The first matching entry is used. To improve performance, place the most commonly used entries near the beginning of the access list.
- An implicit **deny any any** entry exists at the end of an access list unless you include an explicit **permit any any** entry at the end of the list.
- All new entries to an existing list are placed at the end of the list. You cannot add entries to the middle of a list.

This list shows the ethertype values matched by the protocol keywords:

- 0x0600—xns-idp—Xerox XNS IDP
- 0x0BAD—vines-ip—Banyan VINES IP
- 0x0baf—vines-echo—Banyan VINES Echo
- 0x6000—etype-6000—DEC unassigned, experimental
- 0x6001—mop-dump—DEC Maintenance Operation Protocol (MOP) Dump/Load Assistance
- 0x6002—mop-console—DEC MOP Remote Console
- 0x6003—decnet-iv—DEC DECnet Phase IV Route
- 0x6004—lat—DEC Local Area Transport (LAT)
- 0x6005—diagnostic—DEC DECnet Diagnostics
- 0x6007—lavc-sca—DEC Local-Area VAX Cluster (LAVC), SCA
- 0x6008—amber—DEC AMBER
- 0x6009—mumps—DEC MUMPS
- 0x8038—dec-spanning—DEC LANBridge Management
- 0x8039—dsm—DEC DSM/DDP
- 0x8040—netbios—DEC PATHWORKS DECnet NETBIOS Emulation
- 0x8041—msdos—DEC Local Area System Transport
- 0x8042—etype-8042—DEC unassigned
- 0x809B—appletalk—Kinetics EtherTalk (AppleTalk over Ethernet)
- 0x80F3—aarp—Kinetics AppleTalk Address Resolution Protocol (AARP)



Note

Use the **ipx-arpa** and **ipx-non-arpa** keywords to filter IPX traffic.

This example shows how to create a MAC-Layer access list named **mac_layer** that denies **dec-phase-iv** traffic with source address 0000.4700.0001 and destination address 0000.4700.0009, but permits all other traffic:

```
Router(config)# mac access-list extended mac_layer
Router(config-ext-macl)# deny 0000.4700.0001 0.0.0 0000.4700.0009 0.0.0 dec-phase-iv
Router(config-ext-macl)# permit any any
```

Configuring a Class Map (Optional)

These section describe class map configuration:

- [Creating a Class Map, page 24-40](#)
- [Configuring Filtering in a Class Map, page 24-40](#)



Note You can also create class maps during policy map creation with the **policy-map class** command (see the “[Creating a Policy Map Class and Configuring Filtering](#)” section on page 24-42).

Creating a Class Map

To create a class map, perform this task:

Command	Purpose
Router(config)# class-map <i>class_name</i>	Creates a class map.
Router(config)# no class-map <i>class_name</i>	Deletes a class map.

Configuring Filtering in a Class Map



- Except for MAC-Layer ACLs (see the “[Configuring MAC-Layer Named Access Lists \(Optional\)](#)” section on page 24-38), access lists are not documented in this publication. See the reference under **access-list** in the “[Configuring a PFC QoS Policy](#)” section on page 24-37.
- To base microflow policing only on source addresses, you must configure filtering to use only source addresses.
- To base microflow policing only on destination addresses, you must configure filtering to use only destination addresses.

To configure filtering in a class map, perform one of these tasks:

Command	Purpose
Router(config-cmap)# match access-group <i>name acl_index_or_name</i>	(Optional) Configures the class map to filter using an ACL.
Router(config-cmap)# no match access-group <i>name acl_index_or_name</i>	Clears the ACL configuration from the class map.
Router (config-cmap)# match ip precedence <i>ipp_value1 [ipp_value2 [ipp_valueN]]</i>	(Optional—for IP traffic only) Configures the class map to filter on up to eight IP precedence values. Note Does not support source-based or destination-based microflow policing.
Router (config-cmap)# no match ip precedence <i>ipp_value1 [ipp_value2 [ipp_valueN]]</i>	Clears configured IP precedence values from the class map.

Command	Purpose
Router (config-cmap)# match ip dscp dscp_value1 [dscp_value2 [dscp_valueN]]	(Optional—for IP traffic only) Configures the class map to filter on up to eight DSCP values. Note Does not support source-based or destination-based microflow policing.
Router (config-cmap)# no match ip dscp dscp_value1 [dscp_value2 [dscp_valueN]]	Clears configured DSCP values from the class map.

Verifying Class Map Configuration

To verify class map configuration, perform this task:

Command	Purpose
Step 1 Router (config-cmap)# end	Exits configuration mode.
Step 2 Router# show class-map class_name	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:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# class-map ipp5
Router(config-cmap)# match ip precedence 5
Router(config-cmap)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show class-map ipp5
Class Map match-all ipp5 (id 1)
  Match ip precedence 5

Router#
```

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 policy map commands.

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. PFC QoS does not attempt to apply commands from more than one policy map class to matched traffic.

These sections describe policy map configuration:

- [Creating a Policy Map, page 24-42](#)
- [Creating a Policy Map Class and Configuring Filtering, page 24-42](#)
- [Configuring Policy Map Class Actions, page 24-43](#)

Creating a Policy Map

To create a policy map, perform this task:

Command	Purpose
Router(config)# policy-map <i>policy_name</i>	Creates a policy map.
Router(config)# no policy-map <i>policy_name</i>	Deletes the policy map.

Creating a Policy Map Class and Configuring Filtering



- Note**
- PFC QoS does not support the **class class_name destination-address**, **class class_name input-interface**, **class class_name qos-group**, and **class class_name source-address** policy map commands.
 - PFC QoS does not detect the use of unsupported commands until you attach a policy map to an interface (see the “[Attaching a Policy Map to an Interface](#)” section on page 24-48).
 - To base microflow policing only on source addresses, you must configure filtering for the policy-map class to use only source addresses.
 - To base microflow policing only on destination addresses, you must configure filtering for the policy-map class to use only destination addresses.

Policy maps can contain one or more policy map classes. Enter one of these **class** commands to create a policy map class and configure filtering in it.

To create a policy map class and configure it to filter with an already defined class map, perform this task:

Command	Purpose
Router(config-pmap)# class <i>class_name</i>	Creates a policy map class and configures it to filter with a class map (see the “ Creating a Class Map ” section on page 24-40). Note PFC QoS supports class maps that contain a single match command.
Router(config-pmap)# no class <i>class_name</i>	Clears use of the class map.

To create a policy map class and a class map simultaneously, perform this task:

Command	Purpose
Router(config-pmap)# class <i>class_name</i> { access-group <i>acl_index_or_name</i> dscp <i>dscp_1</i> [<i>dscp_2</i> [<i>dscp_N</i>]] precedence <i>ipp_1</i> [<i>ipp_2</i> [<i>ipp_N</i>]]}	Creates a policy map class and creates a class map and configures the policy map class to filter with the class map.
Router(config-pmap)# no class <i>class_name</i>	Note • This command creates a class map that can be used in other policy maps. • The dscp and precedence filtering keywords do not support source-based or destination-based microflow policing. Clears use of the class map (does not delete the class map).

**Note**

- Put all trust-state and policing commands for each type of traffic in the same policy map class.
- PFC QoS does not attempt to apply commands from more than one policy map class to traffic.

Configuring Policy Map Class Actions

When configuring policy map class actions, note the following:

- For hardware-switched traffic, PFC QoS does not support the **bandwidth**, **priority**, **queue-limit**, or **random-detect** policy map class commands. You can configure these commands because they can be used for software-switched traffic.
- PFC QoS does not support the **set mpls** or **set qos-group** policy map class commands.
- PFC QoS supports the **set ip dscp** and **set ip precedence** policy map class commands (see the “Configuring Policy Map Class Marking” section on page 24-44).
- You cannot do all three of the following in a policy map class:
 - Mark traffic with the **set ip dscp** or **set ip precedence** commands
 - Configure the trust state
 - Configure policing

In a policy map class, you can either mark untrusted traffic with the **set ip dscp** or **set ip precedence** commands or do one or both of the following:

- Configure the trust state
- Configure policing

**Note**

When configure policing, you can mark traffic with policing keywords (see the “Configuring Policy Map Class Policing” section on page 24-44).

These sections describe policy map class action configuration:

- [Configuring Policy Map Class Marking, page 24-44](#)
- [Configuring the Policy Map Class Trust State, page 24-44](#)

- Configuring Policy Map Class Policing, page 24-44

Configuring Policy Map Class Marking

PFC QoS supports policy map class marking for untrusted traffic with the **set ip dscp** and **set ip precedence** policy map class commands.

To configure policy map class marking for untrusted traffic, perform this task:

Command	Purpose
Router(config-pmap-c)# set ip {dscp dscp_value precedence ip_precedence_value}	Configures the policy map class to mark matched untrusted traffic with the configured DSCP or IP precedence value.
Router(config-pmap-c)# no set ip {dscp dscp_value precedence ip_precedence_value}	Clears the marking configuration.

Configuring the Policy Map Class Trust State



- Note** You cannot attach a policy map that configures a trust state with the **service-policy output** command.

To configure the policy map class trust state, perform this task:

Command	Purpose
Router(config-pmap-c)# trust {cos dscp ip-precedence}	Configures the policy map class trust state, which selects the value that PFC QoS uses as the source of the internal DSCP value (see the “Internal DSCP Values” section on page 24-14).
Router(config-pmap-c)# no trust	Reverts to the default policy-map class trust state (untrusted).

When configuring the policy map class trust state, note the following:

- Enter the **no trust** command to use the trust state configured on the ingress port (this is the default).
- With the **cos** keyword, PFC QoS sets the internal DSCP value from received or ingress port CoS (see the “Mapping Received CoS Values to Internal DSCP Values” section on page 24-51).
- With the **dscp** keyword, PFC QoS uses received DSCP.
- With the **ip-precedence** keyword, PFC QoS sets DSCP from received IP precedence (see the “Mapping Received IP Precedence Values to Internal DSCP Values” section on page 24-53).

Configuring Policy Map Class Policing

When you configure policy map class policing, note the following:

- PFC QoS does not support the **set-qos-transmit** policer keyword.
- PFC QoS does not support the **set-dscp-transmit** or **set-prec-transmit** keywords as arguments to the **exceed-action** keyword.
- PFC QoS does not detect the use of unsupported keywords until you attach a policy map to an interface (see the “Attaching a Policy Map to an Interface” section on page 24-48).

These sections describe configuration of policy map class policing:

- Using a Named Aggregate Policer, page 24-45

- Configuring a Per-Interface Policer, page 24-45

**Note**

Policing with the **conform-action transmit** keywords sets the port trust state of matched traffic to trust DSCP or to the trust state configured by a **trust** command in the policy map class.

Using a Named Aggregate Policer

To use a named aggregate policer (see the “[Creating Named Aggregate Policers](#)” section on page 24-34), perform this task:

Command	Purpose
Router(config-pmap-c)# police aggregate aggregate_name	Configures the policy map class to use a previously defined named aggregate policer.
Router(config-pmap-c)# no police aggregate aggregate_name	Clears use of the named aggregate policer.

Configuring a Per-Interface Policer

To configure a per-interface policer (see the “[Policers](#)” section on page 24-15), perform this task:

Command	Purpose
Router(config-pmap-c)# police [flow [mask {src-only dest-only full-flow}]] bits_per_second normal_burst_bytes [maximum_burst_bytes] [pir peak_rate_bps] [[[conform-action {drop set-dscp-transmit dscp_value set-prec-transmit ip_precedence_value transmit}] exceed-action {drop policed-dscp transmit}] violate-action {drop policed-dscp transmit}]	Creates a per-interface policer and configures the policy-map class to use it.
Router(config-pmap-c)# no police [flow [mask {src-only dest-only full-flow}]] bits_per_second normal_burst_bytes [maximum_burst_bytes] [pir peak_rate_bps] [[[conform-action {drop set-dscp-transmit dscp_value set-prec-transmit ip_precedence_value transmit}] exceed-action {drop policed-dscp transmit}] violate-action {drop policed-dscp transmit}]	Deletes the per-interface policer from the policy-map class.

When configuring a per-interface policer, note the following:

- Policing uses the Layer 2 frame size.
- See the “[PFC QoS Configuration Guidelines and Restrictions](#)” section on page 24-28 for information about rate and burst size granularity.
- You can enter the **flow** keyword to define a microflow policer. During microflow policing, the following occurs:
 - You can enter the **mask src-only** keywords to base IP flow identification only on IP source addresses, which applies the microflow policer to all IP traffic from each source IP address.

**Note**

To base microflow policing only on source addresses, you must also configure filtering for the policy-map class to use only source addresses.

- You can enter the **mask dest-only** keywords to base IP flow identification only on IP destination addresses, which applies the microflow policer to all IP traffic to each source IP address.



Note To base microflow policing only on destination addresses, you must also configure filtering for the policy-map class to use only destination addresses.

- By default and with the **mask full-flow** keywords, PFC QoS bases IP flow identification on source IP address, destination IP address, the Layer 3 protocol, and Layer 4 port numbers.
- PFC QoS considers MAC-Layer traffic with the same protocol and the same source and destination MAC-Layer addresses to be part of the same flow, including traffic with different ethertypes.
- Microflow policers do not support the *maximum_burst_bytes* parameter, the **pir bits_per_second** keyword and parameter, or the **violate-action** keyword.
- The valid range of values for the CIR *bits_per_second* parameter is as follows:
 - Minimum—32 kilobits per second, entered as 32000
 - Maximum—4 gigabits per second, entered as 4000000000
- The *normal_burst_bytes* parameter sets the CIR token bucket size.
- The *maximum_burst_bytes* parameter sets the PIR token bucket size (not supported with the **flow** keyword)
- When configuring the size of a token bucket, note the following:
 - The minimum token bucket size is 1 kilobyte, entered as 1000 (the *maximum_burst_bytes* parameter must be set larger than the *normal_burst_bytes* parameter)
 - The maximum token bucket size is 32 megabytes, entered as 32000000
 - To sustain a specific rate, set the token bucket size to be at least the rate value divided by 4000, because tokens are removed from the bucket every 1/4000th of a second (0.25 ms).
 - Because the token bucket must be large enough to hold at least one frame, set the parameter larger than the maximum Layer 3 packet size of the traffic being policed.
 - For TCP traffic, configure the token bucket size as a multiple of the TCP window size, with a minimum value at least twice as large as the maximum Layer 3 packet size of the traffic being policed.
- (Not supported with the **flow** keyword.) The valid range of values for the **pir bits_per_second** parameter is as follows:
 - Minimum—32 kilobits per second, entered as 32000 (the value cannot be smaller than the CIR *bits_per_second* parameters)
 - Maximum—4 gigabits per second, entered as 4000000000
- (Optional) You can specify a conform action for matched in-profile traffic as follows:
 - The default conform action is **transmit**, which sets the policy map class trust state to *trust DSCP* unless the policy map class contains a **trust** command (see the “[Policy Maps](#)” section on page 24-14 and the “[Configuring Policy Map Class Actions](#)” section on page 24-43).
 - To set PFC QoS labels in untrusted traffic, you can enter the **set-dscp-transmit** keyword to mark matched untrusted traffic with a new DSCP value or enter the **set-prec-transmit** keyword to mark matched untrusted traffic with a new IP precedence value. The **set-dscp-transmit** and **set-prec-transmit** keywords are only supported for IP traffic. PFC QoS sets egress ToS and CoS from the configured value.

- You can enter the **drop** keyword to drop all matched traffic.
- Ensure that aggregate and microflow policers that are applied to the same traffic each specify the same conform-action behavior.
- (Optional) For traffic that exceeds the CIR, you can specify an exceed action as follows:
 - For marking without policing, you can enter the **transmit** keyword to transmit all matched out-of-profile traffic.
 - The default exceed action is **drop**, except with a *maximum_burst_bytes* parameter (**drop** is not supported with a *maximum_burst_bytes* parameter).



Note When the exceed action is **drop**, PFC QoS ignores any configured violate action.

- 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 the “[Configuring DSCP Markdown Values](#)” section on page 24-53).



Note When you create a policer that does not use the **pir** keyword and the *maximum_burst_bytes* parameter is equal to the *normal_burst_bytes* parameter (which is the case if you do not enter the *maximum_burst_bytes* parameter), the **exceed-action policed-dscp-transmit** keywords cause PFC QoS to mark traffic down as defined by the **policed-dscp max-burst** markdown map.

- (Optional—Not supported with the **flow** keyword) for traffic that exceeds the PIR, you can specify a violate action as follows:
 - For marking without policing, you can enter the **transmit** keyword to transmit all matched out-of-profile traffic.
 - The default violate action is equal to the exceed action.
 - 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 the “[Configuring DSCP Markdown Values](#)” section on page 24-53).



- Aggregate policing works independently on each DFC3-equipped switching module and independently on the PFC3, which supports any non-DFC3-equipped switching modules. Aggregate policing does not combine flow statistics from different DFC3-equipped switching modules. You can display aggregate policing statistics for each DFC3-equipped switching module and for the PFC3 and any non-DFC3-equipped switching modules supported by the PFC3.
- When you apply both ingress policing and egress policing to the same traffic, both the input policy and the output policy must either mark down traffic or drop traffic. PFC QoS does not support ingress markdown with egress drop or ingress drop with egress markdown.

This example shows how to create a policy map named **max-pol-ipp5** that uses the class-map named **ipp5**, which is configured to trust received IP precedence values and is configured with a maximum-capacity aggregate policer and with a microflow policer:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# policy-map max-pol-ipp5
Router(config-pmap)# class ipp5
```

■ Configuring PFC QoS

```
Router(config-pmap-c)# trust ip-precedence
Router(config-pmap-c)# police 2000000000 2000000 conform-action set-prec-transmit 6
exceed-action policed-dscp-transmit
Router(config-pmap-c)# police flow 10000000 10000 conform-action set-prec-transmit 6
exceed-action policed-dscp-transmit
Router(config-pmap-c)# end
```

Verifying Policy Map Configuration

To verify policy map configuration, perform this task:

	Command	Purpose
Step 1	Router(config-pmap-c)# end	Exits policy map class configuration mode. Note Enter additional class commands to create additional classes in the policy map.
Step 2	Router# show policy-map policy_name	Verifies the configuration.

This example shows how to verify the configuration:

```
Router# show policy-map max-pol-ipp5
Policy Map max-pol-ipp5
  class ipp5

  class ipp5
    police flow 10000000 10000 conform-action set-prec-transmit 6 exceed-action
    policed-dscp-transmit
      trust precedence
      police 2000000000 2000000 2000000 conform-action set-prec-transmit 6 exceed-action
    policed-dscp-transmit

Router#
```

Attaching a Policy Map to an Interface

To attach a policy map to an interface, perform this task:

	Command	Purpose
Step 1	Router(config)# interface {{vlan vlan_ID} {type¹ slot/port[.subinterface]} {port-channel number[.subinterface]}}	Selects the interface to configure.
Step 2	Router(config-if)# service-policy [input output] policy_map_name	Attaches a policy map to the interface.
	Router(config-if)# no service-policy [input output] policy_map_name	Removes the policy map from the interface.
Step 3	Router(config-if)# end	Exits configuration mode.
Step 4	Router# show policy-map interface {{vlan vlan_ID} {type¹ slot/port} {port-channel number}}	Verifies the configuration.

1. type = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

**Note**

- PFC QoS supports the **output** keyword only on Layer 3 interfaces (either LAN ports configured as Layer 3 interfaces or VLAN interfaces). You can attach both an input and an output policy map to a Layer 3 interface.
- Policies attached with the **output** keyword do not support microflow policing.
- You cannot set a trust state in policies attached with the **output** keyword.
- See the “[Attaching Policy Maps](#)” section on page 24-17 for more information about attaching policy maps to interfaces.
- You cannot attach a policy map that configures a trust state with the **service-policy output** command.
- Aggregate policing works independently on each DFC3-equipped switching module and independently on the PFC3, which supports any non-DFC3-equipped switching modules. Aggregate policing does not combine flow statistics from different DFC3-equipped switching modules. You can display aggregate policing statistics for each DFC3-equipped switching module and for the PFC3 and any non-DFC3-equipped switching modules supported by the PFC3.
- When you apply both ingress policing and egress policing to the same traffic, both the input policy and the output policy must either mark down traffic or drop traffic. PFC QoS does not support ingress markdown with egress drop or ingress drop with egress markdown.

This example shows how to attach the policy map named **pmap1** to Fast Ethernet port 5/36:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fastethernet 5/36
Router(config-if)# service-policy input pmap1
Router(config-if)# end
```

This example shows how to verify the configuration:

```
Router# show policy-map interface fastethernet 5/36
FastEthernet5/36
  service-policy input: pmap1
    class-map: cmap1 (match-all)
      0 packets, 0 bytes
      5 minute rate 0 bps
      match: ip precedence 5
    class cmap1
      police 8000 8000 conform-action transmit exceed-action drop
      class-map: cmap2 (match-any)
        0 packets, 0 bytes
        5 minute rate 0 bps
        match: ip precedence 2
        0 packets, 0 bytes
        5 minute rate 0 bps
    class cmap2
      police 8000 10000 conform-action transmit exceed-action drop
Router#
```

Configuring Egress DSCP Mutation

These sections describe how to configure egress DSCP mutation:

- [Configuring Named DSCP Mutation Maps](#), page 24-50
- [Attaching an Egress DSCP Mutation Map to an Interface](#), page 24-51

See the “Egress DSCP Mutation” section on page 24-18 for information about how egress DSCP mutation works.

Configuring Named DSCP Mutation Maps

To configure a named DSCP mutation map, perform this task:

Command	Purpose
Step 1 Router(config)# mls qos map dscp-mutation <i>map_name</i> <i>dscp1</i> [<i>dscp2</i> [<i>dscp3</i> [<i>dscp4</i> [<i>dscp5</i> [<i>dscp6</i> [<i>dscp7</i> [<i>dscp8</i>]]]]]]]] to <i>output_dscp</i>	Configures a named DSCP mutation map.
	Reverts to the default map.
Step 2 Router(config)# end	Exits configuration mode.
Step 3 Router# show mls qos maps	Verifies the configuration.

When configuring a named DSCP mutation map, note the following:

- You can enter up to 8 DSCP values that map to a mutated DSCP value.
- You can enter multiple commands to map additional DSCP values to a mutated DSCP value.
- You can enter a separate command for each mutated DSCP value.

This example shows how to map DSCP 30 to mutated DSCP value 8:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# mls qos map dscp-mutation mutmap1 30 to 8
Router(config)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show mls qos map | begin DSCP mutation
DSCP mutation map mutmap1:                                     (dscp= d1d2)
      d1 :   d2  0   1   2   3   4   5   6   7   8   9
      -----
      0 :    00 01 02 03 04 05 06 07 08 09
      1 :    10 11 12 13 14 15 16 17 18 19
      2 :    20 21 22 23 24 25 26 27 28 29
      3 :    08 31 32 33 34 35 36 37 38 39
      4 :    40 41 42 43 44 45 46 47 48 49
      5 :    50 51 52 53 54 55 56 57 58 59
      6 :    60 61 62 63
<...Output Truncated...>
Router#
```



In the DSCP mutation map displays, the marked-down DSCP values are shown in the body of the matrix; the first digit of the original DSCP value is in the column labeled d1 and the second digit is in the top row. In the example shown, DSCP 30 maps to DSCP 08.

Attaching an Egress DSCP Mutation Map to an Interface

To attach an egress DSCP mutation map to an interface, perform this task:

Command	Purpose
Step 1 Router(config)# interface {{vlan vlan_ID} {type¹ slot/port[.subinterface]} {port-channel number[.subinterface]}}	Selects the interface to configure.
Step 2 Router(config-if)# mls qos dscp-mutation mutation_map_name	Attaches an egress DSCP mutation map to the interface.
Router(config-if)# no mls qos dscp-mutation mutation_map_name	Removes the egress DSCP mutation from the interface.
Step 3 Router(config-if)# end	Exits configuration mode.
Step 4 Router# show running-config interface {{vlan vlan_ID} {type¹ slot/port} {port-channel number}}	Verifies the configuration.

1. type = ethernet, fastethernet, gigabitethernet, or tengigabitethernet

This example shows how to attach the egress DSCP mutation map named mutmap1 to Fast Ethernet port 5/36:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fastethernet 5/36
Router(config-if)# mls qos dscp-mutation mutmap1
Router(config-if)# end
```

Configuring DSCP Value Maps

These sections describe how DSCP values are mapped to other values:

- [Mapping Received CoS Values to Internal DSCP Values, page 24-51](#)
- [Mapping Received IP Precedence Values to Internal DSCP Values, page 24-53](#)
- [Configuring DSCP Markdown Values, page 24-53](#)
- [Mapping Internal DSCP Values to Egress CoS Values, page 24-55](#)

Mapping Received CoS Values to Internal DSCP Values

To configure the mapping of received CoS values to the DSCP value that PFC QoS uses internally on the PFC (see the “Internal DSCP Values” section on page 24-14), perform this task:

Command	Purpose
Step 1 Router(config)# mls qos map cos-dscp dscp1 dscp2 dscp3 dscp4 dscp5 dscp6 dscp7 dscp8	Configures the received CoS to internal DSCP map. You must enter 8 DSCP values to which PFC QoS maps CoS values 0 through 7.
Router(config)# no mls qos map cos-dscp	Reverts to the default map.
Step 2 Router(config)# end	Exits configuration mode.
Step 3 Router# show mls qos maps	Verifies the configuration.

This example shows how to configure the received CoS to internal DSCP map:

```
Router# configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Router(config)# mls qos map cos-dscp 0 1 2 3 4 5 6 7  
Router(config)# end  
Router#
```

This example shows how to verify the configuration:

```
Router# show mls qos maps | begin Cos-dscp map  
Cos-dscp map:  
cos:   0   1   2   3   4   5   6   7  
-----  
dscp:   0   1   2   3   4   5   6   7  
<...Output Truncated...>  
Router#
```

Mapping Received IP Precedence Values to Internal DSCP Values

To configure the mapping of received IP precedence values to the DSCP value that PFC QoS uses internally on the PFC (see the “Internal DSCP Values” section on page 24-14), perform this task:

Command	Purpose
Step 1 Router(config)# mls qos map ip-prec-dscp dscp1 dscp2 dscp3 dscp4 dscp5 dscp6 dscp7 dscp8	Configures the received IP precedence to internal DSCP map. You must enter 8 internal DSCP values to which PFC QoS maps received IP precedence values 0 through 7.
Router(config)# no mls qos map ip-prec-dscp	Reverts to the default map.
Step 2 Router(config)# end	Exits configuration mode.
Step 3 Router# show mls qos maps	Verifies the configuration.

This example shows how to configure the received IP precedence to internal DSCP map:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# mls qos map ip-prec-dscp 0 1 2 3 4 5 6 7
Router(config)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show mls qos maps | begin IpPrecedence-dscp map
IpPrecedence-dscp map:
  ipprec:  0   1   2   3   4   5   6   7
  -----
  dscp:    0   1   2   3   4   5   6   7
<...Output Truncated...
Router#
```

Configuring DSCP Markdown Values

To configure the mapping of DSCP markdown values used by policers (see the “Policers” section on page 24-15), perform this task:

Command	Purpose
Step 1 Router(config)# mls qos map policed-dscp {normal-burst max-burst} dscp1 [dscp2 [dscp3 [dscp4 [dscp5 [dscp6 [dscp7 [dscp8]]]]]]] to markdown_dscp	Configures a DSCP markdown map.
Router(config)# no mls qos map policed-dscp {normal-burst max-burst}	Reverts to the default map.
Step 2 Router(config)# end	Exits configuration mode.
Step 3 Router# show mls qos maps	Verifies the configuration.

When configuring a DSCP markdown map, note the following:

- You can enter the **normal-burst** keyword to configure the markdown map used by the **exceed-action policed-dscp-transmit** keywords.

- You can enter the **max-burst** keyword to configure the markdown map used by the **violate-action policed-dscp-transmit** keywords.



Note When you create a policer that does not use the **pir** keyword, and the *maximum_burst_bytes* parameter is equal to the *normal_burst_bytes* parameter (which occurs if you do not enter the *maximum_burst_bytes* parameter), the **exceed-action policed-dscp-transmit** keywords cause PFC QoS to mark traffic down as defined by the **policed-dscp max-burst** markdown map.

- To avoid out-of-sequence packets, configure the markdown maps so that conforming and nonconforming traffic uses the same queue.
- You can enter up to 8 DSCP values that map to a marked-down DSCP value.
- You can enter multiple commands to map additional DSCP values to a marked-down DSCP value.
- You can enter a separate command for each marked-down DSCP value.



Note Configure marked-down DSCP values that map to CoS values consistent with the markdown penalty (see the “[Mapping Internal DSCP Values to Egress CoS Values](#)” section on page 24-55).

This example shows how to map DSCP 1 to marked-down DSCP value 0:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# mls qos map policed-dscp normal-burst 1 to 0
Router(config)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show mls qos map
Normal Burst Policed-dscp map: (dscp= d1d2)
d1 : d2 0 1 2 3 4 5 6 7 8 9
-----
0 : 00 01 02 03 04 05 06 07 08 09
1 : 10 11 12 13 14 15 16 17 18 19
2 : 20 21 22 23 24 25 26 27 28 29
3 : 30 31 32 33 34 35 36 37 38 39
4 : 40 41 42 43 44 45 46 47 48 49
5 : 50 51 52 53 54 55 56 57 58 59
6 : 60 61 62 63

Maximum Burst Policed-dscp map: (dscp= d1d2)
d1 : d2 0 1 2 3 4 5 6 7 8 9
-----
0 : 00 01 02 03 04 05 06 07 08 09
1 : 10 11 12 13 14 15 16 17 18 19
2 : 20 21 22 23 24 25 26 27 28 29
3 : 30 31 32 33 34 35 36 37 38 39
4 : 40 41 42 43 44 45 46 47 48 49
5 : 50 51 52 53 54 55 56 57 58 59
6 : 60 61 62 63
<...Output Truncated...>
Router#
```

**Note**

In the Policed-dscp displays, the marked-down DSCP values are shown in the body of the matrix; the first digit of the original DSCP value is in the column labeled **d1** and the second digit is in the top row. In the example shown, DSCP 41 maps to DSCP 41.

Mapping Internal DSCP Values to Egress CoS Values

To configure the mapping of the DSCP value that PFC QoS uses internally on the PFC to the CoS value used for egress LAN port scheduling and congestion avoidance (see the “Internal DSCP Values” section on page 24-14 and the “LAN Egress Port Features” section on page 24-19), perform this task:

Command	Purpose
Step 1 Router(config)# mls qos map dscp-cos dscp1 [dscp2 [dscp3 [dscp4 [dscp5 [dscp6 [dscp7 [dscp8]]]]]]] to cos_value	Configures the internal DSCP to egress CoS map.
Router(config)# no mls qos map dscp-cos	Reverts to the default map.
Step 2 Router(config)# end	Exits configuration mode.
Step 3 Router# show mls qos maps	Verifies the configuration.

When configuring the internal DSCP to egress CoS map, note the following:

- You can enter up to 8 DSCP values that PFC QoS maps to a CoS value.
- You can enter multiple commands to map additional DSCP values to a CoS value.
- You can enter a separate command for each CoS value.

This example shows how to configure internal DSCP values 0, 8, 16, 24, 32, 40, 48, and 54 to be mapped to egress CoS value 0:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# mls qos map dscp-cos 0 8 16 24 32 40 48 54 to 0
Router(config)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show mls qos map | begin Dscp-cos map
Dscp-cos map:                                         (dscp= d1d2)
  d1 :   d2  0   1   2   3   4   5   6   7   8   9
  -----
  0 :    00 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 00 06
  5 :    06 06 06 06 00 06 07 07 07 07
  6 :    07 07 07 07
<...Output Truncated...>
Router#
```

**Note**

In the Dscp-cos display, the CoS values are shown in the body of the matrix; the first digit of the DSCP value is in the column labeled **d1** and the second digit is in the top row. In the example shown, DSCP values 41 through 47 all map to CoS 05.

Configuring the Trust State of Ethernet LAN Ports

By default, all ingress ports are untrusted. You can configure the port trust state on 1p1q0t, 1p1q8t, and Gigabit Ethernet ports (see the “[Ingress LAN Port Features](#)” section on page 24-9).

To configure the trust state of an ingress port, perform this task:

	Command	Purpose
Step 1	Router(config)# interface {{type ¹ slot/port} {port-channel number}}	Selects the interface to configure.
Step 2	Router(config-if)# mls qos trust [dscp ip-precedence cos]	Configures the trust state of the port.
	Router(config-if)# no mls qos trust	Reverts to the default trust state (untrusted).
Step 3	Router(config-if)# end	Exits configuration mode.
Step 4	Router# show mls qos	Verifies the configuration.

1. *type* = ethernet, fastethernet, gigabitetherent, or tengigabitetherent.

When configuring the trust state of an ingress port, note the following:

- With no other keywords, the **mls qos trust** command is equivalent to **mls qos trust dsep**.
- The **mls qos trust cos** command enables receive-queue drop thresholds. To avoid dropping traffic because of inconsistent CoS values, configure ports with the **mls qos trust cos** command only when the received traffic is ISL or 802.1Q frames carrying CoS values that you know to be consistent with network policy.
- Use the **no mls qos trust** command to set the port state to untrusted.

This example shows how to configure Gigabit Ethernet port 1/1 with the **trust cos** keywords:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface gigabitetherent 1/1
Router(config-if)# mls qos trust cos
Router(config-if)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show queueing interface gigabitetherent 1/1 | include trust
  Trust state: trust COS
Router#
```

Configuring the Ingress LAN Port CoS Value


Note

Whether or not PFC QoS uses the CoS value applied with the **mls qos cos** command depends on the trust state of the port and the trust state of the traffic received through the port. The **mls qos cos** command does not configure the trust state of the port or the trust state of the traffic received through the port.

To use the CoS value applied with the **mls qos cos** command as the basis of internal DSCP (see the “Internal DSCP Values” section on page 24-14):

- On a port that receives only untagged ingress traffic, configure the ingress port as trusted or configure a trust-CoS policy map that matches the ingress traffic.
- On a port that receives tagged ingress traffic, configure a trust-CoS policy map that matches the ingress traffic.

You can configure the CoS value that PFC QoS assigns to untagged frames from ingress LAN ports configured as trusted and to all frames from ingress LAN ports configured as untrusted.

To configure the CoS value for an ingress LAN port, perform this task:

Command	Purpose
Step 1 Router(config)# interface {{type ¹ slot/port} {port-channel number}}	Selects the interface to configure.
Step 2 Router(config-if)# mls qos cos default_cos Router(config-if)# [no] mls qos cos default_cos	Configures the ingress LAN port CoS value. Reverts to the default port CoS value.
Step 3 Router(config-if)# end	Exits configuration mode.
Step 4 Router# show queueing interface {ethernet fastethernet gigabitethernet} slot/port	Verifies the configuration.

1. type = ethernet, fastethernet, gigabitethernet, or tengigabitethernet

This example shows how to configure the CoS 5 as the default on Fast Ethernet port 5/24 and verify the configuration:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fastethernet 5/24
Router(config-if)# mls qos cos 5
Router(config-if)# end
Router# show queueing interface fastethernet 5/24 | include Default cos
    Default COS is 5
Router#
```

Configuring LAN-Port Drop Threshold Percentages

These sections describe LAN-port drop-threshold configuration:

- [Configuring Tail-Drop Threshold Percentages on 1q4t/2q2t LAN Ports, page 24-58](#)
- [Configuring 1p1q4t Standard Receive-Queue Tail-Drop Threshold Percentages, page 24-59](#)
- [Configuring Standard Queue WRED-Drop Thresholds, page 24-60](#)



Note Enter the **show queueing interface {ethernet | fastethernet | gigabitethernet | tengigabitethernet} slot/port | include type** command to see the queue structure of a port.

Configuring Tail-Drop Threshold Percentages on 1q4t/2q2t LAN Ports

The receive- and transmit-queue drop thresholds have this relationship:

- Receive queue 1 (standard) threshold 1 = transmit queue 1 (standard low priority) threshold 1
- Receive queue 1 (standard) threshold 2 = transmit queue 1 (standard low priority) threshold 2
- Receive queue 1 (standard) threshold 3 = transmit queue 2 (standard high priority) threshold 1
- Receive queue 1 (standard) threshold 4 = transmit queue 2 (standard high priority) threshold 2

To configure tail-drop threshold percentages for the standard receive and transmit queues on **1q4t/2q2t** LAN ports (see the “[Transmit Queues](#)” section on page 24-19), perform this task:

	Command	Purpose
Step 1	Router(config)# interface {ethernet fastethernet gigabitethernet} slot/port	Selects the interface to configure.
Step 2	Router(config-if)# wrr-queue threshold queue_id thr1% thr2%	Configures the receive- and transmit-queue tail-drop thresholds.
	Router(config-if)# no wrr-queue threshold [queue_id]	Reverts to the default receive- and transmit-queue tail-drop thresholds.
Step 3	Router(config-if)# end	Exits configuration mode.
Step 4	Router# show queueing interface {ethernet fastethernet gigabitethernet} slot/port	Verifies the configuration.

When configuring the receive- and transmit-queue tail-drop thresholds, note the following:

- You must use the transmit queue and threshold numbers.
- The *queue_id* is 1 for the standard low-priority queue and 2 for the standard high-priority queue.
- The percentages range from 1 to 100. A value of 10 indicates a threshold when the buffer is 10-percent full.
- Always set threshold 2 to 100 percent.

This example shows how to configure receive queue 1/threshold 1 and transmit queue 1/threshold 1 for Gigabit Ethernet port 2/1:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface gigabitethernet 2/1
Router(config-if)# wrr-queue threshold 1 60 100
Router(config-if)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show queueing interface gigabitethernet 2/1
Transmit queues [type = 2q2t]:
<...Output Truncated...>
```

```

queue tail-drop-thresholds
-----
1      60[1] 100[2]
2      40[1] 100[2]

<...Output Truncated...>

Receive queues [type = 1q4t] :

<...Output Truncated...>

queue tail-drop-thresholds
-----
1      60[1] 100[2] 40[3] 100[4]
<...Output Truncated...>
Router#

```



Note Receive-queue tail-drop thresholds are supported only on ingress Gigabit Ethernet LAN ports configured to trust CoS.

Configuring 1p1q4t Standard Receive-Queue Tail-Drop Threshold Percentages



Note Configure **1q4t** standard receive-queue tail-drop threshold percentages with the **wrr-queue threshold** command (see the “Configuring Tail-Drop Threshold Percentages on 1q4t/2q2t LAN Ports” section on page 24-58).

To configure tail-drop threshold percentages for the standard receive queues on a **1p1q4t** ingress LAN port (see the “Receive Queues” section on page 24-10), perform this task:

Command	Purpose
Step 1 Router(config)# interface {fastethernet gigabitetherent} slot/port	Selects the interface to configure.
Step 2 Router(config-if)# rcv-queue threshold queue_id thr1% thr2% thr3% thr4%	Configures the receive-queue tail-drop threshold percentages.
Router(config-if)# no rcv-queue threshold [queue_id]	Reverts to the default receive-queue tail-drop threshold percentages.
Step 3 Router(config-if)# end	Exits configuration mode.
Step 4 Router# show queueing interface {fastethernet gigabitetherent} slot/port	Verifies the configuration.

When configuring the receive-queue tail-drop threshold percentages, note the following:

- The *queue_id* is always 1.
- The percentages range from 1 to 100. A value of 10 indicates a threshold when the buffer is 10-percent full.
- Always set threshold 4 to 100 percent.

This example shows how to configure the receive-queue drop thresholds for Gigabit Ethernet port 1/1:

```

Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface gigabitetherent 1/1

```

Configuring PFC QoS

```
Router(config-if)# rcv-queue threshold 1 60 75 85 100
Router(config-if)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show queueing interface gigabitethernet 1/1 | begin Receive queues
Receive queues [type = 1p1q4t]:
  Queue Id   Scheduling   Num of thresholds
  -----
  1           Standard      4
  2           Priority      1

  Trust state: trust COS

  queue tail-drop-thresholds
  -----
  1       60[1] 75[2] 85[3] 100[4]
<...Output Truncated...>
Router#
```

Configuring Standard Queue WRED-Drop Thresholds

1p2q2t, **1p3q1t**, and **1p2q1t** ports have WRED-drop thresholds in their standard transmit queues.

1p1q8t ports have WRED-drop thresholds in their standard receive queue.



Note **1p3q1t** (transmit), **1p2q1t** (transmit), and **1p1q8t** (receive) ports also have nonconfigurable tail-drop thresholds (see the “[1p3q1t Ports](#)” section on page 24-21).

To configure the WRED-drop thresholds (see the “[Transmit Queues](#)” section on page 24-19), perform this task:

Command	Purpose
Step 1 Router(config)# interface type¹ slot/port	Selects the interface to configure.
Step 2 Router(config-if)# wrr-queue random-detect min-threshold queue_id thr1% [thr2% [thr3% thr4% thr5% thr6% thr7% thr8%]] Router(config-if)# no wrr-queue random-detect min-threshold [queue_id]	Configures the low WRED-drop thresholds. Reverts to the default low WRED-drop thresholds.
Step 3 Router(config-if)# wrr-queue random-detect max-threshold queue_id thr1% [thr2% [thr3% thr4% thr5% thr6% thr7% thr8%]] Router(config-if)# no wrr-queue random-detect max-threshold [queue_id]	Configures the high WRED-drop thresholds. Reverts to the default high WRED-drop thresholds.
Step 4 Router(config-if)# end	Exits configuration mode.
Step 5 Router# show queueing interface type¹ slot/port	Verifies the configuration.

1. *type* = **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

When configuring the WRED-drop thresholds, note the following:

- Each threshold has a low- and a high-WRED value.
- WRED values are a percentage of the queue capacity (the range is from 1 to 100).

- The low-WRED value is the traffic level under which no traffic is dropped. The low-WRED value must be lower than the high-WRED value. Configure the low-WRED value with the **min-threshold** keyword.
- The high-WRED value is the traffic level above which all traffic is dropped. Configure the high-WRED value with the **max-threshold** keyword.



Note Traffic in the queue between the low- and high-WRED values has an increasing chance of being dropped as the queue fills.

- When configuring **1p2q2t** ports, note the following:
 - Queue number 1 is the low-priority standard transmit queue
 - Queue number 2 is high priority standard transmit queue
 - Each queue has two thresholds.
- When configuring **1p3q1t** ports, note the following:
 - Queue number 1 is the low-priority standard transmit queue.
 - Queue number 2 is the medium priority standard transmit queue.
 - Queue number 3 is the high priority standard transmit queue.
 - Each queue has one threshold.
 - When you configure each standard transmit queue, the single percentage that you enter sets the threshold.
- When configuring **1p1q8t** ports, note the following:
 - Queue number 1 is the single standard receive queue.
 - When you configure the single standard receive queue, note the following:
 - The first percentage that you enter sets the lowest-priority threshold.
 - The second percentage that you enter sets the next highest-priority threshold.
 - The eighth percentage that you enter sets the highest-priority threshold.
- When configuring **1p2q1t** ports, note the following:
 - Queue number 1 is the low-priority standard transmit queue
 - Queue number 2 is high priority standard transmit queue
 - When you configure each standard transmit queue, the single percentage that you enter sets the threshold.

This example shows how to configure the low-priority transmit queue high-WRED-drop thresholds for Gigabit Ethernet port 1/1:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface gigabitethernet 1/1
Router(config-if)# wrr-queue random-detect max-threshold 1 70 70
Router(config-if)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show queueing interface gigabitethernet 1/1 | begin Transmit queues
Transmit queues [type = 1p2q2t]:
  Queue Id      Scheduling   Num of thresholds
  -----
    1            WRR low       2
    2            WRR high      2
    3            Priority      1

  queue random-detect-max-thresholds
  -----
    1      40[1] 70[2]
    2      40[1] 70[2]
<...Output Truncated...>
Router#
```

Enabling and Disabling WRED-Drop Thresholds

To enable or disable WRED-drop thresholds on **1p3q1t** or **1p2q1t** transmit queues or **1p1q8t** receive queues, perform this task:

	Command	Purpose
Step 1	Router(config)# interface type¹ slot/port	Selects the interface to configure.
Step 2	Router(config-if)# wrr-queue random-detect queue_id Router(config-if)# no wrr-queue random-detect [queue_id]	Enables WRED-drop thresholds on queue 1, 2, or 3. Reverts to the default WRED-drop thresholds.
Step 3	Router(config-if)# end	Exits configuration mode.
Step 4	Router# show queueing interface type¹ slot/port	Verifies the configuration.

1. *type* = fastethernet or tengigabitethernet

Mapping CoS Values to LAN-Port Drop Thresholds

These sections describe mapping CoS values to LAN-port drop thresholds:

- [Mapping CoS Values to 1q4t/2q2t LAN Ports, page 24-62](#)
- [Mapping CoS Values on 1p1q4t/1p2q2t, 1p1q0t/1p3q1t, and 1p1q8t/1p2q1t LAN Ports, page 24-63](#)

Mapping CoS Values to 1q4t/2q2t LAN Ports



Note Enter the **show queueing interface {ethernet | fastethernet | gigabitethernet | tengigabitethernet} slot/port | include type** command to see the queue structure of a port.

On **1q4t/2q2t** LAN ports, the receive- and transmit-queue tail-drop thresholds have this relationship:

- Receive queue 1 (standard) threshold 1 = transmit queue 1 (standard low priority) threshold 1
- Receive queue 1 (standard) threshold 2 = transmit queue 1 (standard low priority) threshold 2

- Receive queue 1 (standard) threshold 3 = transmit queue 2 (standard high priority) threshold 1
- Receive queue 1 (standard) threshold 4 = transmit queue 2 (standard high priority) threshold 2

To map CoS values to tail-drop thresholds, perform this task:

Command	Purpose
Step 1 Router(config)# interface type ¹ slot/port	Selects the interface to configure.
Step 2 Router(config-if)# wrr-queue cos-map transmit_queue_# threshold_# cos1 [cos2 [cos3 [cos4 [cos5 [cos6 [cos7 [cos8]]]]]]]	Maps CoS values to a tail-drop threshold.
Step 3 Router(config-if)# no wrr-queue cos-map	Reverts to the default mapping.
Step 4 Router(config-if)# end	Exits configuration mode.
Step 5 Router# show queueing interface type ¹ slot/port	Verifies the configuration.

1. type = ethernet, fastethernet, gigabitethernet, or tengigabitethernet

When mapping CoS values to a tail-drop threshold, note the following:

- Use the transmit queue and threshold numbers.
- Queue 1 is the low-priority standard transmit queue.
- Queue 2 is the high-priority standard transmit queue.
- There are two thresholds in each queue.
- Enter up to 8 CoS values to map to the threshold.

This example shows how to map the CoS values 0 and 1 to standard transmit queue 1/threshold 1 for Fast Ethernet port 5/36:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fastethernet 5/36
Router(config-if)# wrr-queue cos-map 1 1 0 1
Router(config-if)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show queueing interface fastethernet 5/36 | begin queue thresh cos-map
      queue thresh cos-map
      -----
      1      1      0 1
      1      2      2 3
      2      1      4 5
      2      2      6 7
<...Output Truncated...>
Router#
```

Mapping CoS Values on 1p1q4t/1p2q2t, 1p1q0t/1p3q1t, and 1p1q8t/1p2q1t LAN Ports



Note Enter the **show queueing interface {ethernet | fastethernet | gigabitethernet | tengigabitethernet} slot/port | include type** command to see the queue structure of a port.

These sections describe how to map CoS values:

- [Mapping CoS Values to Standard Receive-Queue Tail-Drop Thresholds, page 24-64](#)
- [Mapping CoS Values to WRED-Drop Thresholds, page 24-65](#)
- [Mapping CoS Values to Strict-Priority Queues, page 24-66](#)

Mapping CoS Values to Standard Receive-Queue Tail-Drop Thresholds

To map CoS values to the standard receive-queue tail-drop thresholds on **1p1q4t** and **1p1q0t** ingress LAN ports, perform this task:

	Command	Purpose
Step 1	Router(config)# interface {fastethernet gigabitetherent} slot/port	Selects the interface to configure.
Step 2	Router(config-if)# rcv-queue cos-map queue_# threshold_# cos1 [cos2 [cos3 [cos4 [cos5 [cos6 [cos7 [cos8]]]]]]]	Maps CoS values to the standard receive queue tail-drop thresholds. The queue number is always 1.
	Router(config-if)# no rcv-queue cos-map	Reverts to the default mapping.
Step 3	Router(config-if)# end	Exits configuration mode.
Step 4	Router# show queueing interface {fastethernet gigabitetherent} slot/port	Verifies the configuration.

This example shows how to map the CoS values 0 and 1 to threshold 1 in the standard receive queue for Gigabit Ethernet port 1/1:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface gigabitetherent 1/1
Router(config-if)# rcv-queue cos-map 1 1 0 1
Router(config-if)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show queueing interface gigabitetherent 1/1
<...Output Truncated...
    queue thresh cos-map
-----
    1      1      0 1
    1      2      2 3
    1      3      4 5
    1      4      6 7
<...Output Truncated...
Router#
```

Mapping CoS Values to WRED-Drop Thresholds

To map CoS values to WRED-drop thresholds, perform this task:

Command	Purpose
Step 1 Router(config)# interface {fastethernet gigabitethernet} slot/port	Selects the interface to configure.
Step 2 Router(config-if)# wrr-queue cos-map transmit_queue_# threshold_# cos1 [cos2 [cos3 [cos4 [cos5 [cos6 [cos7 [cos8]]]]]]] Router(config-if)# no wrr-queue cos-map	Maps CoS values to a WRED-drop threshold. Reverts to the default mapping.
Step 3 Router(config-if)# end	Exits configuration mode.
Step 4 Router# show queueing interface {fastethernet gigabitethernet} slot/port	Verifies the configuration.

When associating CoS values to a WRED-drop threshold, note the following:

- On **1p2q2t** egress LAN ports:
 - Queue 1 is the low-priority standard transmit queue.
 - Queue 2 is the high-priority standard transmit queue.
 - There are two WRED-drop thresholds in each queue. Threshold 1 is low-priority and threshold 2 is high-priority.
- On **1p3q1t** egress LAN ports:
 - Queue 1 is the low-priority standard transmit queue.
 - Queue 2 is the medium-priority standard transmit queue.
 - Queue 3 is the high-priority standard transmit queue.
 - Each queue has two thresholds. Threshold 0 is the nonconfigurable 100-percent tail-drop threshold. Threshold 1 the WRED-drop threshold (see the “Enabling and Disabling WRED-Drop Thresholds” section on page 24-62 and the “Configuring Standard Queue WRED-Drop Thresholds” section on page 24-60).
- On **1p1q8t** ingress LAN ports:
 - Queue 1 is the standard queue.
 - Queue 1 has nine thresholds. Threshold 0 is the nonconfigurable 100-percent tail-drop threshold. Thresholds 1 through 8 are the WRED-drop thresholds (see the “Enabling and Disabling WRED-Drop Thresholds” section on page 24-62 and the “Configuring Standard Queue WRED-Drop Thresholds” section on page 24-60).
- On **1p2q1t** egress LAN ports:
 - Queue 1 is the standard queue.
 - Queue 1 has two thresholds. Threshold 0 is the nonconfigurable 100-percent tail-drop threshold. Threshold 1 the WRED-drop threshold (see the “Enabling and Disabling WRED-Drop Thresholds” section on page 24-62 and the “Configuring Standard Queue WRED-Drop Thresholds” section on page 24-60).
- You can enter up to 8 CoS values to map to the threshold.

This example shows how to map the CoS values 0 and 1 to standard transmit queue 1/threshold 1 for Fast Ethernet port 5/36:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fastethernet 5/36
Router(config-if)# wrr-queue cos-map 1 1 0 1
Router(config-if)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show queueing interface fastethernet 5/36 | begin queue thresh cos-map
queue thresh cos-map
-----
1      1      0 1
1      2      2 3
2      1      4 5
2      2      6 7
<...Output Truncated...>
Router#
```

Mapping CoS Values to Strict-Priority Queues

To map CoS values to the receive and transmit strict-priority queues on **1p1q4t/1p2q2t**, **1p1q0t/1p3q1t** and **1p1q8t/1p2q1t** LAN ports, perform this task:

	Command	Purpose
Step 1	Router(config)# interface type ¹ slot/port	Selects the interface to configure.
Step 2	Router(config-if)# priority-queue cos-map queue_# cos1 [cos2 [cos3 [cos4 [cos5 [cos6 [cos7 [cos8]]]]]]]	Maps CoS values to the receive and transmit strict-priority queues.
	Router(config-if)# no priority-queue cos-map	Reverts to the default mapping.
Step 3	Router(config-if)# end	Exits configuration mode.
Step 4	Router# show queueing interface type ¹ slot/port	Verifies the configuration.

1. *type* = **fastethernet**, **gigabitetherent**, or **tengigabitetherent**

When mapping CoS values to the strict-priority queues, note the following:

- The queue number is always 1.
- You can enter up to 8 CoS values to map to the queue.

This example shows how to map CoS value 7 to the strict-priority queues on Gigabit Ethernet port 1/1:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface gigabitetherent 1/1
Router(config-if)# priority-queue cos-map 1 7
Router(config-if)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show queueing interface gigabitetherent 1/1
<...Output Truncated...>
Transmit queues [type = 1p2q2t]:
<...Output Truncated...
queue thresh cos-map
```

```

-----
1      1      0 1
1      2      2 3
2      1      4
2      2      6
3      1      5 7

Receive queues [type = 1p1q4t]:
<...Output Truncated...>
queue thresh cos-map
-----
1      1      0 1
1      2      2 3
1      3      4
1      4      6
2      1      5 7
<...Output Truncated...>
Router#

```

Allocating Bandwidth Between LAN-Port Transmit Queues

The switch transmits frames from one standard queue at a time using a WRR algorithm. WRR uses the ratio between queue weight values to decide how much to transmit from one queue before switching to the other. The more the ratio favors a queue, the more transmit bandwidth is allocated to it.

To allocate bandwidth for an egress LAN port, perform this task:

Command	Purpose
Step 1 Router(config)# interface type ¹ slot/port	Selects the interface to configure.
Step 2 Router(config-if)# wrr-queue bandwidth low_priority_queue_weight [medium_priority_queue_weight] high_priority_queue_weight Router(config-if)# no wrr-queue bandwidth	Allocates bandwidth between standard transmit queues. The valid values for weight range from 1 to 255. Reverts to the default bandwidth allocation.
Step 3 Router(config-if)# end	Exits configuration mode.
Step 4 Router# show queueing interface type ¹ slot/port	Verifies the configuration.

1. type = ethernet, fastethernet, gigabitethernet, or tengigabitethernet

This example shows how to allocate a 3-to-1 bandwidth ratio for Gigabit Ethernet port 1/2:

```

Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface gigabitethernet 1/2
Router(config-if)# wrr-queue bandwidth 3 1
Router(config-if)# end
Router#

```

This example shows how to verify the configuration:

```

Router# show queueing interface gigabitethernet 1/2 | include bandwidth
WRR bandwidth ratios:    3 [queue 1]    1 [queue 2]
Router#

```

Setting the Receive-Queue Size Ratio on a 1p1q0t or 1p1q8t Ingress LAN Ports

To set the size ratio between the strict-priority and standard receive queues on a **1p1q0t** or **1p1q8t** ingress LAN ports, perform this task:

Command	Purpose
Step 1 Router(config)# interface {fastethernet tengigabitethernet} slot/port	Selects the interface to configure.
Step 2 Router(config-if)# rcv-queue queue-limit standard_queue_weight strict_priority_queue_weight Router(config-if)# no rcv-queue queue-limit	Sets the size ratio between the strict-priority and standard receive queues. Reverts to the default size ratio.
Step 3 Router(config-if)# end	Exits configuration mode.
Step 4 Router# show queueing interface {fastethernet tengigabitethernet} slot/port	Verifies the configuration.

When setting the receive-queue size ratio, note the following:

- The **rcv-queue queue-limit** command configures ports on a per-ASIC basis.
- Estimate the mix of strict priority-to-standard traffic on your network (for example, 80 percent standard traffic and 20 percent strict-priority traffic).
- Use the estimated percentages as queue weights.
- Valid values are from 1 to 100 percent, except on **1p1q8t** ingress LAN ports, where valid values for the strict priority queue are from 3 to 100 percent.

This example shows how to set the receive-queue size ratio for Fast Ethernet port 2/2:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fastethernet 2/2
Router(config-if)# rcv-queue queue-limit 75 15
Router(config-if)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show queueing interface fastethernet 2/2 | include queue-limit
    queue-limit ratios:      75[queue 1]  15[queue 2]
Router#
```

Setting the LAN-Port Transmit-Queue Size Ratio

To set the transmit-queue size ratio on an egress LAN port, perform this task:

Command	Purpose
Step 1 Router(config)# interface type ¹ slot/port	Selects the interface to configure.
Step 2 Router(config-if)# wrr-queue queue-limit low_priority_queue_weight [medium_priority_queue_weight] high_priority_queue_weight Router(config-if)# no wrr-queue queue-limit	Sets the transmit-queue size ratio between transmit queues. Reverts to the default transmit-queue size ratio.

Command	Purpose
Step 3 Router(config-if)# end	Exits configuration mode.
Step 4 Router# show queueing interface type ¹ slot/port	Verifies the configuration.

1. *type* = ethernet, fastethernet, gigabitethernet, or tengigabitethernet

When setting the transmit-queue size ratio between transmit queues, note the following:

- Estimate the mix of low priority-to-high priority traffic on your network (for example, 80 percent low-priority traffic and 20 percent high-priority traffic).
- On **1p2q2t** egress LAN ports, PFC QoS sets the strict-priority queue size equal to the high priority queue size.
- Use the estimated percentages as queue weights.
- Valid values are from 1 to 100 percent, except on **1p2q1t** egress LAN ports, where valid values for the high priority queue are from 5 to 100 percent.

This example shows how to set the transmit-queue size ratio for Gigabit Ethernet port 1/2:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface gigabitethernet 1/2
Router(config-if)# wrr-queue queue-limit 75 15
Router(config-if)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show queueing interface gigabitethernet 1/2 | include queue-limit
    queue-limit ratios:      75 [queue 1]  25 [queue 2]
Router#
```




CHAPTER

25

Configuring PFC QoS Statistics Data Export

These sections describe PFC QoS statistics data export:

- [Understanding PFC QoS Statistics Data Export, page 25-1](#)
- [PFC QoS Statistics Data Export Default Configuration, page 25-1](#)
- [Configuring PFC QoS Statistics Data Export, page 25-2](#)

Understanding PFC QoS Statistics Data Export

The PFC QoS statistics data export feature generates per-LAN-port and per-aggregate policer utilization information and forwards this information in UDP packets to traffic monitoring, planning, or accounting applications. You can enable PFC QoS statistics data export on a per-LAN-port or on a per-aggregate policer basis. The statistics data generated per port consists of counts of the input and output packets and bytes. The aggregate policer statistics consist of counts of allowed packets and counts of packets exceeding the policed rate.

The PFC QoS statistics data collection occurs periodically at a fixed interval, but you can configure the interval at which the data is exported. PFC QoS statistics collection is enabled by default, and the data export feature is disabled by default for all ports and all aggregate policers configured on the Catalyst 6500 series switch.



Note

The PFC QoS statistics data export feature is completely separate from NetFlow Data Export and does not interact with it.

PFC QoS Statistics Data Export Default Configuration

[Table 25-1](#) shows the PFC QoS default configuration.

Table 25-1 PFC QoS Default Configuration

Feature	Default Value
PFC QoS Data Export	
Global PFC QoS data export	Disabled
Per port PFC QoS data export	Disabled

■ Configuring PFC QoS Statistics Data Export

Table 25-1 PFC QoS Default Configuration (continued)

Feature	Default Value
Per named aggregate policer PFC QoS data export	Disabled
Per class map policer PFC QoS data export	Disabled
PFC QoS data export time interval	300 seconds
Export destination	Not configured
PFC QoS data export field delimiter	Pipe character ()

Configuring PFC QoS Statistics Data Export

These sections describe how to configure PFC QoS statistics data export:

- [Enabling PFC QoS Statistics Data Export Globally, page 25-2](#)
- [Enabling PFC QoS Statistics Data Export for a Port, page 25-3](#)
- [Enabling PFC QoS Statistics Data Export for a Named Aggregate Policer, page 25-4](#)
- [Enabling PFC QoS Statistics Data Export for a Class Map, page 25-5](#)
- [Setting the PFC QoS Statistics Data Export Time Interval, page 25-6](#)
- [Configuring PFC QoS Statistics Data Export Destination Host and UDP Port, page 25-7](#)
- [Setting the PFC QoS Statistics Data Export Field Delimiter, page 25-9](#)

Enabling PFC QoS Statistics Data Export Globally

To enable PFC QoS statistics data export globally, perform this task:

	Command	Purpose
Step 1	Router(config)# mls qos statistics-export	Enables PFC QoS statistics data export globally.
	Router(config)# no mls qos statistics-export	Disables PFC QoS statistics data export globally.
Step 2	Router(config)# end	Exits configuration mode.
Step 3	Router# show mls qos statistics-export info	Verifies the configuration.

This example shows how to enable PFC QoS statistics data export globally and verify the configuration:

```
Router# configure terminal
Router(config)# mls qos statistics-export
Router(config)# end
% Warning: Export destination not set.
% Use 'mls qos statistics-export destination' command to configure the export destination
Router# show mls qos statistics-export info
QoS Statistics Data Export Status and Configuration information
-----
Export Status : enabled
Export Interval : 300 seconds
Export Delimiter : |
Export Destination : Not configured
Router#
```



Note You must enable PFC QoS statistics data export globally for other PFC QoS statistics data export configuration to take effect.

Enabling PFC QoS Statistics Data Export for a Port

To enable PFC QoS statistics data export for a port, perform this task:

Command	Purpose
Step 1 Router(config)# interface type ¹ slot/port	Selects the interface to configure.
Step 2 Router(config-if)# mls qos statistics-export	Enables PFC QoS statistics data export for the port.
Router(config-if)# no mls qos statistics-export	Disables PFC QoS statistics data export for the port.
Step 3 Router(config)# end	Exits configuration mode.
Step 4 Router# show mls qos statistics-export info	Verifies the configuration.

1. *type* = ethernet, fastethernet, gigabitethernet, or tengigabitethernet

This example shows how to enable PFC QoS statistics data export on FastEthernet port 5/24 and verify the configuration:

```
Router# configure terminal
Router(config)# interface fastethernet 5/24
Router(config-if)# mls qos statistics-export
Router(config-if)# end
Router# show mls qos statistics-export info
QoS Statistics Data Export Status and Configuration information
-----
Export Status : enabled
Export Interval : 300 seconds
Export Delimiter : |
Export Destination : Not configured

QoS Statistics Data Export is enabled on following ports:
-----
FastEthernet5/24
Router#
```

When enabled on a port, PFC QoS statistics data export contains the following fields, separated by the delimiter character:

- Export type (“1” for a port)
- Slot/port
- Number of ingress packets
- Number of ingress bytes
- Number of egress packets
- Number of egress bytes
- Time stamp

Enabling PFC QoS Statistics Data Export for a Named Aggregate Policer

To enable PFC QoS statistics data export for a named aggregate policer, perform this task:

Command	Purpose
Step 1 Router(config)# mls qos statistics-export aggregate-policer aggregate_policer_name	Enables PFC QoS statistics data export for a named aggregate policer.
	Router(config)# no mls qos statistics-export aggregate-policer aggregate_policer_name
Step 2 Router(config)# end	Exits configuration mode.
Step 3 Router# show mls qos statistics-export info	Verifies the configuration.

This example shows how to enable PFC QoS statistics data export for an aggregate policer named aggr1M and verify the configuration:

```
Router# configure terminal
Router(config)# mls qos statistics-export aggregate-policer aggr1M
Router(config)# end
Router# show mls qos statistics-export info
QoS Statistics Data Export Status and Configuration information
-----
Export Status : enabled
Export Interval : 300 seconds
Export Delimiter : |
Export Destination : Not configured

QoS Statistics Data Export is enabled on following ports:
-----
FastEthernet5/24

QoS Statistics Data export is enabled on following shared aggregate policers:
-----
aggr1M
Router#
```

When enabled for a named aggregate policer, PFC QoS statistics data export contains the following fields, separated by the delimiter character:

- Export type (“3” for an aggregate policer)
- Aggregate policer name
- Direction (“in”)
- PFC3 or DFC3 slot number
- Number of in-profile bytes
- Number of bytes that exceed the CIR
- Number of bytes that exceed the PIR
- Time stamp

Enabling PFC QoS Statistics Data Export for a Class Map

To enable PFC QoS statistics data export for a class map, perform this task:

Command	Purpose
Step 1 Router(config)# mls qos statistics-export class-map classmap_name	Enables PFC QoS statistics data export for a class map.
Router(config)# no mls qos statistics-export class-map classmap_name	Disables PFC QoS statistics data export for a class map.
Step 2 Router(config)# end	Exits configuration mode.
Step 3 Router# show mls qos statistics-export info	Verifies the configuration.

This example shows how to enable PFC QoS statistics data export for a class map named class3 and verify the configuration:

```
Router# configure terminal
Router(config)# mls qos statistics-export class-map class3
Router(config)# end
Router# show mls qos statistics-export info
QoS Statistics Data Export Status and Configuration information
-----
Export Status : enabled
Export Interval : 300 seconds
Export Delimiter : |
Export Destination : Not configured

QoS Statistics Data Export is enabled on following ports:
-----
FastEthernet5/24

QoS Statistics Data export is enabled on following shared aggregate policers:
-----
aggr1M

QoS Statistics Data Export is enabled on following class-maps:
-----
class3
Router#
```

When enabled for a class map, PFC QoS statistics data export contains the following fields, separated by the delimiter character:

- For data from a physical port:
 - Export type (“4” for a classmap and port)
 - Class map name
 - Direction (“in”)
 - Slot/port
 - Number of in-profile bytes
 - Number of bytes that exceed the CIR
 - Number of bytes that exceed the PIR
 - Time stamp

Configuring PFC QoS Statistics Data Export

- For data from a VLAN interface:
 - Export type (“5” for a class map and VLAN)
 - Classmap name
 - Direction (“in”)
 - PFC3 or DFC3 slot number
 - VLAN ID
 - Number of in-profile bytes
 - Number of bytes that exceed the CIR
 - Number of bytes that exceed the PIR
 - Time stamp
- For data from a port channel interface:
 - Export type (“6” for a class map and port-channel)
 - Class map name
 - Direction (“in”)
 - PFC3 or DFC3 slot number
 - Port channel ID
 - Number of in-profile bytes
 - Number of bytes that exceed the CIR
 - Number of bytes that exceed the PIR
 - Time stamp

Setting the PFC QoS Statistics Data Export Time Interval

To set the time interval for the PFC QoS statistics data export, perform this task:

	Command	Purpose
Step 1	Router(config)# mls qos statistics-export interval interval_in_seconds	Sets the time interval for the PFC QoS statistics data export.
	Router(config)# no mls qos statistics-export interval interval_in_seconds	Note The interval needs to be short enough to avoid counter wraparound with the activity in your configuration, but because exporting PFC QoS statistic creates a significant load on the switch, be careful when decreasing the interval.
Step 2	Router(config)# end	Reverts to the default time interval for the PFC QoS statistics data export.
Step 3	Router# show mls qos statistics-export info	Exits configuration mode.
		Verifies the configuration.

This example shows how to set the PFC QoS statistics data export interval and verify the configuration:

```
Router# configure terminal
Router(config)# mls qos statistics-export interval 250
Router(config)# end
```

```

Router# show mls qos statistics-export info
QoS Statistics Data Export Status and Configuration information
-----
Export Status : enabled
Export Interval : 250 seconds
Export Delimiter : |
Export Destination : Not configured

QoS Statistics Data Export is enabled on following ports:
-----
FastEthernet5/24

QoS Statistics Data export is enabled on following shared aggregate policers:
-----
aggr1M

QoS Statistics Data Export is enabled on following class-maps:
-----
class3
Router#

```

Configuring PFC QoS Statistics Data Export Destination Host and UDP Port

To configure the PFC QoS statistics data export destination host and UDP port number, perform this task:

Command	Purpose
Step 1 Router(config)# mls qos statistics-export destination {host_name host_ip_address} {port port_number syslog [facility facility_name] [severity severity_value]} Router(config)# no mls qos statistics-export destination	Configures the PFC QoS statistics data export destination host and UDP port number. Clears configured values.
Step 2 Router(config)# end	Exits configuration mode.
Step 3 Router# show mls qos statistics-export info	Verifies the configuration.


Note

When the PFC QoS data export destination is a syslog server, the exported data is prefaced with a syslog header.

Table 25-2 lists the supported PFC QoS data export facility and severity parameter values.

Table 25-2 Supported PFC QoS Data Export Facility Parameter Values

Name	Definition	Name	Definition
kern	kernel messages	cron	cron/at subsystem
user	random user-level messages	local0	reserved for local use
mail	mail system	local1	reserved for local use
daemon	system daemons	local2	reserved for local use
auth	security/authentication messages	local3	reserved for local use
syslog	internal syslogd messages	local4	reserved for local use

Table 25-2 Supported PFC QoS Data Export Facility Parameter Values (continued)

Name	Definition	Name	Definition
lpr	line printer subsystem	local5	reserved for local use
news	netnews subsystem	local6	reserved for local use
uucp	uucp subsystem	local7	reserved for local use

Table 25-3 lists the supported PFC QoS data export severity parameter values.

Table 25-3 Supported PFC QoS Data Export Severity Parameter Values

Severity Parameter		
Name	Number	Definition
emerg	0	system is unusable
alert	1	action must be taken immediately
crit	2	critical conditions
err	3	error conditions
warning	4	warning conditions
notice	5	normal but significant condition
info	6	informational
debug	7	debug-level messages

This example shows how to configure 172.20.52.3 as the destination host and syslog as the UDP port number and verify the configuration:

```
Router# configure terminal
Router(config)# mls qos statistics-export destination 172.20.52.3 syslog
Router(config)# end
Router# show mls qos statistics-export info
QoS Statistics Data Export Status and Configuration information
-----
Export Status : enabled
Export Interval : 250 seconds
Export Delimiter : |
Export Destination : 172.20.52.3, UDP port 514 Facility local6, Severity debug

QoS Statistics Data Export is enabled on following ports:
-----
FastEthernet5/24

QoS Statistics Data export is enabled on following shared aggregate policers:
-----
aggr1M

QoS Statistics Data Export is enabled on following class-maps:
-----
class3
```

Setting the PFC QoS Statistics Data Export Field Delimiter

To set the PFC QoS statistics data export field delimiter, perform this task:

Command	Purpose
Step 1 Router(config)# mls qos statistics-export delimiter <i>delimiter_character</i> Router(config)# no mls qos statistics-export delimiter	Sets the PFC QoS statistics data export field delimiter.
	Reverts to the default PFC QoS statistics data export field delimiter
Step 2 Router(config)# end	Exits configuration mode.
Step 3 Router# show mls qos statistics-export info	Verifies the configuration.

This example shows how to set the PFC QoS statistics data export field delimiter and verify the configuration:

```
Router# configure terminal
Router(config)# mls qos statistics-export delimiter ,
Router(config)# end
Router# show mls qos statistics-export info
QoS Statistics Data Export Status and Configuration information
-----
Export Status : enabled
Export Interval : 250 seconds
Export Delimiter : ,
Export Destination : 172.20.52.3, UDP port 514 Facility local6, Severity debug

QoS Statistics Data Export is enabled on following ports:
-----
FastEthernet5/24

QoS Statistics Data export is enabled on following shared aggregate policers:
-----
aggr1M

QoS Statistics Data Export is enabled on following class-maps:
-----
class3
```

■ Configuring PFC QoS Statistics Data Export



Configuring the Cisco IOS Firewall Feature Set

This chapter describes how to configure the Cisco IOS firewall feature set on the Catalyst 6500 series switches:

- [Cisco IOS Firewall Feature Set Support Overview, page 26-1](#)
- [Cisco IOS Firewall Guidelines and Restrictions, page 26-2](#)
- [Additional CBAC Configuration, page 26-3](#)

Cisco IOS Firewall Feature Set Support Overview

The firewall feature set image (s72033-jk9o3sv-mz.122-14.SX) supports these Cisco IOS firewall features:

- Context-Based Access Control (CBAC) —The PFC3 installs entries in the Netflow table to direct flows that require CBAC to the MSFC3 where the CBAC is applied in software on the MSFC3.
- Authentication Proxy—After authentication on the MSFC3, the PFC3 provides TCAM support for the authentication policy.
- Port-to-Application Mapping (PAM)—PAM is done in software on the MSFC3.

For more information about Cisco IOS firewall features, refer to the following publications:

- *Cisco IOS Security Configuration Guide*, Release 12.2, “Traffic Filtering and Firewalls” chapter and these sections:
 - the “Cisco IOS Firewall Overview” at this URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/ftrawf1/scffwl.htm
 - the “Configuring Context-Based Access Control” at this URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/ftrawf1/cfcac.htm
 - the “Configuring Authentication Proxy” at this URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/ftrawf1/cfahp.htm
- *Cisco IOS Security Command Reference* publication at this URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_r/index.htm

The following features are supported with and without the use of a Cisco IOS firewall image:

- Standard access lists and static extended access lists
- Lock-and-key (dynamic access lists)
- IP session filtering (reflexive access lists)
- TCP intercept
- Security server support
- Network address translation
- Neighbor router authentication
- Event logging
- User authentication and authorization



Note Catalyst 6500 series switches support the Intrusion Detection System Module (IDSM) (WS-X6381-IDS). Catalyst 6500 series switches do not support the Cisco IOS firewall IDS feature, which is configured with the **ip audit** command.

Cisco IOS Firewall Guidelines and Restrictions

Follow these guidelines and restrictions when configuring the Cisco IOS firewall features:

- On other platforms, if you enter the **ip inspect** command on a port, CBAC modifies ACLs on other ports to permit the inspected traffic to flow through the network device. On Catalyst 6500 series switches, you must enter the **mls ip inspect** command to permit traffic through any ACLs that would deny the traffic through other ports. Refer to the “[Additional CBAC Configuration](#)” section on [page 26-3](#) for more information.
- Reflexive ACLs and CBAC have conflicting flow mask requirements. Reflexive ACLs are processed in software on the MSFC3.
- CBAC is incompatible with VACLs. You can configure CBAC and VACLs on the switch but not in the same subnet (VLAN).



Note The Intrusion Detection System Module (IDSM) uses VACLs to select traffic. To use the IDSM in a subnet where CBAC is configured, enter the **mls ip ids acl_name** interface command, where *acl_name* is configured to select traffic for the IDSM.

- To inspect Microsoft NetMeeting (2.0 or greater) traffic, turn on both **h323** and **tcp** inspection.
- To inspect web traffic, turn on **tcp** inspection. To avoid reduced performance, do not turn on **http** inspection to block Java.
- QoS and CBAC do not interact or interfere with each other.
- You can configure CBAC on physical ports configured as Layer 3 interfaces and on VLAN interfaces.
- You cannot configure VACLs and CBAC on the same interface.

Additional CBAC Configuration

You need to do additional CBAC configuration on the Catalyst 6500 series switches. On a network device other than a Catalyst 6500 series switch, when ports are configured to deny traffic, CBAC permits traffic to flow bidirectionally through the port if it is configured with the **ip inspect** command. The same situation applies to any other port that the traffic needs to go through, as shown in this example:

```
Router(config)# ip inspect name permit_ftp ftp
Router(config)# interface vlan 100
Router(config-if)# ip inspect permit_ftp in
Router(config-if)# ip access-group deny_ftp_a in
Router(config-if)# ip access-group deny_ftp_b out
Router(config-if)# exit
Router(config)# interface vlan 200
Router(config-if)# ip access-group deny_ftp_c in
Router(config-if)# ip access-group deny_ftp_d out
Router(config-if)# exit
Router(config)# interface vlan 300
Router(config-if)# ip access-group deny_ftp_e in
Router(config-if)# ip access-group deny_ftp_f out
Router(config-if)# end
```

If the FTP session enters on VLAN 100 and needs to leave on VLAN 200, CBAC permits the FTP traffic through ACLs deny_ftp_a, deny_ftp_b, deny_ftp_c, and deny_ftp_d. If another FTP session enters on VLAN 100 and needs to leave on VLAN 300, CBAC permits the FTP traffic through ACLs deny_ftp_a, deny_ftp_b, deny_ftp_e, and deny_ftp_f.

On a Catalyst 6500 series switch, when ports are configured to deny traffic, CBAC permits traffic to flow bidirectionally only through the port configured with the **ip inspect** command. You must configure other ports with the **mls ip inspect** command.

If the FTP session enters on VLAN 100 and needs to leave on VLAN 200, CBAC on a Catalyst 6500 series switch permits the FTP traffic only through ACLs deny_ftp_a and deny_ftp_b. To permit the traffic through ACLs deny_ftp_c and deny_ftp_d, you must enter the **mls ip inspect deny_ftp_c** and **mls ip inspect deny_ftp_d** commands, as shown in this example:

```
Router(config)# mls ip inspect deny_ftp_c
Router(config)# mls ip inspect deny_ftp_d
```

FTP traffic cannot leave on VLAN 300 unless you enter the **mls ip inspect deny_ftp_e** and **mls ip inspect deny_ftp_f** commands. Enter the **show fm insp [detail]** command to verify the configuration.

The **show fm insp [detail]** command displays the list of ACLs and ports on which CBAC is configured and the status (ACTIVE or INACTIVE), as shown in this example:

```
Router# show fm insp
      interface:Vlan305(in) status :ACTIVE
      acl name:deny
      interfaces:
          Vlan305(out):status ACTIVE
```

On VLAN 305, inspection is active in the inbound direction and no ACL exists. ACL **deny** is applied on VLAN 305 in the outbound direction and inspection is active.

To display all of the flow information, use the **detail** keyword.

If a VACL is configured on the port before configuring CBAC, the status displayed is INACTIVE; otherwise, it is ACTIVE. If PFC resources are exhausted, the command displays the word “BRIDGE” followed by the number of currently active NetFlow requests that failed, which have been sent to the MSFC3 for processing.

■ Additional CBAC Configuration



Configuring IEEE 802.1X Port-Based Authentication

This chapter describes how to configure IEEE 802.1X port-based authentication to prevent unauthorized devices (clients) from gaining access to the network.

**Note**

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication.

This chapter consists of these sections:

- [Understanding 802.1X Port-Based Authentication, page 27-1](#)
- [Default 802.1X Port-Based Authentication Configuration, page 27-5](#)
- [802.1X Port-Based Authentication Guidelines and Restrictions, page 27-6](#)
- [Configuring 802.1X Port-Based Authentication, page 27-7](#)
- [Displaying 802.1X Status, page 27-15](#)

Understanding 802.1X Port-Based Authentication

The IEEE 802.1X standard defines 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 authenticates each client connected to a switch port and assigns the port to a VLAN 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.

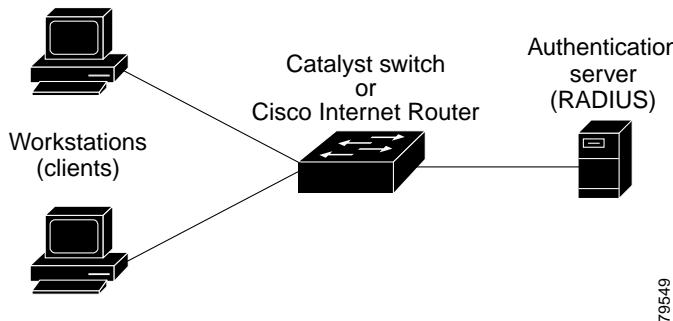
These sections describe IEEE 802.1X port-based authentication:

- [Device Roles, page 27-2](#)
- [Authentication Initiation and Message Exchange, page 27-3](#)
- [Ports in Authorized and Unauthorized States, page 27-4](#)
- [Supported Topologies, page 27-4](#)

Device Roles

With 802.1X port-based authentication, the devices in the network have specific roles as shown in Figure 27-1.

Figure 27-1 802.1X Device Roles



79549

The specific roles shown in Figure 27-1 are as follows:

- *Client*—The device (workstation) that requests access to the LAN and switch services and responds to requests from the switch. The workstation must be running 802.1X-compliant client software such as that offered in the Microsoft Windows XP operating system. (The client is the *supplicant* in the IEEE 802.1X specification.)



Note To resolve Windows XP network connectivity and 802.1X port-based authentication issues, read 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 or not 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 uses a client-server model in which secure authentication information is exchanged between the RADIUS server and one or more RADIUS clients.
- *Switch* (also called the *authenticator* and *back-end authenticator*)—Controls the 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 reencapsulated 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.

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 transitions from down to up. The switch 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). When the client receives the frame, it responds with an EAP-response/identity frame.

If the client does not receive an EAP-request/identity frame from the switch during bootup, the client can initiate authentication by sending an EAPOL-start frame, which prompts the switch to request the client's identity.

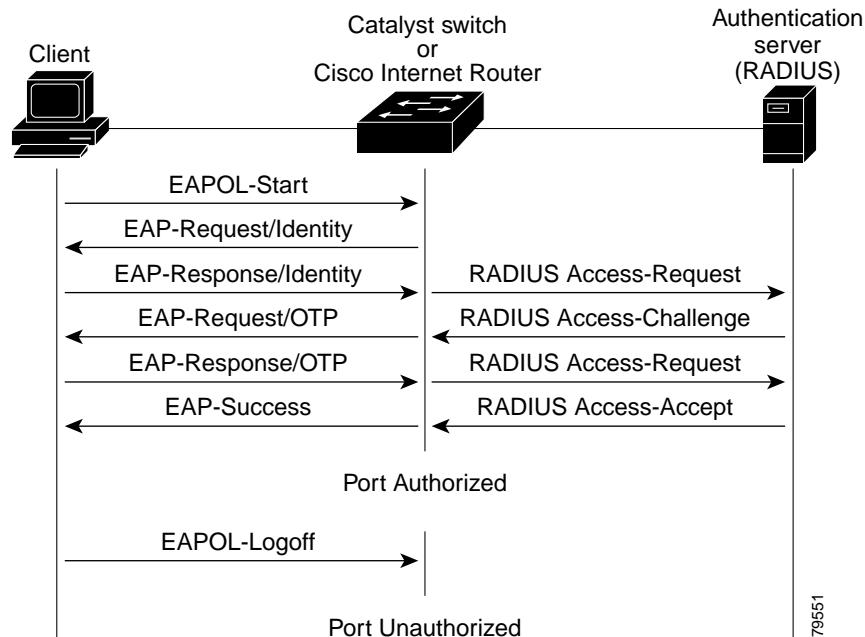

Note

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. For more information, see the “[Ports in Authorized and Unauthorized States](#)” section on page 27-4.

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. For more information, see the “[Ports in Authorized and Unauthorized States](#)” section on page 27-4.

The specific exchange of EAP frames depends on the authentication method being used. [Figure 27-2](#) shows a message exchange initiated by the client using the One-Time-Password (OTP) authentication method with a RADIUS server.

Figure 27-2 Message Exchange



79551

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.

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 for 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 control the port authorization state by using the **dot1x port-control** interface configuration command and these keywords:

- **force-authorized**—Disables 802.1X port-based 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 port-based 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.

Supported Topologies

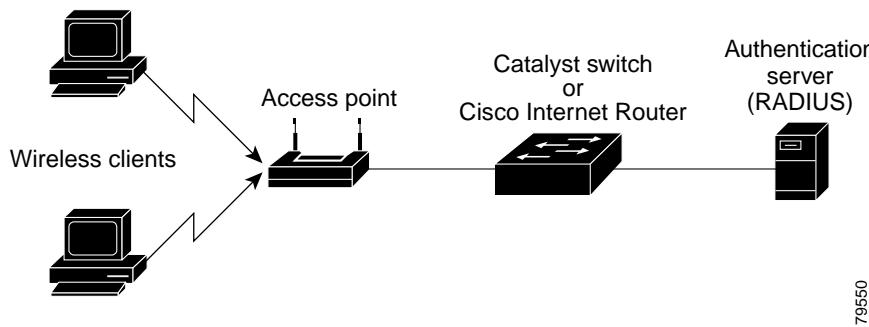
The 802.1X port-based authentication is supported in two topologies:

- Point-to-point
- Wireless LAN

In a point-to-point configuration (see [Figure 27-1 on page 27-2](#)), 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 27-3](#) shows 802.1X port-based authentication in a wireless LAN. The 802.1X port is configured as a multiple-host port that becomes authorized as soon as one 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 (reauthentication fails or an EAPOL-logoff message is received), the switch denies access to the network to all of the attached clients. In this topology, the wireless access point is responsible for authenticating the clients attached to it, and the wireless access point acts as a client to the switch.

Figure 27-3 Wireless LAN Example



Default 802.1X Port-Based Authentication Configuration

[Table 27-1](#) shows the default 802.1X configuration.

Table 27-1 Default 802.1X Configuration

Feature	Default Setting
Authentication, authorization, and accounting (AAA)	Disabled
RADIUS server IP address	None specified
RADIUS server UDP authentication port	1812
RADIUS server key	None specified
Per-interface 802.1X protocol enable state	Disabled (force-authorized) Note The port transmits and receives normal traffic without 802.1X-based authentication of the client.
Periodic reauthentication	Disabled
Number of seconds between reauthentication attempts	3600 seconds
Quiet period	60 seconds (number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client)

Table 27-1 Default 802.1X Configuration (continued)

Feature	Default Setting
Retransmission time	30 seconds (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 times (number of times that the switch will send an EAP-request/identity frame before restarting the authentication process)
Multiple host support	Disabled
Client timeout period	30 seconds (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 seconds (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)

802.1X Port-Based Authentication Guidelines and Restrictions

Follow these guidelines and restrictions when configuring 802.1X port-based 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.
 - EtherChannel port—Before enabling 802.1X on the port, you must first remove it from the EtherChannel port-channel interface. If you try to enable 802.1X on an EtherChannel port-channel interface or on an individual 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 individual port of an EtherChannel, the port does not join the EtherChannel.
 - Secure port—you cannot configure a secure port as 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.
 - Switch Port Analyzer (SPAN) destination port—you can enable 802.1X on a port that is a SPAN destination port; however, 802.1X is disabled until the port is removed as a SPAN destination port. You can enable 802.1X on a SPAN source port.

Configuring 802.1X Port-Based Authentication

These sections describe how to configure 802.1X port-based authentication:

- [Enabling 802.1X Port-Based Authentication, page 27-7](#)
- [Configuring Switch-to-RADIUS-Server Communication, page 27-8](#)
- [Enabling Periodic Reauthentication, page 27-10](#)
- [Manually Reauthenticating the Client Connected to a Port, page 27-11](#)
- [Initializing Authentication for the Client Connected to a Port, page 27-11](#)
- [Changing the Quiet Period, page 27-11](#)
- [Changing the Switch-to-Client Retransmission Time, page 27-12](#)
- [Setting the Switch-to-Client Frame Retransmission Number, page 27-14](#)
- [Enabling Multiple Hosts, page 27-14](#)
- [Resetting the 802.1X Configuration to the Default Values, page 27-15](#)

Enabling 802.1X Port-Based 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 Router(config)# aaa new-model Router(config)# no aaa new-model	Enables AAA. Disables AAA.
Step 2 Router(config)# aaa authentication dot1x {default} method1 [method2...] Router(config)# no aaa authentication dot1x {default list_name}	Creates an 802.1X port-based authentication method list. Clears the configured method list.
Step 3 Router(config)# dot1x system-auth-control Router(config)# no dot1x system-auth-control	Globally enables 802.1X port-based authentication. Globally disables 802.1X port-based authentication.
Step 4 Router(config)# interface type ¹ slot/port	Enters interface configuration mode and specifies the interface to be enabled for 802.1X port-based authentication.
Step 5 Router(config-if)# dot1x port-control auto Router(config-if)# no dot1x port-control auto	Enables 802.1X port-based authentication on the interface. Disables 802.1X port-based authentication on the interface.

Command	Purpose
Step 6 Router(config)# end	Returns to privileged EXEC mode.
Step 7 Router# show dot1x all	Verifies your entries. Check the Status column in the 802.1X Port Summary section of the display. An <i>enabled</i> status means the port-control value is set either to auto or to force-unauthorized .

1. type = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

When you enable 802.1X port-based authentication, note the following syntax information:

- To create a default list that is used when a named list is *not* specified in the **authentication** command, use the **default** keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all interfaces.
- Enter at least one of these keywords:
 - **group radius**—Use the list of all RADIUS servers for authentication.
 - **none**—Use no authentication. The client is automatically authenticated by the switch without using the information supplied by the client.

This example shows how to enable AAA and 802.1X on Fast Ethernet port 5/1:

```
Router# configure terminal
Router(config)# aaa new-model
Router(config)# aaa authentication dot1x default group radius
Router(config)# dot1x system-auth-control
Router(config)# interface fastethernet 5/1
Router(config-if)# dot1x port-control auto
Router(config-if)# end
```

This example shows how to verify the configuration:

```
Router# show dot1x all
```

```
Dot1x Info for interface FastEthernet5/1
-----
AuthSM State      = FORCE UNAUTHORIZED
BendSM State     = IDLE
PortStatus        = UNAUTHORIZED
MaxReq           = 2
MultiHosts        = Disabled
Port Control      = Force UnAuthorized
QuietPeriod       = 60 Seconds
Re-authentication = Disabled
ReAuthPeriod      = 3600 Seconds
ServerTimeout     = 30 Seconds
SuppTimeout       = 30 Seconds
TxPeriod          = 30 Seconds
```

Configuring Switch-to-RADIUS-Server Communication

RADIUS security servers are identified by any of the following:

- Host name
- Host IP address

- Host name and specific UDP port numbers
- 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 failover backup to the first one. The RADIUS host entries are tried in the order that they were configured.

To configure the RADIUS server parameters, perform this task:

Command	Purpose
Step 1 Router(config)# ip radius source-interface <i>interface_name</i>	Specifies that the RADIUS packets have the IP address of the indicated interface.
	Prevents the RADIUS packets from having the IP address of the previously indicated interface.
Step 2 Router(config)# radius-server host { <i>hostname</i> <i>ip_address</i> }	Configures the RADIUS server host name or IP address on the switch.
	If you want to use multiple RADIUS servers, reenter this command.
	Router(config)# no radius-server host { <i>hostname</i> <i>ip_address</i> }
Step 3 Router(config)# radius-server key <i>string</i>	Deletes the specified RADIUS server.
	Configures the authorization and encryption key used between the switch and the RADIUS daemon running on the RADIUS server.
Step 4 Router(config)# end	Returns to privileged EXEC mode.

When you configure the RADIUS server parameters, note the following syntax information:

- For *hostname* or *ip_address*, specify the host name or IP address of the remote RADIUS server.
- Specify the **key string** on a separate command line.
- For **key string**, 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.
- When you specify the **key string**, 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.
- 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. For more information, refer to the *Cisco IOS Security Configuration Guide*, Release 12.2, publication and the *Cisco IOS Security Command Reference*, Release 12.2, publication at this URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/index.htm>

**Note**

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. For more information, refer to the RADIUS server documentation.

This example shows how to configure the RADIUS server parameters on the switch:

```
Router# configure terminal
Router(config)# ip radius source-interface VLAN80
Router(config)# radius-server host 172.120.39.46
Router(config)# radius-server key rad123
Router(config)# end
```

Enabling Periodic Reauthentication

You can enable periodic 802.1X client reauthentication and specify how often it occurs. If you do not specify a time period before enabling reauthentication, the number of seconds between reauthentication attempts is 3600.

Automatic 802.1X client reauthentication is a global setting and cannot be set for clients connected to individual ports. To manually reauthenticate the client connected to a specific port, see the “[Manually Reauthenticating the Client Connected to a Port](#)” section on page 27-11.

To enable periodic reauthentication of the client and to configure the number of seconds between reauthentication attempts, perform this task:

	Command	Purpose
Step 1	Router(config)# interface type ¹ slot/port	Selects an interface to configure.
Step 2	Router(config-if)# dot1x reauthentication	Enables periodic reauthentication of the client, which is disabled by default.
	Router(config-if)# no dot1x reauthentication	Disables periodic reauthentication of the client.
Step 3	Router(config-if)# dot1x timeout re-authperiod seconds	Sets the number of seconds between reauthentication attempts. The range is 1 to 4294967295; the default is 3600 seconds. This command affects the behavior of the switch only if periodic reauthentication is enabled.
	Router(config-if)# no dot1x timeout re-authperiod	Returns to the default reauthorization period.
Step 4	Router(config-if)# end	Returns to privileged EXEC mode.
Step 5	Router# show dot1x all	Verifies your entries.

1. type = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

This example shows how to enable periodic reauthentication and set the number of seconds between reauthentication attempts to 4000:

```
Router(config-if)# dot1x reauthentication
Router(config-if)# dot1x timeout re-authperiod 4000
```

Manually Reauthenticating the Client Connected to a Port



Note Reauthentication does not disturb the status of an already authorized port.

To manually reauthenticate the client connected to a port, perform this task:

Command	Purpose
Step 1 Router# dot1x re-authenticate interface type¹ slot/port	Manually reauthenticates the client connected to a port.
Step 2 Router# show dot1x all	Verifies your entries.

1. *type* = ethernet, fastethernet, gigabitethernet, or tengigabitethernet

This example shows how to manually reauthenticate the client connected to Fast Ethernet port 5/1:

```
Router# dot1x re-authenticate interface fastethernet 5/1
Starting reauthentication on FastEthernet 5/1
```

Initializing Authentication for the Client Connected to a Port



Note Initializing authentication disables any existing authentication before authenticating the client connected to the port.

To initialize the authentication for the client connected to a port, perform this task:

Command	Purpose
Step 3 Router# dot1x initialize interface type¹ slot/port	Initializes the authentication for the client connected to a port.
Step 4 Router# show dot1x all	Verifies your entries.

1. *type* = ethernet, fastethernet, gigabitethernet, or tengigabitethernet

This example shows how to initialize the authentication for the client connected to Fast Ethernet port 5/1:

```
Router# dot1x initialize interface fastethernet 5/1
Starting reauthentication on FastEthernet 5/1
```

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 smaller number than the default.

To change the quiet period, perform this task:

	Command	Purpose
Step 1	Router(config)# interface type ¹ slot/port	Selects an interface to configure.
Step 2	Router(config-if)# dot1x timeout quiet-period seconds	Sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client. The range is 0 to 65535 seconds; the default is 60.
	Router(config-if)# no dot1x timeout quiet-period	Returns to the default quiet time.
Step 3	Router(config-if)# end	Returns to privileged EXEC mode.
Step 4	Router# show dot1x all	Verifies your entries.

1. *type* = **ethernet**, **fastethernet**, **gigabitether**net, or **tengigabitether**net

This example shows how to set the quiet time on the switch to 30 seconds:

```
Router(config-if)# 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	Router(config)# interface type ¹ slot/port	Selects an interface to configure.
Step 2	Router(config-if)# dot1x timeout tx-period seconds	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. The range is 1 to 65535 seconds; the default is 30.
	Router(config-if)# dot1x timeout tx-period	Returns to the default retransmission time.
Step 3	Router(config-if)# end	Returns to privileged EXEC mode.
Step 4	Router# show dot1x all	Verifies your entries.

1. *type* = **ethernet**, **fastethernet**, **gigabitether**net, or **tengigabitether**net

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

```
Router(config)# dot1x timeout tx-period 60
```

Setting the Switch-to-Client Retransmission Time for EAP-Request Frames

The client notifies the switch that it received the EAP-request frame. If the switch does not receive this notification, the switch waits a set period of time, and then retransmits the frame. You may set the amount of time that the switch waits for notification from 1 to 65535 seconds. (The default is 30 seconds.)

To set the switch-to-client retransmission time for the EAP-request frames, perform this task:

	Command	Purpose
Step 1	Router(config)# interface type ¹ slot/port	Selects an interface to configure.
Step 2	Router(config-if)# dot1x timeout supp-timeout seconds	Sets the switch-to-client retransmission time for the EAP-request frame.
	Router(config-if)# no dot1x timeout supp-timeout	Returns to the default retransmission time.
Step 3	Router# end	Returns to privileged EXEC mode.
Step 4	Router# show dot1x all	Verifies your entries.

1. *type* = ethernet, fastethernet, gigabitethernet, or tengigabitethernet

This example shows how to set the switch-to-client retransmission time for the EAP-request frame to 25 seconds:

```
Router(config-if)# dot1x timeout supp-timeout 25
```

Setting the Switch-to-Authentication-Server Retransmission Time for Layer 4 Packets

The authentication server notifies the switch each time it receives a Layer 4 packet. If the switch does not receive a notification after sending a packet, the switch waits a set period of time and then retransmits the packet. You may set the amount of time that the switch waits for notification from 1 to 65535 seconds. (The default is 30 seconds.)

To set the value for the retransmission of Layer 4 packets from the switch to the authentication server, perform this task:

	Command	Purpose
Step 1	Router(config)# interface type ¹ slot/port	Selects an interface to configure.
Step 2	Router(config-if)# dot1x timeout server-timeout seconds	Sets the switch-to-authentication-server retransmission time for Layer 4 packets.
	Router(config-if)# no dot1x timeout server-timeout	Returns to the default retransmission time.
Step 3	Router(config-if)# end	Returns to privileged EXEC mode.
Step 4	Router# show dot1x all	Verifies your entries.

1. *type* = ethernet, fastethernet, gigabitethernet, or tengigabitethernet

This example shows how to set the switch-to-authentication-server retransmission time for Layer 4 packets to 25 seconds:

```
Router(config-if)# dot1x timeout server-timeout 25
```

Setting the Switch-to-Client Frame Retransmission Number

In addition to changing the switch-to-client retransmission time, you can change the number of times that the switch sends an EAP-request/identity frame (assuming no response is received) to the client before restarting the authentication process.


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 set the switch-to-client frame retransmission number, perform this task:

Command	Purpose
Step 1 Router(config)# interface type ¹ slot/port	Selects an interface to configure.
Step 2 Router(config-if)# dot1x max-req count	Sets the number of times that the switch sends an EAP-request/identity frame to the client before restarting the authentication process. The range is 1 to 10; the default is 2.
Router(config-if)# no dot1x max-req	Returns to the default retransmission number.
Step 3 Router(config-if)# end	Returns to privileged EXEC mode.
Step 4 Router# show dot1x all	Verifies your entries.

1. type = ethernet, fastethernet, gigabitetherent, or tengigabitetherent

This example shows how to set 5 as the number of times that the switch sends an EAP-request/identity request before restarting the authentication process:

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

Enabling Multiple Hosts

You can attach multiple hosts to a single 802.1X-enabled port as shown in [Figure 27-3 on page 27-5](#). 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 (reauthentication 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 Router(config)# interface type¹ slot/port	Selects an interface to configure.
Step 2 Router(config-if)# dot1x multi-hosts	Allows multiple hosts (clients) on an 802.1X-authorized port. Make sure that the dot1x port-control interface configuration command is set to auto for the specified interface.
Router(config-if)# no dot1x multi-hosts	Disables multiple hosts on the port.
Step 3 Router(config-if)# end	Returns to privileged EXEC mode.
Step 4 Router# show dot1x interface type¹ slot/port	Verifies your entries.

1. *type = ethernet, fastethernet, gigabitethernet, or tengigabitethernet*

This example shows how to enable 802.1X on Fast Ethernet interface 5/1 and to allow multiple hosts:

```
Router(config)# interface fastethernet 5/1
Router(config-if)# dot1x port-control auto
Router(config-if)# dot1x multi-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 Router(config)# interface type¹ slot/port	Selects an interface to configure.
Step 2 Router(config-if)# dot1x default	Resets the configurable 802.1X parameters to the default values.
Step 3 Router(config-if)# end	Returns to privileged EXEC mode.
Step 4 Router# show dot1x all	Verifies your entries.

1. *type = ethernet, fastethernet, gigabitethernet, or tengigabitethernet*

Displaying 802.1X Status

To display global 802.1X administrative and operational status for the switch, use the **show dot1x** 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.

For detailed information about the fields in these displays, refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication.

■ Displaying 802.1X Status



Configuring Port Security

This chapter describes how to configure the port security feature.



Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication.

This chapter consists of these sections:

- [Understanding Port Security, page 28-1](#)
- [Default Port Security Configuration, page 28-2](#)
- [Port Security Guidelines and Restrictions, page 28-2](#)
- [Configuring Port Security, page 28-2](#)
- [Displaying Port Security Settings, page 28-5](#)

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. If a workstation with a secure MAC that is address configured or learned on one secure port attempts to access another secure port, a violation is flagged.

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, set the maximum number of addresses to one and configure the MAC address of the attached device.

A security violation occurs if the maximum number of secure MAC addresses have 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 three violation modes: protect, restrict, or shutdown (see the “Configuring Port Security” section on page 28-2.)

Default Port Security Configuration

Table 28-1 shows the default port security configuration for an interface.

Table 28-1 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.

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.

Configuring Port Security

These sections describe how to configure port security:

- [Configuring Port Security on an Interface, page 28-3](#)
- [Configuring Port Security Aging, page 28-4](#)

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 Router(config)# interface <i>interface_id</i>	Enters interface configuration mode and enters the physical interface to configure, for example gigabitethernet 3/1 .
Step 2 Router(config-if)# switchport mode access	Sets the interface mode as access; an interface in the default mode (dynamic desirable) cannot be configured as a secure port.
Step 3 Router(config-if)# switchport port-security	Enables port security on the interface.
Step 4 Router(config-if)# switchport port-security maximum <i>value</i>	(Optional) Sets the maximum number of secure MAC addresses for the interface. The range is 1 to 128; the default is 128.
Step 5 Router(config-if)# switchport port-security violation {protect restrict shutdown}	(Optional) Sets the violation mode and the action to be taken when a security violation is detected.
Step 6 Router(config-if)# switchport port-security mac-address <i>mac_address</i>	(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 7 Router(config-if)# end	Returns to privileged EXEC mode.
Step 8 Router# show port-security interface <i>interface_id</i> Router# show port-security address	Verifies your entries.

When configuring port security, note the following syntax information about port security violation modes:

- **protect**—Drops packets with unknown source addresses until you remove a sufficient number of secure MAC addresses to drop below the maximum value.
- **restrict**—Drops packets with unknown source addresses until you remove a sufficient number of secure MAC addresses to drop below the maximum value and causes the SecurityViolation counter to increment.
- **shutdown**—Puts the interface into the error-disabled state immediately and sends an SNMP trap notification.



Note

When port security is enabled, if an address learned or configured on one secure interface is seen on another secure interface in the same VLAN, port security puts the interface into the error-disabled state immediately.

To bring a secure port out of the error-disabled state, enter the **errdisable recovery cause psecureViolation** global configuration command or you can manually reenable it by entering the **shutdown** and **no shut down** interface configuration commands.

Configuring Port Security

To return the interface to the default condition (not a secure port), enter the **no switchport port-security** interface configuration command.

To return the interface to the default number of secure MAC addresses, enter the **no switchport port-security maximum value** command.

To delete a MAC address from the address table, enter the **no switchport port-security mac-address mac_address** command.

To return the violation mode to the default condition (shutdown mode), enter the **no switchport port-security violation {protocol | restrict}** command.

This example shows how to enable port security on Fast Ethernet port 12 and to set the maximum number of secure addresses to 5. The violation mode is the default, and no secure MAC addresses are configured.

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fastethernet 3/12
Router(config-if)# switchport mode access
Router(config-if)# switchport port-security
Router(config-if)# switchport port-security maximum 5
Router(config-if)# end
Router# show port-security interface fastethernet 3/12
Security Enabled:Yes, Port Status:SecureUp
Violation Mode:Shutdown
Max. Addrs:5, Current Addrs:0, Configure Addrs:0
```

This example shows how to configure a secure MAC address on Fast Ethernet port 12 and verify the configuration:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fastethernet 5/12
Router(config-if)# switchport mode access
Router(config-if)# switchport port-security
Router(config-if)# switchport port-security mac-address 1000.2000.3000
Router(config-if)# end
Router# show port-security address
      Secure Mac Address Table
-----
Vlan     Mac Address          Type            Ports
----  -----  -----  -----
1       1000.2000.3000        SecureConfigured   Fa5/12
```

Configuring Port Security Aging

You can use port security aging to set the aging time 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 Router(config)# interface interface_id	Enters interface configuration mode for the port on which you want to enable port security aging.
Step 2 Router(config-if)# switchport port-security aging time aging_time	Sets the aging time for the secure port. For <i>time</i> , specify the aging time for this port. The valid aging-time range is from 1 to 1440 minutes. All the secure addresses age out exactly after the time (minutes) specified lapses and are removed from the secure address list.
Router(config-if)# no switchport port-security aging time	Disables aging.
Step 3 Router(config-if)# end	Returns to privileged EXEC mode.
Step 4 Router# show port security [interface interface_id] [address]	Verifies your entries.

This example shows how to set the aging time as 2 hours for the secure addresses on the Fast Ethernet interface 5/1:

```
Router(config)# interface fastethernet 5/1
Router(config-if)# switchport port-security aging time 120
```

This example shows how to set the aging time as 2 minutes:

```
Router(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

The **show interfaces interface_id switchport** privileged EXEC command displays the interface traffic suppression and control configuration. The **show interfaces counters** privileged EXEC commands display the count of discarded packets. The **show storm control** and **show port-security** privileged EXEC commands display those features.

To display traffic control information, enter one or more of these commands:

Command	Purpose
Router# show port-security [interface interface_id]	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.
Router# show port-security [interface interface_id] address	Displays all secure MAC addresses configured on all switch interfaces or on a specified interface with aging information for each address.

■ Displaying Port Security Settings

This example displays output from the **show port-security** command when you do not enter an interface:

```
Router# show port-security
Secure Port      MaxSecureAddr  CurrentAddr  SecurityViolation  Security
Action          (Count)       (Count)       (Count)
-----
Fa5/1           11            11            0             Shutdown
Fa5/5           15            5             0             Restrict
Fa5/11          5             4             0             Protect
-----
Total Addresses in System: 21
Max Addresses limit in System: 128
```

This example displays output from the **show port-security** command for a specified interface:

```
Router# show port-security interface fastethernet 5/1
Port Security: Enabled
Port status: SecureUp
Violation mode: Shutdown
Maximum MAC Addresses: 11
Total MAC Addresses: 11
Configured MAC Addresses: 3
Aging time: 20 mins
Aging type: Inactivity
SecureStatic address aging: Enabled
Security Violation count: 0
```

This example displays output from the **show port-security address** privileged EXEC command:

```
Router# show port-security address
      Secure Mac Address Table
-----
Vlan   Mac Address      Type        Ports  Remaining Age
                                         (mins)
-----
1     0001.0001.0001    SecureDynamic Fa5/1    15 (I)
1     0001.0001.0002    SecureDynamic Fa5/1    15 (I)
1     0001.0001.1111    SecureConfigured Fa5/1    16 (I)
1     0001.0001.1112    SecureConfigured Fa5/1    -
1     0001.0001.1113    SecureConfigured Fa5/1    -
1     0005.0005.0001    SecureConfigured Fa5/5    23
1     0005.0005.0002    SecureConfigured Fa5/5    23
1     0005.0005.0003    SecureConfigured Fa5/5    23
1     0011.0011.0001    SecureConfigured Fa5/11   25 (I)
1     0011.0011.0002    SecureConfigured Fa5/11   25 (I)
-----
Total Addresses in System: 10
Max Addresses limit in System: 128
```



Configuring Traffic Storm Control

This chapter describes how to configure the traffic storm control feature on the Catalyst 6500 series switches.

**Note**

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication.

This chapter consists of these sections:

- [Understanding Traffic Storm Control, page 29-1](#)
- [Default Traffic Storm Control Configuration, page 29-2](#)
- [Enabling Traffic Storm Control, page 29-2](#)

Understanding Traffic Storm Control

A traffic storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. The traffic storm control feature prevents LAN ports from being disrupted by a broadcast, multicast, or unicast traffic storm on physical interfaces.

Traffic storm control (also called traffic suppression) monitors incoming traffic levels over a 1-second traffic storm control interval and, during the interval, compares the traffic level with the traffic storm control level that you configure. The traffic storm control level is a percentage of the total available bandwidth of the port. Each port has a single traffic storm control level that is used for all types of traffic (broadcast, multicast, and unicast).

**Note**

-
- The switch supports multicast and unicast traffic storm control only on Gigabit Ethernet LAN ports.
 - The switch supports broadcast traffic storm control on all LAN ports.
 - Traffic storm control does not suppress spanning tree packets. Except for spanning tree packets, traffic storm control does not differentiate between control traffic and data traffic.
-

Traffic storm control monitors the level of each traffic type for which you enable traffic storm control in 1-second traffic storm control intervals. Within an interval, when the ingress traffic for which traffic storm control is enabled reaches the traffic storm control level that is configured on the port, traffic storm control drops the traffic until the traffic storm control interval ends.

■ Default Traffic Storm Control Configuration

The following are examples of traffic storm control behavior:

- If you enable broadcast traffic storm control, and broadcast traffic exceeds the level within a 1-second traffic storm control interval, traffic storm control drops all broadcast traffic until the end of the traffic storm control interval.
- If you enable broadcast and multicast traffic storm control, and the combined broadcast and multicast traffic exceeds the level within a 1-second traffic storm control interval, traffic storm control drops all broadcast and multicast traffic until the end of the traffic storm control interval.
- If you enable broadcast and multicast traffic storm control, and broadcast traffic exceeds the level within a 1-second traffic storm control interval, traffic storm control drops all broadcast and multicast traffic until the end of the traffic storm control interval.
- If you enable broadcast and multicast traffic storm control, and multicast traffic exceeds the level within a 1-second traffic storm control interval, traffic storm control drops all broadcast and multicast traffic until the end of the traffic storm control interval.

Default Traffic Storm Control Configuration

Traffic storm control is disabled by default.

Enabling Traffic Storm Control

To enable traffic storm control, perform this task:

	Command	Purpose
Step 1	Router(config)# interface {{type ¹ slot/port} {port-channel number}}	Selects an interface to configure.
Step 2	Router(config-if)# storm-control broadcast level level[.level]	Enables broadcast traffic storm control on the interface, configures the traffic storm control level, and applies the traffic storm control level to all traffic storm control modes enabled on the interface.
	Router(config-if)# no storm-control broadcast level	Disables broadcast traffic storm control on the interface.
Step 3	Router(config-if)# storm-control multicast level level[.level]	Enables multicast traffic storm control on the interface, configures the traffic storm control level, and applies the traffic storm control level to all traffic storm control modes enabled on the interface.
	Note The storm-control multicast command is supported only on Gigabit Ethernet interfaces. Router(config-if)# no storm-control multicast level	
Step 4	Router(config-if)# storm-control unicast level level[.level]	Enables unicast traffic storm control on the interface, configures the traffic storm control level, and applies the traffic storm control level to all traffic storm control modes enabled on the interface.
	Note The storm-control unicast command is supported only on Gigabit Ethernet interfaces. Router(config-if)# no storm-control unicast level	

Command	Purpose
Step 5 Router(config-if)# end	Exits configuration mode.
Step 6 Router# show running-config interface	Verifies the configuration.

1. `type = ethernet, fastethernet, gigabitethernet, or tengigabitethernet`

When configuring the traffic storm control level, note the following:

- You can configure traffic storm control on an EtherChannel (a port channel interface).
- Do not configure traffic storm control on ports that are members of an EtherChannel. Configuring traffic storm control on ports that are configured as members of an EtherChannel puts the ports into a suspended state.
- Specify the level as a percentage of the total interface bandwidth:
 - The level can be from 0 to 100.
 - The optional fraction of a level can be from 0 to 99.
 - 100 percent means no traffic storm control.
 - 0.0 percent suppresses all traffic.

Because of hardware limitations and the method by which packets of different sizes are counted, the level percentage is an approximation. Depending on the sizes of the frames making up the incoming traffic, the actual enforced level might differ from the configured level by several percentage points.

This example shows how to enable multicast traffic storm control on Gigabit Ethernet interface 3/16 and how to configure the traffic storm control level at 70.5 percent. This configuration applies the traffic storm control level to all traffic storm control modes enabled on Gigabit Ethernet interface 3/16:

```
Router# configure terminal
Router(config)# interface gigabitethernet 3/16
Router(config-if)# storm-control multicast level 70.5
Router(config-if)# end
```

Displaying Traffic Storm Control Settings

To display traffic storm control information, use the commands described in Table 29-1.

Table 29-1 Commands for Displaying Traffic Storm Control Status and Configuration

Command	Purpose
Router# show interfaces [{type ¹ slot/port} {port-channel number}] switchport	Displays the administrative and operational status of all Layer 2 LAN ports or the specified Layer 2 LAN port.
Router# show interfaces [{type ¹ slot/port} {port-channel number}] counters broadcast Router# show interfaces [{type ¹ slot/port} {port-channel number}] counters multicast Router# show interfaces [{type ¹ slot/port} {port-channel number}] counters unicast	There is a single counter for all suppressed traffic. These commands all display the same discard count, which shows the total number of packets discarded for all three traffic storm control modes, on all interfaces or on the specified interface.

1. `type = ethernet, fastethernet, gigabitethernet, or tengigabitethernet`

■ Displaying Traffic Storm Control Settings**Note**

The **show interfaces [{interface_type slot/port} | {port-channel number}] counters** command does not display the discard count. You must use one of the traffic-type keywords: **broadcast**, **multicast**, or **unicast**, which all display the same discard count.



Configuring CDP

This chapter contains information about how to configure Cisco Discovery Protocol (CDP) on the Catalyst 6500 series switches, which supplements the information in these publications:

- The *Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.2, “System Management,” “Configuring Cisco Discovery Protocol (CDP)” at this URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/fcfprt3/fcf015.htm
- The *Cisco IOS Configuration Fundamentals Command Reference*, Release 12.2, “System Management Commands,” “CDP Commands” publication at this URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_r/ffrprt3/frf015.htm

This chapter consists of these sections:

- [Understanding How CDP Works, page 30-1](#)
- [Configuring CDP, page 30-1](#)

Understanding How CDP Works

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. This feature 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

These sections describe how to configure CDP:

- [Enabling CDP Globally, page 30-2](#)
- [Displaying the CDP Global Configuration, page 30-2](#)
- [Enabling CDP on a Port, page 30-2](#)

- Displaying the CDP Interface Configuration, page 30-3
- Monitoring and Maintaining CDP, page 30-3

Enabling CDP Globally

To enable CDP globally, perform this task:

Command	Purpose
Router(config)# cdp run	Enables CDP globally.
Router(config)# no cdp run	Disables CDP globally.

This example shows how to enable CDP globally:

```
Router(config)# cdp run
```

Displaying the CDP Global Configuration

To display the CDP configuration, perform this task:

Command	Purpose
Router# show cdp	Displays global CDP information.

This example shows how to display the CDP configuration:

```
Router# show cdp
Global CDP information:
    Sending CDP packets every 120 seconds
    Sending a holdtime value of 180 seconds
    Sending CDPv2 advertisements is enabled
Router#
```

For additional CDP show commands, see the “[Monitoring and Maintaining CDP](#)” section on page 30-3.

Enabling CDP on a Port

To enable CDP on a port, perform this task:

	Command	Purpose
Step 1	Router(config)# interface {type¹ slot/port} {port-channel number}	Selects the port to configure.
Step 2	Router(config-if)# cdp enable	Enables CDP on the port.
	Router(config-if)# no cdp enable	Disables CDP on the port.

1. type = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

This example shows how to enable CDP on Fast Ethernet port 5/1:

```
Router(config)# interface fastethernet 5/1
Router(config-if)# cdp enable
```

Displaying the CDP Interface Configuration

To display the CDP configuration for a port, perform this task:

Command	Purpose
Router# show cdp interface [{ {type ¹ slot/port} {port-channel number}}]	Displays information about ports where CDP is enabled.

1. type = ethernet, fastethernet, gigabitetherent, or tengigabitetherent

This example shows how to display the CDP configuration of Fast Ethernet port 5/1:

```
Router# 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
Router#
```

Monitoring and Maintaining CDP

To monitor and maintain CDP on your device, perform one or more of these tasks:

Command	Purpose
Router# clear cdp counters	Resets the traffic counters to zero.
Router# clear cdp table	Clears information about neighbors from the CDP table.
Router# show cdp	Displays global information such as frequency of transmissions and the holdtime for packets being transmitted.
Router# show cdp entry entry_name [protocol version]	Displays information about a specific neighbor. The display can be limited to protocol or version information.
Router# show cdp interface [type ¹ slot/port]	Displays information about interfaces on which CDP is enabled.
Router# show cdp neighbors [type ¹ slot/port] [detail]	Displays information about neighbors. The display can be limited to neighbors on a specific interface and expanded to provide more detailed information.
Router# show cdp traffic	Displays CDP counters, including the number of packets sent and received and checksum errors.
Router# show debugging	Displays information about the types of debugging that are enabled. Refer to the <i>Debug Command Reference</i> publication for more information about CDP debug commands.

1. type = ethernet, fastethernet, gigabitetherent, or tengigabitetherent

This example shows how to clear CDP counter configuration:

```
Router# clear cdp counters
```

This example shows how to display information about the neighboring equipment:

```
Router# 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	Holddtme	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



Configuring UDLD

This chapter describes how to configure the UniDirectional Link Detection (UDLD) protocol on the Catalyst 6500 series switches.



Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication.

This chapter consists of these sections:

- [Understanding How UDLD Works, page 31-1](#)
- [Default UDLD Configuration, page 31-3](#)
- [Configuring UDLD, page 31-3](#)

Understanding How UDLD Works

These sections describe how UDLD works:

- [UDLD Overview, page 31-1](#)
- [UDLD Aggressive Mode, page 31-2](#)

UDLD Overview

The UDLD protocol allows devices connected through fiber-optic or copper (for example, Category 5 cabling) Ethernet cables connected to LAN ports to monitor the physical configuration of the cables and detect when a unidirectional link exists. When a unidirectional link is detected, UDLD shuts down the affected LAN port 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 protocols 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 LAN ports. 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.

■ Understanding How UDLD Works

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. 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 at Layer 1, then UDLD at Layer 2 determines whether those fibers are connected correctly and whether traffic is flowing bidirectionally between the correct neighbors. This check cannot be performed by autonegotiation, because autonegotiation operates at Layer 1.

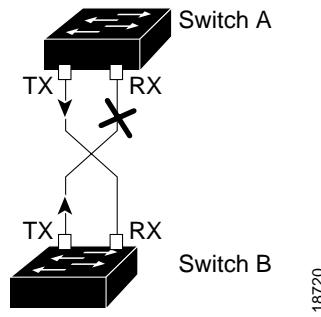
The Catalyst 6500 series switch periodically transmits UDLD packets to neighbor devices on LAN ports with UDLD enabled. If the packets are echoed back within a specific time frame and they are lacking a specific acknowledgment (echo), the link is flagged as unidirectional and the LAN port is shut down. 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 LAN ports to avoid sending unnecessary control traffic on this type of media since it is often used for access ports.

Figure 31-1 shows an example of a unidirectional link condition. Switch B successfully receives traffic from Switch A on the port. However, Switch A does not receive traffic from Switch B on the same port. UDLD detects the problem and disables the port.

Figure 31-1 Unidirectional Link



18720

UDLD Aggressive Mode

UDLD aggressive mode is disabled by default. Configure UDLD aggressive mode only on point-to-point links between network devices that support UDLD aggressive mode. With UDLD aggressive mode enabled, when a port on a bidirectional link that has a UDLD neighbor relationship established stops receiving UDLD packets, UDLD tries to reestablish the connection with the neighbor. After eight failed retries, the port is disabled.

To prevent spanning tree loops, nonaggressive UDLD with the default interval of 15 seconds is fast enough to shut down a unidirectional link before a blocking port transitions to the forwarding state (with default spanning tree parameters).

When you enable UDLD aggressive mode, you receive additional benefits in the following situations:

- One side of a link has a port stuck (both Tx and Rx)
- One side of a link remains up while the other side of the link has gone down

In these cases, UDLD aggressive mode disables one of the ports on the link, which prevents traffic from being discarded.

Default UDLD Configuration

Table 31-1 shows the default UDLD configuration.

Table 31-1 UDLD Default Configuration

Feature	Default Value
UDLD global enable state	Globally disabled
UDLD aggressive mode	Disabled
UDLD per-port enable state for fiber-optic media	Enabled on all Ethernet fiber-optic LAN ports
UDLD per-port enable state for twisted-pair (copper) media	Disabled on all Ethernet 10/100 and 1000BASE-TX LAN ports

Configuring UDLD

These sections describe how to configure UDLD:

- [Enabling UDLD Globally, page 31-3](#)
- [Enabling UDLD on Individual LAN Interfaces, page 31-4](#)
- [Disabling UDLD on Fiber-Optic LAN Interfaces, page 31-4](#)
- [Configuring the UDLD Probe Message Interval, page 31-5](#)
- [Resetting Disabled LAN Interfaces, page 31-5](#)

Enabling UDLD Globally

To enable UDLD globally on all fiber-optic LAN ports, perform this task:

Command	Purpose
Router(config)# udld {enable aggressive}	Enables UDLD globally on fiber-optic LAN ports. Note This command only configures fiber-optic LAN ports. Individual LAN port configuration overrides the setting of this command.
Router(config)# no udld {enable aggressive}	Disables UDLD globally on fiber-optic LAN ports.

Enabling UDLD on Individual LAN Interfaces

To enable UDLD on individual LAN ports, perform this task:

Command	Purpose
Step 1 Router(config)# interface type¹ slot/port	Selects the LAN port to configure.
Step 2 Router(config-if)# udld port [aggressive] Router(config-if)# no udld port [aggressive]	Enables UDLD on a specific LAN port. Enter the aggressive keyword to enable aggressive mode. On a fiber-optic LAN port, this command overrides the udld enable global configuration command setting. Disables UDLD on a nonfiber-optic LAN port. Note On fiber-optic LAN ports, the no udld port command reverts the LAN port configuration to the udld enable global configuration command setting.
Step 3 Router# show udld type¹ slot/number	Verifies the configuration.

1. *type* = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

Disabling UDLD on Fiber-Optic LAN Interfaces

To disable UDLD on individual fiber-optic LAN ports, perform this task:

Command	Purpose
Step 1 Router(config)# interface type¹ slot/port	Selects the LAN port to configure.
Step 2 Router(config-if)# udld port disable Router(config-if)# no udld port disable	Disables UDLD on a fiber-optic LAN port. Reverts to the udld enable global configuration command setting. Note This command is only supported on fiber-optic LAN ports.
Step 3 Router# show udld type¹ slot/number	Verifies the configuration.

1. *type* = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

Configuring the UDLD Probe Message Interval

To configure the time between UDLD probe messages on ports that are in advertisement mode and are currently determined to be bidirectional, perform this task:

Command	Purpose
Step 1 Router(config)# udld message time interval	Configures the time between UDLD probe messages on ports that are in advertisement mode and are currently determined to be bidirectional; valid values are from 7 to 90 seconds.
	Router(config)# no udld message
Step 2 Router# show udld type¹ slot/number	Verifies the configuration.

1. *type* = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

Resetting Disabled LAN Interfaces

To reset all LAN ports that have been shut down by UDLD, perform this task:

Command	Purpose
Router# udld reset	Resets all LAN ports that have been shut down by UDLD.

■ Configuring UDLD



Configuring NetFlow and NDE

This chapter describes how to configure NetFlow statistics collection and NetFlow Data Export (NDE) on the Catalyst 6500 series switches.



Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication and the Release 12.2 publications at this URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/index.htm>

This chapter consists of these sections:

- [Understanding How NetFlow and NDE Work, page 32-1](#)
- [Default NetFlow and NDE Configuration, page 32-8](#)
- [Configuring NetFlow and NDE, page 32-8](#)

Understanding How NetFlow and NDE Work

These sections describe how NetFlow and NDE work:

- [NetFlow and NDE Overview, page 32-2](#)
- [NetFlow and NDE on the MSFC3, page 32-2](#)
- [NetFlow and NDE on the PFC3, page 32-2](#)



Note

- NDE does not support bridged traffic or Internetwork Packet Exchange (IPX) traffic.
- NetFlow and NDE do not support IP multicast traffic. You can display NetFlow statistics for IP multicast traffic with the **show mls ip multicast** command.
- The NetFlow configuration does not affect Layer 3 switching in hardware done by the Policy Feature Card 3 (PFC3).
- If the NetFlow table has more than 64,000 entries, there is an increased probability that there will be insufficient room to store statistics.
- No statistics are available for flows that are switched when the NetFlow table is full.

NetFlow and NDE Overview

NetFlow collects statistics globally from traffic that flows through the switch and stores the statistics in the NetFlow table. Two NetFlow options reduce the volume of statistics collected:

- Sampled NetFlow, which reduces the number of statistics collected
- NetFlow aggregation, which merges collected statistics



Note NetFlow aggregation uses NDE version 8.

NDE makes routed-traffic statistics available for analysis by an external data collector. You can use NDE for all IP unicast traffic that is Layer 3-switched on the PFC3 and all IP unicast traffic that is routed in software on the Multilayer Switch Feature Card 3 (MSFC3). NDE exports global statistics.

NetFlow and NDE on the MSFC3

The NetFlow cache on the MSFC3 captures statistics for flows routed in software. The MSFC3 supports sampled NetFlow and NetFlow aggregation for traffic routed in software. For more information, refer to this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fswtch_c/swprt2/index.htm

The MSFC3 supports NetFlow ToS-based router aggregation, described at this URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s15/dtnfltos.htm>

NetFlow and NDE on the PFC3

The NetFlow cache on the PFC3 captures statistics for flows routed in hardware. The PFC3 supports sampled NetFlow and NetFlow aggregation for traffic routed in hardware. The PFC3 does not support NetFlow ToS-Based Router Aggregation.

These sections describe NetFlow and NDE on the PFC3 in more detail:

- [Flow Masks, page 32-3](#)
- [NDE Versions, page 32-3](#)
- [MLS Cache Entries, page 32-6](#)
- [Sampled NetFlow, page 32-7](#)
- [NetFlow Aggregation, page 32-7](#)

Flow Masks

The PFC3 uses one of these flow masks to create NetFlow entries:

- source-only—A less-specific flow mask. The PFC3 maintains one entry for each source IP address. All flows from a given source IP address use this entry.
- destination—A less-specific flow mask. The PFC3 maintains one entry for each destination IP address. All flows to a given destination IP address use this entry.
- destination-source—A more-specific flow mask. The PFC3 maintains one entry for each source and destination IP address pair. All flows between same source and destination IP addresses use this entry.
- destination-source-interface—A more-specific flow mask. Adds the source VLAN SNMP ifIndex to the information in the destination-source flow mask.
- full—A more-specific flow mask. The PFC3 creates and maintains a separate cache entry for each IP flow. A full entry includes the source IP address, destination IP address, protocol, and protocol interfaces.
- full-interface—The most-specific flow mask. Adds the source VLAN SNMP ifIndex to the information in the full-flow mask.

NetFlow uses only one flow mask for all statistics.

NDE Versions

NDE on the PFC3 supports NDE versions 5 and 7 for the statistics captured on the PFC3. NetFlow aggregation uses version 8.

Some fields in the flow records might not have values, depending on the current flow mask. Unsupported fields contain a zero (0).

The following tables describe the supported NDE fields:

- [Table 32-1](#)—Version 5 header format
- [Table 32-2](#)—Version 5 flow record format
- [Table 32-3](#)—Version 7 header format
- [Table 32-4](#)—Version 7 flow record format

Table 32-1 NDE Version 5 Header Format

Bytes	Content	Description
0–1	version	NetFlow export format version number
2–3	count	Number of flows exported in this packet (1–30)
4–7	SysUptime	Current time in milliseconds since router booted
8–11	unix_secs	Current seconds since 0000 UTC 1970
12–15	unix_nsecs	Residual nanoseconds since 0000 UTC 1970
16–19	flow_sequence	Sequence counter of total flows seen
20–21	engine_type	Type of flow switching engine
21–23	engine_id	Slot number of the flow switching engine

Table 32-2 NDE Version 5 Flow Record Format

Bytes	Content	Description	Flow masks: • X=Populated • A=Additional field (see the “Populating Additional NDE Fields” section on page 32-14)					
			Source	Destination	Destination Source	Destination Source Interface	Full	Full Interface
0–3	srcaddr	Source IP address	X		X	X	X	X
4–7	dstaddr	Destination IP address		X	X	X	X	X
8–11	nexthop	Next hop router’s IP address		A ¹	A	A	A	A
12–13	input	Ingress interface SNMP ifIndex				X		X
14–15	output	Egress interface SNMP ifIndex		A ¹	A	A	A	A
16–19	dPkts	Packets in the flow	X	X	X	X	X	X
20–23	dOctets	Octets (bytes) in the flow	X	X	X	X	X	X
24–27	first	SysUptime at start of the flow	X	X	X	X	X	X
28–31	last	SysUptime at the time the last packet of the flow was received	X	X	X	X	X	X
32–33	srcport	Layer 4 source port number or equivalent					X	X
34–35	dstport	Layer 4 destination port number or equivalent					X	X
36	pad1	Unused (zero) byte						
37	tcp_flags	Cumulative OR of TCP flags						
38	prot	Layer 4 protocol (for example, 6=TCP, 17=UDP)					X	X
39	tos	IP type-of-service byte						
40–41	src_as	Autonomous system number of the source, either origin or peer	X		X	X	X	X
42–43	dst_as	Autonomous system number of the destination, either origin or peer		X	X	X	X	X
44–45	src_mask	Source address prefix mask bits	X		X	X	X	X
46–47	dst_mask	Destination address prefix mask bits		X	X	X	X	X
48	pad2	Pad 2 is unused (zero) bytes						

1. With the destination flow mask, the “Next hop router’s IP address” field and the “Output interface’s SNMP ifIndex” field might not contain information that is accurate for all flows.

Table 32-3 NDE Version 7 Header Format

Bytes	Content	Description
0–1	version	NetFlow export format version number
2–3	count	Number of flows exported in this packet (1–30)
4–7	SysUptime	Current time in milliseconds since router booted
8–11	unix_secs	Current seconds since 0000 UTC 1970
12–15	unix_nsecs	Residual nanoseconds since 0000 UTC 1970
16–19	flow_sequence	Sequence counter of total flows seen
20–24	reserved	Unused (zero) bytes

Table 32-4 NDE Version 7 Flow Record Format

Bytes	Content	Description	Flow masks: • X=Populated • A=Additional field (see the “Populating Additional NDE Fields” section on page 32-14)					
			Source	Destination	Destination Source	Destination Source Interface	Full	Full Interface
0–3	srcaddr	Source IP address	X		X	X	X	X
4–7	dstaddr	Destination IP address		X	X	X	X	X
8–11	nexthop	Next hop router’s IP address		A ¹	A	A	A	A
12–13	input	Ingress interface SNMP ifIndex				X		X
14–15	output	Egress interface SNMP ifIndex		A ¹	A	A	A	A
16–19	dPkts	Packets in the flow	X	X	X	X	X	X
20–23	dOctets	Octets (bytes) in the flow	X	X	X	X	X	X
24–27	First	SysUptime at start of the flow	X	X	X	X	X	X
28–31	Last	SysUptime at the time the last packet of the flow was received	X	X	X	X	X	X
32–33	srcport	Layer 4 source port number or equivalent					X	X
34–35	dstport	Layer 4 destination port number or equivalent					X	X
36	flags	Flow mask in use	X	X	X	X	X	X
37	tcp_flags	Cumulative OR of TCP flags						
38	prot	Layer 4 protocol (for example, 6=TCP, 17=UDP)					X	X
39	tos	IP type-of-service byte						
40–41	src_as	Autonomous system number of the source, either origin or peer	X		X	X	X	X

Table 32-4 NDE Version 7 Flow Record Format (continued)

Bytes	Content	Description	Flow masks: • X=Populated • A=Additional field (see the “Populating Additional NDE Fields” section on page 32-14)					
			Source	Destination	Destination Source	Destination Source Interface	Full	Full Interface
42–43	dst_as	Autonomous system number of the destination, either origin or peer		X	X	X	X	X
44–45	src_mask	Source address prefix mask bits	X		X	X	X	X
46–47	dst_mask	Destination address prefix mask bits		X	X	X	X	X
48	pad2	Pad 2 is unused (zero) bytes						
49–50	MLS RP	IP address of MLS router		X	X	X	X	X

- With the destination flow mask, the “Next hop router’s IP address” field and the “Output interface’s SNMP ifIndex” field might not contain information that is accurate for all flows.

MLS Cache Entries

NetFlow captures statistics for Layer 3-switched flows in the NetFlow cache on the PFC3.

NetFlow maintains traffic statistics for each active flow in the NetFlow cache and increments the statistics when packets within each flow are switched. Periodically, NDE exports summarized traffic statistics for all expired flows, which the external data collector receives and processes.

Exported NetFlow data contains statistics for the flow entries in the NetFlow cache that have expired since the last export. Flow entries in the NetFlow cache expire and are flushed from the NetFlow cache when one of the following conditions occurs:

- The entry ages out.
- The entry is cleared by the user.
- An interface goes down.
- Route flaps occur.

To ensure periodic reporting of continuously active flows, entries for continuously active flows expire at the end of the interval configured with the **mls aging long** command (default 32 minutes).

NDE packets go to the external data collector either when the number of recently expired flows reaches a predetermined maximum or after 30 seconds.

By default, all expired flows are exported unless they are filtered. If you configure a filter, NDE only exports expired and purged flows that match the filter criteria. NDE flow filters are stored in NVRAM and are not cleared when NDE is disabled. See the “Configuring NDE Flow Filters” section on page 32-17 for NDE filter configuration procedures.

Sampled NetFlow

The Sampled NetFlow feature captures data for a subset of the Layer 3-switched IP packets instead of for all packets in a flow. Sampled NetFlow substantially decreases the Supervisor Engine 720 CPU utilization.

With the Supervisor Engine 720, sampled NetFlow uses the full-interface flow mask, and you can enable or disable sampled NetFlow on each LAN port.

You can configure sampled NetFlow to use time-based sampling or packet-based sampling.

[Table 32-5](#) lists the time-based sampling rates and export intervals.

Table 32-5 Time-Based Sampling Rates, Sampling Times, and Export Intervals

Sampling Rate	Sampling Time (Milliseconds)	Export Interval (Milliseconds)
1 in 64	64	4096
1 in 128	32	4096
1 in 256	16	4096
1 in 512	8	4096
1 in 1024	4	4096
1 in 2048	4	8192
1 in 4096	4	16384
1 in 8192	4	32768

If you configure 64 as the rate, the sampled NetFlow feature uses traffic from the first 64 milliseconds of a flow every 4096 milliseconds. If the rate is 2048, the sampled NetFlow feature uses traffic from the first 4 milliseconds of a flow every 8192 milliseconds. With time-based sampled NetFlow, the export interval is not configurable.

Packet-based sampled NetFlow uses this formula to sample a flow: the number of times sampled is approximately the length divided by the rate (*packets_in_flow/sampling_rate*). For example, if the flow is 32,768 packets long and the sampling rate is 1024, the flow is sampled approximately 32 times (32,768/1,024). With packet-based sampled NetFlow, the export interval is configurable.

NetFlow Aggregation

For complete information about NetFlow aggregation as supported on the PFC3 and DFC3s, refer to this publication:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fswtch_c/swprt2/xcfnfov.htm#1001212

Default NetFlow and NDE Configuration

[Table 32-6](#) shows the default NetFlow and NDE configuration.

Table 32-6 Default NetFlow and NDE Configuration

Feature	Default Value
NDE	Disabled
NDE source addresses	None
NDE data collector address and UDP port	None
NDE filters	None
Sampled NetFlow	Disabled
NetFlow Aggregation	Disabled
Populating additional NDE fields	Enabled

Configuring NetFlow and NDE

These sections describe how to configure NetFlow and NDE:

- [Configuring NetFlow and NDE on the PFC3, page 32-8](#)
- [Configuring NetFlow and NDE on the MSFC3, page 32-14](#)
- [Displaying the NDE Address and Port Configuration, page 32-16](#)
- [Configuring NDE Flow Filters, page 32-17](#)
- [Displaying the NDE Configuration, page 32-19](#)



Note

- You must enable NetFlow on the MSFC3 Layer 3 interfaces to support NDE on the PFC3 and NDE on the MSFC3.
- You must enable NDE on the MSFC3 to support NDE on the PFC3.
- When you configure NAT and NDE on an interface, the PFC3 sends all traffic in fragmented packets to the MSFC3 to be processed in software. (CSCdz51590)

Configuring NetFlow and NDE on the PFC3

These sections describe how to configure NetFlow and NDE on the PFC3:

- [Configuring NetFlow on the PFC3, page 32-9](#)
- [Configuring NDE on the PFC3, page 32-13](#)

Configuring NetFlow on the PFC3

These sections describe how to configure NetFlow statistics collection on the PFC3:

- [Enabling NetFlow on the PFC3, page 32-9](#)
- [Configuring Sampled NetFlow, page 32-9](#)
- [Configuring NetFlow Aggregation on the PFC3, page 32-10](#)
- [Setting the Minimum IP MLS Flow Mask, page 32-11](#)
- [Configuring the MLS Aging Time, page 32-11](#)

Enabling NetFlow on the PFC3

To enable NetFlow statistics collection on the PFC3, perform this task:

Command	Purpose
Router(config)# mls netflow	Enables NetFlow on the PFC3.
Router(config)# no mls netflow	Disables NetFlow on the PFC3.

This example shows how to enable NetFlow statistics collection:

```
Router(config)# mls netflow
```

Configuring Sampled NetFlow

These sections describe how to configure sampled NetFlow on the PFC3:

- [Configuring Sampled NetFlow Globally, page 32-9](#)
- [Configuring Sampled NetFlow on a Layer 3 Interface, page 32-10](#)



Note NDE on the MSFC3 does not support sampled NetFlow.

Configuring Sampled NetFlow Globally

To configure sampled NetFlow globally, perform this task:

Command	Purpose
Step 1 Router(config)# mls sampling {time-based rate packet-based rate [interval]}	Enables sampled NetFlow and configures the rate. For packet-based sampling, optionally configures the export interval.
Router(config)# no mls sampling	Clears the sampled NetFlow configuration.
Step 2 Router(config)# end	Exits configuration mode.

When you configure sampled NetFlow globally, note the following syntax information:

- The valid values for *rate* are 64, 128, 256, 512, 1024, 2048, 4096, and 8192.
- The valid values for the packet-based export *interval* are from 4000 through 16,000.

See the “[Sampled NetFlow](#)” section on page 32-7 for more information.

Configuring Sampled NetFlow on a Layer 3 Interface


Note

- With the full-interface or destination-source-interface flow masks, you can enable or disable sampled NetFlow on individual Layer 3 interfaces. With all other flow masks, sampled NetFlow is enabled or disabled globally.
- The Layer 3 interface must be configured with an IP address.

To configure sampled NetFlow on a Layer 3 interface, perform this task:

	Command	Purpose
Step 1	Router(config)# interface {vian vlan_ID type¹ slot/port}	Selects a Layer 3 interface to configure.
Step 2	Router(config-if)# mls netflow sampling	Enables sampled NetFlow on the Layer 3 interface.
	Router(config-if)# no mls netflow sampling	Disables sampled NetFlow on the Layer 3 interface.
Step 3	Router(config)# end	Exits configuration mode.

- type = ethernet, fastethernet, gigabitethernet, or tengigabitethernet*

This example shows how to enable sampled NetFlow on Fast Ethernet port 5/12:

```
Router# configure terminal
Router(config)# interface fastethernet 5/12
Router(config-if)# mls netflow sampling
Router(config)# end
Router#
```

Configuring NetFlow Aggregation on the PFC3

NetFlow aggregation is configured automatically on the PFC3 and DFC3s when you configure NetFlow aggregation on the MSFC3 (see the “[Configuring NetFlow Aggregation on the MSFC3](#)” section on page 32-14).

To display NetFlow aggregation cache information for the PFC3 or DFC3s, perform this task:

	Command	Purpose
	Router # show ip cache flow aggregation {as destination-prefix prefix protocol-port source-prefix} module slot_num	Displays the NetFlow aggregation cache information.
	Router # show mls netflow aggregation flowmask	Displays the NetFlow aggregation flow mask information.


Note

The PFC3 and DFC3s do not support NetFlow ToS-based router aggregation.

This example shows how to display the NetFlow aggregation cache information:

```
Router# show ip cache flow aggregation destination-prefix module 1
IPFLOW_DST_PREFIX_AGGREGATION records and statistics for module :1
IP Flow Switching Cache, 278544 bytes
2 active, 4094 inactive, 6 added
236 ager polls, 0 flow alloc failures
```

```

Active flows timeout in 30 minutes
Inactive flows timeout in 15 seconds
Dst If Dst Prefix Msk AS Flows Pkts B/Pk Active
Gi7/9 9.1.0.0 /16 0 3003 12M 64 1699.8
Gi7/10 11.1.0.0 /16 0 3000 9873K 64 1699.8
Router#

```

This example shows how to display the NetFlow aggregation flow mask information:

```

Router# show mls netflow aggregation flowmask
Current flowmask set for netflow aggregation : Vlan Full Flow
Netflow aggregations configured/enabled :
    AS Aggregation
    PROTOCOL-PORT Aggregation
    SOURCE-PREFIX Aggregation
    DESTINATION-PREFIX Aggregation
Router#

```

Setting the Minimum IP MLS Flow Mask

You can set the minimum specificity of the flow mask for the NetFlow cache on the PFC3 (see the “[Flow Masks](#)” section on page 32-3). The actual flow mask that is used will have at least the specificity configured by the **mls flow ip** command.

To set the minimum IP MLS flow mask, perform this task:

Command	Purpose
Router(config)# mls flow ip {source destination destination-source interface-destination-source full interface-full}	Sets the minimum IP MLS flow mask for the protocol.
Router(config)# no mls flow ip	Reverts to the default IP MLS flow mask (null).

This example shows how to set the minimum IP MLS flow mask:

```
Router(config)# mls flow ip destination
```

To display the IP MLS flow mask configuration, perform this task:

Command	Purpose
Router# show mls netflow flowmask	Displays the flow mask configuration.

This example shows how to display the MLS flow mask configuration:

```

Router# show mls netflow flowmask
current ip flowmask for unicast: destination address
Router#

```

Configuring the MLS Aging Time

The MLS aging time (default 300 seconds) applies to all NetFlow cache entries. You can configure the normal aging time in the range of 32 to 4092 seconds. Flows can age as much as 4 seconds sooner or later than the configured interval. On average, flows age within 2 seconds of the configured value.

Other events might cause MLS entries to be purged, such as routing changes or a change in link state.



- Note** If the number of MLS entries exceeds 64,000, only adjacency statistics might be available for some flows.

To keep the NetFlow cache size below 64,000 entries, enable the following parameters when using the **mls aging** command:

- **normal**—Configures the wait before aging out and deleting shortcut entries in the Layer 3 table.
- **fast aging**—Configures an efficient process to age out entries created for flows that only switch a few packets, and then are never used again. The **fast aging** parameter uses the **time** keyword value to check if at least the **threshold** keyword value of packets have been switched for each flow. If a flow has not switched the threshold number of packets during the time interval, then the entry in the Layer 3 table is aged out.
- **long**—Configures entries for deletion that have been up for the specified value even if the Layer 3 entry is in use. Long aging is used to prevent counter wraparound, which can cause inaccurate statistics.

A typical cache entry that is removed is the entry for flows to and from a Domain Name Server (DNS) or TFTP server. This entry might not be used again after it is created. The PFC3 saves space in the NetFlow cache for other data when it detects and ages out these entries.

If you need to enable MLS fast aging time, initially set the value to 128 seconds. If the size of the NetFlow cache continues to grow over 64K entries, decrease the setting until the cache size stays below 64,000. If the cache continues to grow over 64,000 entries, decrease the normal MLS aging time.

To configure the MLS aging time, perform this task:

Command	Purpose
Router(config)# mls aging {fast [threshold {1-128} time {1-128}] long 64-1920 normal 32-4092}	Configures the MLS aging time for a NetFlow cache entry.
Router(config)# no mls aging fast	Disables fast aging.
Router(config)# no mls aging {long normal}	Reverts to the default MLS aging time.

This example displays how to configure the MLS aging time:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# mls aging fast threshold 64 time 30
```

To display the MLS aging-time configuration, perform this task:

Command	Purpose
Router# show mls netflow aging	Displays the MLS aging-time configuration.

This example shows how to display the MLS aging-time configuration:

```
Router# show mls netflow aging
enable timeout packet threshold
-----
normal aging true 300 N/A
fast aging true 32 100
long aging true 900 N/A
Router#
```

Configuring NDE on the PFC3

- Enabling NDE From the PFC3, page 32-13
- Enabling NDE for Ingress Traffic on a Layer 3 Interface, page 32-13
- Populating Additional NDE Fields, page 32-14

Enabling NDE From the PFC3

To enable NDE from the PFC3, perform this task:

Command	Purpose
Router(config)# mls nde sender [version {5 7}]	Enables NDE from the PFC3 and (optionally) configures the NDE version.
Router(config)# no mls nde sender	Disables NDE from the PFC3.
Router(config)# no mls nde sender version	Reverts to the default (version 7).


Note

NDE from the PFC3 uses the source interface configured for the MSFC3 (see the “Configuring the MSFC3 NDE Source Layer 3 Interface” section on page 32-15).

This example shows how to enable NDE from the PFC3:

```
Router(config)# mls nde sender
```

This example shows how to enable NDE from the PFC3 and configure NDE version 5:

```
Router(config)# mls nde sender version 5
```

Enabling NDE for Ingress Traffic on a Layer 3 Interface

To enable NDE for ingress traffic on a Layer 3 interface, perform this task:

Command	Purpose
Step 1 Router(config)# interface {vian <i>vlan_ID</i> type ¹ <i>slot/port</i> }	Selects a Layer 3 interface to configure.
Step 2 Router(config-if)# ip flow-export ingress	Enables NDE for ingress traffic on the Layer 3 interface.
Router(config-if)# no ip flow-export ingress	
Step 3 Router(config-if)# end	Exits configuration mode.

1. *type* = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

This example shows how to enable NDE for ingress traffic on Fast Ethernet interface 5/24:

```
Router(config)# interface fastethernet 5/24
Router(config-if)# ip flow-export ingress
```

Populating Additional NDE Fields

You can configure NDE to populate the following additional fields in the NDE packets:

- IP address of the next hop router
- Egress interface SNMP ifIndex

Not all of the additional fields are populated with all flow masks. See the “[NDE Versions](#)” section on [page 32-3](#) for additional information.

To populate the additional fields in NDE packets, perform this task:

Command	Purpose
Router(config)# mls nde interface	Populates additional fields in NDE packets.
Router(config)# no mls nde interface	Disables population of the additional fields.

This example shows how to populate the additional fields in NDE packets:

```
Router(config)# mls nde interface
```

Configuring NetFlow and NDE on the MSFC3

This section supplements the NetFlow procedures at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cger/switch_r/index.htm

These sections describe how to configure NDE on the MSFC3:

- [Enabling NetFlow on the MSFC3, page 32-14](#)
- [Configuring NetFlow Aggregation on the MSFC3, page 32-14](#)
- [Configuring the MSFC3 NDE Source Layer 3 Interface, page 32-15](#)
- [Configuring the NDE Destination, page 32-15](#)

Enabling NetFlow on the MSFC3

To enable NetFlow on the MSFC3, perform this task for each Layer 3 interface from which you want NDE:

Step	Command	Purpose
Step 1	Router(config)# interface {vian <i>vlan_ID</i> } {type ¹ <i>slot/port</i> } {port-channel <i>port_channel_number</i> }	Selects an interface to configure.
Step 2	Router(config-if)# ip route-cache flow	Enables NetFlow.

1. type = ethernet, fastethernet, gigabitetherent, tengigabitetherent, or ge-wan

Configuring NetFlow Aggregation on the MSFC3

To configure NetFlow aggregation on the MSFC3, use the procedures at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cger/fswtch_c/swprt2/xcfnfc.htm#1001058

To configure NetFlow ToS-based router aggregation on the MSFC3, use the procedures at this URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s15/dtnfltos.htm>


Note

- When you configure NetFlow aggregation on the MSFC3, it is configured automatically on the PFC3 and DFC3s (see the “Configuring NetFlow Aggregation on the PFC3” section on page 32-10).
- The PFC3 and DFC3s do not support NetFlow ToS-based router aggregation.

Configuring the MSFC3 NDE Source Layer 3 Interface

To configure the Layer 3 interface used as the source of the NDE packets containing statistics from the MSFC3, perform this task:

Command	Purpose
<pre>Router(config)# ip flow-export source {{vlan vlan_ID} {type¹ slot/port} {port-channel number} {loopback number}}</pre>	Configures the interface used as the source of the NDE packets containing statistics from the MSFC3. Note the following configuration guidelines: <ul style="list-style-type: none"> • You must select an interface configured with an IP address. • You can use a loopback interface.
<pre>Router(config)# no ip flow-export source</pre>	Clears the NDE source interface configuration.

1. type = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

This example shows how to configure a loopback interface as the NDE flow source:

```
Router(config)# ip flow-export source loopback 0
Router(config)#

```

Configuring the NDE Destination

To configure the destination IP address and UDP port to receive the NDE statistics, perform this task:

Command	Purpose
<pre>Router(config)# ip flow-export destination ip_address udp_port_number</pre>	Configures the NDE destination IP address and UDP port.
<pre>Router(config)# no ip flow-export destination</pre>	Clears the NDE destination configuration.

This example shows how to configure the NDE flow destination IP address and UDP port:

```
Router(config)# ip flow-export destination 172.20.52.37 200
```

**Note**

The destination address and UDP port number are saved in NVRAM and are preserved if NDE is disabled and reenabled or if the switch is power cycled. If you are using the NetFlow FlowCollector application for data collection, verify that the UDP port number you configure is the same port number shown in the FlowCollector's nfconfig.file. This file is located at /opt/csconfc/config/nfconfig.file in the FlowCollector application.

Displaying the NDE Address and Port Configuration

To display the NDE address and port configuration, perform these tasks:

Command	Purpose
Router# show mls nde	Displays the NDE export flow IP address and UDP port configuration.
Router# show ip flow export	Displays the NDE export flow IP address, UDP port, and the NDE source interface configuration.

This example shows how to display the NDE export flow source IP address and UDP port configuration:

```
Router# show mls nde
Netflow Data Export enabled
  Exporting flows to 10.34.12.245 (9999)
  Exporting flows from 10.6.58.7 (55425)
  Version: 7
  Include Filter not configured
  Exclude Filter is:
    source: ip address 11.1.1.0, mask 255.255.255.0
  Total Netflow Data Export Packets are:
    49 packets, 0 no packets, 247 records
  Total Netflow Data Export Send Errors:
    IPWRITE_NO_FIB = 0
    IPWRITE_ADJ_FAILED = 0
    IPWRITE_PROCESS = 0
    IPWRITE_ENQUEUE_FAILED = 0
    IPWRITE_IPC_FAILED = 0
    IPWRITE_OUTPUT_FAILED = 0
    IPWRITE_MTU_FAILED = 0
    IPWRITE_ENCAPFIX_FAILED = 0
  Netflow Aggregation Enabled
    source-prefix aggregation export is disabled
    destination-prefix aggregation exporting flows to 10.34.12.245 (9999)
    10.34.12.246 (9909)
      exported 84 packets, 94 records
      prefix aggregation export is disabled
Router#
```

This example shows how to display the NDE export flow IP address, UDP port, and the NDE source interface configuration:

```
Router# show ip flow export
Flow export is enabled
  Exporting flows to 172.20.52.37 (200)
  Exporting using source interface FastEthernet5/8
  Version 1 flow records
    0 flows exported in 0 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
Router#
```

Configuring NDE Flow Filters

These sections describe NDE flow filters:

- [NDE Flow Filter Overview, page 32-17](#)
- [Configuring a Port Flow Filter, page 32-17](#)
- [Configuring a Host and Port Filter, page 32-18](#)
- [Configuring a Host Flow Filter, page 32-18](#)
- [Configuring a Protocol Flow Filter, page 32-18](#)

NDE Flow Filter Overview

By default, all expired flows are exported until you configure a filter. After you configure a filter, only expired and purged flows matching the specified filter criteria are exported. Filter values are stored in NVRAM and are not cleared when NDE is disabled.

To display the configuration of the NDE flow filters you configure, use the **show mls nde** command described in the “[Displaying the NDE Configuration](#)” section on page 32-19.

Configuring a Port Flow Filter

To configure a destination or source port flow filter, perform this task:

Command	Purpose
Router(config)# mls nde flow {exclude include} {dest-port number src-port number}	Configures a port flow filter for an NDE flow.
Router(config)# no mls nde flow {exclude include}	Clears the port flow filter configuration.

This example shows how to configure a port flow filter so that only expired flows to destination port 23 are exported (assuming the flow mask is set to full):

```
Router(config)# mls nde flow include dest-port 35
Router(config) #
```

Configuring a Host and Port Filter

To configure a host and TCP/UDP port flow filter, perform this task:

Command	Purpose
Router(config)# mls nde flow {exclude include} {destination ip_address mask source ip_address mask {dest-port number src-port number}}	Configures a host and port flow filter for an NDE flow.
Router(config)# no mls nde flow {exclude include}	Clears the port flow filter configuration.

This example shows how to configure a source host and destination TCP/UDP port flow filter so that only expired flows from host 171.69.194.140 to destination port 23 are exported (assuming the flow mask is set to ip-flow):

```
Router(config)# mls nde flow exclude destination 2.2.2.2 255.255.255.0 dest-port 23
```

Configuring a Host Flow Filter

To configure a destination or source host flow filter, perform this task:

Command	Purpose
Router(config)# mls nde flow {exclude include} {destination ip_address mask source ip_address mask protocol {tcp {dest-port number src-port number} udp {dest-port number src-port number}}}	Configures a host flow filter for an NDE flow.
Router(config)# no mls nde flow {exclude include}	Clears port filter configuration.

This example shows how to configure a host flow filter to include and export only destinations to host 172.20.52.37:

```
Router(config)# mls nde flow include destination 172.20.52.37 255.255.255.224
Router(config)#

```

Configuring a Protocol Flow Filter

To configure a protocol flow filter, perform this task:

Command	Purpose
Router(config)# mls nde flow {exclude include} protocol {tcp {dest-port number src-port number} udp {dest-port number src-port number}}	Configures a protocol flow filter for an NDE flow.
Router(config)# no mls nde flow {exclude include}	Clears port filter configuration.

This example shows how to configure a TCP protocol flow filter so that only expired flows from destination port 35 are exported:

```
Router(config)# mls nde flow include protocol tcp dest-port 35
Router(config)#

```

To display the status of the NDE flow filters, use the **show mls nde** command described in the “[Displaying the NDE Configuration](#)” section on page 32-19.

Displaying the NDE Configuration

To display the NDE configuration, perform this task:

Command	Purpose
Router# show mls nde	Displays the NDE configuration.

This example shows how to display the NDE configuration:

```
Router# show mls nde
Netflow Data Export enabled
Exporting flows to 10.34.12.245 (9988) 10.34.12.245 (9999)
Exporting flows from 10.6.58.7 (57673)
Version: 7
Include Filter not configured
Exclude Filter not configured
Total Netflow Data Export Packets are:
    508 packets, 0 no packets, 3985 records
Total Netflow Data Export Send Errors:
    IPWRITE_NO_FIB = 0
    IPWRITE_ADJ_FAILED = 0
    IPWRITE_PROCESS = 0
    IPWRITE_ENQUEUE_FAILED = 0
    IPWRITE_IPC_FAILED = 0
    IPWRITE_OUTPUT_FAILED = 0
    IPWRITE_MTU_FAILED = 0
    IPWRITE_ENCAPFIX_FAILED = 0
Netflow Aggregation Enabled
Router#
```




Configuring Local SPAN and RSPAN

This chapter describes how to configure local Switched Port Analyzer (SPAN) and remote SPAN (RSPAN) on the Catalyst 6500 series switches.

This chapter consists of these sections:

- [Understanding How Local SPAN and RSPAN Work, page 33-1](#)
- [Local SPAN and RSPAN Configuration Guidelines and Restrictions, page 33-5](#)
- [Configuring Local SPAN and RSPAN, page 33-8](#)



Note For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication.

Understanding How Local SPAN and RSPAN Work

These sections describe how local SPAN and RSPAN work:

- [Local SPAN and RSPAN Overview, page 33-1](#)
- [Local SPAN and RSPAN Sessions, page 33-3](#)
- [Monitored Traffic, page 33-4](#)
- [SPAN Sources, page 33-4](#)
- [Destination Ports, page 33-5](#)

Local SPAN and RSPAN Overview

Local SPAN and RSPAN both select network traffic to send to a network analyzer such as a SwitchProbe device or other Remote Monitoring (RMON) probe. SPAN does not affect the switching of network traffic on source ports or VLANs. SPAN sends a copy of the packets received or transmitted by the source ports and VLANs to the destination port. You must dedicate the destination port for SPAN use.

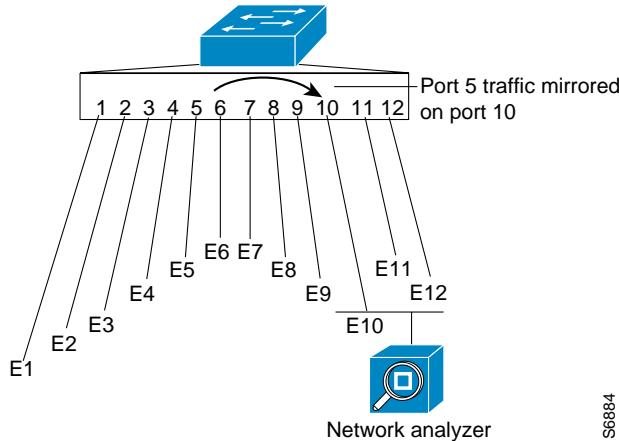
These sections provide an overview of local SPAN and RSPAN:

- [Local SPAN Overview, page 33-2](#)
- [RSPAN Overview, page 33-3](#)

Local SPAN Overview

Local SPAN supports source ports, source VLANs, and destination ports on the same Catalyst 6500 series switch. Local SPAN copies traffic from one or more source ports in any VLAN or from one or more VLANs to a destination port for analysis (see [Figure 33-1](#)). For example, as shown in [Figure 33-1](#), all traffic on Ethernet port 5 (the source port) is copied to Ethernet port 10. A network analyzer on Ethernet port 10 receives all network traffic from Ethernet port 5 without being physically attached to Ethernet port 5.

Figure 33-1 Example SPAN Configuration



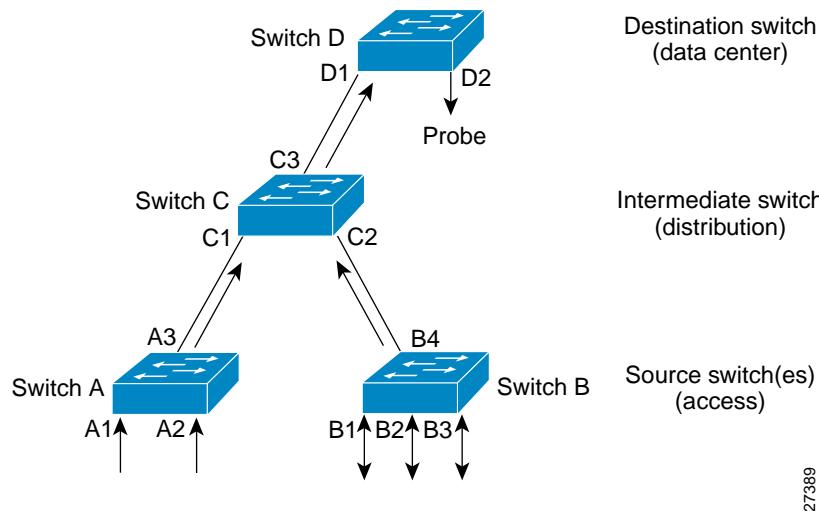
RSPAN Overview

RSPAN supports source ports, source VLANs, and destination ports on different switches, which provides remote monitoring of multiple switches across your network (see [Figure 33-2](#)). The traffic for each RSPAN session is carried over a user-specified RSPAN VLAN that is dedicated for that RSPAN session in all participating switches.

The RSPAN source ports can be trunks carrying the RSPAN VLAN. Local SPAN and RSPAN do not monitor the RSPAN traffic in the RSPAN VLAN seen on a source trunk.

The RSPAN traffic from the source ports or source VLANs is switched to the RSPAN VLAN and then forwarded to destination ports, which are in the RSPAN VLAN. The sources (ports or VLANs) in an RSPAN session can be different on different source switches but must be the same for all sources on each RSPAN source switch. Each RSPAN source switch must have either ports or VLANs as RSPAN sources.

Figure 33-2 RSPAN Configuration



Local SPAN and RSPAN Sessions

SPAN sessions (local or remote) allow you to monitor traffic on one or more ports, or one or more VLANs, and send the monitored traffic to one or more destination ports.

A local SPAN session is an association of a set of source ports and source VLANs with one or more destination ports. You configure a local SPAN session on a single network device. Local SPAN does not have separate source and destination sessions.

RSPAN consists of an RSPAN source session, an RSPAN VLAN, and an RSPAN destination session. You separately configure RSPAN source sessions and destination sessions on different network devices. To configure an RSPAN source session on one network device, you associate a set of source ports and VLANs with an RSPAN VLAN. To configure an RSPAN destination session on another device, you associate the destination port with the RSPAN VLAN.

Monitored Traffic

These sections describe the traffic that SPAN (local or remote) can monitor:

- [Monitored Traffic Direction, page 33-4](#)
- [Monitored Traffic Type, page 33-4](#)
- [Duplicate Traffic, page 33-4](#)

Monitored Traffic Direction

You can configure SPAN sessions to monitor ingress network traffic (called ingress SPAN), or to monitor egress network traffic (called egress SPAN), or to monitor traffic flowing in both directions.

Ingress SPAN copies network traffic received by the source ports and VLANs for analysis at the destination port. Egress SPAN copies network traffic transmitted from the source ports and VLANs. When you enter the **both** keyword, SPAN copies the network traffic received and transmitted by the source ports and VLANs to the destination port.

Monitored Traffic Type

By default, local SPAN monitors all network traffic, including multicast and bridge protocol data unit (BPDU) frames. RSPAN does not support BPDU monitoring.

Duplicate Traffic

In some configurations, SPAN sends multiple copies of the same source traffic to the destination port. For example, in a configuration with a bidirectional SPAN session (both ingress and egress) for two SPAN sources, called s1 and s2, to a SPAN destination port, called d1, if a packet enters the switch through s1 and is sent for egress from the switch to s2, ingress SPAN at s1 sends a copy of the packet to SPAN destination d1 and egress SPAN at s2 sends a copy of the packet to SPAN destination d1. If the packet was Layer 2 switched from s1 to s2, both SPAN packets would be the same. If the packet was Layer 3 switched from s1 to s2, the Layer-3 rewrite would alter the source and destination Layer 2 addresses, in which case the SPAN packets would be different.

SPAN Sources

These sections describe local SPAN and RSPAN sources:

- [Source Ports, page 33-4](#)
- [Source VLANs, page 33-5](#)

Source Ports

A source port is a port monitored for network traffic analysis. You can configure both switched and routed ports as SPAN source ports. SPAN can monitor one or more source ports in a single SPAN session. You can configure source ports in any VLAN. Trunk ports can be configured as source ports and mixed with nontrunk source ports, but SPAN does not copy the encapsulation from a source trunk port.

Source VLANs

A source VLAN is a VLAN monitored for network traffic analysis. VLAN-based SPAN (VSPAN) uses a VLAN as the SPAN source. All the ports in the source VLANs become source ports.

Destination Ports

A destination port is a Layer 2 or Layer 3 LAN port to which SPAN sends traffic for analysis.

When you configure a port as a SPAN destination port, it can no longer receive any traffic. When you configure a port as a SPAN destination port, the port is dedicated for use only by the SPAN feature. A SPAN destination port does not forward any traffic except that required for the SPAN session.

You can configure trunk ports as destination ports, which allows destination trunk ports to transmit encapsulated traffic. With earlier releases, trunk ports stop trunking when you configure them as a destination port.

Local SPAN and RSPAN Configuration Guidelines and Restrictions

These sections describe local SPAN and RSPAN configuration guidelines and restrictions:

- [Local SPAN and RSPAN Session Limits, page 33-5](#)
- [Local SPAN and RSPAN Source and Destination Limits, page 33-6](#)
- [Local SPAN and RSPAN Guidelines and Restrictions, page 33-6](#)
- [VSPAN Guidelines and Restrictions, page 33-7](#)
- [RSPAN Guidelines and Restrictions, page 33-7](#)

Local SPAN and RSPAN Session Limits

These are the local SPAN and RSPAN session limits:

Total Sessions per Switch	Local SPAN Sessions	RSPAN Source Sessions	RSPAN Destination Sessions
66	2 (ingress or egress or both)	0	64
	1 (ingress or egress or both)	1 (ingress or egress or both)	
	0	2 (ingress or egress or both)	

Local SPAN and RSPAN Source and Destination Limits

These are the local SPAN and RSPAN source and destination limits:

	Local SPAN Sessions	RSPAN Source Sessions	RSPAN Destination Sessions
Egress sources	1	1	1 RSPAN VLAN
Ingress sources	64	64	
Destinations per session	64	1 RSPAN VLAN	64

Local SPAN and RSPAN Guidelines and Restrictions

These guidelines and restrictions apply to both local SPAN and RSPAN:

- You need a network analyzer to monitor destination ports.
- You can configure both Layer 2 LAN ports (LAN ports configured with the **switchport** command) and Layer 3 LAN ports (LAN ports not configured with the **switchport** command) as sources or destinations.
- You can configure destination ports as trunks to capture tagged traffic. With earlier releases, if you configure a trunk port as a destination port, SPAN suspends trunking on the port.
- A port specified as a destination port in one SPAN session cannot be a destination port for another SPAN session.
- A port configured as a destination port cannot be configured as a source port.
- A port channel interface (an EtherChannel) can be a source.
- You cannot configure active member ports of an EtherChannel as source ports. Inactive member ports of an EtherChannel can be configured as sources but they are put into the suspended state and carry no traffic.
- A port channel interface (an EtherChannel) cannot be a destination.
- You cannot configure active member ports of an EtherChannel as destination ports. Inactive member ports of an EtherChannel can be configured as destinations but they are put into the suspended state and carry no traffic.
- You cannot mix individual source ports and source VLANs within a single session.
- If you specify multiple ingress source ports, the ports can belong to different VLANs.
- You cannot mix source VLANs and filter VLANs within a session. You can have source VLANs or filter VLANs, but not both at the same time.
- When enabled, local SPAN or RSPAN uses any previously entered configuration.
- When you specify sources and do not specify a traffic direction (ingress, egress, or both), “both” is used by default.
- You cannot configure destination ports to receive ingress traffic.
- Destination ports never participate in any spanning tree instance. Local SPAN includes BPDU monitoring in the monitored traffic, so any BPDU seen on the destination port are from the source port. RSPAN does not support BPDU monitoring.

- All packets sent through the switch for transmission from a port configured as an egress source are copied to the destination port, including packets that do not exit the switch through the port because STP has put the port into the blocking state, or on a trunk port because STP has put the VLAN into the blocking state on the trunk port.

VSPAN Guidelines and Restrictions

These are VSPAN guidelines and restrictions:

- For VSPAN sessions with both ingress and egress configured, two packets are forwarded from the destination port if the packets get switched on the same VLAN (one as ingress traffic from the ingress port and one as egress traffic from the egress port).
- VSPAN only monitors traffic that leaves or enters Layer 2 ports in the VLAN.
 - If you configure a VLAN as an ingress source and traffic gets routed into the monitored VLAN, the routed traffic is not monitored because it never appears as ingress traffic entering a Layer 2 port in the VLAN.
 - If you configure a VLAN as an egress source and traffic gets routed out of the monitored VLAN, the routed traffic is not monitored because it never appears as egress traffic leaving a Layer 2 port in the VLAN.

RSPAN Guidelines and Restrictions

These are RSPAN guidelines and restrictions:

- Any network device that supports RSPAN VLANs can be an RSPAN intermediate device.
- Networks impose no limit on the number of RSPAN VLANs that the networks carry.
- Intermediate switches might impose limits on the number of RSPAN VLANs that they can support.
- You must configure the RSPAN VLANs in all source, intermediate, and destination network devices. If enabled, the VLAN Trunking Protocol (VTP) can propagate configuration of VLANs numbered 1 through 1024 as RSPAN VLANs. You must manually configure VLANs numbered higher than 1024 as RSPAN VLANs on all source, intermediate, and destination network devices.
- If you enable VTP and VTP pruning, RSPAN traffic is pruned in the trunks to prevent the unwanted flooding of RSPAN traffic across the network.
- RSPAN VLANs can be used only for RSPAN traffic.
- Do not configure a VLAN used to carry management traffic as an RSPAN VLAN.
- Do not assign access ports to RSPAN VLANs. RSPAN puts access ports in an RSPAN VLAN into the suspended state.
- Do not configure any ports in an RSPAN VLAN except those selected to carry RSPAN traffic.
- MAC address learning is disabled on the RSPAN VLAN.
- You can use an output access control list (ACL) on the RSPAN VLAN in the RSPAN source switch to filter the traffic sent to an RSPAN destination.
- RSPAN does not support BPDU monitoring.
- Do not configure RSPAN VLANs as sources in VSPAN sessions.

- You can configure any VLAN as an RSPAN VLAN as long as all participating network devices support configuration of RSPAN VLANs and you use the same RSPAN VLAN for each RSPAN session in all participating network devices.
- 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 Local SPAN and RSPAN

These sections describe how to configure local SPAN and RSPAN:

- [Local SPAN and RSPAN Configuration Overview, page 33-8](#)
- [Configuring RSPAN VLANs, page 33-8](#)
- [Configuring Local or RSPAN Sources, page 33-9](#)
- [Monitoring Specific Source VLANs on a Source Trunk Port, page 33-10](#)
- [Configuring Local SPAN and RSPAN Destinations, page 33-10](#)
- [Verifying the Configuration, page 33-12](#)
- [Configuration Examples, page 33-12](#)

Local SPAN and RSPAN Configuration Overview

To configure a local SPAN session, use the same session number for the sources and the destination ports.

To configure an RSPAN source session, use the same session number for a source and a destination RSPAN VLAN.

To configure an RSPAN destination session, use the same session number for a source RSPAN VLAN and a destination port.

Configuring RSPAN VLANs

To configure a VLAN as an RSPAN VLAN, perform this task:

Command	Purpose
Step 1 Router(config)# vlan <i>vlan_ID{ [-vlan_ID] [,vlan_ID] }</i>	Creates or modifies an Ethernet VLAN, a range of Ethernet VLANs, or several Ethernet VLANs specified in a comma-separated list (do not enter space characters).
Step 2 Router(config-vlan)# remote-span Router(config-vlan)# no remote-span	Configures the VLAN as an RSPAN VLAN. Clears the RSPAN VLAN configuration.
Step 3 Router(config-vlan)# end	Updates the VLAN database and returns to privileged EXEC mode.

Configuring Local or RSPAN Sources

**Note**

To configure an RSPAN source session, configure a source with an RSPAN VLAN as the destination. To configure an RSPAN destination session, configure an RSPAN VLAN as the source and a port as the destination.

To configure a local SPAN or RSPAN source, perform this task:

Command	Purpose
<pre>Router(config)# monitor session session_number source {{single_interface interface_list interface_range mixed_interface_list single_vlan vlan_list vlan_range mixed_vlan_list} [rx tx both]} {remote vlan rspan_vlan_ID}}</pre>	Configures the session number, the source ports, VLANs, or RSPAN VLAN, and the traffic direction to be monitored.
<pre>Router(config)# no monitor session {session_number all local range session_range[,session_range],...] remote}</pre>	Clears the monitor configuration.

When configuring monitor sessions, note the following syntax information:

- *single_interface* is **interface** *type slot/port*; *type* is **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**.
- *interface_list* is *single_interface* , *single_interface* , *single_interface* ...

**Note**

In lists, you must enter a space before and after the comma. In ranges, you must enter a space before and after the dash.

- *interface_range* is **interface** *type slot/first_port - last_port*
- *mixed_interface_list* is, in any order, *single_interface* , *interface_range* , ...
- *single_vlan* is the ID number of a single VLAN.
- *vlan_list* is *single_vlan* , *single_vlan* , *single_vlan* ...
- *vlan_range* is *first_vlan_ID - last_vlan_ID*
- *mixed_vlan_list* is, in any order, *single_vlan* , *vlan_range* , ...

When clearing monitor sessions, note the following syntax information:

- The **no monitor session** *number* command entered with no other parameters clears session *session_number*.
- *session_range* is *first_session_number-last_session_number*

**Note**

In the **no monitor session range** command, do not enter spaces before or after the dash. If you enter multiple ranges, do not enter spaces before or after the commas.

This example shows how to configure session 1 to monitor bidirectional traffic from Fast Ethernet port 5/1:

```
Router(config)# monitor session 1 source interface fastethernet 5/1
```

Monitoring Specific Source VLANs on a Source Trunk Port

To monitor specific VLANs when the local or RSPAN source is a trunk port, perform this task:

Command	Purpose
Router(config)# monitor session session_number filter {vlan_ID} [, -]	Monitors specific VLANs when the source is a trunk port.
Router(config)# no monitor session session_number filter {vlan_ID}	Clears trunk source configuration.

This example shows how to monitor VLANs 1 through 5 and VLAN 9 when the source is a trunk port:

```
Router(config)# monitor session 2 filter vlan 1 - 5 , 9
```

Configuring Local SPAN and RSPAN Destinations

These sections describe how to configure local SPAN and RSPAN destinations:

- [Configuring a Destination Port as an Unconditional Trunk, page 33-10](#)
- [Configuring a Local or RSPAN Destination, page 33-11](#)

Configuring a Destination Port as an Unconditional Trunk

To tag the monitored traffic, configure the destination port as a trunk.

To configure the destination port as a trunk, perform this task:

Step	Command	Purpose
Step 1	Router(config)# interface type¹ slot/port	Selects the LAN port to configure.
Step 2	Router(config-if)# switchport	Configures the LAN port for Layer 2 switching (required only if the LAN port is not already configured for Layer 2 switching).
Step 3	Router(config-if)# switchport trunk encapsulation {isl dot1q}	Configures the encapsulation, which configures the Layer 2 switching port as either an ISL or 802.1Q trunk.
Step 4	Router(config-if)# switchport mode trunk	Configures the port to trunk unconditionally.
Step 5	Router(config-if)# switchport nonegotiate	Configures the trunk not to use DTP.

1. *type* = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

This example shows how to configure a port as an unconditional IEEE 802.1q trunk:

```
Router(config)# interface fastethernet 5/12
Router(config-if)# switchport
Router(config-if)# switchport trunk encapsulation dot1q
Router(config-if)# switchport mode trunk
Router(config-if)# switchport nonegotiate
```

Configuring a Local or RSPAN Destination

**Note**

To configure an RSPAN source session, configure a source with an RSPAN VLAN as the destination. To configure an RSPAN destination session, configure an RSPAN VLAN as the source and a port as the destination.

To configure a local or RSPAN destination, perform this task:

Command	Purpose
Router(config)# monitor session session_number destination {single_interface interface_list interface_range mixed_interface_list} {remote vlan rspan_vlan_ID}	Configures the session number and the destination ports or RSPAN VLAN.
Router(config)# no monitor session {session_number all local range session_range[,session_range],... remote}	Clears the monitor configuration.

**Note**

To tag the monitored traffic, you must configure the port to trunk unconditionally before you configure it as a destination (see the “Configuring a Destination Port as an Unconditional Trunk” section on page 33-10).

When configuring monitor sessions, note the following syntax information:

- *single_interface* is **interface type slot/port**; **type** is **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**.
- *interface_list* is *single_interface* , *single_interface* , *single_interface* ...

**Note**

In lists, you must enter a space before and after the comma. In ranges, you must enter a space before and after the dash.

- *interface_range* is **interface type slot/first_port - last_port**
- *mixed_interface_list* is, in any order, *single_interface* , *interface_range* , ...

When clearing monitor sessions, note the following syntax information:

- Enter the **no monitor session number** command with no other parameters to clear session *session_number*.
- *session_range* is *first_session_number-last_session_number*

**Note**

In the **no monitor session range** command, do not enter spaces before or after the dash. If you enter multiple ranges, do not enter spaces before or after the commas.

This example shows how to configure Fast Ethernet port 5/48 as the destination for SPAN session 1:

```
Router(config)# monitor session 1 destination interface fastethernet 5/48
```

Verifying the Configuration

This example shows how to verify the configuration of session 2:

```
Router# show monitor session 2
Session 2
-----
Type : Remote Source Session

Source Ports:
    RX Only:      Fa3/1
Dest RSPAN VLAN:  901
Router#
```

This example shows how to display the full details of session 2:

```
Router# show monitor session 2 detail
Session 2
-----
Type : Remote Source Session

Source Ports:
    RX Only:      Fa1/1-3
    TX Only:      None
    Both:        None
Source VLANs:
    RX Only:      None
    TX Only:      None
    Both:        None
Source RSPAN VLAN: None
Destination Ports: None
Filter VLANs:      None
Dest RSPAN VLAN:  901
```

Configuration Examples

This example shows how to configure RSPAN source session 2:

```
Router(config)# monitor session 2 source interface fastethernet1/1 - 3 rx
Router(config)# monitor session 2 destination remote vlan 901
```

This example shows how to clear the configuration for sessions 1 and 2:

```
Router(config)# no monitor session range 1-2
```

This example shows how to configure an RSPAN source session with multiple sources:

```
Router(config)# monitor session 2 source interface fastethernet 5/15 , 7/3 rx
Router(config)# monitor session 2 source interface gigabitethernet 1/2 tx
Router(config)# monitor session 2 source interface port-channel 102
Router(config)# monitor session 2 source filter vlan 2 - 3
Router(config)# monitor session 2 destination remote vlan 901
```

This example shows how to remove sources for a session:

```
Router(config)# no monitor session 2 source interface fastethernet 5/15 , 7/3
```

This example shows how to remove options for sources for a session:

```
Router(config)# no monitor session 2 source interface gigabitethernet 1/2
Router(config)# no monitor session 2 source interface port-channel 102 tx
```

This example shows how to remove VLAN filtering for a session:

```
Router(config)# no monitor session 2 filter vlan 3
```

This example shows how to configure an RSPAN destination session:

```
Router(config)# monitor session 8 source remote vlan 901
Router(config)# monitor session 8 destination interface fastethernet 1/2 , 2/3
```




Configuring SNMP IfIndex Persistence

This chapter describes how to configure the SNMP ifIndex persistence feature on Catalyst 6500 series switches.

This chapter consists of these sections:

- [Understanding SNMP IfIndex Persistence, page 34-1](#)
- [Configuring SNMP IfIndex Persistence, page 34-1](#)

Understanding SNMP IfIndex Persistence

The SNMP ifIndex persistence feature provides an interface index (ifIndex) value that is retained and used when the switch reboots. The ifIndex value is a unique identifying number associated with a physical or logical interface.

There is no requirement in the relevant RFCs that the correspondence between particular ifIndex values and their interfaces be maintained when the switch reboots, but many applications (for example, device inventory, billing, and fault detection) require maintenance of this correspondence.

You can poll the switch at regular intervals to correlate the interfaces to the ifIndexes, but it is not practical to poll constantly. The SNMP ifIndex persistence feature provides permanent ifIndex values, which eliminates the need to poll interfaces.

The following definitions are based on RFC 2233, “The Interfaces Group MIB using SMIv2.” The following terms are values in the Interfaces MIB (IF-MIB):

- **ifIndex**—A unique number (greater than zero) that identifies each interface for SNMP identification of that interface.
- **ifName**—The text-based name of the interface, for example, “ethernet 3/1.”
- **ifDescr**—A description of the interface. Recommended information for this description includes the name of the manufacturer, the product name, and the version of the interface hardware and software.

Configuring SNMP IfIndex Persistence

These sections describe how to configure SNMP ifIndex persistence:

- [Enabling SNMP IfIndex Persistence Globally, page 34-2](#) (Optional)
- [Enabling and Disabling SNMP IfIndex Persistence on Specific Interfaces, page 34-2](#) (Optional)

Configuring SNMP IfIndex Persistence

Note To verify that ifIndex commands have been configured, use the **more system:running-config** command.

Enabling SNMP IfIndex Persistence Globally

SNMP ifIndex persistence is disabled by default. To globally enable SNMP ifIndex persistence, perform this task:

Command	Purpose
Router(config)# snmp-server ifindex persist	Globally enables SNMP ifIndex persistence.

In the following example, SNMP ifIndex persistence is enabled for all interfaces:

```
router(config)# snmp-server ifindex persist
```

Disabling SNMP IfIndex Persistence Globally

To globally disable SNMP ifIndex persistence after enabling it, perform this task:

Command	Purpose
Router(config)# no snmp-server ifindex persist	Globally disables SNMP ifIndex persistence.

In the following example, SNMP ifIndex persistence is disabled for all interfaces:

```
router(config)# no snmp-server ifindex persist
```

Enabling and Disabling SNMP IfIndex Persistence on Specific Interfaces

To enable SNMP ifIndex persistence only on a specific interface, perform this task:

	Command	Purpose
Step 1	Router(config)# interface {vlan vlan_ID} {type¹ slot/port} {port-channel port_channel_number}	Selects an interface to configure.
Step 2	Router(config-if)# snmp ifindex persist	Enables SNMP ifIndex persistence on the specified interface.
	Router(config-if)# no snmp ifindex persist	Disables SNMP ifIndex persistence on the specified interface.
Step 3	Router(config-if)# exit	Exits interface configuration mode.

1. type = any supported interface type.

**Note**

The **[no] snmp ifindex persistence** interface command cannot be used on subinterfaces. A command applied to an interface is automatically applied to all the subinterfaces associated with that interface.

In the following example, SNMP ifIndex persistence is enabled for Ethernet interface 3/1 only:

```
router(config)# interface ethernet 3/1
router(config-if)# snmp ifindex persist
router(config-if)# exit
```

In the following example, SNMP ifIndex persistence is disabled for Ethernet interface 3/1 only:

```
router(config)# interface ethernet 3/1
router(config-if)# no snmp ifindex persist
router(config-if)# exit
```

Clearing SNMP IfIndex Persistence Configuration from a Specific Interface

To clear the interface-specific SNMP ifIndex persistence setting and configure the interface to use the global configuration setting, perform this task:

Command	Purpose
Step 1 Router(config)# <i>interface type slot/port</i>	Enters interface configuration mode for the specified interface. Note that the syntax of the interface command will vary depending on the platform you are using.
Step 2 Router(config-if)# snmp ifindex clear	Clears any interface-specific SNMP ifIndex persistence configuration for the specified interface and returns to the global configuration setting.
Step 3 Router(config-if)# exit	Exits interface configuration mode.

In the following example, any previous setting for SNMP ifIndex persistence on Ethernet interface 3/1 is removed from the configuration. If SNMP ifIndex persistence is globally enabled, SNMP ifIndex persistence will be enabled for Ethernet interface 3/1. If SNMP ifIndex persistence is globally disabled, SNMP ifIndex persistence will be disabled for Ethernet interface 3/1.

```
router(config)# interface ethernet 3/1
router(config-if)# snmp ifindex clear
router(config-if)# exit
```

■ Configuring SNMP IfIndex Persistence



Power Management and Environmental Monitoring

This chapter describes the power management and environmental monitoring features in the Catalyst 6500 series switches.



For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication.

This chapter consists of these sections:

- [Understanding How Power Management Works, page 35-1](#)
- [Understanding How Environmental Monitoring Works, page 35-4](#)

Understanding How Power Management Works

These sections describe power management in the Catalyst 6500 series switches:

- [Enabling or Disabling Power Redundancy, page 35-2](#)
- [Powering Modules Off and On, page 35-3](#)
- [Viewing System Power Status, page 35-3](#)
- [Power Cycling Modules, page 35-4](#)
- [Determining System Power Requirements, page 35-4](#)
- [Determining System Power Requirements, page 35-4](#)



In systems with redundant power supplies, both power supplies must be of the same wattage. The Catalyst 6500 series switches allow you to use both AC-input and DC-input power supplies in the same chassis. For detailed information on supported power supply configurations, refer to the *Catalyst 6500 Series Switch Installation Guide*.

The modules have different power requirements, and some configurations require more power than a single power supply can provide. The power management feature allows you to power all installed modules with two power supplies. However, redundancy is not supported in this configuration because the total power drawn from both power supplies is at no time greater than the capability of one supply. Redundant and nonredundant power configurations are described in the following sections.

To determine the power requirements for your system, see the “[Determining System Power Requirements](#)” section on page 35-4.

Enabling or Disabling Power Redundancy

To disable or enable redundancy (redundancy is enabled by default) from global configuration mode enter the **power redundancy-mode combined | redundant** commands. You can change the configuration of the power supplies to redundant or nonredundant at any time.

To disable redundancy, use the **combined** keyword. In a nonredundant configuration, the power available to the system is the combined power capability of both power supplies. The system powers up as many modules as the combined capacity allows. However, if one power supply fails and there is not enough power for all of the previously powered-up modules, the system powers down those modules.

To enable redundancy use the **redundant** keyword. In a redundant configuration, the total power drawn from both power supplies is not greater than the capability of one power supply. If one supply malfunctions, the other supply can take over the entire system load. When you install and power up two power supplies, each concurrently provides approximately half of the required power to the system. Load sharing and redundancy are enabled automatically; no software configuration is required.

To view the current state of modules and the total power available for modules enter the **show power** command (see the “[Viewing System Power Status](#)” section on page 35-3).

Table 35-1 describes how the system responds to changes in the power supply configuration.

Table 35-1 Effects of Power Supply Configuration Changes

Configuration Change	Effect
Redundant to nonredundant	<ul style="list-style-type: none"> System log and syslog messages are generated. System power is increased to the combined power capability of both power supplies. Modules marked <i>power-deny</i> in the show power oper state field are brought up if there is sufficient power.
Nonredundant to redundant (both power supplies must be of equal wattage)	<ul style="list-style-type: none"> System log and syslog messages are generated. System power is decreased to the power capability of one supply. If there is not enough power for all previously powered-up modules, some modules are powered down and marked as <i>power-deny</i> in the show power oper state field.
Equal wattage power supply is inserted with redundancy enabled	<ul style="list-style-type: none"> System log and syslog messages are generated. System power equals the power capability of one supply. No change in module status because the power capability is unchanged.
Equal wattage power supply is inserted with redundancy disabled	<ul style="list-style-type: none"> System log and syslog messages are generated. System power is increased to the combined power capability of both power supplies. Modules marked <i>power-deny</i> in the show power oper state field are brought up if there is sufficient power.
Higher or lower wattage power supply is inserted with redundancy enabled	<ul style="list-style-type: none"> System log and syslog messages are generated. The system does not allow you to operate a power supply of different wattage even if the wattage is higher than the installed supply. The inserted supply shuts down.

Table 35-1 Effects of Power Supply Configuration Changes (continued)

Configuration Change	Effect
Higher or lower wattage power supply is inserted with redundancy disabled	<ul style="list-style-type: none"> System log and syslog messages are generated. System power is increased to the combined power capability of both power supplies. Modules marked <i>power-deny</i> in the show power oper state field are brought up if there is sufficient power.
Power supply is removed with redundancy enabled	<ul style="list-style-type: none"> System log and syslog messages are generated. No change in module status because the power capability is unchanged.
Power supply is removed with redundancy disabled	<ul style="list-style-type: none"> System log and syslog messages are generated. System power is decreased to the power capability of one supply. If there is not enough power for all previously powered-up modules, some modules are powered down and marked as <i>power-deny</i> in the show power oper state field.
System is booted with power supplies of different wattage installed and redundancy enabled	<ul style="list-style-type: none"> System log and syslog messages are generated. The system does not allow you to have power supplies of different wattage installed in a redundant configuration. The lower wattage supply shuts down.
System is booted with power supplies of equal or different wattage installed and redundancy disabled	<ul style="list-style-type: none"> System log and syslog messages are generated. System power equals the combined power capability of both power supplies. The system powers up as many modules as the combined capacity allows.

Powering Modules Off and On

You can power down a module from the CLI by entering the **no power enable module slot** command.



Note When you enter the **no power enable module slot** command to power down a module, the module's configuration is not saved.

From global configuration mode, enter the **power enable module slot** command to turn the power on for a module that was previously powered down.

Viewing System Power Status

You can view the current power status of system components by entering the **show power** command as follows:

```
Router# show power
system power redundancy mode = redundant
system power total =      1153.32 Watts (27.46 Amps @ 42V)
system power used =        397.74 Watts ( 9.47 Amps @ 42V)
system power available =   755.58 Watts (17.99 Amps @ 42V)
                                         Power-Capacity PS-Fan Output Oper
                                         Watts    A @42V Status Status State
PS      Type
----- -----
1      WS-CAC-2500W      1153.32 27.46  OK      OK      on
2      none
```

■ Understanding How Environmental Monitoring Works

Slot	Card-Type	Pwr-Requested Watts	Pwr-Allocated A @42V	Admin State	Oper State
1	WS-X6K-SUP2-2GE	142.38	3.39	142.38	3.39 on on
2	-	-	-	142.38	3.39 - -
5	WS-X6248-RJ-45	112.98	2.69	112.98	2.69 on on
Router#					

Power Cycling Modules

You can power cycle (reset) a module from global configuration mode, by entering the **power cycle module slot** command. The module powers off for 5 seconds and then powers on.

Determining System Power Requirements

The power supply size determines the system power requirements. When you use the 1000 W and 1300 W power supplies you might have configuration limitations depending on the size of chassis and type of modules installed. For information about power consumption, refer to the *Release Notes for the Catalyst 6000 Family Switches and Cisco 7600 Internet Router for Cisco IOS* publication at this URL:
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/index.htm>

Understanding How Environmental Monitoring Works

Environmental monitoring of chassis components provides early-warning indications of possible component failures which ensure a safe and reliable system operation and avoids network interruptions. This section describes the monitoring of these critical system components, which allows you to identify and rapidly correct hardware-related problems in your system.

Monitoring System Environmental Status

To display system status information, enter the **show environment [alarm | cooling | status | temperature]** command. The keywords display the following information:

- **alarm**—Displays environmental alarms.
 - **status**—Displays alarm status.
 - **thresholds**—Displays alarm thresholds.
- **cooling**—Displays fan tray status, chassis cooling capacity, ambient temperature, and per slot cooling capacity.
- **status**—Displays field-replaceable unit (FRU) operational status and power and temperature information.
- **temperature**—Displays FRU temperature information.

To view the system status information, enter the **show environment** command as follows:

```
Router# show environment
environmental alarms:
  no alarms

Router# show environment alarm
```

```
environmental alarms:  
    no alarms  
  
Router# show environment cooling  
fan-tray 1:  
    fan-tray 1 fan-fail: failed  
fan-tray 2:  
    fan 2 type: FAN-MOD-9  
    fan-tray 2 fan-fail: OK  
chassis cooling capacity: 690 cfm  
ambient temperature: 55C  
chassis per slot cooling capacity: 75 cfm  
                                ["40C (user-specified)" if temp-controlled]  
  
    module 1 cooling requirement: 70 cfm  
    module 2 cooling requirement: 70 cfm  
    module 5 cooling requirement: 30 cfm  
    module 6 cooling requirement: 70 cfm  
    module 8 cooling requirement: 70 cfm  
    module 9 cooling requirement: 30 cfm  
  
Router# show environment status  
backplane:  
    operating clock count: 2  
    operating VTT count: 3  
fan-tray 1:  
    fan-tray 1 type: WS-9SLOT-FAN  
    fan-tray 1 fan-fail: OK  
VTT 1:  
    VTT 1 OK: OK  
    VTT 1 outlet temperature: 33C  
VTT 2:  
    VTT 2 OK: OK  
    VTT 2 outlet temperature: 35C  
VTT 3:  
    VTT 3 OK: OK  
    VTT 3 outlet temperature: 33C  
clock 1:  
    clock 1 OK: OK, clock 1 clock-inuse: in-use  
clock 2:  
    clock 2 OK: OK, clock 2 clock-inuse: not-in-use  
power-supply 1:  
    power-supply 1 fan-fail: OK  
    power-supply 1 power-output-fail: OK  
module 1:  
    module 1 power-output-fail: OK  
    module 1 outlet temperature: 30C  
    module 1 device-2 temperature: 35C  
    RP 1 outlet temperature: 35C  
    RP 1 inlet temperature: 36C  
    EARL 1 outlet temperature: 33C  
    EARL 1 inlet temperature: 31C  
module 2:  
    module 2 power-output-fail: OK  
    module 2 outlet temperature: 31C  
    module 2 inlet temperature: 29C  
module 3:  
    module 3 power-output-fail: OK  
    module 3 outlet temperature: 36C  
    module 3 inlet temperature: 29C  
module 4:  
    module 4 power-output-fail: OK  
    module 4 outlet temperature: 32C  
    module 4 inlet temperature: 32C  
module 5:
```

■ Understanding How Environmental Monitoring Works

```

module 5 power-output-fail: OK
module 5 outlet temperature: 39C
module 5 inlet temperature: 34C
module 7:
  module 7 power-output-fail: OK
  module 7 outlet temperature: 42C
  module 7 inlet temperature: 29C
  EARL 7 outlet temperature: 45C
  EARL 7 inlet temperature: 32C
module 9:
  module 9 power-output-fail: OK
  module 9 outlet temperature: 41C
  module 9 inlet temperature: 36C
  EARL 9 outlet temperature: 33C
  EARL 9 inlet temperature: N/O

```

Understanding LED Environmental Indications

The LEDs can indicate two alarm types: major and minor. Major alarms indicate a critical problem that could lead to the system being shut down. Minor alarms are for informational purposes only, giving you notice of a problem that could turn critical if corrective action is not taken.

When the system has an alarm (major or minor), that indicates an overtemperature condition, the alarm is not canceled nor is any action taken (such as module reset or shutdown) for 5 minutes. If the temperature falls 5°C (41°F) below the alarm threshold during this period, the alarm is canceled.

[Table 35-2](#) lists the environmental indicators for the supervisor engine and switching modules.



Note Refer to the *Catalyst 6500 Series Switch Module Installation Guide* for additional information on LEDs, including the supervisor engine SYSTEM LED.

Table 35-2 Environmental Monitoring for Supervisor Engine and Switching Modules

Component	Alarm Type	LED Indication	Action
Supervisor engine temperature sensor exceeds major threshold ¹	Major	STATUS ² LED red ³	Generates syslog message and an SNMP trap. If there is a redundancy situation, the system switches to a redundant supervisor engine and the active supervisor engine shuts down. If there is no redundancy situation and the overtemperature condition is not corrected, the system shuts down after 5 minutes.
Supervisor engine temperature sensor exceeds minor threshold	Minor	STATUS LED orange	Generates syslog message and an SNMP trap. Monitors the condition.
Redundant supervisor engine temperature sensor exceeds major or minor threshold	Major	STATUS LED red	Generates syslog message and an SNMP trap. If a major alarm is generated and the overtemperature condition is not corrected, the system shuts down after 5 minutes.
	Minor	STATUS LED orange	Monitors the condition if a minor alarm is generated.

Table 35-2 Environmental Monitoring for Supervisor Engine and Switching Modules (continued)

Component	Alarm Type	LED Indication	Action
Switching module temperature sensor exceeds major threshold	Major	STATUS LED red	Generates syslog message and SNMP. Powers down the module ⁴ .
Switching module temperature sensor exceeds minor threshold	Minor	STATUS LED orange	Generates syslog message and an SNMP trap. Monitors the condition.

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.
3. The STATUS LED is red on the failed supervisor engine. If there is no redundant supervisor, the SYSTEM LED is red also.
4. See the “[Understanding How Power Management Works](#)” section on page 35-1 for instructions.

■ Understanding How Environmental Monitoring Works



Configuring Online Diagnostics

This chapter describes how to configure the online diagnostics on the Catalyst 6500 series switches:



Note For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference*.

This chapter consists of these sections:

- [Understanding How Online Diagnostics Work, page 36-1](#)
- [Configuring Online Diagnostics, page 36-2](#)
- [Running Online Diagnostic Tests, page 36-4](#)

Understanding How Online Diagnostics Work

With online diagnostics, you can test and verify the hardware functionality of the Catalyst 6500 series supervisor engine, modules, and switch while the switch is connected to a live network.

The online diagnostics contain packet switching tests that check different hardware components and verify the data path and control signals. Disruptive online diagnostic tests, such as the built in self test (BIST) and the disruptive loopback test, and non-disruptive online diagnostic tests, such as packet switching, run during bootup, line card online insertion and removal (OIR), and system reset. The nondisruptive online diagnostic tests run as part of background health monitoring or at the user's request (on-demand).

The online diagnostics detect problems in the following areas:

- Hardware components
- Interfaces (GBICs, Ethernet ports, and so forth)
- Connectors (loose connectors, bent pins, and so forth)
- Solder joints
- Memory (failure over time)

Online diagnostics is one of the requirements for the high availability feature. High availability is a set of quality standards that seek to limit the impact of equipment failures on the network. A key part of high availability is detecting hardware failures and taking corrective action while the switch runs in a live network. Online diagnostics in high availability detect hardware failures and provide feedback to high availability software components to make switchover decisions.

Online diagnostics are categorized as bootup, on-demand, schedule, or health monitoring diagnostics. Bootup diagnostics run during bootup, module OIR, or switchover to a backup supervisor engine; on-demand diagnostics run from the CLI; schedule diagnostics run at user-designated intervals or specified times when the switch is connected to a live network; and health-monitoring runs in the background.

Configuring Online Diagnostics

These sections describe how to configure online diagnostics:

- [Setting Bootup Online Diagnostics Level, page 36-2](#)
- [Configuring On-Demand Online Diagnostics, page 36-2](#)
- [Scheduling Online Diagnostics, page 36-3](#)

Setting Bootup Online Diagnostics Level

You can set the bootup diagnostics level as minimal or complete or you can bypass the bootup diagnostics entirely. Enter the **complete** keyword to run all diagnostic tests; enter the **minimal** keyword to run only EARL tests for the supervisor engine and loopback tests for all ports in the switch. Enter the **no** form of the command to bypass all diagnostic tests. The default bootup diagnostics level is minimal.



Note The diagnostic level applies to the entire switch and cannot be configured on a per-module basis.

To set the bootup diagnostic level, perform this task:

Command	Purpose
Router(config)# diagnostic bootup level {minimal complete}	Sets the bootup diagnostic level.

This example shows how to set the bootup online diagnostic level:

```
Router(config)# diagnostic bootup level complete
Router(config)#

```

This example shows how to display the bootup online diagnostic level:

```
Router(config)# show diagnostic bootup level
Router(config)#

```

Configuring On-Demand Online Diagnostics

You can run the OnDemand online diagnostic tests from the CLI. You can set the execution action to either stop or continue the test when a failure is detected or to stop the test after a certain number of failures using the failure count setting. You can configure a test to run multiple times using the iteration setting.

To set the bootup diagnostic level, perform this task:

Command	Purpose
Router(config)# diagnostic ondemand {iteration iteration-count} {action-on-error {continue stop} [error-count]}	Configures on-demand diagnostic tests to run, how many times to run (iterations), and what action to take when errors are found.

This example shows how to set the on-demand testing iteration count:

```
Router(config)# diagnostic ondemand iteration 3
Router(config)#
```

This example shows how to set the execution action when an error is detected:

```
Router(config)# diagnostic ondemand action-on-error continue 2
Router(config)#
```

Scheduling Online Diagnostics

You can schedule online diagnostics to run at a designated time of day or on a daily, weekly, or monthly basis for a specific module. You can schedule tests to run only once or to repeat at an interval. Use the **no** form of this command to remove the scheduling.

To schedule online diagnostics, perform this task:

Command	Purpose
Router(config)# diagnostic schedule {module num} test {test-id test-id-range all} [port {num num-range all}] {on mm dd yyyy hh:mm} {daily hh:mm} {weekly day-of-week hh:mm}	Schedules on-demand diagnostic tests for a specific date and time, how many times to run (iterations), and what action to take when errors are found.

This example shows how to schedule diagnostic testing on a specific date and time for a specific module and port:

```
Router(config)# diagnostic schedule module 1 test 1,2,5-9 port 3 on january 3 2003 23:32
Router(config)#
```

This example shows how to schedule diagnostic testing to occur daily at a certain time for a specific port and module:

```
Router(config)# diagnostic schedule module 1 test 1,2,5-9 port 3 daily 12:34
Router(config)#
```

This example shows how to schedule diagnostic testing to occur weekly on a certain day for a specific port and module:

```
Router(config)# diagnostic schedule module 1 test 1,2,5-9 port 3 weekly friday 09:23
Router(config)#
```

Configuring Health-Monitoring Diagnostics

You can configure health-monitoring diagnostic testing on specified modules while the switch is connected to a live network. You can configure the execution interval for each health monitoring test, whether or not to generate a system message upon test failure, or to enable or disable an individual test. Use the **no** form of this command to disable testing.

To configure health monitoring diagnostic testing, perform this task:

Command	Purpose
Step 1 Router(config)# diagnostic monitor interval {module num} test {test-id test-id-range all} [hour hh] [min mm] [second ss] [millisec ms] [day]	Configures the health-monitoring interval of the specified tests for the specified module. The no form of this command will change the interval to the default interval, or zero.
Step 2 Router(config)# [no] diagnostic monitor {module num} test {test-id test-id-range all}	Enables or disables health-monitoring diagnostic tests.

This example shows how to configure the specified test to run every 2 minutes:

```
Router(config)# diagnostic monitor interval module 1 test 1 min 2
Router(config)#
```

This example shows how to run the test on the specified module if health monitoring has not previously been enabled:

```
Router(config)# diagnostic monitor module 1 test 1
```

This example shows how to enable the generation of a syslog message when any health monitoring test fails:

```
Router(config)# diagnostic monitor syslog
Router(config)#
```

Running Online Diagnostic Tests

After you configure online diagnostics, you can start or stop diagnostic tests or display the test results. You can also see which tests are configured for each module and what diagnostic tests have already run.

These sections describe how to run online diagnostic tests after they have been configured:

- [Starting and Stopping Online Diagnostic Tests, page 36-4](#)
- [Displaying Online Diagnostic Tests and Test Results, page 36-5](#)

Starting and Stopping Online Diagnostic Tests

After you configure diagnostic tests to run on the switch or individual modules, you can use the **start** and **stop** to begin or end a diagnostic test.

To start or stop an online diagnostic command, perform one of these tasks:

Command	Purpose
<code>diagnostic start {module num} test {test-id test-id-range minimal per-port non-disruptive all} [port {num port#-range all}]</code>	Starts a diagnostic test on a specific module and port or range of ports.
<code>diagnostic stop {module num}</code>	Stops a diagnostic test on a specific module.

This example shows how to start a diagnostic test on a specific module:

```
Router# diagnostic start module 1 test 5
Module 1:Running test(s) 5 may disrupt normal system operation
Do you want to run disruptive tests? [no]yes
00:48:14:Running OnDemand Diagnostics [Iteration #1] ...
00:48:14:%DIAG-SP-6-TEST_RUNNING:Module 1:Running TestNewLearn{ID=5} ...
00:48:14:%DIAG-SP-6-TEST_OK:Module 1:TestNewLearn{ID=5} has completed successfully
00:48:14:Running OnDemand Diagnostics [Iteration #2] ...
00:48:14:%DIAG-SP-6-TEST_RUNNING:Module 1:Running TestNewLearn{ID=5} ...
00:48:14:%DIAG-SP-6-TEST_OK:Module 1:TestNewLearn{ID=5} has completed successfully
Router#
```

This example shows how to stop a diagnostic test on a specific module:

```
Router# diagnostic stop module 3
Router#
```

Displaying Online Diagnostic Tests and Test Results

You can display the online diagnostic tests that are configured for specific modules and check the results of the tests using the **show** commands.

To display the diagnostic tests that are configured for a module, perform this task:

Command	Purpose
<code>show diagnostic content [module num]</code>	Displays the online diagnostics configured for a module.

This example shows how to display the online diagnostics that are configured on a module:

```
Router# show diagnostic content module 5
Module 5:

Diagnostics test suite attributes:
M/C/* - Minimal bootup level test / Complete bootup level test / NA
B/* - Basic ondemand test / NA
P/V/* - Per port test / Per device test / NA
D/N/* - Disruptive test / Non-disruptive test / NA
S/* - Only applicable to standby unit / NA
X/* - Not a health monitoring test / NA
F/* - Fixed monitoring interval test / NA
E/* - Always enabled monitoring test / NA
A/I - Monitoring is active / Monitoring is inactive
R/* - Reset supervisor and power-down line cards / NA

Testing Interval
ID    Test Name          Attributes      (day hh:mm:ss.ms)
===== ===== ===== ===== ===== =====
1)  TestScratchRegister -----> ***N***A*  000 00:00:30.00
2)  TestSPRPInbandPing -----> ***N***A*  000 00:00:15.00
```

■ Running Online Diagnostic Tests

```

3) TestGBICIntegrity -----> **PD****I* not configured
4) TestActiveToStandbyLoopback -----> M**PDS***I* not configured
5) TestLoopback -----> M**PD****I* not configured
6) TestNewLearn -----> M**N****I* not configured
7) TestIndexLearn -----> M**N****I* not configured
8) TestDontLearn -----> M**D****I* not configured
9) TestConditionalLearn -----> M**N****I* not configured
10) TestBadBpdu -----> M**D****I* not configured
11) TestTrap -----> M**D****I* not configured
12) TestMatch -----> M**D****I* not configured
13) TestCapture -----> M**D****I* not configured
14) TestProtocolMatch -----> M**D****I* not configured
15) TestChannel -----> M**D****I* not configured
16) TestIPv4FibShortcut -----> M**N****I* not configured
17) TestL3Capture2 -----> M**N****I* not configured
18) TestL3VlanMet -----> M**N****I* not configured
19) TestIngressSpan -----> M**N****I* not configured
20) TestEgressSpan -----> M**N****I* not configured
21) TestIPv6FibShortcut -----> M**N****I* not configured
22) TestMPLSFibShortcut -----> M**N****I* not configured
23) TestNATFibShortcut -----> M**N****I* not configured
24) TestAclPermit -----> M**N****I* not configured
25) TestAclDeny -----> M**D****I* not configured
26) TestQoSSTcam -----> M**D****I* not configured
27) TestNetflowInlineRewrite -----> C*PD****I* not configured
28) TestFabricSnakeForward -----> M**N****I* not configured
29) TestFabricSnakeBackward -----> M**N****I* not configured
30) TestFibTcam - RESET -----> ***D****IR not configured
Router#

```

This example shows how to display the online diagnostic results for a module:

```

Router# show diagnostic result module 5
Current bootup diagnostic level:minimal

Module 5:

Overall Diagnostic Result for Module 5 :PASS
Diagnostic level at card bootup:minimal

Test results:(. = Pass, F = Fail, U = Untested)

1) TestScratchRegister -----> .
2) TestSPRPInbandPing -----> .
3) TestGBICIntegrity:
   Port 1 2
   -----
   U  U

4) TestActiveToStandbyLoopback:
   Port 1 2
   -----
   U  U

5) TestLoopback:
   Port 1 2
   -----
   .

```

```

6) TestNewLearn -----> .
7) TestIndexLearn -----> .
8) TestDontLearn -----> .
9) TestConditionalLearn -----> .
10) TestBadBpdu -----> .
11) TestTrap -----> .
12) TestMatch -----> .
13) TestCapture -----> .
14) TestProtocolMatch -----> .
15) TestChannel -----> .
16) TestIPv4FibShortcut -----> .
17) TestL3Capture2 -----> .
18) TestL3VlanMet -----> .
19) TestIngressSpan -----> .
20) TestEgressSpan -----> .
21) TestIPv6FibShortcut -----> .
22) TestMPLSFibShortcut -----> .
23) TestNATFibShortcut -----> .
24) TestAclPermit -----> .
25) TestAclDeny -----> .
26) TestQoSSTcam -----> .
27) TestNetflowInlineRewrite:

      Port   1   2
      -----
           U   U

28) TestFabricSnakeForward -----> .
29) TestFabricSnakeBackward -----> .
30) TestFibTcam - RESET -----> U
Router#

```

This example shows how to display the detailed online diagnostic results for a module:

```

Router# show diagnostic result module 5 detail
Current bootup diagnostic level:minimal

Module 5:

Overall Diagnostic Result for Module 5 :PASS
Diagnostic level at card bootup:minimal

Test results:(. = Pass, F = Fail, U = Untested)



---


1) TestScratchRegister -----> .

Error code -----> 0 (DIAG_SUCCESS)
Total run count -----> 330
Last test execution time ----> May 12 2003 14:49:36
First test failure time -----> n/a
Last test failure time -----> n/a
Last test pass time -----> May 12 2003 14:49:36
Total failure count -----> 0
Consecutive failure count ---> 0



---


2) TestSPRPInbandPing -----> .

Error code -----> 0 (DIAG_SUCCESS)
Total run count -----> 660

```

■ Running Online Diagnostic Tests

```
Last test execution time ----> May 12 2003 14:49:38
First test failure time -----> n/a
Last test failure time -----> n/a
Last test pass time -----> May 12 2003 14:49:38
Total failure count -----> 0
Consecutive failure count ---> 0
```

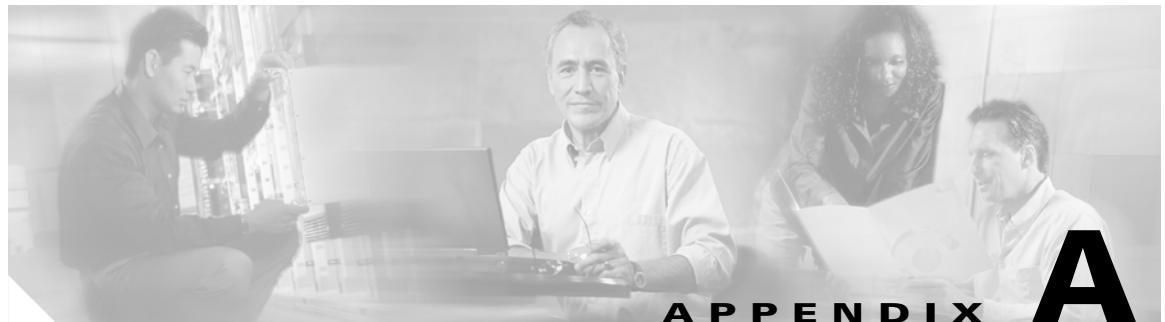
3) TestGBICIntegrity:

Port	1	2

U	U	

```
Error code -----> 0 (DIAG_SUCCESS)
Total run count -----> 0
Last test execution time ----> n/a
First test failure time -----> n/a
Last test failure time -----> n/a
Last test pass time -----> n/a
Total failure count -----> 0
Consecutive failure count ---> 0
```

Router#



APPENDIX

A

Acronyms

Table A-1 defines the acronyms used in this publication.

Table A-1 List of Acronyms

Acronym	Expansion
AAL	ATM adaptation layer
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
ATA	Analog Telephone Adaptor
ATM	Asynchronous Transfer Mode
AV	attribute value
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

Table A-1 List of Acronyms (continued)

Acronym	Expansion
CEF	Cisco Express Forwarding
CHAP	Challenge Handshake Authentication Protocol
CIR	committed information rate
CLI	command-line interface
CLNS	Connection-Less Network Service
CMNS	Connection-Mode Network Service
COPS	Common Open Policy Server
COPS-DS	Common Open Policy Server Differentiated Services
CoS	class of service
CPLD	Complex Programmable Logic Device
CRC	cyclic redundancy check
CRF	concentrator relay function
CST	Common Spanning Tree
CUDD	University of Colorado Decision Diagram
DCC	Data Country Code
dCEF	distributed Cisco Express Forwarding
DDR	dial-on-demand routing
DE	discard eligibility
DEC	Digital Equipment Corporation
DFC	Distributed Forwarding Card
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
dot1q	802.1Q
DRAM	dynamic RAM
DRiP	Dual Ring Protocol
DSAP	destination service access point
DSCP	differentiated services code point
DSPU	downstream SNA Physical Units
DTP	Dynamic Trunking Protocol

Table A-1 List of Acronyms (continued)

Acronym	Expansion
DTR	data terminal ready
DXI	data exchange interface
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
EOF	end of file
ESI	end-system identifier
FAT	File Allocation Table
FECN	forward explicit congestion notification
FM	feature manager
FRU	field replaceable unit
fsck	file system consistency check
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
IDSIM	Intrusion Detection System Module
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

Table A-1 List of Acronyms (continued)

Acronym	Expansion
ISL	Inter-Switch Link
ISO	International Organization of Standardization
ISR	Integrated SONET router
LAN	local area network
LANE	LAN Emulation
LAPB	Link Access Procedure, Balanced
LCP	Link Control Protocol
LDA	Local Director Acceleration
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
MD5	Message Digest 5
MFD	multicast fast drop
MSFC	Multilayer Switch Feature Card
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
MSFC	Multilayer Switching Feature Card
MSM	Multilayer Switch Module
MTU	maximum transmission unit
MVAP	multiple VLAN access port
NAM	Network Analysis Module
NBP	Name Binding Protocol
NCIA	Native Client Interface Architecture
NDE	NetFlow Data Export

Table A-1 List of Acronyms (continued)

Acronym	Expansion
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
OAM	Operation, Administration, and Maintenance
ODM	order dependent merge
OSI	Open System Interconnection
OSM	Optical Services Module
OSPF	open shortest path first
PAE	port access entity
PAgP	Port Aggregation Protocol
PBD	packet buffer daughterboard
PC	Personal Computer (formerly PCMCIA)
PCM	pulse code modulation
PCR	peak cell rate
PDP	policy decision point
PDU	protocol data unit
PEP	policy enforcement point
PFC	Policy Feature Card
PGM	Pragmatic General Multicast
PHY	physical sublayer
PIB	policy information base
PPP	Point-to-Point Protocol
PRID	Policy Rule Identifiers
PVST+	Per VLAN Spanning Tree+
QDM	QoS device manager
QM	QoS manager
QoS	quality of service
RACL	router interface access control list
RADIUS	Remote Access Dial-In User Service
RAM	random-access memory
RCP	Remote Copy Protocol
RGMP	Router-Ports Group Management Protocol

Table A-1 List of Acronyms (continued)

Acronym	Expansion
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
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
SREC	S-Record format, Motorola defined format for ROM contents
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

Table A-1 List of Acronyms (continued)

Acronym	Expansion
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
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
WAN	wide area network
WCCP	Web Cache Communications Protocol
WFQ	weighted fair queueing
WRED	weighted random early detection
WRR	weighted round-robin
XNS	Xerox Network System



Numerics

4K VLANs (support for 4,096 VLANs) **10-2**

802.10 SAID (default) **10-6**

802.1Q

 encapsulation **7-3**

 Layer 2 protocol tunneling

 See Layer 2 protocol tunneling

 mapping to ISL VLANs **10-12**

 trunks **7-2**

 restrictions **7-5**

 tunneling

 configuration guidelines **13-3**

 configuring tunnel ports **13-5**

 overview **13-1**

802.1s

 See MST

802.1w

 See MST

802.1X

 See port-based authentication

802.3ad

 See LACP

802.3Z Flow Control **5-13**

A

AAA **21-1, 22-1, 26-1**

abbreviating commands **2-5**

access control entries and lists **21-1, 22-1, 26-1**

access port, configuring **7-13**

ACEs and ACLs **21-1, 22-1, 26-1**

acronyms, list of **A-1**

addresses

 IP, see IP addresses

 MAC, see MAC addresses

advertisements, VTP **9-2**

aggregate policing

 see QoS policing

aging-time

 IP MLS **32-11**

alarms

 major **36-6**

 minor **36-6**

audience **xvii**

authentication

 See also port-based authentication

Authentication, Authorization, and Accounting (AAA) **21-1, 22-1, 26-1**

authorized ports with 802.1X **27-4**

auto-sync command **6-6**

auxiliary VLAN

 See voice VLAN

B

BackboneFast

 See STP BackboneFast

blocking state, STP **14-7**

boot bootldr command **3-26**

boot command **3-22**

boot config command **3-26**

BOOTLDR environment variable

 (example) **3-27**

configuring **3-26**

setting **3-26**

boot loader image **3-26**
 boot system command **3-21, 3-26**
 boot system flash command **3-22**
 BPDU guard
 See STP BPDU guard
 bridge ID
 See STP bridge ID
 bridge priority, STP **14-28**
 bridge protocol data units
 see BPDUs
 broadcast storms
 see traffic-storm control

C

cautions for passwords
 encrypting **3-17**
 TACACS+ **3-17**
 CDP
 configuration task lists **30-1**
 enabling on an interface **30-2**
 monitoring and maintaining **30-3**
 overview **30-1**
 cdp enable command **30-2**
 CEF **17-1**
 configuring
 MSFC2 **17-5**
 supervisor engine **17-5**
 examples **17-3**
 Layer 3 switching **17-2**
 packet rewrite **17-2**
 CEF for PFC2
 See CEF
 CGMP **19-1**
 channel-group group
 command **8-7**
 command example **8-8**
 checking
 configuration, system **3-10**
 Cisco Discovery Protocol
 See CDP
 Cisco Group Management Protocol
 See CGMP
 Cisco IOS Unicast Reverse Path Forwarding **21-2**
 CIST **14-14**
 class command **24-42, 24-43**
 class-map command **24-38**
 class map configuration **24-40**
 clear cdp counters command **30-3**
 clear cdp table command **30-3**
 clear counters command **5-17**
 clear interface command **5-17**
 clear mls ip multicast statistics command
 clears IP MMLS statistics **18-23**
 CLI
 accessing **2-1**
 backing out one level **2-5**
 console configuration mode **2-5**
 getting list of commands **2-5**
 global configuration mode **2-5**
 history substitution **2-3**
 interface configuration mode **2-5**
 privileged EXEC mode **2-5**
 ROM monitor **2-6**
 software basics **2-4**
 command line processing **2-3**
 commands, getting list of **2-5**
 Common and Internal Spanning Tree
 See also CIST **14-14**
 Common Spanning Tree
 See CST **14-14**
 community ports **11-1**
 community VLANs **11-2**
 CONFIG_FILE environment variable
 configuration file, viewing **3-26**
 description **3-25**
 config-register command **3-23**
 config terminal command **3-10**

- configuration
 file, saving **3-11**
 interfaces **3-8 to 3-9**
 register
 changing settings **3-23**
 configuration **3-21 to 3-24**
 settings at startup **3-22**
 configuration register boot field
 listing value **3-24**
 modification tasks **3-23**
 configure command **3-9**
 configure terminal command **3-23, 5-2**
 configuring **24-41**
 global parameters
 procedure **3-3**
 sample configuration **3-3 to 3-8**
 interfaces **3-8 to 3-9**
 using configuration mode **3-10**
 congestion avoidance
 see QoS congestion avoidance
 console configuration mode **2-5**
 copy running-config startup-config command **3-11**
 copy system
 running-config nvram
 startup-config command **3-26**
 CoS
 override priority **12-7, 12-8**
 counters
 clearing interface **5-17**
 CST **14-14**
 common spanning tree **14-16**
-
- D**
- dCEF **17-4, 17-6**
 debug commands
 IP MMLS **18-23**
 default configuration
 802.1X **27-5**
- IP MMLS **18-6**
 supervisor engine **3-1**
 UDLD **31-3**
 voice VLAN **12-4**
 VTP **9-5**
 default gateway, configuring **3-11**
 default NDE configuration **32-8**
 default VLAN **7-9**
 description command **5-15**
 destination-ip flow mask **32-3**
 destination-source-ip flow mask **32-3**
 differentiated services codepoint
 See QoS DSCP
 dir command **3-26**
 distributed Cisco Express Forwarding
 See dCEF
 documentation, related **xix**
 document organization **xvii**
 drop thresholds
 see QoS congestion avoidance
 DSCP
 See QoS DSCP
 duplex command **5-8, 5-9**
 duplex mode
 configuring interface **5-7**
-
- E**
- enable command **3-10, 3-23**
 enable mode **2-5**
 enabling
 IP MMLS
 on router interfaces **18-10**
 encapsulation **7-3**
 environmental monitoring
 LED indications **36-6**
 SNMP traps **36-6**
 supervisor engine and switching modules **36-6**
 Syslog messages **36-6**

- using CLI commands **36-4**
- environment variables
- BOOTLDR
 - (example) **3-27**
 - setting **3-26**
- CONFIG_FILE **3-25**
- controlling **3-26**
- viewing **3-26**
- erase startup-config command
 - configuration files cleared with **3-14**
- EtherChannel
 - channel-group group
 - command **8-7**
 - command example **8-8**
 - configuration guidelines **8-5**
 - configuring
 - Layer 2 **8-7**
 - configuring (tasks) **8-6**
 - DFC restriction, see CSCdt27074 in the Release Notes
 - interface port-channel
 - command example **8-7**
 - interface port-channel (command) **8-6**
 - lacp system-priority
 - command example **8-10**
 - Layer 2
 - configuring **8-7**
 - load balancing
 - configuring **8-10**
 - understanding **8-4**
 - modes **8-2**
 - PAgP
 - Understanding **8-3**
 - port-channel interfaces **8-4**
 - port-channel load-balance
 - command **8-10**
 - command example **8-11**
 - STP **8-4**
 - understanding **8-1**
 - EtherChannel Guard
 - See STP EtherChannel Guard
 - Ethernet
 - setting port duplex **5-14**
 - examples
 - configuration
 - interface **3-8 to 3-9**
 - software configuration register **3-21 to 3-24**
 - configuring global parameters **3-3**
 - extended range VLANs **10-2**
 - See VLANs
 - Extensible Authentication Protocol over LAN **27-1**

F

 - fabric switching mode
 - See switch fabric module
 - fastethernet **5-2**
 - fiber-optic, detecting unidirectional links **31-1**
 - filters, NDE
 - destination host filter, specifying **32-18**
 - destination TCP/UDP port, specifying **32-17**
 - overview **32-6**
 - protocol **32-18**
 - source host and destination TCP/UDP port **32-18**
 - Flash memory
 - configuration process **3-25**
 - configuring router to boot from **3-25**
 - loading system image from **3-24**
 - security precautions **3-25**
 - write protection **3-25**
 - flow control **5-13**
 - flow masks
 - IP MLS
 - destination-ip **32-3**
 - destination-source-ip **32-3**
 - interface-destination-source-ip **32-3**
 - ip-full **32-3**
 - ip-interface-full **32-3**
 - minimum **32-11**

overview **32-3**
 flows
 IP MMLS
 completely and partially switched **18-3**
 forward-delay time, STP **14-30**
 frame distribution
 See EtherChannel load balancing

G

gateway, configuring **3-11**
 global configuration mode **2-5**
 global parameters, configuring **3-3**

H

hardware Layer 3 switching
 guidelines **17-5**
 hello time, STP **14-30**
 history
 CLI **2-3**

I

I-BPDU **14-14**
 ICMP unreachable messages **22-1**
 IEEE 802.10 SAID (default) **10-6**
 IEEE 802.1Q
 See 802.1Q
 IEEE 802.1s
 See MST
 IEEE 802.1w
 See MST
 IEEE 802.3ad
 See LACP
 IEEE 802.3Z Flow Control **5-13**
 IGMP
 configuration guidelines **19-7**
 enabling **19-9**
 Internet Group Management Protocol **19-1**
 join messages **19-2**
 leave processing
 enabling **19-11**
 queries **19-3**
 query interval
 configuring **19-11**
 snooping
 fast leave **19-5**
 joining multicast group **19-2**
 leaving multicast group **19-4**
 understanding **19-2**
 snooping querier
 enabling **19-8**
 understanding **19-2**
 IGMPv3 **18-9**
 IGMP v3lite **18-9**
 IGRP, configuring **3-7**
 interface
 command **3-10**
 configuration **3-8 to 3-9**
 configuration mode **2-5**
 Layer 2 modes **7-4**
 number **5-2**
 parameters, configuring **3-8**
 interface-destination-source-ip flow mask **32-3**
 interface port-channel
 command example **8-7**
 interface port-channel (command) **8-6**
 interfaces
 configuring **5-2**
 configuring, duplex mode **5-6**
 configuring, speed **5-6**
 configuring, overview **5-1**
 counters, clearing **5-17**
 descriptive name, adding **5-15**
 displaying information about **5-16**
 maintaining **5-16**

- monitoring **5-16**
- naming **5-15**
- range of **5-4**
- restarting **5-18**
- shutting down
 - task **5-18**
- interfaces command **5-1, 5-2**
- interfaces range command **5-4**
- interfaces range macro command **5-5**
- Interior Gateway Routing Protocol
 - See IGRP, configuring
- Internal Sub Tree Protocol
 - See ISTP **14-14**
- Internet Group Management Protocol
 - See IGMP
- IP
 - default gateway, configuring **3-11**
 - static routes **3-12**
- IP accounting, IP MMLS and **18-8**
- IP addresses
 - assigned by BOOTP protocol **3-13**
 - set to default **3-14**
- IP CEF
 - topology (figure) **17-4**
- ip flow-export destination command **32-15**
- ip flow-export source command **32-15**
- ip-full flow mask **32-3**
- ip http server **1-1**
- ip-interface-full flow mask **32-3**
- IP MLS
 - aging-time **32-11**
 - flow masks
 - destination-ip **32-3**
 - destination-source-ip **32-3**
 - interface-destination-source-ip **32-3**
 - ip-full **32-3**
 - ip-interface-full **32-3**
 - minimum **32-11**
 - overview **32-3**
- NDE
 - See NDE
- IP MMLS
 - cache, overview **18-2**
 - configuration guideline **18-7**
 - debug commands **18-23**
 - default configuration **18-6**
 - enabling
 - on router interfaces **18-10**
 - flows
 - completely and partially switched **18-3**
 - Layer 3 MLS cache **18-2**
 - overview **18-2**
 - packet rewrite **18-3**
 - router
 - displaying interface information **18-14**
 - enabling globally **18-9**
 - enabling on interfaces **18-10**
 - multicast routing table, displaying **18-17**
 - PIM, enabling **18-9**
 - switch
 - statistics, clearing **18-23**
 - unsupported features **18-8**
- IP multicast
 - IGMP snooping and **19-8**
 - overview **19-1**
- IP multicast MLS
 - See IP MMLS
- ip multicast-routing command
 - enabling IP multicast **18-9**
- IP phone
 - configuring **12-5**
- ip pim command
 - enabling IP PIM **18-9, 18-10**
- IPsec **26-2**
- ISL encapsulation **7-3**
- ISL trunks **7-2**
- isolated port **11-1**
- isolated VLANs **11-2**

ISTP **14-14**

J

join messages, IGMP **19-2**

jumbo frames **5-10**

K

keyboard shortcuts **2-3**

L

LACP

 system ID **8-4**

Layer 2

 configuring interfaces **7-6**

 access port **7-13**

 trunk **7-7**

 defaults **7-4**

 interface modes **7-4**

 show interfaces **5-12, 5-13, 7-6, 7-12**

 switching

 understanding **7-1**

 trunks

 understanding **7-2**

VLAN

 interface assignment **10-12**

Layer 2 Interfaces

 configuring **7-1**

Layer 2 protocol tunneling

 configuring Layer 2 tunnels **13-7**

 overview **13-6**

Layer 3

 IP MMLS and MLS cache **18-2**

Layer 3 switched packet rewrite

 CEF **17-2**

Layer 3 switching

CEF **17-2**

Layer 4 port operations (ACLs) **22-3**

leave processing, IGMP

 enabling **19-11**

link negotiation **5-8**

load balancing **14-14**

logical operation unit

 See LOU

loop guard

 See STP loop guard

LOU

 description **22-3**

 determining maximum number of **22-3**

M

MAC address

 adding to BOOTP configuration file **3-14**

MAC address-based blocking **21-1**

main-cpu command **6-6**

mapping 802.1Q VLANs to ISL VLANs **10-12**

markdown

 see QoS markdown

marking

 see QoS

maximum aging time, STP **14-31**

microflow policing rule

 see QoS policing

MLS

 configuring threshold **18-12**

MSFC

 threshold **18-12**

mls aging command

 configuring IP MLS **32-12**

mls flow command

 configuring IP MLS **32-10, 32-11, 32-14**

mls ip multicast command

 enabling IP MMLS **18-10, 18-11, 18-12, 18-13, 18-14, 18-20, 18-21**

- mls nde flow command
 configuring a host and port filter **32-18**
 configuring a host flow filter **32-18**
 configuring a port filter **32-17**
 configuring a protocol flow filter **32-18**
 mls nde src_address command **32-9, 32-13**
 monitoring
 traffic suppression **28-5**
- MST **14-14**
 boundary ports **14-18**
 configuration **14-17**
 configuring **14-32**
 edge ports **14-18**
 enabling **14-32**
 hop count **14-19**
 instances **14-17**
 interoperability **14-15**
 interoperability with PVST+ **14-14**
 link type **14-19**
 master **14-18**
 message age **14-19**
 regions **14-17**
- MSTP
 M-record **14-14**
 M-tree **14-14**
 MTU size (default) **10-6**
 multicast
 IGMP snooping and **19-8**
 NetFlow statistics **32-1**
 non-RPF **18-5**
 overview **19-1**
 RGMP **20-2**
 multicast, displaying routing table **18-17**
 multicast groups
 joining **19-2**
 leaving **19-4**
 multicast multilayer switching
 See IP MMLS
 multicast RPF **18-2**
- multicast storms
 see traffic-storm control
- multilayer switch feature card
 see MSFC
- multiple forwarding paths **14-14**
 multiple path RPF check **21-2**
 Multiple Spanning Tree
 See MST
- Multiple Spanning Tree Protocol
 See MSTP **14-14**
-
- N**
- native vlan **7-10**
 NDE
 configuration, displaying **32-19**
 displaying configuration **32-19**
 enabling **32-8**
 filters
 destination host, specifying **32-18**
 destination TCP/UDP port, specifying **32-17**
 overview **32-6**
 protocol, specifying **32-18**
 source host and destination TCP/UDP port,
 specifying **32-18**
 multicast **32-1**
 overview **32-1**
 specifying
 destination host filters **32-18**
 destination TCP/UDP port filters **32-18**
 protocol filters **32-18**
 NDE configuration, default **32-8**
 NetFlow Data Export
 See NDE
- network fault tolerance **14-14**
 network management
 configuring **30-1**
 non-RPF multicast **18-5**
 nonvolatile random-access memory

See NVRAM
 normal-range VLANs
 See VLANs
 NVRAM
 saving settings **3-11**

O

OIR **5-15**
 online diagnostics
 configuring **36-2**
 overview **36-1**
 running tests **36-4**
 understanding **36-1**
 online insertion and removal
 See OIR
 operating system image
 See system image
 out of profile
 see QoS out of profile

P

packet rewrite
 CEF **17-2**
 IP MMLS and **18-3**
 packets
 multicast **23-3**
 PAgP
 understanding **8-3**
 passwords
 configuring
 enable password **3-15**
 enable secret **3-15**
 line password **3-16**
 static enable password **3-15**
 TACACS+ **3-16**
 TACACS+ (caution) **3-17**
 encrypting **3-17**
 (caution) **3-17**
 recovering lost enable passwords **3-19**
 PBR **1-2, 16-2**
 PFC2
 NetFlow
 table, displaying entries **17-6**
 PIM, IP MMLS and **18-9**
 police command **24-45**
 policing
 See QoS policing
 policy **24-37**
 policy-based routing
 See PBR
 policy map **24-41**
 attaching to an interface **24-48**
 policy-map command **24-38, 24-42**
 Port Aggregation Protocol
 see PAgP
 port-based authentication
 authentication server
 defined **27-2**
 RADIUS server **27-2**
 client, defined **27-2**
 configuration guidelines **27-6**
 configuring
 initializing authentication of a client **27-11**
 manual reauthentication of a client **27-11**
 quiet period **27-11**
 RADIUS server **27-10**
 RADIUS server parameters on the switch **27-8**
 switch-to-authentication-server retransmission time **27-13**
 switch-to-client EAP-request frame retransmission time **27-13**
 switch-to-client frame-retransmission number **27-14**
 switch-to-client retransmission time **27-12**
 default configuration **27-5**
 described **27-1**

- device roles **27-2**
- displaying statistics **27-15**
- EAPOL-start frame **27-3**
- EAP-request/identity frame **27-3**
- EAP-response/identity frame **27-3**
- enabling
 - 802.1X authentication **27-7, 27-8**
 - periodic reauthentication **27-10**
- encapsulation **27-2**
- initiation and message exchange **27-3**
- method lists **27-7**
- ports
 - authorization state and dot1x port-control command **27-4**
 - authorized and unauthorized **27-4**
- resetting to default values **27-15**
- switch
 - as proxy **27-2**
 - RADIUS client **27-2**
 - topologies, supported **27-4**
- port-based QoS features
 - see QoS
- port-channel
 - see EtherChannel
- port-channel load-balance
 - command **8-10**
 - command example **8-10, 8-11**
- port cost, STP **14-27**
- port debounce timer
 - disabling **5-14**
 - displaying **5-14**
 - enabling **5-14**
- PortFast
 - See STP PortFast
- PortFast BPDU filtering
 - See STP PortFast BPDU filtering
- port negotiation **5-8**
- port priority, STP **14-25**
- ports
 - secure **28-1**
 - setting the debounce timer **5-14**
 - port security
 - aging **28-5**
 - configuring **28-3**
 - default configuration **28-2**
 - described **28-1**
 - displaying **28-6**
 - violations **28-2**
 - with other features **28-2**
 - power management
 - enabling/disabling redundancy **36-2**
 - overview **36-1**
 - powering modules up or down **36-3**
 - system power requirements, nine-slot chassis **36-4**
 - primary VLANs **11-2**
 - priority
 - overriding CoS **12-7, 12-8**
 - private VLANs **11-1**
 - community VLANs **11-2**
 - configuration guidelines **11-2**
 - configuring **11-4**
 - host ports **11-8**
 - promiscuous ports **11-9**
 - routing secondary VLAN ingress traffic **11-7**
 - secondary VLANs with primary VLANs **11-6**
 - VLANs as private **11-5**
 - isolated VLANs **11-2**
 - ports
 - community **11-1**
 - isolated **11-1**
 - promiscuous **11-1**
 - primary VLANs **11-2**
 - secondary VLANs **11-2**
 - trunks **11-2**
 - privileged EXEC mode **2-5**
 - privileges
 - changing default **3-18**
 - configuring

- multiple levels [3-17](#)
 - privilege level [3-18](#)
 - exiting [3-19](#)
 - logging in [3-18](#)
 - procedures
 - global parameters, configuring [3-3 to 3-8](#)
 - interfaces, configuring [3-8 to 3-9](#)
 - using configuration mode [3-10](#)
 - promiscuous ports [11-1](#)
 - protocol tunneling
 - See Layer 2 protocol tunneling [13-6](#)
 - pruning, VTP
 - See VTP, pruning
 - PVLANs
 - See private VLANs
 - PVRST
 - See Rapid-PVST [14-13](#)
-
- Q**
 - QoS ACL [24-14](#)
 - attaching [24-17](#)
 - QoS classification (definition) [24-3](#)
 - QoS congestion avoidance
 - definition [24-3](#)
 - receive queue [24-11](#)
 - QoS CoS
 - and ToS final L3 Switching Engine values [24-18](#)
 - and ToS final values from L3 Switching Engine [24-18](#)
 - definition [24-2](#)
 - port value, configuring [24-56](#)
 - QoS default configuration [24-21, 25-1](#)
 - QoS definitions [24-2](#)
 - QoS drop thresholds
 - see QoS congestion avoidance
 - QoS DSCP
 - definition [24-2](#)
 - internal values [24-14](#)
 - maps, configuring [24-51](#)
 - QoS dual transmit queue thresholds
 - configuring [24-57](#)
 - QoS Ethernet egress port
 - feature summary [24-9](#)
 - scheduling [24-20](#)
 - scheduling, congestion avoidance, and marking [24-8, 24-18](#)
 - QoS Ethernet ingress port
 - classification, marking, scheduling, and congestion avoidance [24-5](#)
 - feature summary [24-8](#)
 - marking, scheduling, congestion avoidance, and classification [24-9](#)
 - scheduling [24-11](#)
 - scheduling and congestion avoidance [24-10](#)
 - QoS feature set summary [24-8](#)
 - QoS final L3 Switching Engine CoS and ToS values [24-18](#)
 - QoS internal DSCP values [24-14](#)
 - QoS L3 Switching Engine
 - classification, marking, and policing [24-6, 24-13](#)
 - feature summary [24-9](#)
 - QoS labels (definition) [24-2](#)
 - QoS mapping
 - CoS values to DSCP values [24-51](#)
 - DSCP markdown values [24-22, 24-25, 24-53](#)
 - DSCP mutation [24-50](#)
 - DSCP values to CoS values [24-55](#)
 - IP precedence values to DSCP values [24-53](#)
 - QoS markdown [24-15](#)
 - QoS marking [24-21](#)
 - definition [24-3](#)
 - trusted ports [24-10](#)
 - untrusted ports [24-10](#)
 - QoS MSFC
 - marking [24-7](#)
 - QoS multilayer switch feature card [24-9](#)
 - QoS out of profile [24-15](#)
 - QoS policing
 - definition [24-4](#)

microflow, enabling for nonrouted traffic **24-32, 24-33**
QoS policing rule **24-15**
 aggregate **24-16**
 creating **24-37**
 microflow **24-16**
QoS port
 trust state **24-56**
QoS port-based or VLAN-based **24-33**
QoS port keywords **24-9**
QoS queues
 transmit, allocating bandwidth between **24-67**
QoS receive queue **24-10, 24-66**
 drop thresholds **24-13**
 tail-drop thresholds
 configuring **24-59**
QoS scheduling (definition) **24-3**
QoS single-receive, dual-transmit queue ports
 configuring **24-62**
QoS statistics data export **25-1**
 configuring **25-2**
 configuring destination host **25-7**
 configuring time interval **25-6, 25-9**
QoS strict priority receive queue **24-10**
QoS ToS
 and CoS final values from L3 Switching Engine **24-18**
 definition **24-2**
QoS traffic flow through QoS features **24-4**
QoS transmit queue
 size ratio **24-67, 24-68**
QoS transmit queues **24-19, 24-64**
QoS triple transmit queue WRED drop thresholds **24-60**
QoS trust-cos
 port keyword **24-9**
QoS trust-dscp
 port keyword **24-9**
QoS trust-iprec
 port keyword **24-9**
QoS untrusted port keyword **24-9**
QoS VLAN-based or port-based **24-17, 24-33**

QoS WRED drop thresholds **24-60**
 queries, IGMP **19-3**

R

range
 command **5-4**
 macro **5-5**
 of interfaces **5-4**
Rapid-PVST
 enabling **14-31**
 overview **14-13**
Rapid Spanning Tree
 See RSTP **14-12**
rapid spanning tree protocol **14-14**
receive queues
 see QoS receive queues
reduced MAC address **14-2**
redundancy (RPR+) **6-1**
 configuring **6-5**
 configuring supervisor engine **6-5**
 displaying supervisor engine configuration **6-7**
 redundancy command **6-6**
 route processor redundancy plus **6-2**
related documentation **xix**
reload command **3-23**
reserved-range VLANs
 See VLANs
rewrite, packet
 CEF **17-2**
 IP MMLS **18-3**
RGMP **20-1**
 overview **20-2**
 packet types **20-2**
RIF cache monitoring **5-16**
rommon command **3-24**
ROM monitor
 boot process and **3-20**
CLI **2-6**

- root bridge, STP **14-23**
- root guard
See STP root guard
- route processor redundancy
See redundancy (RPR+)
- router-port group management protocol
See RGMP
- routing table, multicast **18-17**
- RPF
failure **18-5**
multicast **18-2**
non-RPF multicast **18-5**
unicast **21-2**
- RPR+
See redundancy (RPR+)
- RSTP **14-14**
port roles **14-12**
port states **14-13**
-
- S**
- SAID **10-6**
- sample configuration **3-2 to 3-10**
- Sampled NetFlow
description **32-7**
- saving the configuration file **3-11**
- scheduling
see QoS
- secondary VLANs **11-2**
- secure ports, configuring **28-1**
- security
configuring **21-1, 22-1, 26-1**
port **28-1**
- security precautions with Flash memory card **3-25**
- serial interfaces
clearing **5-17**
synchronous
maintaining **5-17**
- service-policy command **24-38**
- service-policy input command **24-48, 24-51**
- set power redundancy enable/disable command **36-2**
- setup command **3-2**
- show boot command **3-26**
- show bootvar command **3-26**
- show catalyst6000 chassis-mac-address command **14-3**
- show cdp command **30-2, 30-3**
- show cdp entry command **30-3**
- show cdp interface command **30-3**
- show cdp neighbors command **30-3**
- show cdp traffic command **30-3**
- show configuration command **5-15**
- show debugging command **30-3**
- show eobc command **5-16**
- show hardware command **5-3**
- show history command **2-4**
- show ibc command **5-16**
- show interfaces command **5-2, 5-12, 5-13, 5-15, 5-16, 7-6, 7-12**
clearing interface counters **5-17**
displaying, interface type numbers **5-2**
displaying, speed and duplex mode **5-9**
- show ip flow export command
displaying NDE export flow IP address and UDP port **32-16**
- show ip interface command
displaying IP MMLS interfaces **18-15**
- show ip mroute command
displaying IP multicast routing table **18-17**
- show ip pim interface command
displaying IP MMLS router configuration **18-15**
- show mls aging command **32-12**
- show mls entry command **17-6**
- show mls ip multicast group command
displaying IP MMLS group **18-18, 18-21**
- show mls ip multicast interface command
displaying IP MMLS interface **18-18, 18-21**
- show mls ip multicast source command
displaying IP MMLS source **18-18, 18-21**
- show mls ip multicast statistics command

- displaying IP MMLS statistics **18-18, 18-21**
- show mls ip multicast summary
 - displaying IP MMLS configuration **18-18, 18-21**
- show mls nde command **32-19**
 - displaying NDE flow IP address **32-16**
- show mls rp command
 - displaying IP MLS configuration **32-11**
- show module command **6-7**
- show protocols command **5-16**
- show rif command **5-16**
- show running-config command **3-10, 5-15, 5-16**
- show startup-config command **3-11**
- show version command **3-9, 3-23, 3-24, 5-16**
- shutdown command **5-18**
- shutdown interfaces
 - result **5-18**
- Single Spanning Tree
 - See SST **14-14**
- slot number, description **5-1**
- SNMP
 - support and documentation **1-1**
- snooping
 - See IGMP snooping
- software configuration register functions **3-21 to 3-24**
- source-only-ip flow mask **32-3**
- source specific multicast with IGMPv3, IGMP v3lite, and URD **18-9**
- SPAN
 - configuration guidelines **33-5**
 - configuring **33-8**
 - destinations **33-10**
 - sources **33-9**
 - VLAN filtering **33-10**
 - overview **33-1**
- spanning-tree backbonefast
 - command **15-13, 15-14**
 - command example **15-13, 15-14**
- spanning-tree cost
 - command **14-27**
- spanning-tree portfast
 - command example **14-27, 14-28**
- spanning-tree portfast bpdu-guard
 - command **15-11**
- spanning-tree port-priority
 - command **14-25, 14-26**
- spanning-tree uplinkfast
 - command **15-12**
 - command example **15-12**
- spanning-tree vlan
 - command **14-21, 14-22, 14-24, 14-25, 15-14**
 - command example **14-21, 14-23, 14-24, 14-25**
- spanning-tree vlan cost
 - command **14-27**
- spanning-tree vlan forward-time
 - command **14-30**
 - command example **14-31**
- spanning-tree vlan hello-time
 - command **14-30**
 - command example **14-30**
- spanning-tree vlan max-age
 - command **14-31**
 - command example **14-31**
- spanning-tree vlan port-priority
 - command **14-25**
 - command example **14-26**
- spanning-tree vlan priority
 - command **14-29**
 - command example **14-29**
- speed
 - configuring interface **5-7**
- speed command **4-2, 5-7**
- SST **14-14**
 - interoperability **14-15**
- static route, configuring **3-12**
- statistics
 - 802.1X **27-15**

storm control
 see traffic-storm control

STP
 configuring **14-20**
 bridge priority **14-28**
 enabling **14-21, 14-22**
 forward-delay time **14-30**
 hello time **14-30**
 maximum aging time **14-31**
 port cost **14-27**
 port priority **14-25**
 root bridge **14-23**
 secondary root switch **14-24**
 defaults **14-19**
 EtherChannel **8-4**
 understanding **14-1**
 802.1Q Trunks **14-11**
 Blocking State **14-7**
 BPDUs **14-3**
 disabled state **14-11**
 forwarding state **14-10**
 learning state **14-9**
 listening state **14-8**
 overview **14-2**
 port states **14-5**
 protocol timers **14-4**
 root bridge election **14-4**
 topology **14-5**

STP BackboneFast
 and MST **14-15**
 configuring **15-13**
 figure
 adding a switch **15-7**
 spanning-tree backbonefast
 command **15-13, 15-14**
 command example **15-13, 15-14**
 understanding **15-4**

STP BPDU Guard
 and MST **14-15**

configuring **15-11**
 spanning-tree portfast bpdu-guard
 command **15-11**
 understanding **15-2**
 STP bridge ID **14-2**
 STP EtherChannel guard **15-6**
 STP loop guard
 and MST **14-15**
 configuring **15-15**
 overview **15-6**
 STP PortFast
 and MST **14-15**
 BPDU filter
 configuring **15-10**
 BPDU filtering **15-2**
 configuring **15-8**
 spanning-tree portfast
 command **15-8, 15-9**
 command example **15-8**
 understanding **15-2**
 STP Portfast BPDU filtering
 and MST **14-15**
 STP root guard **15-6, 15-14**
 and MST **14-15**
 STP UplinkFast
 and MST **14-15**
 configuring **15-12**
 spanning-tree uplinkfast
 command **15-12**
 command example **15-12**
 understanding **15-3**
 strict-priority queue
 see QoS strict priority

supervisor engine
 configuring **3-1**
 default configuration **3-1**
 default gateways **3-11**
 environmental monitoring **36-4**
 redundancy **6-1**

ROM monitor **3-20**
 startup configuration **3-20**
 static routes **3-12**
 synchronizing configurations **6-6**
 supervisor engine redundancy
 configuring **6-5**
 supervisor engines
 displaying redundancy configuration **6-7**
Switched Port Analyzer
 See SPAN
 switch fabric module **4-2**
 configuring **4-4**
 monitoring **4-4**
 switchport
 configuring **7-13**
 example **7-12**
 show interfaces **5-12, 5-13, 7-6, 7-12**
 switchport access vlan **7-9, 7-13**
 example **7-14**
 switchport mode access **7-4, 7-13**
 example **7-14**
 switchport mode dynamic **7-8**
 switchport mode dynamic auto **7-4**
 switchport mode dynamic desirable **7-4**
 default **7-4**
 example **7-12**
 switchport mode trunk **7-4, 7-8**
 switchport nonegotiate **7-4**
 switchport trunk allowed vlan **7-10**
 switchport trunk encapsulation **7-8**
 switchport trunk encapsulation dot1q **7-3**
 example **7-12**
 switchport trunk encapsulation isl **7-3**
 switchport trunk encapsulation negotiate **7-3**
 default **7-4**
 switchport trunk native vlan **7-10**
 switchport trunk pruning vlan **7-11**
 system
 configuration register

configuration **3-21 to 3-24**
 settings at startup **3-22**
 configuring global parameters **3-3 to 3-8**
 system image
 determining if and how to load **3-22**
 loading from Flash **3-24**

T

TACACS+ **21-1, 22-1, 26-1**
TCP Intercept **21-2**
 Telnet
 accessing CLI **2-2**
 thresholds
 see QoS congestion avoidance
 traffic-storm control
 command
 broadcast **29-2**
 described **29-1**
 monitoring **29-3**
 thresholds **29-1**
 traffic suppression
 see traffic-storm control
 translational bridge numbers (defaults) **10-6**
 transmit queues
 see QoS transmit queues
 trunks **7-2**
 802.1Q Restrictions **7-5**
 allowed VLANs **7-10**
 configuring **7-7**
 default interface configuration **7-7**
 default VLAN **7-9**
 different VTP domains **7-3**
 encapsulation **7-3**
 native vlan **7-10**
 private VLANs **11-2**
 to non-DTP device **7-4**
 VLAN 1 minimization **7-11**
 trust-dscp

-
- see QoS trust-dscp
- trust-iprec**
- see QoS trust-iprec
- tunneling, 802.1Q
- See 802.1Q **13-1**
-
- U**
- UDLD**
- default configuration **31-3**
 - enabling
 - globally **31-3**
 - on ports **31-4**
 - overview **31-1**
- unauthorized ports with 802.1X **27-4**
- unicast RPF** **21-2**
- unicast storms
- see traffic-storm control
- UniDirectional Link Detection Protocol**
- see UDLD
- untrusted
- see QoS trust-cos
 - see QoS untrusted
- UplinkFast**
- See STP UplinkFast
- URD** **18-9**
- User-Based Rate Limiting** **24-16, 24-45**
- user EXEC mode** **2-5**
-
- V**
- VACLs** **23-1**
- configuring **23-4**
 - examples **23-8**
- Layer 3 VLAN interfaces **23-7**
- Layer 4 port operations **22-2**
- logging
- configuration example **23-9**
- configuring **23-8**
- restrictions **23-8**
- MAC address based **23-4**
- multicast packets **23-3**
- overview **23-1**
- SVIs **23-7**
- WAN interfaces **23-1**
- virtual LAN
- See VLANs
- vlan**
- command **10-10, 10-12, 32-9, 32-10, 32-13, 33-8**
 - command example **10-11**
- vlan database**
- command **10-10, 10-12, 32-9, 32-10, 32-13, 33-8**
 - example **10-11**
- vlan mapping dot1q**
- command **10-13**
 - command example **10-13**
- VLANs**
- allowed on trunk **7-10**
 - configuration guidelines **10-8**
 - configuration options
 - global configuration mode **10-9**
 - VLAN database mode **10-9**
 - configuring **10-1**
 - configuring (tasks) **10-9**
 - defaults **10-6**
 - extended range **10-2**
 - ID (default) **10-6**
 - interface assignment **10-12**
 - name (default) **10-6**
 - normal range **10-2**
 - private
 - See private VLANs
 - reserved range **10-2**
 - support for 4,096 VLANs **10-2**
 - token ring **10-3**
 - trunks
 - understanding **7-2**

understanding **10-1**
VLAN 1 minimization **7-11**
VTP domain **10-3**
VLAN Trunking Protocol
See VTP

voice VLAN

Cisco 7960 phone, port connections **12-1**
configuration guidelines **12-4**
configuring IP phone for data traffic
 override CoS of incoming frame **12-7, 12-8**
configuring ports for voice traffic in
 802.1Q frames **12-5**
connecting to an IP phone **12-5**
default configuration **12-4**
overview **12-1**

VTP

advertisements **9-2**
client, configuring **9-8**
configuration guidelines **9-5**
default configuration **9-5**
disabling **9-8**
domains **9-2**
 VLANs **10-3**
modes
 client **9-2**
 server **9-2**
 transparent **9-2**
monitoring **9-10**
overview **9-1**
pruning
 configuration **7-11**
 configuring **9-7**
 overview **9-3**
server, configuring **9-8**
statistics **9-10**
transparent mode, configuring **9-8**
version 2
 enabling **9-7**
 overview **9-3**

W

web browser interface **1-1**
WRED **24-60**