

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

General Information

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

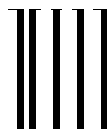
Document Information

Document Title:	Catalyst 4500 Series, Catalyst 2948G, Catalyst 2980G Switches Software Configuration Guide		
Part Number:	78-15486-01	S/W Release (if applicable):	7.7
On a scale of 1–5 (5 being the best), please let us know how we rate in the following areas:			
____ The document is complete.	____ The information is accurate.		
____ The information is well organized.	____ The information I wanted was easy to find.		
____ The document is written at my technical level of understanding.	____ The information I found was useful to my job.		
Please comment on our lowest scores: _____			

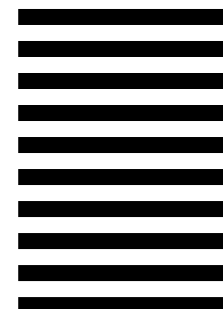
Mailing Information

Organization	Date	
Contact Name		
Mailing Address		
City	State/Province	Zip/Postal Code
Country	Phone ()	Extension
E-mail	Fax ()	
May we contact you further concerning our documentation? ____ Yes ____ No		
You can also send us your comments by e-mail to bug-doc@cisco.com , or by fax to 408-527-8089 .		

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



NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES



BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 4631 SAN JOSE CA

POSTAGE WILL BE PAID BY ADDRESSEE

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





CISCO Confidential - DRAFT



Catalyst 4500 Series, Catalyst 2948G, Catalyst 2980G Switches Software Configuration Guide

Release 7.7

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-7815486=
Text Part Number: 78-15486-01



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

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

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

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

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

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

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0303R)

Catalyst 4500 Series, Catalyst 2948G, Catalyst 2980G Switches Software Configuration Guide
Copyright © 2000-2003, Cisco Systems, Inc.
All rights reserved.



Preface xxiii

Audience xxiii

Organization xxiii

Related Documentation xxv

Conventions xxvi

Obtaining Documentation xxvii

 Cisco.com xxvii

 Documentation CD-ROM xxvii

 Ordering Documentation xxvii

 Documentation Feedback xxviii

Obtaining Technical Assistance xxviii

 Cisco.com xxviii

 Technical Assistance Center xxix

Obtaining Additional Publications and Information xxx

CHAPTER 1

Product Overview 1-1

Catalyst 4000 Family Switches 1-1

Catalyst 2948G Switch 1-2

Catalyst 2980G Switch 1-3

Supervisor Engine Software 1-3

CHAPTER 2

Using the Command-Line Interface 2-1

Switch CLI Overview 2-1

Accessing the Switch CLI 2-2

 Accessing the CLI Through the Console Port 2-2

 Accessing the CLI Through Telnet 2-3

Switch CLI Command Modes 2-3

Accessing Help 2-4

Command-Line Editing 2-5

History Substitution 2-6

Abbreviating a Command 2-6

Completing a Partial Command 2-6

Scrolling Through Command Output 2-6

CISCO Confidential - DRAFT

Using Command Aliases	2-7
Specifying Modules, Ports, and VLANs	2-7
Specifying MAC Addresses	2-8
Specifying IP Addresses, Host Names, and IP Aliases	2-8
ROM Monitor CLI	2-9
Example of a Catalyst 4003 Bootup Display	2-9

CHAPTER 3

Configuring the Switch IP Address and Default Gateway	3-1
Understanding How the Switch Management Interfaces Work	3-1
Understanding How Automatic IP Configuration Works	3-2
Automatic IP Configuration Overview	3-2
Understanding DHCP	3-3
Understanding RARP	3-4
Preparing to Configure the IP Address and Default Gateway	3-4
Default IP Address and Default Gateway Configuration	3-5
Setting the In-Band (sc0) Interface IP Address	3-5
Setting the Management Ethernet (me1) Interface IP Address	3-6
Configuring Default Gateways	3-6
Configuring the SLIP (sl0) Interface on the Console Port	3-8
Using DHCP or RARP to Obtain an IP Address Configuration	3-9
Renewing and Releasing a DHCP-Assigned IP Address	3-10

CHAPTER 4

Configuring Ethernet and Fast Ethernet Switching	4-1
Understanding How Ethernet Works	4-1
Ethernet Overview	4-1
Switching Frames Between Segments	4-2
Building the Address Table	4-2
Default Ethernet and Fast Ethernet Configurations	4-2
Configuring Ethernet and Fast Ethernet Ports	4-3
Setting Ethernet and Fast Ethernet Port Names	4-3
Setting Ethernet and Fast Ethernet Port Priority Levels	4-4
Setting Ethernet and Fast Ethernet Port Speeds	4-4
Setting Ethernet and Fast Ethernet Port Duplex Modes	4-5
Setting Ethernet and Fast Ethernet Port Debounce Timers	4-6
Configuring errdisable State Ethernet and Fast Ethernet Port Timeout Periods	4-7
Checking Ethernet and Fast Ethernet Port Connectivity	4-8

*CISCO Confidential - DRAFT***CHAPTER 5****Configuring Gigabit Ethernet Switching 5-1**

- Understanding How Gigabit Ethernet Works 5-1
 - Understanding How Gigabit Ethernet Flow Control Works 5-1
 - Understanding How Port Negotiation Works 5-3
 - Understanding How Oversubscribed Gigabit Ethernet Works 5-3
- Default Gigabit Ethernet Configuration 5-6
- Configuring Gigabit Ethernet Ports 5-7
 - Assigning Gigabit Ethernet Port Names 5-7
 - Configuring Gigabit Ethernet Port Priority Levels 5-7
 - Configuring Flow Control on Gigabit Ethernet Ports 5-8
 - Enabling Port Negotiation on Gigabit Ethernet Ports 5-9
 - Disabling Port Negotiation 5-9
 - Configuring errdisable State Gigabit Ethernet Port Timeout Periods 5-9
 - Checking Gigabit Ethernet Port Connectivity 5-10

CHAPTER 6**Configuring Fast EtherChannel and Gigabit EtherChannel 6-1**

- Understanding How EtherChannel Works 6-1
 - EtherChannel Overview 6-2
 - Understanding Frame Distribution 6-2
 - Hardware Support for EtherChannel 6-2
- PAgP and LACP 6-2
- EtherChannel Configuration Guidelines and Restrictions 6-3
 - Guidelines for Configuring a Port 6-3
 - Guidelines for Configuring VLANs and Trunks 6-4
 - EtherChannel Interaction with other Features 6-4
- Understanding the PAgP 6-5
 - PAgP Modes 6-5
 - Understanding Administrative Groups and EtherChannel IDs 6-6
- Configuring EtherChannel Using PAgP 6-6
 - Creating an EtherChannel 6-7
 - Defining an EtherChannel Administrative Group 6-7
 - Setting the EtherChannel Spanning Tree Port Cost 6-8
 - Setting the EtherChannel Spanning Tree Port VLAN Cost 6-9
 - Removing an EtherChannel Bundle 6-9
 - Displaying EtherChannel Configuration Information 6-10
 - Displaying EtherChannel Traffic Statistics 6-11
 - Displaying EtherChannel PAgP Statistics 6-12
- EtherChannel Configuration Examples 6-12

CISCO Confidential - DRAFT

Configuration Example of a Four-Port Fast EtherChannel	6-12
Configuration Example of Two-Port Gigabit EtherChannel	6-14
Understanding the LACP	6-16
LACP Modes	6-16
LACP Parameters	6-17
Configuring EtherChannel Using LACP	6-18
Specifying the EtherChannel Protocol	6-18
Specifying the System Priority	6-19
Specifying the Port Priority	6-19
Specifying an Administrative Key Value	6-19
Changing the Channel Mode	6-20
Specifying the Channel Path Cost	6-21
Specifying the Channel VLAN Cost	6-21
Clearing LACP Statistics	6-21
Displaying EtherChannel Traffic Utilization	6-21
Disabling an EtherChannel	6-22
Displaying Spanning Tree-Related Information for EtherChannels	6-22

CHAPTER 7

Configuring Spanning Tree 7-1

Understanding How STPs Work	7-2
Understanding How a Topology Is Created	7-2
Understanding How a Switch or Port Becomes the Root Switch or Root Port	7-3
Understanding BPDUs	7-3
Understanding Spanning Tree Port States	7-4
Understanding How PVST+ and MISTP Modes Work	7-10
PVST+ Mode	7-11
Rapid PVST+	7-11
MISTP Mode	7-11
MISTP-PVST+ Mode	7-12
Understanding How Bridge Identifiers Work	7-12
MAC Address Allocation	7-12
MAC Address Reduction	7-12
Understanding How MST Works	7-13
Rapid Spanning Tree Protocol	7-14
MST-to-SST Interoperability	7-16
Common Spanning Tree	7-17
MST Instances	7-17
MST Configuration	7-17
MST Region	7-18

CISCO Confidential - DRAFT

Message Age and Hop Count	7-19
MST-to-PVST+ Interoperability	7-19
Understanding How BPDU Skewing Works	7-20
Using PVST+	7-21
Default PVST+ Configuration	7-21
Setting the PVST+ Bridge ID Priority	7-21
Configuring the PVST+ Port Cost	7-23
Configuring PVST+ Port Priority	7-23
Configuring the PVST+ Default Port Cost Mode	7-24
Configuring the PVST+ Port VLAN Cost	7-25
Configuring the PVST+ Port VLAN Priority	7-25
Disabling the PVST+ Mode on a VLAN	7-26
Using Rapid PVST+	7-26
Using MISTP-PVST+ or MISTP	7-28
Default MISTP Mode Configuration	7-28
Setting the MISTP-PVST+ Mode or MISTP Mode	7-29
Configuring the MISTP Bridge ID Priority	7-30
Enabling an MISTP Instance	7-33
Mapping VLANs to an MISTP Instance	7-34
Disabling MISTP-PVST+ or MISTP	7-36
Configuring a Root Switch	7-36
Configuring a Primary Root Switch	7-36
Configuring a Secondary Root Switch	7-37
Configuring a Root Switch to Improve Convergence	7-38
Using Root Guard—Preventing Switches from Becoming Root	7-39
Configuring Spanning Tree Timers	7-40
Configuring the Hello Time	7-40
Configuring the Forward Delay Time	7-41
Configuring the Maximum Aging Time	7-41
Configuring MST	7-42
Enabling MST	7-42
Mapping and Unmapping VLANs to an MST Instance	7-50
Configuring Spanning Tree BPDU Skewing	7-53

CHAPTER 8

Configuring Spanning Tree PortFast, BPDU Guard, BPDU Filter, UplinkFast, BackboneFast, and Loop Guard 8-1

Understanding How PortFast Works	8-1
Understanding How PortFast BPDU Guard Works	8-2

CISCO Confidential - DRAFT

Understanding How PortFast BPDU Filtering Works	8-2
Understanding How UplinkFast Works	8-3
Understanding How BackboneFast Works	8-4
Understanding How Loop Guard Works	8-6
Configuring PortFast	8-8
Enabling PortFast on an Access Port	8-8
Enabling PortFast on a Trunk Port	8-9
Disabling PortFast	8-10
Resetting PortFast	8-10
Configuring PortFast BPDU Guard	8-11
Enabling PortFast BPDU Guard	8-11
Disabling PortFast BPDU Guard	8-12
Configuring PortFast BPDU Filtering	8-13
Enabling PortFast BPDU Filtering	8-13
Disabling PortFast BPDU Filtering	8-14
Configuring UplinkFast	8-14
Enabling UplinkFast	8-14
Disabling UplinkFast	8-16
Configuring BackboneFast	8-16
Enabling BackboneFast	8-17
Displaying BackboneFast Statistics	8-17
Disabling BackboneFast	8-18
Configuring Loop Guard	8-18
Enabling Loop Guard	8-18
Disabling Loop Guard	8-19

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
Default VTP Configuration	9-5
VTP Configuration Guidelines	9-5
Configuring VTP on the Switch	9-5
Configuring a VTP Server	9-6
Configuring a VTP Client	9-6

CISCO Confidential - DRAFT

Configuring VTP Transparent Mode	9-7
Disabling VTP Using the Off Mode	9-8
Enabling VTP Version 2	9-8
Disabling VTP Version 2	9-9
Configuring VTP Pruning	9-9
Disabling VTP Pruning	9-10
Displaying VTP Statistics	9-11

CHAPTER 10**Configuring VLANs 10-1**

Understanding How VLANs Work	10-1
VLAN Ranges	10-3
Configurable VLAN Parameters	10-3
VLAN Default Configuration	10-4
VLAN Configuration Guidelines	10-4
Configuring VLANs on the Switch	10-5
Creating or Modifying an Ethernet VLAN	10-5
Creating or Modifying a Normal-Range Ethernet VLAN	10-6
Creating or Modifying an Extended-Range VLAN	10-8
Assigning Switch Ports to a VLAN	10-9
Mapping 802.1Q VLANs to ISL VLANs	10-10
Clearing 802.1Q-to-ISL VLAN Mappings	10-11
Deleting a VLAN	10-11
Configuring Auxiliary VLANs	10-12
Understanding Auxiliary VLANs	10-12
Configuring Private VLANs	10-15
Private VLAN Configuration Guidelines	10-16
Creating a Private VLAN	10-17
Viewing the Port Capability of a Private VLAN Port	10-20
Deleting a Private VLAN	10-20
Deleting an Isolated or Community VLAN	10-21
Deleting a Private VLAN Mapping	10-21

CHAPTER 11**Configuring VLAN Trunks on Fast Ethernet and Gigabit Ethernet Ports 11-1**

Understanding How VLAN Trunks Work	11-1
Trunking Overview	11-1
Trunking Modes and Encapsulation Types	11-2
Trunking Support	11-3
802.1Q Trunk Restrictions	11-4

CISCO Confidential - DRAFT

Default Trunk Configuration	11-5
Configuring a Trunk Link	11-5
Configuring an 802.1Q Trunk	11-5
Defining the Allowed VLANs on a Trunk	11-6
Disabling a Trunk Port	11-7
Disabling VLAN 1 on a Trunk Link	11-8
Example VLAN Trunk Configurations	11-9
802.1Q Trunk over a Gigabit EtherChannel Link Example	11-9
Load-Sharing VLAN Traffic over Parallel Trunks Example	11-12
802.1Q Nonnegotiate Trunk Configuration Example	11-19

CHAPTER 12

Configuring Dynamic VLAN Membership with VMPS	12-1
Understanding How VMPS Works	12-1
VMPS and Dynamic Port Hardware and Software Requirements	12-2
Default VMPS and Dynamic Port Configuration	12-2
Configuration Guidelines for Dynamic Ports and VMPS	12-3
Configuring VMPS	12-4
Creating the VMPS Database	12-4
Configuring the VMPS Server	12-7
Configuring VMPS Clients	12-7
Monitoring VMPS	12-8
Maintaining VMPS	12-9
Configuring Static Ports	12-10
Troubleshooting VMPS and Dynamic Port VLAN Membership	12-10
Troubleshooting VMPS	12-10
Troubleshooting Dynamic Ports	12-11
VMPS Example	12-11
Dynamic Port VLAN Membership with Auxiliary VLANs	12-13
Configuration Guidelines	12-14
Configuring Dynamic Port VLAN Membership with Auxiliary VLANs	12-14

CHAPTER 13

Configuring GVRP	13-1
Understanding How GVRP Works	13-1
GVRP Hardware and Software Requirements	13-1
Default GVRP Configuration	13-2
GVRP Configuration Guidelines	13-2
Configuring GVRP on the Switch	13-2
Enabling GVRP Globally	13-2

CISCO Confidential - DRAFT

Enabling GVRP on Individual 802.1Q Trunk Ports	13-3
Enabling GVRP Dynamic VLAN Creation	13-4
Configuring GVRP Registration	13-4
Sending GVRP VLAN Declarations from Blocking Ports	13-6
Setting the GARP Timers	13-6
Displaying GVRP Statistics	13-7
Clearing GVRP Statistics	13-8
Disabling GVRP on Individual 802.1Q Trunk Ports	13-8
Disabling GVRP Globally	13-8

CHAPTER 14

Configuring QoS 14-1

Understanding How QoS Works	14-1
QoS Overview	14-1
Understanding QoS Terminology	14-2
Understanding Classification and Marking at the Ingress Port	14-3
Understanding Scheduling	14-3
Software Requirements	14-4
QoS Default Configuration	14-4
Configuring QoS on the Switch	14-4
Enabling QoS Globally	14-5
Configuring the Default CoS Value for the Switch	14-5
Reverting to the Default Switch CoS Value	14-5
Mapping CoS Values to Transmit Queues and Drop Thresholds	14-6
Reverting to the Default CoS-to-Transmit Queue and Drop Threshold Mapping	14-6
Displaying QoS Information	14-7
Reverting to QoS Defaults	14-7
Disabling QoS	14-7

CHAPTER 15

Configuring Multicast Services 15-1

Understanding How Multicasting Works	15-1
Understanding Multicasting and Multicast Services Operation	15-1
Joining a Multicast Group	15-2
Leaving a Multicast Group	15-2
Understanding GMRP Operation	15-3
Configuring CGMP	15-3
CGMP Hardware and Software Requirements	15-4
Default CGMP Configuration	15-4
Enabling CGMP	15-4
Enabling CGMP Leave Processing	15-5

CISCO Confidential - DRAFT

Enabling CGMP Fast-Leave Processing	15-5
Displaying Multicast Router Information	15-5
Displaying Multicast Group Information	15-6
Displaying CGMP Statistics	15-7
Disabling CGMP Leave Processing	15-7
Disabling CGMP Fast-Leave Processing	15-7
Disabling CGMP	15-8
Configuring GMRP	15-8
GMRP Software Requirements	15-8
Default GMRP Configuration	15-8
Enabling GMRP Globally	15-9
Enabling GMRP on Individual Switch Ports	15-9
Disabling GMRP on Individual Switch Ports	15-10
Enabling GMRP Forward-All Option	15-11
Disabling GMRP Forward-All Option	15-11
Configuring GMRP Registration	15-11
Setting the GARP Timers	15-13
Displaying GMRP Statistics	15-14
Clearing GMRP Statistics	15-14
Disabling GMRP	15-15
Configuring Multicast Router Ports and Group Entries	15-15
Specifying Multicast Router Ports	15-15
Configuring Multicast Groups	15-16
Disabling Multicast Router Ports	15-16
Disabling Multicast Group Entries	15-17
Filtering IGMP Traffic	15-17
Using IGMP Traffic Filtering	15-17
IGMP Software Requirements	15-18
Default IGMP Filter Configuration	15-18
IGMP Multicast Filter Activation	15-18
Configuring Port IP Multicast Filtering	15-19
CHAPTER 16	
Configuring Port Security	16-1
Understanding How Port Security Works	16-1
Allowing Traffic Based on the Host MAC Address	16-1
Restricting Traffic Based on the Host MAC Address	16-2
Blocking Unicast Flood Packets on Secure Ports	16-3
Port Security Configuration Guidelines	16-3
Configuring Port Security on the Switch	16-3

CISCO Confidential - DRAFT

Enabling Port Security	16-3
Setting the Maximum Number of Secure MAC Addresses	16-4
Setting the Port Security Age Time	16-5
Clearing MAC Addresses	16-5
Configuring Unicast Flood Blocking on Secure Ports	16-5
Enabling MAC Address Notification	16-6
Setting the Security Violation Action	16-8
Setting the Shutdown Time	16-8
Disabling Port Security	16-9
Restricting Traffic for a Host MAC Address	16-9
Monitoring Port Security	16-10

CHAPTER 17

Configuring Unicast Flood Blocking	17-1
Understanding How Unicast Flood Blocking Works	17-1
Configuration Guidelines for Unicast Flood Blocking	17-2
Configuring Unicast Flood Blocking on the Switch	17-2
Enabling Unicast Flood Blocking	17-2
Disabling Unicast Flood Blocking	17-3
Displaying Unicast Flood Blocking	17-3

CHAPTER 18

Configuring the IP Permit List	18-1
Understanding How the IP Permit List Works	18-1
IP Permit List Default Configuration	18-2
Configuring the IP Permit List on the Switch	18-2
Adding IP Addresses to the IP Permit List	18-2
Enabling the IP Permit List	18-3
Disabling the IP Permit List	18-4
Clearing an IP Permit List Entry	18-4

CHAPTER 19

Configuring Protocol Filtering	19-1
Understanding How Protocol Filtering Works	19-1
Default Protocol Filtering Configuration	19-2
Configuring Protocol Filtering on the Switch	19-2
Configuring Protocol Filtering	19-2
Disabling Protocol Filtering	19-3

CHAPTER 20

Checking Status and Connectivity	20-1
Checking Module Status	20-1

CISCO Confidential - DRAFT

Checking Port Status	20-2
Displaying the Port MAC Address	20-4
Displaying Port Capabilities	20-5
Using Telnet	20-6
Changing the Login Timer	20-6
Using Secure Shell Encryption for Telnet Sessions	20-7
Monitoring User Sessions	20-7
Using Ping	20-9
Understanding How Ping Works	20-9
Executing Ping	20-10
Using Layer 2 Traceroute	20-11
Layer 2 Traceroute Usage Guidelines	20-11
Identifying a Layer 2 Path	20-11
Using IP Traceroute	20-12
Understanding How IP Traceroute Works	20-12
Executing IP Traceroute	20-12

CHAPTER 21

Configuring CDP 21-1

Understanding How CDP Works	21-1
Default CDP Configuration	21-2
Configuring CDP on the Switch	21-2
Setting the CDP Global Enable State	21-2
Setting the CDP Enable State on a Port	21-2
Setting the CDP Message Interval	21-4
Setting the CDP Holdtime	21-4
Displaying CDP Neighbor Information	21-5

CHAPTER 22

Using Switch TopN Reports 22-1

Understanding How Switch TopN Reports Works	22-1
Running Switch TopN Reports Without the Background Option	22-2
Running Switch TopN Reports with the Background Option	22-2
Running and Viewing Switch TopN Reports	22-3

CHAPTER 23

Configuring UDLD 23-1

Understanding How UDLD Works	23-1
UDLD Software and Hardware Requirements	23-2
Default UDLD Configuration	23-2

CISCO Confidential - DRAFT

Configuring UDLD on the Switch	23-3
Enabling UDLD Globally	23-3
Enabling UDLD on Individual Ports	23-4
Disabling UDLD on Individual Ports	23-4
Disabling UDLD Globally	23-4
Specifying the UDLD Message Interval	23-5
Enabling UDLD Aggressive Mode	23-5
Displaying the UDLD Configuration	23-6

CHAPTER 24

Configuring SNMP	24-1
SNMP Terminology	24-1
Understanding How SNMP Works	24-3
Security Models and Levels	24-4
SNMP ifindex Persistence Feature	24-4
Understanding How SNMPv1 and SNMPv2c Work	24-5
SNMPv1 and SNMPv2c Default Configuration	24-6
Configuring SNMPv1 and SNMPv2c from an NMS	24-6
Configuring SNMPv1 and SNMPv2c from the CLI	24-6
SNMPv1 and SNMPv2c Enhancements in Software Release 7.5(1)	24-7
Understanding SNMPv3	24-11
Benefits of SNMPv3	24-11
SNMP Entity	24-11
Configuring SNMPv3 from an NMS	24-14
Configuring SNMPv3 from the CLI	24-14
Using CiscoWorks2000	24-17

CHAPTER 25

Configuring RMON	25-1
Understanding How RMON Works	25-1
Enabling RMON	25-2
Viewing RMON Data	25-2
Supported RMON and RMON2 MIB Objects	25-2

CHAPTER 26

Configuring SPAN and RSPAN	26-1
Understanding How SPAN and RSPAN Work	26-1
SPAN Session	26-1
Destination Port	26-2
Source Port	26-2
Reflector Port	26-3

CISCO Confidential - DRAFT

Ingress SPAN	26-3
Egress SPAN	26-3
VSPAN	26-3
Trunk VLAN Filtering	26-4
SPAN Traffic	26-4
SPAN and RSPAN Session Limits	26-4
Configuring SPAN	26-4
Understanding How SPAN Works	26-4
SPAN Configuration Guidelines	26-5
Configuring SPAN	26-6
Configuring RSPAN	26-8
RSPAN Software and Hardware Requirements	26-8
Understanding How RSPAN Works	26-8
RSPAN Configuration Guidelines	26-9
Configuring RSPAN	26-10
RSPAN Configuration Examples	26-13

CHAPTER 27

Administering the Switch	27-1
Setting the System Name and System Prompt	27-1
Configuring a System Name and Prompt	27-2
Setting the System Contact and Location	27-3
Setting the System Clock	27-4
Creating a Login Banner	27-4
Configuring a Login Banner	27-4
Clearing the Login Banner	27-5
Enabling or Disabling the “Cisco Systems Console” Telnet Login Banner	27-5
Defining and Using Command Aliases	27-6
Defining and Using IP Aliases	27-7
Configuring Permanent and Static ARP Entries	27-8
Configuring Static Routes	27-9
Scheduling a System Reset	27-10
Scheduling a Reset at a Specific Time	27-10
Scheduling a Reset Within a Specified Amount of Time	27-11
Generating System Status Reports for Tech Support	27-12

CHAPTER 28

Power Management	28-1
Understanding How Power Management Works on the Catalyst 4500 Series Switches	28-1
Power Management Overview	28-1

CISCO Confidential - DRAFT

Understanding Power Management Modes	28-2
Available Power for Power Supplies	28-3
Power Management Limitations	28-4
1400 W DC Power Supply Guidelines and Restrictions	28-5
Understanding How Power Management Works on the Catalyst 4006 Switch	28-6
Understanding Power Redundancy	28-6
1+1 Redundancy Mode Guidelines and Restrictions	28-7
1+1 Redundancy Mode Limitations	28-7
Power Consumption for Modules	28-9
Migrating a Supervisor Engine II from a Catalyst 4006 Switch to a Catalyst 4500 Series Switch	28-10
Understanding How Inline Power Works	28-11
Inline Power Management Modes	28-12
Power Requirements	28-12
Phone Detection Summary	28-14
Configuring Power Management	28-14
Setting Redundant Mode for the Catalyst 4500 Series Switches	28-14
Setting Combined Mode on the Catalyst 4500 Series Switches	28-15
Setting the DC Power Input	28-15
Setting the Power Budget for the Catalyst 4006 Switch	28-16
Displaying System Information	28-17
Migrating a Supervisor Engine II from a Catalyst 4006 Switch to a Catalyst 4500 Series Switch	28-18
Configuring Inline Power	28-18
Setting the Power Mode of a Port or Group of Ports	28-18
Setting the Default Power Allocation for a Port	28-19
Displaying the Power Status for Modules and Individual Ports	28-19

CHAPTER 29

Configuring VoIP 29-1

Hardware and Software Requirements	29-1
Overview of IP Phones	29-2
Configuring VoIP on a Switch	29-3

CHAPTER 30

Configuring Switch Access Using AAA 30-1

Understanding How Authentication Works	30-1
Understanding How Login Authentication Works	30-2
Understanding How Local Authentication Works	30-2
Understanding How Local User Authentication Works	30-3
Understanding How TACACS+ Authentication Works	30-3
Understanding How RADIUS Authentication Works	30-4

CISCO Confidential - DRAFT

Understanding How Kerberos Authentication Works	30-5
Configuring Authentication	30-8
Authentication Default Configuration	30-8
Authentication Configuration Guidelines	30-9
Configuring Login Authentication	30-9
Configuring Local Authentication	30-11
Configuring Local User Authentication	30-15
Configuring TACACS+ Authentication	30-17
Configuring RADIUS Authentication	30-23
Configuring Kerberos Authentication	30-30
Authentication Example	30-39
Understanding How Authorization Works	30-40
Authorization Events	30-40
TACACS+ Primary and Fallback Options	30-40
TACACS+ Command Authorization	30-41
RADIUS Authorization	30-41
Configuring Authorization	30-41
Authorization Default Configuration	30-42
TACACS+ Authorization Configuration Guidelines	30-42
Configuring TACACS+ Authorization	30-42
Authorization Example	30-45
Understanding How Accounting Works	30-46
Accounting Overview	30-46
Accounting Events	30-47
Specifying When to Create Accounting Records	30-47
Specifying RADIUS Servers	30-47
Updating the Server	30-48
Suppressing Accounting	30-48
Configuring Accounting	30-49
Accounting Default Configuration	30-49
Accounting Configuration Guidelines	30-49
Configuring Accounting	30-49
Accounting Example	30-52

CHAPTER 31

Configuring 802.1x Authentication 31-1

Understanding How 802.1x Authentication Works	31-1
Device Roles	31-2
Authentication Initiation and Message Exchange	31-3
Ports in Authorized and Unauthorized States	31-4

CISCO Confidential - DRAFT

Authentication Server	31-5
802.1x Parameters Configurable on the Switch	31-5
802.1x VLAN Assignment Using a RADIUS Server	31-6
Authentication Default Configuration	31-7
Authentication Configuration Guidelines	31-7
Configuring 802.1x Authentication on the Switch	31-8
Enabling 802.1x Globally	31-8
Disabling 802.1x Globally	31-8
Enabling and Initializing 802.1x Authentication for Individual Ports	31-9
Setting and Enabling Automatic Reauthentication of the Host	31-9
Manually Reauthenticating the Host	31-10
Enabling Multiple Hosts	31-10
Disabling Multiple Hosts	31-11
Setting the Quiet Period	31-11
Setting the Authenticator-to-Host Retransmission Time for EAP-Request/Identity Frames	31-11
Setting the Supplicant-to-Host Retransmission Time for EAP-Request Frames	31-12
Setting the Back-End Authenticator-to-Authentication-Server Retransmission Time for Transport Layer Packets	31-12
Setting the Back-End Authenticator-to-Host Frame-Retransmission Number	31-13
Setting the Shutdown Timeout Period	31-13
Setting the Back-End Authenticator-to-Host Frame-Retransmission Number	31-13
Setting the Back-End Authenticator-to-Host Frame-Retransmission Number	31-14
Resetting the 802.1x Configuration Parameters to the Default Values	31-14
Setting the Trace Severity	31-15
Using the show Commands	31-15

CHAPTER 32

Modifying the Switch Boot Configuration 32-1

Understanding How the Switch Boot Configuration Works	32-1
Understanding the Boot Process	32-1
Understanding the ROM Monitor	32-2
Understanding the Configuration Register	32-2
Understanding the BOOT Environment Variable	32-3
Understanding the CONFIG_FILE Environment Variable	32-3
Default Switch Boot Configuration	32-4
Setting the Configuration Register	32-4
Setting the Boot Field in the Configuration Register	32-4
Setting CONFIG_FILE Recurrence	32-5
Setting the Switch to Ignore the NVRAM Configuration	32-6
Setting the BOOT Environment Variable	32-6

CISCO Confidential - DRAFT

Setting the BOOT Environment Variable	32-6
Clearing the BOOT Environment Variable Settings	32-7
Setting and Clearing the CONFIG_FILE Environment Variable	32-7
Setting the CONFIG_FILE Environment Variable	32-7
Clearing CONFIG_FILE Environment Variable Entries	32-8
Displaying the Switch Boot Configuration	32-8

CHAPTER 33

Working with System Software Images 33-1

Software Image Naming Conventions	33-1
Downloading System Software Images to the Switch Using TFTP	33-1
Understanding How TFTP Software Image Downloads Work	33-2
Preparing to Download an Image Using TFTP	33-2
Downloading Supervisor Engine Images Using TFTP	33-2
Sample TFTP Download Procedures	33-3
Uploading System Software Images to a TFTP Server	33-4
Preparing to Upload an Image to a TFTP Server	33-4
Uploading Software Images to a TFTP Server	33-5
Downloading System Software Images to the Switch Using rcp	33-5
Understanding How rcp Software Image Downloads Work	33-5
Preparing to Download an Image Using rcp	33-6
Downloading Supervisor Engine Images Using rcp	33-6
Sample rcp Download Procedures	33-7
Uploading System Software Images to an rcp Server	33-8
Preparing to Upload an Image to an rcp Server	33-8
Uploading Software Images to an rcp Server	33-9
Upgrading the ROM Monitor	33-9

CHAPTER 34

Working With the Flash File System 34-1

Working the Flash File System on the Switch	34-1
Setting the Default Flash Device	34-1
Setting the Text File Configuration Mode	34-2
Listing the Files on a Flash Device	34-2
Displaying the Contents of a File on a Flash Device	34-3
Copying Files	34-4
Deleting Files	34-5
Restoring Deleted Files	34-6
Verifying a File Checksum	34-6

CISCO Confidential - DRAFT

CHAPTER 35**Working with Configuration Files 35-1**

- Creating and Using Configuration Files Guidelines 35-1
- Creating a Configuration File 35-2
- Configuring the Switch Using a File in Flash Memory 35-2
- Copying Configuration Files Using TFTP 35-3
 - Downloading Configuration Files from a TFTP Server 35-3
 - Uploading Configuration Files to a TFTP Server 35-4
- Copying Configuration Files Using rcp 35-5
 - Downloading Configuration Files from an rcp Server 35-5
 - Uploading Configuration Files to an rcp Server 35-6
- Clearing the Configuration 35-7

CHAPTER 36**Configuring Switch Acceleration 36-1**

- Understanding How Switch Acceleration Works 36-1
- Configuring Switch Acceleration on the Switch 36-2
 - Enabling Switch Acceleration 36-3
 - Displaying Switch Acceleration Information 36-3
- Backplane Channel Module 36-3

CHAPTER 37**Configuring System Message Logging 37-1**

- Understanding How System Message Logging Works 37-1
- System Log Message Format 37-3
- Default System Message Logging Configuration 37-3
- System Log Message Format 37-4
- Configuring System Message Logging on the Switch 37-4
 - Configuring Session Logging Settings 37-5
 - Configuring the System Message Logging Levels 37-6
 - Enabling and Disabling the Logging Time Stamp 37-6
 - Setting the Logging Buffer Size 37-6
 - Limiting the Number of syslog Messages 37-7
 - Configuring the syslog Daemon on a UNIX syslog Server 37-7
 - Configuring syslog Servers 37-8
 - Displaying the Logging Configuration 37-9
 - Displaying System Messages 37-10

CHAPTER 38**Configuring DNS 38-1**

- Understanding How DNS Works 38-1

CISCO Confidential - DRAFT

Default DNS Configuration	38-1
Configuring DNS on the Switch	38-2
Setting Up and Enabling DNS	38-2
Clearing a DNS Server	38-3
Clearing the DNS Domain Name	38-3
Disabling DNS	38-3

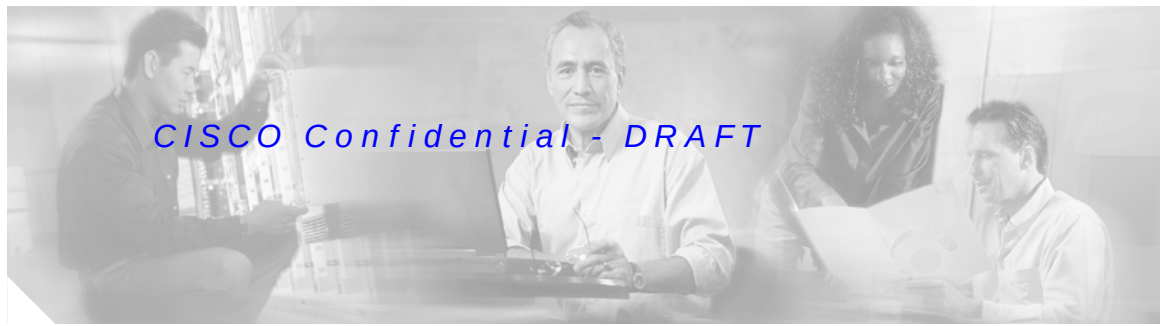
CHAPTER 39

Configuring NTP	39-1
Understanding How NTP Works	39-1
Default NTP Configuration	39-2
Configuring NTP on the Switch	39-2
Enabling NTP in Broadcast-Client Mode	39-2
Configuring NTP in Client Mode	39-3
Configuring Authentication in Client Mode	39-4
Setting the Time Zone	39-5
Enabling the Daylight Saving Time Adjustment	39-5
Disabling the Daylight Saving Time Adjustment	39-7
Clearing the Time Zone	39-7
Clearing NTP Servers	39-7
Disabling NTP	39-7

APPENDIX A

Acronyms	A-1

INDEX



Preface

This preface describes who should read the *Software Configuration Guide*, how it is organized, and its document conventions.

Audience

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

Organization

This publication is organized as follows:

Chapter	Title	Description
Chapter 1	Product Overview	Presents an overview of the Catalyst enterprise LAN switches.
Chapter 2	Using the Command-Line Interface	Describes how to use the different command-line interfaces (CLIs).
Chapter 3	Configuring the Switch IP Address and Default Gateway	Describes how to perform a baseline configuration of the switch.
Chapter 4	Configuring Ethernet and Fast Ethernet Switching	Describes how to configure Ethernet and Fast Ethernet switching on the switch.
Chapter 5	Configuring Gigabit Ethernet Switching	Describes how to configure Gigabit Ethernet switching on the switch.
Chapter 6	Configuring Fast EtherChannel and Gigabit EtherChannel	Describes how to configure Fast EtherChannel and Gigabit EtherChannel port bundles.
Chapter 7	Configuring Spanning Tree	Describes how to configure the Spanning Tree Protocol and explains how spanning tree works.
Chapter 8	Configuring Spanning Tree PortFast, BPDU Guard, BPDU Filter, UplinkFast, BackboneFast, and Loop Guard	Describes how to configure the spanning tree PortFast, UplinkFast, and BackboneFast features.

CISCO Confidential - DRAFT

Chapter	Title	Description
Chapter 9	Configuring VTP	Describes how to configure VLAN Trunking Protocol (VTP) on the switch.
Chapter 10	Configuring VLANs	Describes how to configure VLANs and private VLANs on the switch.
Chapter 11	Configuring VLAN Trunks on Fast Ethernet and Gigabit Ethernet Ports	Describes how to configure Inter-Switch Link (ISL) and IEEE 802.1Q VLAN trunks on Fast Ethernet and Gigabit Ethernet ports.
Chapter 12	Configuring Dynamic VLAN Membership with VMPS	Describes how to configure VLAN Membership Policy Server (VMPS) and dynamic ports on the switch.
Chapter 13	Configuring GVRP	Describes how to configure GARP VLAN Registration Protocol (GVRP) on the switch.
Chapter 14	Configuring QoS	Describes how to configure quality of service (QoS).
Chapter 15	Configuring Multicast Services	Describes how to configure Cisco Group Management Protocol (CGMP), Internet Group Management Protocol (IGMP) snooping, and GARP Multicast Registration Protocol (GMRP) on the switch.
Chapter 16	Configuring Port Security	Describes how to configure port security on the switch.
Chapter 17	Configuring Unicast Flood Blocking	Describes how to configure unicast flood blocking on the switch.
Chapter 18	Configuring the IP Permit List	Describes how to configure IP permit list on the switch.
Chapter 19	Configuring Protocol Filtering	Describes how to configure protocol filtering on Ethernet, Fast Ethernet, and Gigabit Ethernet ports.
Chapter 20	Checking Status and Connectivity	Describes how to display information about modules and switch ports and how to check connectivity using ping, Telnet, and IP traceroute.
Chapter 21	Configuring CDP	Describes how to configure Cisco Discovery Protocol (CDP) on the switch.
Chapter 22	Using Switch TopN Reports	Describes how to generate switch TopN reports on the switch.
Chapter 23	Configuring UDLD	Describes how to configure the UniDirectional Link Detection (UDLD) protocol on the switch.
Chapter 24	Configuring SNMP	Describes how to configure the Simple Network Management Protocol (SNMP) on the switch.
Chapter 25	Configuring RMON	Describes how to configure Remote Monitoring (RMON) on the switch.
Chapter 26	Configuring SPAN and RSPAN	Describes how to configure the Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) on the switch.

CISCO Confidential - DRAFT

Chapter	Title	Description
Chapter 27	Administering the Switch	Describes how to set the system name, create a login banner, and perform other administrative tasks on the switch.
Chapter 28	Power Management	Describes power management on the Catalyst 4000 Series switches and the Catalyst 4500 Series switches, and configuring inline power.
Chapter 29	Configuring VoIP	Describes how to configure your voice-over-IP network.
Chapter 30	Configuring Switch Access Using AAA	Describes how to configure local and TACACS+ authentication on the switch.
Chapter 31	Configuring 802.1x Authentication	Describes how to configure IEEE 802.1x authentication on the switch.
Chapter 32	Modifying the Switch Boot Configuration	Describes how to modify the switch boot configuration, including the BOOT environment variable and the configuration register.
Chapter 33	Working with System Software Images	Describes how to download and upload system software images.
Chapter 34	Working With the Flash File System	Describes how to work with the Flash file system available on some switch platforms.
Chapter 35	Working with Configuration Files	Describes how to create, download, and upload switch configuration files.
Chapter 36	Configuring Switch Acceleration	Describes the Backplane Channel module and the switch acceleration feature.
Chapter 37	Configuring System Message Logging	Describes how to configure system message logging (syslog) on the switch.
Chapter 38	Configuring DNS	Describes how to configure Domain Name System (DNS) on the switch.
Chapter 39	Configuring NTP	Describes how to configure Network Time Protocol (NTP) on the switch.

Related Documentation

The following publications are available for the Catalyst enterprise LAN switches:

- *Catalyst 4000 Series Installation Guide*
- *Catalyst 4500 Series Installation Guide*
- *Catalyst 4912G Installation Guide*
- *Catalyst 2948G and 2980G Installation Guide*
- *Catalyst 4000 Family, 2948G, and 2980G Switches Quick Software Configuration*
- *Catalyst 4500 Series, Catalyst 2948G, and Catalyst 2980G Switches Command Reference*
- *System Message Guide - Catalyst Family Switches*
- *Release Notes for Catalyst 4000 Family Supervisor Engine Software Release 7.x*

Conventions

Throughout this publication, these conventions are used in reference to switch platforms:

- Catalyst enterprise LAN switches—Refers to the Catalyst 4000 family, Catalyst 2948G, and Catalyst 2980G switches.
- Catalyst 4000 family switches—Refers to the Catalyst 4000 series and Catalyst 4500 series switches. The Catalyst 4000 series includes the Catalyst 4003, Catalyst 4006, and Catalyst 4912G switches. The Catalyst 4500 series includes the Catalyst 4503 and Catalyst 4506 switches.

Command descriptions use these conventions:

boldface font	Commands, command options, and keywords are in boldface .
<i>italic font</i>	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.

Instructions and screen examples use these conventions:

screen font	Terminal sessions and information that the system displays are in screen font.
boldface screen font	Information you must enter is in boldface screen font .
<i>italic screen font</i>	Arguments for which you supply values are in <i>italic screen font</i> .
Ctrl-D	The key combination Ctrl-D means to hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords are in angle brackets.
[]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.
.	Indicates that screen output not relevant to the example was removed to save space and preserve clarity.

Notes use these conventions:



Note

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

Cautions use these conventions:

CISCO Confidential - DRAFT**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 web sites 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 monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Registered Cisco.com users can order the Documentation CD-ROM (product number DOC-CONDOCCD=) through the online Subscription Store:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

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

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products Marketplace:

<http://www.cisco.com/en/US/partner/ordering/index.shtml>

- Registered Cisco.com users can order the Documentation CD-ROM (Customer Order Number DOC-CONDOCCD=) through the online Subscription Store:

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

CISCO Confidential - DRAFT

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

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

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

You can submit your comments by mail by using the response card 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://www.cisco.com>

CISCO Confidential - DRAFT

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The avenue 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.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Cisco TAC Website

You can use the Cisco TAC website to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. 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/en/US/support/index.html>

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC website so that you can describe the situation in your own words 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 level of 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.

CISCO Confidential - DRAFT

Obtaining Additional Publications and Information

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

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

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

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary*, *Internetworking Technology Handbook*, *Internetworking Troubleshooting Guide*, and the *Internetworking Design Guide*. For current Cisco Press titles and other information, go to Cisco Press online at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco monthly periodical that provides industry professionals with the latest information about the field of networking. You can access *Packet* magazine at this URL:

http://www.cisco.com/en/US/about/ac123/ac114/about_cisco_packet_magazine.html

- *iQ Magazine* is the Cisco monthly periodical that provides business leaders and decision makers with the latest information about the networking industry. You can access *iQ Magazine* at this URL:

http://business.cisco.com/prod/tree.taf%3fasset_id=44699&public_view=true&kbns=1.html

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in the design, development, and operation of 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, with current offerings in network training listed at this URL:

http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html



Product Overview

The Catalyst enterprise LAN switches facilitate the migration from traditional shared-hub LANs to large-scale, fully integrated internetworks. These switches provide switched connections to individual workstations, servers, LAN segments, backbones, or other switches, using a variety of media.

This chapter consists of these sections:

- [Catalyst 4000 Family Switches, page 1-1](#)
- [Catalyst 2948G Switch, page 1-2](#)
- [Catalyst 2980G Switch, page 1-3](#)
- [Supervisor Engine Software, page 1-3](#)

Catalyst 4000 Family Switches



Note

For installation information and a complete description of the Catalyst 4000 family switch hardware, refer to the *Catalyst 4000 Family Installation Guide*, *Catalyst 4500 Series Installation Guide*, and the *Catalyst 4912G Installation Guide*.

[Table 1-1](#) describes the Catalyst 4000 family switches.

Table 1-1 Catalyst 4000 Family Switches

Product Number	Chassis Description
Catalyst 4000 Series	
WS-C4003	Catalyst 4003 • Modular 3-slot chassis • Optional redundant power supplies
WS-C4006	Catalyst 4006 • Modular 6-slot chassis • 30-Gbps backplane • Two power supplies with optional third power supply

*CISCO Confidential - DRAFT***Table 1-1 Catalyst 4000 Family Switches (continued)**

Product Number	Chassis Description
WS-C4912G	Catalyst 4912G - Fixed-configuration switch 12-Gbps backplane - Optional redundant power supplies 12 1000BASE-X (GBIC) Gigabit Ethernet ports
Catalyst 4500 Series	
WS-C4503	Catalyst 4503 - Modular 3-slot chassis 28-Gbps full duplex backplane - Optional redundant power supplies
WS-C4506	Catalyst 4506 - Modular 6-slot chassis 64 Gbps full duplex - Optional redundant power supplies

Catalyst 2948G Switch

**Note**

For installation information and a complete description of the Catalyst 2948G switch hardware, refer to the *Catalyst 2948G and 2980G Installation Guide*.

[Table 1-2](#) describes the Catalyst 2948G switch.

Table 1-2 Catalyst 2948G Switch

Product Number	Chassis Description
WS-C2948G	Catalyst 2948G - Fixed-configuration switch 12-Gbps backplane - Optional redundant power supplies - Two 1000BASE-X (GBIC) Gigabit Ethernet ports 48 10/100BASE-TX Fast Ethernet ports

CISCO Confidential - DRAFT

Catalyst 2980G Switch

**Note**

For installation information and a complete description of the Catalyst 2980G switch hardware, refer to the *Catalyst 2948G and 2980G Installation Guide*.

[Table 1-3](#) describes the Catalyst 2980G switch.

Table 1-3 Catalyst 2980G Switch

Product Number	Chassis Description
WS-C2980G-A	Catalyst 2980G • Fixed-configuration switch • 12-Gbps backplane • Optional redundant power supplies • Two 1000BASE-X (GBIC) Gigabit Ethernet ports • 80 10/100BASE-TX Fast Ethernet ports

Supervisor Engine Software

The supervisor engine software is factory installed on every supervisor engine module or fixed-configuration switch. Some modules require an additional software image, which is factory installed on the module.

The Catalyst enterprise LAN switches share a command-line interface (CLI) with which you can configure modules and ports on the switches. For more information, see [Chapter 2, “Using the Command-Line Interface.”](#) For descriptions of the available CLI commands, refer to the *Catalyst 4500 Series, Catalyst 2948G, and Catalyst 2980G Switches Command Reference*.

CISCO Confidential - DRAFT

Using the Command-Line Interface

This chapter describes the command-line interface (CLI) that you use to configure the Catalyst enterprise LAN switches and modules.

**Note**

For descriptions of all switch and ROM monitor commands, refer to the *Catalyst 4500 Series, Catalyst 2948G, and Catalyst 2980G Switches Command Reference*. For descriptions of the commands used to configure the Route Switch Module (RSM) and Route Switch Feature Card (RSFC), refer to the Cisco IOS software command reference publications.

This chapter consists of these sections:

- [Switch CLI Overview, page 2-1](#)
- [Accessing the Switch CLI, page 2-2](#)
- [Switch CLI Command Modes, page 2-3](#)
- [Accessing Help, page 2-4](#)
- [Command-Line Editing, page 2-5](#)
- [History Substitution, page 2-6](#)
- [Abbreviating a Command, page 2-6](#)
- [Completing a Partial Command, page 2-6](#)
- [Scrolling Through Command Output, page 2-6](#)
- [Using Command Aliases, page 2-7](#)
- [Specifying Modules, Ports, and VLANs, page 2-7](#)
- [Specifying MAC Addresses, page 2-8](#)
- [Specifying IP Addresses, Host Names, and IP Aliases, page 2-8](#)
- [ROM Monitor CLI, page 2-9](#)
- [Example of a Catalyst 4003 Bootup Display, page 2-9](#)

Switch CLI Overview

The switch CLI is a basic command-line interpreter, similar to the UNIX C shell. However, switch commands are not case sensitive. You can abbreviate commands and parameters as long as they contain enough letters to be distinguished from any other currently available commands or parameters.

CISCO Confidential - DRAFT

The Catalyst enterprise LAN switches are multi-module systems. Commands you enter from the CLI might apply to the entire system or to a specific module, port, or VLAN.

You configure the switch using **set** and **clear** commands. Enter **set** commands to change switch parameters. Use **clear** commands (or in some cases, use **set** commands) to overwrite or erase configuration parameters. Use **show** commands to display the current configuration and to monitor the switch.

Accessing the Switch CLI

You can access the CLI through the supervisor engine console port or through a Telnet session.

These sections describe how to access the switch CLI:

- [Accessing the CLI Through the Console Port, page 2-2](#)
- [Accessing the CLI Through Telnet, page 2-3](#)

Accessing the CLI Through the Console Port

**Note**

For complete information on how to connect a terminal to the supervisor engine console port, refer to the hardware documentation for your switch.

To access the switch CLI through the console port, you first must connect a console terminal to the console port through an EIA/TIA-232 (RS-232) cable. Make sure that the terminal is connected to the switch and that the terminal is on.

To access the switch CLI through the console port, follow these steps:

-
- Step 1** Connect to the supervisor engine console port using the appropriate application or commands on the terminal (for example, using a terminal emulation program on a PC or using the **tip** command on a UNIX system).
- Step 2** If the switch is not on, power up the switch. The bootup display should appear on the screen (see the [“Example of a Catalyst 4003 Bootup Display”](#) section on page 2-9). If the switch is already booted, press **Enter** to see this display:

```
Cisco Systems, Inc. Console
```

```
Enter password:
```

After you successfully connect to the switch through the console port, you can use normal-mode commands to monitor the switch or enter privileged mode to change the configuration. For more information, see the [“Switch CLI Command Modes”](#) section on page 2-3.

Accessing the CLI Through Telnet

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

**Note**

For more information about using Telnet, see the [“Using Telnet” section on page 20-6](#).

To access the switch CLI from a remote host using Telnet, follow these steps:

- Step 1** Make sure that the switch is on and is properly configured with an IP address and default gateway, if necessary.
- Step 2** Using the appropriate application or command on your host system, Telnet to the switch using the IP address or the DNS host name of the switch. (You must configure DNS properly on the switch and on your network name server in order to use DNS host names. For more information on DNS, see [Chapter 38, “Configuring DNS.”](#))

This example shows how to use the **telnet** command to connect to a switch with the DNS host name Catalyst_1.

```
unix_host% telnet Catalyst_1
Trying 172.16.10.10...
Connected to Catalyst_1.
Escape character is '^['.
```

```
Cisco Systems Console
```

```
Enter password:
```

After you successfully connect to the switch using Telnet, you can use normal-mode commands to monitor the switch or enter privileged mode to change the configuration. For more information, see the following section.

Switch CLI Command Modes

The switch CLI supports two modes of operation:

- Normal (also called login or user mode)
- Privileged (also called enable mode)

Both modes are password protected. Use normal-mode commands for system monitoring. Use privileged-mode commands to change the system configuration.

**Note**

For complete information on configuring passwords and controlling access to the switch, see [Chapter 30, “Configuring Switch Access Using AAA.”](#)

To enter normal command mode, follow these steps:

CISCO Confidential - DRAFT

Step 1 Connect to the switch CLI through the console port or using Telnet (for more information, see the “Accessing the Switch CLI” section on page 2-2).

Step 2 On a new switch, the normal-mode password is null. If you are connecting to a new switch, press **Return** at the Enter Password prompt. Otherwise, enter the normal-mode password for the switch.

You will see the user-level command-line prompt.

```
Enter Password: <normal_mode_password>
Console>
```

Step 3 To disconnect from the switch CLI, enter the **exit** command.

```
Console> exit
Session Disconnected...
```

```
Cisco Systems Console          Fri Aug 27 1999, 16:14:41
```

```
Enter password:
```

Many commands (for example, commands that modify the configuration) can be used only in privileged mode. To enter and exit privileged command mode, follow these steps:

Step 1 From normal mode, enter the **enable** command. On a new switch, the privileged-mode password is null. If you are connecting to a new switch, press **Return** at the Enter Password prompt. Otherwise, enter the privileged-mode password for the switch.

```
Console> enable
Enter password: <privileged_mode_password>
Console> (enable)
```

Step 2 To exit privileged mode and return to normal mode, enter the **disable** command.

```
Console> (enable) disable
Console>
```

Accessing Help

Enter **help** or **?** in normal or privileged mode to see the commands available in those modes. Command usage, the help menu, and, when appropriate, parameter ranges are provided if you enter a command using the wrong number of arguments or inappropriate arguments.

Additionally, appending **?** to a command displays a list of valid keywords and arguments for the command. Insert a space between the last parameter and the question mark (?). For example, eight parameters are used by the **set mls** command. To see these parameters, enter **set ip ?** at the privileged mode prompt. The system displays all valid keywords and arguments as follows:

```
Console> (enable) set ip ?
alias          Set alias for IP Address
dns            Set DNS information
fragmentation  Set IP fragmentation enable/disable
http           Set IP HTTP server information
permit        Set IP Permit List
redirect       Set ICMP redirect enable/disable
route          Set IP routing table entry
```


CISCO Confidential - DRAFT

```

unreachable          Set ICMP unreachable messages
Console> (enable) set ip

```

**Note**

The system repeats the command you entered without the question mark (?).

To use the partial-keyword-lookup function, enter ? to display a list of commands that begin with a specific set of characters. Do not insert a space between the last letter of the variable and the question mark (?). For example, enter **co?** at the privileged prompt to display a list of commands that start with **co**. The system displays all commands that begin with **co**, as follows:

```

Console> (enable) co?
  configure          Configure system from network
  copy               Copy files between TFTP/RCP/module/flash devices
Console> (enable) co

```

**Note**

The system repeats the command you entered without the question mark (?).

Command-Line Editing

The switch CLI supports a number of command-line editing keystrokes. [Table 2-1](#) lists the keystrokes you can use when entering and editing switch commands.

Table 2-1 Command-Line Editing Keystrokes

Keystroke	Function
Ctrl-A	Jumps to the first character of the command line.
Ctrl-B or the Left Arrow key ¹	Moves the cursor back one character.
Ctrl-C	Escapes and terminates prompts and lengthy tasks.
Ctrl-D	Deletes the character at the cursor.
Ctrl-E	Jumps to the end of the current command line.
Ctrl-F or the Right Arrow key ¹	Moves the cursor forward one character.
Ctrl-K	Deletes from the cursor to the end of the command line.
Ctrl-L; Ctrl-R	Repeats current command line on a new line.
Ctrl-N or the Down Arrow key ¹	Enters next command line from the history buffer.
Ctrl-P or the Up Arrow key ¹	Enters previous command line from the history buffer.
Ctrl-U; Ctrl-X	Deletes from the cursor to the beginning of the command line.
Ctrl-W	Deletes last word typed.
Esc B	Moves the cursor backward one word.
Esc D	Deletes from the cursor to the end of the word.
Esc F	Moves the cursor forward one word.
Delete key or Backspace key	Erases characters on the command line.

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

CISCO Confidential - DRAFT

History Substitution

The history buffer stores the last 20 commands that you entered during a terminal session. History substitution allows you to repeat these commands using special abbreviated commands, that are similar to those used on the UNIX command line. [Table 2-2](#) lists the history substitution commands.

Table 2-2 History Substitution Commands

Command	Function
To repeat recent commands:	
!!	Repeats the most recent command.
!-nn	Repeats the <i>nn</i> th most recent command.
!n	Repeats command <i>n</i> .
!aaa	Repeats the command beginning with string <i>aaa</i> .
!?aaa	Repeats the command containing the string <i>aaa</i> .
To modify and repeat the most recent command:	
^aaa^bbb	Replaces the string <i>aaa</i> with the string <i>bbb</i> in the most recent command.
To add a string to the end of a previous command and repeat it:	
!!aaa	Adds string <i>aaa</i> to the end of the most recent command.
!n aaa	Adds string <i>aaa</i> to the end of command <i>n</i> .
!aaa bbb	Adds string <i>bbb</i> to the end of the command beginning with string <i>aaa</i> .
!?aaa bbb	Adds string <i>bbb</i> to the end of the command containing the string <i>aaa</i> .

Abbreviating a Command

When typing a command, you can abbreviate any command or keyword to the number of characters that uniquely define the command. For example, you can abbreviate the **show** command to **sh**. After entering the command at the system prompt, press **Return** to execute the command.

Completing a Partial Command

The **Tab** key allows you to use the command-completion feature. When you enter a unique partial character string and press **Tab**, the system completes the command or keyword on the command line. For example, if you enter **co** and press the **Tab** key, the system completes the command as **configure** because it is the only command that matches the criteria.

Scrolling Through Command Output

When the output of a command fills more than one terminal screen, the output is displayed through the More program; a ---More--- prompt is displayed at the bottom of the screen. The More program is used for any output that has more lines than can be displayed on the terminal screen, including **show** command output. To view the next line or screen, use the following tasks.

CISCO Confidential - DRAFT

Task	Keystrokes
To scroll down one line	Press the Return key
To scroll down one screen	Press the Spacebar
To quit from the More program	Press the Q key

Using Command Aliases

Aliases are not case sensitive; also, some aliases cannot be abbreviated. [Table 2-3](#) lists the switch CLI aliases that cannot be abbreviated.

Table 2-3 Command Aliases That Cannot Be Abbreviated

Alias	Command
?	help
batch	configure
di	show
exit	quit
logout	quit

Specifying Modules, Ports, and VLANs

The Catalyst 4000 family switches sequentially number modules, ports, and VLANs, beginning with 1. The supervisor engine module is module 1, residing in slot 1.

To designate a specific module, use the module number. In most systems, the module number and the slot number are the same.

The fixed-configuration switches have two logical modules. The Catalyst 4912G, the Catalyst 2948G, and the Catalyst 2980G switches have two modules but only one slot. When you enter configuration commands on these switches, you must refer to the module number, not the slot number. For example, all of the user-configurable ports on these switches are logically on module 2.

On modules that have user-configurable ports, the left-most port is always port 1. To designate a specific port on a specific module, the command syntax is *mod_num/port_num*. For example, **3/1** specifies module 3, port 1. On the Catalyst 4912G, the Catalyst 2948G, and the Catalyst 2980G switches, the left-most switch port is numbered 2/1 instead of 1/1 because logically the ports are located on module 2.

With many commands, you can enter lists of ports. To specify a range of ports, use a comma-separated list (do not insert spaces) to specify individual ports or a hyphen (-) between the port numbers to specify a range of ports.

[Table 2-4](#) shows examples of how to designate ports and port ranges.

*CISCO Confidential - DRAFT***Table 2-4 Designating Ports and Port Ranges**

Example	Function
2/1	Specifies port 1 on module 2
3/4-8	Specifies ports 4, 5, 6, 7, and 8 on module 3
5/2,5/4,6/10	Specifies ports 2 and 4 on module 5 and port 10 on module 6
3/1-2,4/8	Specifies ports 1 and 2 on module 3 and port 8 on module 4

VLANs are identified using the VLAN ID, a single number that is associated with the VLAN. To specify a list of VLANs, use a comma-separated list (do not insert spaces) to specify individual VLANs or a hyphen (-) between the VLAN numbers to specify a range of VLANs.

[Table 2-5](#) shows examples of how to designate VLANs and VLAN ranges.

Table 2-5 Designating VLANs and VLAN Ranges

Example	Function
10	Specifies VLAN 10
5, 10, 15	Specifies VLANs 5, 10, and 15
10-50, 500	Specifies VLANs 10 through 50, inclusive, and VLAN 500

Specifying MAC Addresses

Some commands require that you specify a MAC address, which must be designated in a standard format. The MAC address format must be six hexadecimal numbers separated by hyphens, as shown in this example:

```
00-00-0c-24-d2-fe
```

Specifying IP Addresses, Host Names, and IP Aliases

Some commands require an IP address, IP host name, or IP alias. The IP address format is 32 bits, written in dotted decimal format, as shown in the following example:

```
172.16.10.1
```

If DNS is configured properly on the switch, you can use IP host names instead of IP addresses. For information on configuring DNS, see [Chapter 38, “Configuring DNS.”](#)

You can also configure IP aliases on the switch, which you can use in place of IP addresses. IP aliases can be used for most commands that use an IP address, except for commands that define the IP address or IP alias. For information on using IP aliases, see the [“Defining and Using IP Aliases” section on page 27-7.](#)

You can enter ROM monitor mode by pressing **Ctrl-C** within the first 5 seconds of startup. Once you are in ROM monitor mode, the prompt changes to `rommon>`. Enter the `?` command to see the available ROM monitor commands.



Note

Example of a Catalyst 4003 Bootup Display

```
WS-X4012 bootrom version 4.5(1), built on 1999.03.29 21:04:04
H/W Revisions:    Meteor: 4    Comet: 8    Board: 2
Supervisor MAC addresses: 00:d0:58:70:a1:00 through 00:d0:58:70:a4:ff (1024 addresses)
Installed memory: 32 MB
Testing LEDs.... done!
The system will autoboot in 5 seconds.
Type control-C to prevent autobooting.
rommon 1 >
The system will now begin autobooting.
Autobooting image: "bootflash:cat4000.5-1-1a.bin"
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCC#####
Starting Off-line Diagnostics
Mapping in TempFs
Board type is WS-X4012
DiagBootMode value is "post"
Loading diagnostics...
```

```
Power-on-self-test for Module 1:  WS-X4012
Status: (. = Pass, F = Fail)
processor: .           cpu sdr: .           temperature sensor: .
enet console port: .  nvram: .             switch sram: .
switch registers: .   switch port 0: .       switch port 1: .
switch port 2: .      switch port 3: .       switch port 4: .
switch port 5: .      switch port 6: .       switch port 7: .
switch port 8: .      switch port 9: .       switch port 10: .
switch port 11: .     switch bandwidth: .
```

Module 1 Passed

```
Power-on-self-test for Module 2:  WS-X4148
Port status: (. = Pass, F = Fail)
 1: .   2: .   3: .   4: .   5: .   6: .   7: .   8: .
 9: .  10: .  11: .  12: .  13: .  14: .  15: .  16: .
17: .  18: .  19: .  20: .  21: .  22: .  23: .  24: .
25: .  26: .  27: .  28: .  29: .  30: .  31: .  32: .
33: .  34: .  35: .  36: .  37: .  38: .  39: .  40: .
```

CISCO Confidential - DRAFT

41: . 42: . 43: . 44: . 45: . 46: . 47: . 48: .

Module 2 Passed

Power-on-self-test for Module 3: WS-X4306
 Port status: (. = Pass, F = Fail, ? = no GBIC)
 1: . 2: . 3: . 4: ? 5: ? 6: ?

Module 3 Passed

Exiting Off-line Diagnostics

IP address for Catalyst not configured
 BOOTP/DHCP will commence after the ports are online
 Ports are coming online ...

Cisco Systems, Inc. Console

Enter password:
 1999 Aug 12 14:34:05 %SYS-5-MOD_OK:Module 1 is online
 1999 Aug 12 14:34:08 %SYS-5-MOD_OK:Module 3 is online
 1999 Aug 12 14:34:11 %SYS-5-MOD_OK:Module 2 is online
 Sending RARP request with address 00:d0:58:70:a4:ff
 Sending BOOTP request with address: 00:d0:58:70:a4:ff
 Sending RARP request with address 00:d0:58:70:a4:ff
 Sending BOOTP request with address: 00:d0:58:70:a4:ff
 Sending RARP request with address 00:d0:58:70:a4:ff
 Sending BOOTP request with address: 00:d0:58:70:a4:ff
 Sending RARP request with address 00:d0:58:70:a4:ff
 Sending BOOTP request with address: 00:d0:58:70:a4:ff
 Sending RARP request with address 00:d0:58:70:a4:ff
 Sending BOOTP request with address: 00:d0:58:70:a4:ff
 Sending RARP request with address 00:d0:58:70:a4:ff
 Sending BOOTP request with address: 00:d0:58:70:a4:ff
 Sending RARP request with address 00:d0:58:70:a4:ff
 Sending BOOTP request with address: 00:d0:58:70:a4:ff
 Sending RARP request with address 00:d0:58:70:a4:ff
 Sending BOOTP request with address: 00:d0:58:70:a4:ff
 Sending RARP request with address 00:d0:58:70:a4:ff
 Sending BOOTP request with address: 00:d0:58:70:a4:ff
 No bootp or rarp response received

**Note**

The system initiates DHCP/BOOTP and Reverse Address Resolution Protocol (RARP) requests at startup only when the sc0 interface IP address is set to 0.0.0.0. For more information, see the [“Using DHCP or RARP to Obtain an IP Address Configuration”](#) section on page 3-9.

Configuring the Switch IP Address and Default Gateway

This chapter describes how to configure the IP address, subnet mask, and default gateway on the Catalyst enterprise LAN switches.

**Note**

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 4500 Series, Catalyst 2948G, and Catalyst 2980G Switches Command Reference*.

This chapter consists of these sections:

- [Understanding How the Switch Management Interfaces Work, page 3-1](#)
- [Understanding How Automatic IP Configuration Works, page 3-2](#)
- [Preparing to Configure the IP Address and Default Gateway, page 3-4](#)
- [Default IP Address and Default Gateway Configuration, page 3-5](#)
- [Setting the In-Band \(sc0\) Interface IP Address, page 3-5](#)
- [Setting the Management Ethernet \(me1\) Interface IP Address, page 3-6](#)
- [Configuring Default Gateways, page 3-6](#)
- [Configuring the SLIP \(sl0\) Interface on the Console Port, page 3-8](#)
- [Using DHCP or RARP to Obtain an IP Address Configuration, page 3-9](#)
- [Renewing and Releasing a DHCP-Assigned IP Address, page 3-10](#)

Understanding How the Switch Management Interfaces Work

The Catalyst 4000 family, the Catalyst 2948G, and the Catalyst 2980G switches have three management interfaces:

- In-band interface (sc0)
- SLIP interface (sl0)
- Management Ethernet interface (me1)

The in-band (sc0) management interface is connected to the switching fabric and participates in all of the functions of a normal switch port, such as spanning tree, Cisco Discovery Protocol (CDP), and VLAN membership. The out-of-band management interfaces (me1 and sl0) are not connected to the switching fabric and do not participate in any of these functions.

CISCO Confidential - DRAFT

When you configure the IP address, subnet mask, and broadcast address (and when you configure VLAN membership on the sc0 interface) of the sc0 or me1 interface, you can access the switch through Telnet or SNMP. When you configure the SLIP (sl0) interface, you can open a point-to-point connection to the switch through the console port from a workstation.

All IP traffic that is generated by the switch (for example, a Telnet session that is opened from the switch to a host) is forwarded according to the entries in the switch IP routing table. For intersubnetwork communication to occur, you must configure at least one default gateway for the sc0 or me1 interface. The switch IP routing table is used to forward traffic originating on the switch only, not for forwarding traffic sent by devices that are connected to the switch.

Because sc0 and me1 are two distinct interfaces, they potentially can have duplicate IP addresses or overlapping subnets. Therefore, when you enter a command that causes sc0 and me1 to have the same IP address or occupy the same subnet, the switch software brings one of the interfaces down.

In most cases, the switch software brings down the sc0 interface after you confirm the change. However, when the switch boots with the IP address 0.0.0.0 configured on both the sc0 and me1 interfaces, the me1 interface is brought down to allow BOOTP and RARP requests to broadcast out the sc0 interface.

**Note**

When the switch boots with the IP address 0.0.0.0 configured on both the sc0 and me1 interfaces, the me1 interface is automatically brought down by the switch software. You are not asked to confirm the change, and no console messages or traps are generated in this case.

Duplicate IP addresses and equal subnets are allowed on the sc0 and me1 interfaces if one of the interfaces is configured down. Non-equal subnets are not allowed (for example, sc0 with IP address 10.1.1.1 and subnet mask 255.0.0.0 and me1 with IP address 10.1.1.2 and subnet mask 255.255.255.0).

Understanding How Automatic IP Configuration Works

These sections describe how the switch can obtain its IP configuration automatically:

- [Automatic IP Configuration Overview, page 3-2](#)
- [Understanding DHCP, page 3-3](#)
- [Understanding RARP, page 3-4](#)

Automatic IP Configuration Overview

The switch can obtain its IP configuration automatically using one of the following protocols:

- Dynamic Host Configuration Protocol (DHCP)
- Reverse Address Resolution Protocol (RARP)

The switch makes DHCP and RARP requests only if the sc0 interface IP address is set to 0.0.0.0 when the switch boots up. This address is the default for a new switch or a switch whose configuration file has been cleared using the **clear config all** command. DHCP and RARP requests are only broadcast out the sc0 interface.

**Note**

If the CONFIG_FILE environment variable is set, all configuration files are processed before the switch determines whether to broadcast DHCP and RARP requests. For more information about the CONFIG_FILE environment variable, see [Chapter 32, “Modifying the Switch Boot Configuration.”](#)

CISCO Confidential - DRAFT

If both the sc0 and me1 interfaces are unconfigured (IP address 0.0.0.0), the me1 interface is brought down to allow the switch to broadcast requests on the sc0 interface. If the me1 interface is configured and the sc0 interface is not, requests are not sent. Similarly, if the sc0 interface is not configured but the interface is configured down, requests are not sent.

Understanding DHCP

In software release 5.2 and later releases, the switch can obtain an IP address and other IP configuration information using DHCP.

There are three methods for obtaining an IP address from the DHCP server:

- Manual allocation—The network administrator maps the switch MAC address to an IP address at the DHCP server.
- Automatic allocation—The switch obtains an IP address when it first contacts the DHCP server. The address is permanently assigned to the switch.
- Dynamic allocation—The switch obtains a “leased” IP address for a specified period of time. The IP address is revoked at the end of this period, and the switch surrenders the address. The switch must request another IP address.

In addition to the sc0 interface IP address, the switch can obtain the subnet mask, broadcast address, default gateway address, and other information. DHCP-learned values are not used if user-configured values are present.

The switch broadcasts a DHCPDISCOVER message 1 to 10 seconds after all of the switch ports are online. The switch always requests an infinite lease time in the DHCPDISCOVER message.

If a DHCP or Bootstrap Protocol (BOOTP) server responds to the request, the switch takes appropriate action. If a DHCPOFFER message is received from a DHCP server, the switch processes all the supported options that are contained in the message. [Table 3-1](#) shows the supported DHCP options. Other options that are specified in the DHCPOFFER message are ignored.

Table 3-1 Supported DHCP Options

Code	Option
1	Subnet mask
2	Time offset
3	Router
6	Domain name server
12	Hostname
15	Domain name
28	Broadcast address
33	Static route
42	NTP servers
51	IP address lease time
52	Option overload
61	Client-identifier
66	TFTP server name

CISCO Confidential - DRAFT

If a BOOTP response is received from a BOOTP server, the switch sets the in-band (sc0) interface IP address to the address that is specified in the BOOTP response.

If no DHCPOFFER message or BOOTP response is received in reply, the switch rebroadcasts the request using an exponential backoff algorithm (the amount of time between requests increases exponentially). If no response is received after 10 minutes, the sc0 interface IP address remains set to 0.0.0.0 (provided that RARP requests fail as well).

If you reset or power cycle a switch with a DHCP- or BOOTP-obtained IP address, the information learned from DHCP or BOOTP is retained. At boot up, the switch attempts to renew the lease on the IP address. If no reply is received, the switch retains the current IP address.

Understanding RARP

With RARP, you map the switch MAC address to an IP address on the RARP server. The switch retrieves its IP address from the server automatically when it boots up.

The switch broadcasts ten RARP requests after all of the switch ports are online. If a response is received, the switch sets the in-band (sc0) interface IP address to the address that is specified in the RARP response.

If no reply is received, the sc0 interface IP address remains set to 0.0.0.0 (provided that DHCP requests fail as well).

If you reset or power cycle a switch with a RARP-obtained IP address, the information that is learned from RARP is retained.

Preparing to Configure the IP Address and Default Gateway

Before you configure the switch IP address and default gateway, obtain the following information, as appropriate:

- IP address for the switch (sc0 and me1 interfaces only)
- Subnet mask/number of subnet bits (sc0 and me1 interfaces only)
- (Optional) Broadcast address (sc0 and me1 interfaces only)
- VLAN membership (sc0 interface only)
- SLIP and SLIP destination addresses (sl0 interface only)
- Interface connection type:
 - In-band (sc0) interface

Configure this interface when assigning an IP address, subnet mask, and VLAN to the in-band management interface on the switch.
 - Out-of-band management Ethernet (me1) interface

Configure this interface when assigning an IP address and subnet mask to the out-of-band management Ethernet interface on the switch.
 - SLIP (sl0) interface

Configure this interface when setting up a point-to-point SLIP connection between a terminal and the switch.

CISCO Confidential - DRAFT

Default IP Address and Default Gateway Configuration

Table 3-2 shows the default IP address and default gateway configuration.

Table 3-2 Switch IP Address and Default Gateway Default Configuration

Feature	Default Value
In-band (sc0) interface	- IP address, subnet mask, and broadcast address set to 0.0.0.0 - Assigned to VLAN 1
Management Ethernet (me1) interface	IP address, subnet mask, and broadcast address set to 0.0.0.0
Default gateway address	Set to 0.0.0.0 with a metric of 0
SLIP (sl0) interface	- IP address and SLIP destination address set to 0.0.0.0 - SLIP for the console port is not active (set to detach)

Setting the In-Band (sc0) Interface IP Address

Before you can Telnet to the switch or use Simple Network Management Protocol (SNMP) to manage the switch, you must assign an IP address to either the in-band (sc0) logical interface or the management Ethernet (me1) interface.

You can specify the subnet mask (*netmask*) using the number of subnet bits or using the subnet mask in dotted decimal format.

To set the IP address and VLAN membership of the in-band (sc0) management interface, perform this task in privileged mode:

	Task	Command
Step 1	Assign an IP address, subnet mask (or number of subnet bits), and (optional) broadcast address to the in-band (sc0) interface.	set interface sc0 [<i>ip_addr</i> [/ <i>netmask</i>] [<i>broadcast</i>]]
Step 2	Assign the in-band interface to the proper VLAN (make sure that the VLAN is associated with the network to which the IP address belongs).	set interface sc0 [<i>vlan</i>]
Step 3	If necessary, bring the interface up.	set interface sc0 up
Step 4	Verify the interface configuration.	show interface

This example shows how to assign an IP address, specify the number of subnet bits, and specify the VLAN assignment for the in-band (sc0) interface:

```
Console> (enable) set interface sc0 172.20.52.124/29
Interface sc0 IP address and netmask set.
Console> (enable) set interface sc0 5
Interface sc0 vlan set.
Console> (enable)
```

This example shows how to specify the VLAN assignment, assign an IP address, specify the subnet mask in dotted decimal format, and verify the configuration:

```
Console> (enable) set interface sc0 5 172.20.52.124/255.255.255.248
Interface sc0 vlan set, IP address and netmask set.
Console> (enable) show interface
sl0: flags=51<UP,POINTOPOINT,RUNNING>
    slip 0.0.0.0 dest 0.0.0.0
sc0: flags=63<UP,BROADCAST,RUNNING>
    vlan 5 inet 172.20.52.124 netmask 255.255.255.248 broadcast 172.20.52.17
Console> (enable)
```

Setting the Management Ethernet (me1) Interface IP Address

Before you can Telnet to the switch or use SNMP to manage the switch, you must assign an IP address to either the in-band (sc0) logical interface or the management Ethernet (me1) interface. The me1 interface is present only on the Catalyst 4000 family, Catalyst 2948G, and Catalyst 2980G switches.

You can specify the subnet mask (*netmask*) using the number of subnet bits or using the subnet mask in dotted decimal format.

To set the management Ethernet (me1) interface IP address, perform this task in privileged mode:

	Task	Command
Step 1	Assign an IP address and subnet mask to the management Ethernet (me1) interface.	set interface me1 [<i>ip_addr[/netmask]</i>]
Step 2	If necessary, bring the interface up.	set interface me1 up
Step 3	Verify the interface configuration.	show interface

This example shows how to assign an IP address and subnet mask to the management Ethernet (me1) interface and how to verify the interface configuration:

```
Console> (enable) set interface me1 172.20.52.12/255.255.255.224
Interface me1 IP address and netmask set.
Console> (enable) show interface
sl0: flags=51<UP,POINTOPOINT,RUNNING>
    slip 0.0.0.0 dest 0.0.0.0
sc0: flags=63<UP,BROADCAST,RUNNING>
    vlan 1 inet 0.0.0.0 netmask 0.0.0.0 broadcast 0.0.0.0
me1: flags=63<UP,BROADCAST,RUNNING>
    inet 172.20.52.12 netmask 255.255.255.224 broadcast 172.20.52.31
Console> (enable)
```

Configuring Default Gateways

The supervisor engine sends IP packets that are destined for other IP subnets to the default gateway (typically a router interface in the same network or subnet as the switch IP address). The switch does not use the IP routing table to forward traffic from connected devices, only IP traffic generated by the switch itself (for example, Telnet, TFTP, and ping).



Note

In some cases, you might want to configure static IP routes in addition to default gateways. For information on configuring static routes, see the [“Configuring Static Routes” section on page 27-9](#).

CISCO Confidential - DRAFT

You can define up to three default IP gateways. Use the **primary** keyword to make a gateway the primary gateway. If you do not specify a primary default gateway, the first gateway that is configured is the primary gateway. If more than one gateway is designated as primary, the last primary gateway that is configured is the primary default gateway.

The switch sends all off-network IP traffic to the primary default gateway. If connectivity to the primary gateway is lost, the switch attempts to use the backup gateways in the order they were configured. The switch sends periodic ping messages to determine whether each default gateway is up or down. If connectivity to the primary gateway is restored, the switch resumes sending traffic to the primary.

If both the in-band (sc0) and management Ethernet (me1) interfaces are configured when you specify default gateways, then the switch software automatically determines through which interface each default gateway can be reached.

To specify one or more default gateways, perform this task in privileged mode:

	Task	Command
Step 1	Configure a default IP gateway address for the switch.	set ip route default gateway [metric] [primary]
Step 2	(Optional) Configure additional default gateways for the switch.	set ip route default gateway [metric] [primary]
Step 3	Verify that the default gateways appear correctly in the IP routing table.	show ip route

To remove default gateway entries, perform one of these tasks in privileged mode:

Task	Command
Clear an individual default gateway entry.	clear ip route default gateway
Clear all default gateways and static routes.	clear ip route all

This example shows how to configure three default gateways on the switch and how to verify the default gateway configuration:

```

Console> (enable) set ip route default 10.1.1.10
Route added.
Console> (enable) set ip route default 10.1.1.20
Route added.
Console> (enable) set ip route default 10.1.1.1 primary
Route added.
Console> (enable) show ip route
Fragmentation    Redirect    Unreachable
-----
enabled          enabled     enabled

```

```

The primary gateway: 10.1.1.1
Destination      Gateway          RouteMask        Flags    Use      Interface
-----
default          10.1.1.1         0x0              UG       6        sc0
default          10.1.1.20        0x0              G        0        sc0
default          10.1.1.10        0x0              G        0        sc0
10.0.0.0         10.1.1.100       0xff000000       U        75       sc0
default          default          0xff000000       UH       0        sl0
Console> (enable)

```

CISCO Confidential - DRAFT

This example shows how to configure two default gateways on a Catalyst 4000 family, Catalyst 2948G, or Catalyst 2980G switch, with one default gateway reachable through the sc0 interface and one reachable through the me1 interface:

```

Console> (enable) show interface
sl0: flags=50<DOWN,POINTOPOINT,RUNNING>
      slip 0.0.0.0 dest 0.0.0.0
sc0: flags=63<UP,BROADCAST,RUNNING>
      vlan 5 inet 172.20.52.38 netmask 255.255.255.240 broadcast 172.20.52.47
me1: flags=63<UP,BROADCAST,RUNNING>
      inet 10.1.1.100 netmask 255.255.255.0 broadcast 10.1.1.255
Console> (enable) set ip route default 172.20.52.33
Route added.
Console> (enable) set ip route default 10.1.1.1
Route added.
Console> (enable) show ip route
Fragmentation    Redirect    Unreachable
-----
enabled          enabled    enabled

The primary gateway: 172.20.52.33
Destination      Gateway      RouteMask    Flags    Use    Interface
-----
default          10.1.1.1     0x0          G        0      me1
default          172.20.52.33 0x0          UG       12     sc0
172.20.52.32     4000-2       0xffffffff0  U        180    sc0
10.1.1.0         10.1.1.100   0xffffffff00 U        22     me1
Console> (enable)

```

Configuring the SLIP (sl0) Interface on the Console Port

Use the SLIP (sl0) interface for point-to-point SLIP connections between the switch and an IP host.



Caution

You *must* use the console port for the SLIP connection. When the SLIP connection is enabled and SLIP is attached on the console port, an EIA/TIA-232 terminal cannot connect through the console port. If you are connected to the switch CLI through the console port and you enter the **slip attach** command, you will lose the console port connection. Use Telnet to access the switch, enter privileged mode, and enter the **slip detach** command to restore the console port connection.

To enable and attach SLIP on the console port, perform this task:

	Task	Command
Step 1	Access the switch from a remote host with Telnet.	telnet {host_name ip_addr}
Step 2	Enter privileged mode on the switch.	enable
Step 3	Set the console port SLIP address and the destination address of the attached host.	set interface sl0 slip_addr dest_addr
Step 4	Verify the SLIP interface configuration.	show interface
Step 5	Enable SLIP for the console port.	slip attach

To disable SLIP on the console port, perform this task:

CISCO Confidential - DRAFT

	Task	Command
Step 1	Access the switch from a remote host with Telnet.	telnet { <i>host_name</i> <i>ip_addr</i> }
Step 2	Enter privileged mode on the switch.	enable
Step 3	Disable SLIP for the console port.	slip detach

This example shows how to configure SLIP on the console port and verify the configuration:

```
sparc20% telnet 172.20.52.38
Trying 172.20.52.38 ...
Connected to 172.20.52.38.
Escape character is '^J'.

Cisco Systems, Inc. Console

Enter password:
Console> enable

Enter password:
Console> (enable) set interface sl0 10.1.1.1 10.1.1.2
Interface sl0 slip and destination address set.
Console> (enable) show interface
sl0: flags=51<UP,POINTOPOINT,RUNNING>
      slip 10.1.1.1 dest 10.1.1.2
sc0: flags=63<UP,BROADCAST,RUNNING>
      vlan 522 inet 172.20.52.38 netmask 255.255.255.240 broadcast 172.20.52.7
me1: flags=62<DOWN,BROADCAST,RUNNING>
      inet 10.1.1.100 netmask 255.255.255.0 broadcast 10.1.1.255
Console> (enable) slip attach
Console Port now running SLIP.

Console> (enable) slip detach
SLIP detached on Console port.
Console> (enable)
```

Using DHCP or RARP to Obtain an IP Address Configuration



Note

For complete information on how the switch uses DHCP or RARP to obtain its IP configuration, see the [“Understanding How Automatic IP Configuration Works” section on page 3-2](#).

To use DHCP or RARP to obtain an IP address for the switch, perform this task:

	Task	Command
Step 1	Make sure that there is a DHCP, BOOTP, or RARP server on the network.	—
Step 2	Obtain the last address in the MAC address range for module 1 (the supervisor engine). This address is displayed under the MAC-Address(es) heading. (With DHCP, this step is necessary only if using the manual allocation method.)	show module

CISCO Confidential - DRAFT

	Task	Command
Step 3	Add an entry for each switch in the DHCP, BOOTP, or RARP server configuration, mapping the MAC address of the switch to the IP configuration information for the switch. (With DHCP, this step is necessary only with the manual or automatic allocation methods.)	—
Step 4	Set the sc0 interface IP address to 0.0.0.0.	set interface sc0 0.0.0.0
Step 5	Reset the switch. The switch broadcasts DHCP and RARP requests only when the switch boots up.	reset system
Step 6	When the switch reboots, confirm that the sc0 interface IP address, subnet mask, and broadcast address are set correctly.	show interface
Step 7	For DHCP, confirm that other options (such as the default gateway address) are set correctly.	show ip route

This example shows the switch broadcasting a DHCP request, receiving a DHCP offer, and configuring the IP address and other IP parameters according to the contents of the DHCP offer:

```

Console> (enable) Sending RARP request with address 00:90:0c:5a:8f:ff
Sending DHCP packet with address: 00:90:0c:5a:8f:ff
dhcpooffer
Sending DHCP packet with address: 00:90:0c:5a:8f:ff
Timezone set to '', offset from UTC is 7 hours 58 minutes
Timezone set to '', offset from UTC is 7 hours 58 minutes
172.16.30.32 added to DNS server table as primary server.
172.16.31.32 added to DNS server table as backup server.
172.16.32.32 added to DNS server table as backup server.
NTP server 172.16.25.253 added
NTP server 172.16.25.252 added
%MGMT-5-DHCP_S:Assigned IP address 172.20.25.244 from DHCP Server 172.20.25.254
Console> (enable) show interface
sl0: flags=51<UP,POINTOPOINT,RUNNING>
    slip 0.0.0.0 dest 0.0.0.0
sc0: flags=63<UP,BROADCAST,RUNNING>
    vlan 1 inet 172.20.25.244 netmask 255.255.255.0 broadcast 172.20.25.255
dhcp server: 172.20.25.254
Console>

```

Renewing and Releasing a DHCP-Assigned IP Address

If you are using DHCP for IP address assignment, you can perform either of these tasks:

- Renew—Renew the lease on a DHCP-assigned IP address.
- Release—Release the lease on a DHCP-assigned IP address.

To renew or release a DHCP-assigned IP address on the in-band (sc0) management interface, perform one of these tasks in privileged mode:

Task	Command
Renew the lease on a DHCP-assigned IP address.	set interface sc0 dhcp renew
Release the lease on a DHCP-assigned IP address.	set interface sc0 dhcp release

CISCO Confidential - DRAFT

This example shows how to renew the lease on a DHCP-assigned IP address:

```
Console> (enable) set interface sc0 dhcp renew  
Renewing IP address...  
Console> (enable) Sending DHCP packet with address: 00:90:0c:5a:8f:ff  
<...output truncated...>
```

This example shows how to release the lease on a DHCP-assigned IP address:

```
Console> (enable) set interface sc0 dhcp release  
Releasing IP address...  
Console> (enable) Sending DHCP packet with address: 00:90:0c:5a:8f:ff  
Done  
  
Console> (enable)
```

CISCO Confidential - DRAFT

Configuring Ethernet and Fast Ethernet Switching

This chapter describes how to configure Ethernet and Fast Ethernet switching on the Catalyst enterprise LAN switches. The configuration procedures in this chapter apply to Ethernet and Fast Ethernet switch ports on switching modules and fixed-configuration switches, as well as to supervisor engine Fast Ethernet uplink ports.

**Note**

For complete information on installing Catalyst 4000 family Fast Ethernet modules, refer to the *Catalyst 4000 Family Installation Guide*.

**Note**

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 4500 Series, Catalyst 2948G, and Catalyst 2980G Switches Command Reference*.

This chapter consists of these sections:

- [Understanding How Ethernet Works, page 4-1](#)
- [Default Ethernet and Fast Ethernet Configurations, page 4-2](#)
- [Configuring Ethernet and Fast Ethernet Ports, page 4-3](#)

Understanding How Ethernet Works

These sections describe how Ethernet switching works on the Catalyst enterprise LAN switches:

- [Ethernet Overview, page 4-1](#)
- [Switching Frames Between Segments, page 4-2](#)
- [Building the Address Table, page 4-2](#)

Ethernet Overview

The Catalyst enterprise LAN switches support simultaneous, parallel conversations between 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.

CISCO Confidential - DRAFT

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

Because the major bottleneck in Ethernet networks is usually due to collisions, an effective solution is full-duplex communication, which is an option for each port on the switches (Gigabit Ethernet ports support *only* full duplex). 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 for Ethernet ports is 20 Mbps, for Fast Ethernet ports it is 200 Mbps, and for Gigabit Ethernet ports it is 2 Gbps.

Switching Frames Between Segments

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

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

To reduce degradation, the Catalyst enterprise LAN switches treat each port as an individual segment. When stations on different ports need to communicate, the switch forwards frames from one port to the other at wire speed to ensure that each session receives the full bandwidth that is available.

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

Building the Address Table

The switch builds the address table by using the source address of the frames received. When the switch receives a frame for a destination address that is not yet listed in its address table, it floods the frame to all ports of the same virtual LAN (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 port without flooding to all ports.

The address table can store at least 16,000 address entries without flooding any entries. The switch uses an aging mechanism, which is 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.

Default Ethernet and Fast Ethernet Configurations

Table 4-1 lists the Ethernet and Fast Ethernet default configurations.

*CISCO Confidential - DRAFT***Table 4-1 Ethernet and Fast Ethernet Default Configurations**

Feature	Default Value
Port enable state	All ports are enabled
Port name	None
Port priority	Normal
Duplex mode	- Autonegotiate speed and duplex for 10/100-Mbps Fast Ethernet ports - Autonegotiate duplex for 100-Mbps Fast Ethernet ports
Native VLAN	VLAN 1
Spanning tree port cost	- Port cost of 100 for 10-Mbps Ethernet ports - Port cost of 19 for 10/100-Mbps Fast Ethernet ports - Port cost of 19 for 100-Mbps Fast Ethernet ports
Fast EtherChannel	Disabled on all Fast Ethernet ports (auto mode)

Configuring Ethernet and Fast Ethernet Ports

These sections describe how to configure Ethernet and Fast Ethernet switching ports on the Catalyst enterprise LAN switches:

- [Setting Ethernet and Fast Ethernet Port Names, page 4-3](#)
- [Setting Ethernet and Fast Ethernet Port Priority Levels, page 4-4](#)
- [Setting Ethernet and Fast Ethernet Port Speeds, page 4-4](#)
- [Setting Ethernet and Fast Ethernet Port Duplex Modes, page 4-5](#)
- [Setting Ethernet and Fast Ethernet Port Debounce Timers, page 4-6](#)
- [Configuring errdisable State Ethernet and Fast Ethernet Port Timeout Periods, page 4-7](#)
- [Checking Ethernet and Fast Ethernet Port Connectivity, page 4-8](#)

**Note**

For information on configuring Fast EtherChannel, see [Chapter 6, “Configuring Fast EtherChannel and Gigabit EtherChannel.”](#)

Setting Ethernet and Fast Ethernet Port Names

You can assign names to the ports on Ethernet and Fast Ethernet modules to facilitate switch administration.

To assign a name to a port, perform this task in privileged mode:

	Task	Command
Step 1	Assign a name to a port.	set port name <i>mod_num/port_num</i> [<i>name_string</i>]
Step 2	Verify that the port name is configured.	show port [<i>mod_num[/port_num]</i>]

CISCO Confidential - DRAFT

This example shows how to set the name for ports 1/1 and 1/2 and how to verify that the port names are configured correctly:

```

Console> (enable) set port name 1/1 Router Connection
Port 1/1 name set.
Console> (enable) set port name 1/2 Server Link
Port 1/2 name set.
Console> (enable) show port 1
Port  Name                Status      Vlan      Level Duplex Speed Type
-----
 1/1 Router Connection    connected trunk    normal half  100 100BaseTX
 1/2 Server Link          connected trunk    normal half  100 100BaseTX

<...output truncated...>

Last-Time-Cleared
-----
Tue Jun 16 1998, 16:25:57
Console> (enable)

```

Setting Ethernet and Fast Ethernet Port Priority Levels

You can configure the priority level of each port. When ports request access to the switching bus simultaneously, the switch uses port priority level to determine the order in which to give ports access.

To set the port priority level, perform this task in privileged mode:

	Task	Command
Step 1	Configure the priority level for a port.	set port level <i>mod_num/port_num</i> {normal high}
Step 2	Verify that the port priority level is configured correctly.	show port [<i>mod_num</i> [/port_num]]

This example shows how to set the port priority level to high for port 1/1 and verify that the port priority is configured correctly:

```

Console> (enable) set port level 1/1 high
Port 1/1 level set to high.
Console> (enable) show port 1
Port  Name                Status      Vlan      Level Duplex Speed Type
-----
 1/1 Router Connection    connected trunk    high   half  100 100BaseTX
 1/2 Server Link          connected trunk    normal half  100 100BaseTX

<...output truncated...>

Last-Time-Cleared
-----
Tue Jun 16 1998, 16:25:57
Console> (enable)

```

Setting Ethernet and Fast Ethernet Port Speeds

You can configure the port speed on 10/100-Mbps Fast Ethernet modules. Use the **auto** keyword to have the port autonegotiate speed and duplex mode with the neighboring port.

CISCO Confidential - DRAFT**Caution**

Make sure that the device on the other end of the link is also configured for autonegotiation, or a port speed or duplex mismatch will result.

**Note**

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

To set the port speed for a 10/100-Mbps port, perform this task in privileged mode:

	Task	Command
Step 1	Set the port speed of a 10/100-Mbps Fast Ethernet port.	set port speed <i>mod num/port num</i> { 10 100 auto }
Step 2	Verify that the speed of the port is configured correctly.	show port [<i>mod_num</i> [/ <i>port_num</i>]]

This example shows how to set the port speed to 100 Mbps on port 2/2:

```
Console> (enable) set port speed 2/2 100
Port 2/2 speed set to 100 Mbps.
Console> (enable)
```

This example shows how to make port 2/1 autonegotiate speed and duplex with the neighbor port:

```
Console> (enable) set port speed 2/1 auto
Port 2/1 speed set to auto-sensing mode.
Console> (enable)
```

Setting Ethernet and Fast Ethernet Port Duplex Modes

You can set the port duplex mode to full or half duplex for Ethernet and Fast Ethernet ports.

**Note**

If the port speed is set to **auto** on a 10/100-Mbps Fast Ethernet port, both speed and duplex are autonegotiated. You cannot change the duplex mode of ports that are configured for autonegotiation. For information on enabling and disabling autonegotiation on 10/100 Fast Ethernet ports, see the [“Setting Ethernet and Fast Ethernet Port Speeds”](#) section on page 4-4.

To set the duplex mode of a port, perform this task in privileged mode:

	Task	Command
Step 1	Set the duplex mode of a port.	set port duplex <i>mod num/port num</i> { full half }
Step 2	Verify that the duplex mode of the port is configured correctly.	show port [<i>mod_num</i> [/ <i>port_num</i>]]

This example shows how to set the duplex mode to half duplex on port 2/1:

```
Console> (enable) set port duplex 2/1 half
Port 2/1 set to half-duplex.
Console> (enable)
```

CISCO Confidential - DRAFT

Setting Ethernet and Fast Ethernet Port Debounce Timers

You can set the port debounce timer on a per-port basis for Ethernet, Fast Ethernet, and Gigabit Ethernet ports. When you set the port debounce timer, the switch delays notifying the main processor of a link down; this delay in notification can decrease traffic loss due to network reconfiguration.



Caution

Enabling the port debounce timer will delay link-up and link-down detections, resulting in loss of data traffic during the debouncing period. This situation might delay the convergence and reconvergence of various Layer 2 and Layer 3 protocols.

Table 4-2 lists the time delay that occurs before the switch notifies the main processor of a link down before and after the switch enables the debounce timer.

Table 4-2 Switch Notification Delays for the Port Debounce Timer

Port Type	Delay Time	
	With Debounce Timer Disabled	With Debounce Timer Enabled
10/100 ports	0 ms	3.1 sec
100BASE-FX ports	0 ms	3.1 sec
10/100/1000BASE-TX ports	0 ms	3.1 sec
Gigabit TX ports	0 ms	3.1 sec
Fiber Gigabit ports	0 ms	3.1 sec
		Note The delay time is the time that the port is physically down, and once the port is up, the time the software needs to complete autonegotiation.

To set the debounce timer on a port, perform this task in privileged mode:

	Task	Command
Step 1	Enable the debounce timer for a port.	set port debounce <i>mod num/port num {enable disable}</i>
Step 2	Verify that the debounce timer of the port is configured correctly.	show port debounce [<i>mod mod_num/port_num</i>]

This example shows how to enable the debounce timer for module 2 on port 1:

```
Console> (enable) set port debounce 2/1 enable
Debounce is enabled on port 2/1
Warning: Enabling port debounce causes Link Up/Down detections to be delayed.
It results in loss of data traffic during debouncing period, which might
affect the convergence/reconvergence of various Layer 2 and Layer 3 protocols.
Use with caution.
Console> (enable)
```

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

CISCO Confidential - DRAFT

```

Console> (enable) show port debounce
Port    Debounce link timer
-----
2/1     enable
2/2     disable
Console> (enable)

```

Configuring errdisable State Ethernet and Fast Ethernet Port Timeout Periods

A port is in errdisable state if it has been enabled in NVRAM but disabled at runtime by any process. For example, if the UniDirectional Link Detection (UDLD) detects a unidirectional link, the port shuts down at runtime. However, because the NVRAM configuration for the port is enabled (you have not disabled the port), the port status is shown as errdisable.

Currently, if a port goes into an errdisable state for whatever reason, it isreenabled automatically after a selected time interval. With the new timeout enhancement, you can manually prevent a particular port from being enabled by setting the errdisable timeout for that particular port to disable; you can do this with the **set port errdisable-timeout mod/port disable** command.



Note

The timeout enhancement does not have an effect on the *reason* value that is specified in the **set errdisable-timeout** command.

A global timer is maintained for all the ports. At every *t* seconds, where *t* is the user-configurable timeout, a process checks to see if any ports are in errdisable state. If so, only those ports that have the errdisable timeout set (“enabled”) are reenabled through System Control Protocol (SCP) messages.

By default, all the errdisabled ports are reenabled when the global timer times out.

You can enable or disable errdisable timeout for any of the *reasons* available for the **set errdisable-timeout** command. If you specify a reason of **other**, only those ports that have been put in errdisable state due to causes *other* than those listed in the command syntax are enabled for errdisable timeout. If you specify a reason of **all**, all ports that are errdisabled for any reason are enabled for errdisable timeout.

This feature is disabled by default. The default interval for enabling a port is 300 seconds. The allowable interval range is 30 to 86,400 seconds (30 seconds to 24 hours).

This example shows how to prevent port 3/3 from being enabled when it goes into errdisable state:

```

Console> (enable) set port errdisable-timeout 3/3 disable
Successfully disabled errdisable-timeout for port 3/3.
Console> (enable)

```

This example shows how to enable errdisable timeout when the reason is BPDU guard (**bpdu-guard**):

```

Console> (enable) set errdisable-timeout enable bpdu-guard
Successfully enabled errdisable-timeout for bpdu-guard.
Console> (enable)

```

This example shows how to set the errdisable timeout interval to 450 seconds:

```

Console> (enable) set errdisable-timeout interval 450
Successfully set errdisable timeout to 450 seconds.
Console>(enable)

```

This example shows how to display the errdisable timeout configuration:

```

Console> (enable) show errdisable-timeout
ErrDisable Reason    Timeout Status

```

CISCO Confidential - DRAFT

```

-----
bpduguard      Enable
channel-misconfig Disable
duplex-mismatch Enable
udld           Enable
other          Disable

Interval: 300 seconds

Ports that will be enabled at the next timeout:
Port  ErrDisable Reason
-----
3/1   udld
3/8   bpduguard
6/5   udld
7/24 duplex-mismatch
Console> (enable)

```

Checking Ethernet and Fast Ethernet Port Connectivity



Note

For more detailed information on checking connectivity, see [Chapter 20, “Checking Status and Connectivity.”](#)

Use the **ping** and **tracert** commands to test connectivity out Ethernet or Fast Ethernet ports.

To check connectivity out a port, perform this task in privileged mode:

	Task	Command
Step 1	Ping a remote host that is located out the port you want to test.	ping [-s] host [packet_size] [packet_count]
Step 2	Trace the hop-by-hop route of packets from the switch to a remote host that is located out the port you want to test.	tracert host
Step 3	If the host is unresponsive, check the IP address and default gateway that are configured on the switch.	show interface show ip route

This example shows how to ping a remote host and how to trace the hop-by-hop path of packets through the network using **tracert**:

```

Console> (enable) ping somehost
somehost is alive
Console> (enable) tracert somehost
tracert to somehost.company.com (10.1.2.3), 30 hops max, 40 byte packets
 1 engineering-1.company.com (173.31.192.206) 2 ms 1 ms 1 ms
 2 engineering-2.company.com (173.31.196.204) 2 ms 3 ms 2 ms
 3 gateway_a.company.com (173.16.1.201) 6 ms 3 ms 3 ms
 4 somehost.company.com (10.1.2.3) 3 ms * 2 ms
Console> (enable)

```



Configuring Gigabit Ethernet Switching

This chapter describes how to configure Gigabit Ethernet switching on the Catalyst enterprise LAN switches. The configuration procedures in this chapter apply to Gigabit Ethernet switching modules, fixed-configuration switches, and uplink ports on the supervisor engine.



Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 4500 Series, Catalyst 2948G, and Catalyst 2980G Switches Command Reference*.

This chapter consists of these sections:

- [Understanding How Gigabit Ethernet Works, page 5-1](#)
- [Default Gigabit Ethernet Configuration, page 5-6](#)
- [Configuring Gigabit Ethernet Ports, page 5-7](#)

Understanding How Gigabit Ethernet Works

The following sections describe how Gigabit Ethernet works.

Understanding How Gigabit Ethernet Flow Control Works

Flow control is a feature that Gigabit Ethernet ports use to inhibit the transmission of incoming packets. If a buffer on a Gigabit Ethernet port runs out of space, the port transmits a special packet that requests remote ports to delay sending packets for a period of time. This special packet is called a *pause frame*.

Sending and Receiving Pause Frames

All Catalyst 4000 family Gigabit Ethernet ports can receive and process pause frames from other devices. However, not all Catalyst 4000 family Gigabit Ethernet ports can transmit pause frames to other devices.

[Table 5-1](#) identifies the Catalyst Gigabit Ethernet switches, modules, and ports that can transmit pause frames to other devices.

Table 5-1 Send Capability by Switch Type, Module, and Ports

Switch Type	Module	Ports	Send
Catalyst 4000 Catalyst 4500	All modules except WS-X4418-GB and WS-X4412-2GB-T	All ports except for the oversubscribed ports listed below	No
Catalyst 4000 Catalyst 4500	WS-X4418-GB	Uplink ports (1–2)	No
Catalyst 4000 Catalyst 4500	WS-X4418-GB	Oversubscribed ports (3–18)	Yes
Catalyst 4000 Catalyst 4500	WS-X4412-2GB-T	Uplink ports (13–14)	No
Catalyst 4000 Catalyst 4500	WS-X4412-2GB-T	Oversubscribed ports (1–12)	Yes
Catalyst 4000 Catalyst 4500	WS-X4424-GB-RJ45	All ports	Yes
Catalyst 4000 Catalyst 4500	WS-X4448-GB-RJ45	All ports	Yes
Catalyst 4000 Catalyst 4500	WS-X4448-GB-LX	All ports	Yes
Catalyst 2948G	All ports	All ports	No
Catalyst 2980G	All modules	All ports	No

Using Flow-Control Keywords

Table 5-2 describes the guidelines for using different configurations of the **send** and **receive** keywords with the **set port flowcontrol** command.

Table 5-2 Send and Receive Keyword Configurations

Configuration	Description
send on	Enables a local port to send pause frames to a remote port. Enter send on when a remote port is set to receive on or receive desired .
send off	Prevents a local port from sending pause frames to a remote port. Enter send off when a remote port is set to receive off or receive desired .
send desired	Indicates preference to send pause frames, but autonegotiates flow control. You can enter send desired when a remote port is set to receive on , receive off , or receive desired .
receive on	Enables a local port to process pause frames that a remote port sends. Enter receive on when a remote port is set to send on or send desired .
receive off	Prevents a local port from processing pause frames. Enter receive off when a remote port is set to send off or send desired .
receive desired	Indicates preference to process pause frames, but autonegotiates flow control. You can enter receive desired when a remote port is set to send on , send off , or send desired .

Understanding How Port Negotiation Works



Caution

Unlike autonegotiation with 10/100 Fast Ethernet, Gigabit Ethernet port negotiation does not involve negotiating port speed. You *cannot* disable port negotiation on Gigabit Ethernet ports using the **set port speed** command.



Note

Port negotiation is not supported on 1000BASE-T Gigabit Ethernet ports.

With Gigabit Ethernet ports, port negotiation is used to exchange flow-control parameters, remote fault information, and duplex information (even though Cisco Gigabit Ethernet ports only support full-duplex mode). With Gigabit Ethernet ports, you configure port negotiation using the **set port negotiation** command. Gigabit Ethernet port negotiation is enabled by default.

The ports on both ends of a Gigabit Ethernet link must have the same setting. The link will not come up if the ports at each end of the link are set inconsistently (port negotiation enabled on one port and disabled on the other). [Table 5-3](#) shows the four possible port negotiation configurations for a Gigabit Ethernet link and the resulting link status for each configuration.

Table 5-3 Gigabit Ethernet Port Negotiation Configuration and Possible Link States

Port Negotiation State		Link Status	
Near End ¹	Far End ²	Near End	Far End
Off	Off	Up	Up
On	On	Up	Up
Off	On	Up	Down
On	Off	Down	Up

1. Near End refers to the local Gigabit EtherChannel module port.
2. Far End refers to the remote port at the other end of the Gigabit link.



Note

On 1000BASE-T Gigabit Ethernet ports, you cannot configure speed or duplex mode. With this release, 1000BASE-T ports operate only in the default configuration where the speed is 1000 and duplex mode is full. You cannot disable autonegotiation at this time. On a 1000BASE-T port, you can configure flow control and enable or disable a port. To determine which features a 1000BASE-T Gigabit Ethernet port supports, enter the **show port capabilities** command.

Understanding How Oversubscribed Gigabit Ethernet Works

The Catalyst 4000 family Gigabit Ethernet modules provide a network-backbone connection for multiple servers or high-end workstations. The following modules are supported:

- WS-X4412-2GB-T

This 1000BASE-T 14-port module provides 2 dedicated uplink module ports (GBIC) and 12 oversubscribed ports (possible blocking).

- WS-X4418-GB

This 1000BASE-X 18-port module provides 2 dedicated uplink module ports (GBIC) and 16 oversubscribed ports (possible blocking).

- WS-X4424-GB-RJ45

This 10/100/100BASE-TX module provides 24 oversubscribed ports (possible blocking).

- WS-X4448-GB-RJ24

This 10/100/100BASE-TX module provides 48 oversubscribed ports (possible blocking).

- WS-X4448-LX

This Gigabit Ethernet optical line terminator module provides 48 oversubscribed ports (possible blocking).

On all modules, each uplink module port has 1-Gbps dedicated bandwidth. These ports typically connect to the network backbone.

Table 5-4 lists the uplink module port IDs for each module.

Table 5-4 Uplink Port Module IDs for Gigabit Ethernet Modules

Module	Port ID
WS-X4412-2GB-T	13 14
WS-X4418-GB	1 2

On all modules, the oversubscribed ports are segmented into groups of four ports each. Each group of four ports shares 1 Gbps of bandwidth. The average bandwidth that clients and servers need to connect to ports in the same group should not exceed 1 Gbps.

Table 5-5 shows how the oversubscribed ports are grouped for module WS-4412-2GB-TX.

Table 5-5 Oversubscribed Port Groupings for Module WS-4412-2GB-TX

1, 2, 3, 4	5, 6, 7, 8	9, 10, 11, 12	Uplink Ports (13, 14)

Table 5-6 shows how the oversubscribed ports are grouped for module WS-4418-2GB.

Table 5-6 Oversubscribed Port Groupings for Module WS-4418-2GB

Uplink Ports (1, 2)	3, 4, 5, 6, 7, 8, 9, 10	11, 12, 13, 14, 15, 16, 17, 18

Table 5-7 shows how the oversubscribed ports are grouped for module WS-X4424-GB-RJ45.

Table 5-7 Oversubscribed Port Groupings for Module WS-X4424-GB-RJ45

1, 2, 3, 4	5, 6, 7, 8	9, 10, 11, 12	13, 14, 15, 16	17, 18, 19, 20	21, 22, 23, 24

Table 5-8 shows how the oversubscribed ports are grouped for module WS-X4448-GB-RJ45.

Table 5-8 Oversubscribed Port Groupings for Module WS-X4448-GB-RJ45

1, 2, 3, 4, 5, 6, 7, 8	9, 10, 11, 12, 13, 14, 15, 16	17, 18, 19, 20, 21, 22, 23, 24	25, 26, 27, 28, 29, 30, 31, 32	33, 34, 35, 36, 37, 38, 39, 40	41, 42, 43, 44, 45, 46, 47, 48

Table 5-9 shows how the oversubscribed ports are grouped for module WS-X4448-GB-LX.

Table 5-9 Oversubscribed Port Groupings for Module WS-X4448-GB-LX

1, 3, 5, 7, 9, 11, 13, 15	2, 4, 6, 8, 10, 12, 14, 16	17, 19, 21, 23, 25, 27, 29, 31	18, 20, 22, 24, 26, 28, 30, 32	33, 35, 37, 39, 41, 43, 45, 47	34, 36, 38, 40, 42, 44, 46, 48

The oversubscribed Gigabit Ethernet ports are designed for end-station connections. We do not recommend connecting these ports to switches or routers.

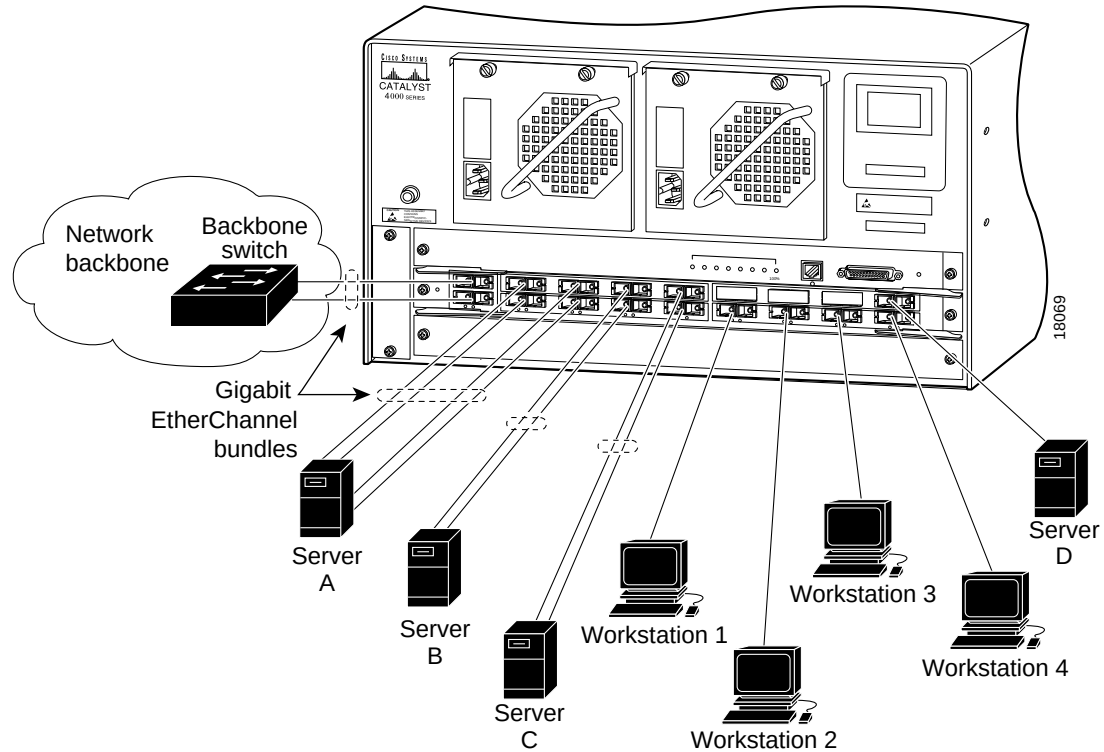
Each group of four or eight oversubscribed ports has a buffer for incoming frames to allow connected devices to transmit traffic simultaneously. Because the inbound buffer is small, the default (and recommended) flow-control configuration for the oversubscribed ports is **receive desired** and **transmit on**.

You can bundle multiple oversubscribed ports into a Gigabit EtherChannel link to connect to channel-capable servers. Bundling multiple oversubscribed ports in the same port group increases the total available bandwidth and provides redundancy with quick failover for links to servers and hosts that support the Port Aggregation Protocol (PAgP).

Oversubscribed Gigabit Ethernet Example

Figure 5-1 shows an example of an 18-port server switching module (WS-X4418-GB) connecting multiple network servers and high-end workstations to the Gigabit Ethernet network backbone. These configurations are shown:

- Server A, equipped with channel- and trunk-capable network interface cards (NICs), connects to the switch through a four-port Gigabit EtherChannel trunk link. Two ports are in one oversubscribed port group and two are in another. The switch can burst up to 2-Gbps bandwidth in each direction while averaging 250 Mbps for each connected port (1 Gbps total).
- Servers B and C, also with channel- and trunk-capable NICs, share the oversubscribed port groups that are used by Server A. Each server has one port in each oversubscribed port group and can burst up to 2-Gbps of traffic over channeled connections to and from the switch (Tx and Rx) while maintaining an average of 250 Mbps for each connected port (500 Mbps total) in each direction.
- Server D is the only device that is connected to the oversubscribed port group and can use the full 1-Gbps bandwidth.
- Workstations 1 through 4 are high-end workstations. Each workstation connects to a port in one oversubscribed port group. Each workstation can burst up to 1-Gbps bandwidth while averaging 250 Mbps in each direction.
- The network backbone connection is through a two-port Gigabit EtherChannel trunk link providing 2-Gbps bandwidth.

Figure 5-1 Example of a Server Switching Network Topology

Default Gigabit Ethernet Configuration

Table 5-10 shows the Gigabit Ethernet default configuration.

Table 5-10 Gigabit Ethernet Default Configuration

Feature	Default Value
Port enable state	All ports are enabled
Port name	None
Port priority	Normal
Duplex mode	Full duplex
Flow control	- Oversubscribed Gigabit Ethernet ports (ports 3–18 on WS-X4418-GB): Flow control set to desired for receive (Rx) and on for transmit (Tx) - All others: Flow control set to off for receive (Rx) and desired for transmit (Tx)
Port negotiation	Enabled
Spanning Tree Protocol	Enabled for VLAN 1
Native VLAN	VLAN 1
Spanning tree port cost	4
Gigabit EtherChannel	Disabled on all Gigabit Ethernet ports (auto mode)

Configuring Gigabit Ethernet Ports

The following sections describe how to configure Gigabit Ethernet switching ports on the Catalyst enterprise LAN switches.



Note

For information on configuring Gigabit EtherChannel, see [Chapter 6, “Configuring Fast EtherChannel and Gigabit EtherChannel.”](#)

Assigning Gigabit Ethernet Port Names

You can assign names to the ports on Gigabit Ethernet modules to facilitate switch administration.

To assign a name to a port, perform this task in privileged mode:

	Task	Command
Step 1	Assign a name to a port.	set port name <i>mod_num/port_num</i> [<i>name_string</i>]
Step 2	Verify that the port name is configured.	show port [<i>mod_num</i> [/ <i>port_num</i>]]

This example shows how to assign the name for ports 2/1 and 2/2 and how to verify that the port names are configured correctly:

```
Console> (enable) set port name 2/1 Backbone Connection
```

```
Port 2/1 name set.
```

```
Console> (enable) set port name 2/2 Wiring Closet
```

```
Port 2/2 name set.
```

```
Console> (enable) show port 2
```

Port	Name	Status	Vlan	Level	Duplex	Speed	Type
2/1	Backbone Connectio	connected	trunk	normal	full	1000	1000BASESX
2/2	Wiring Closet	notconnect	1	normal	full	1000	1000BASESX

```
<...output truncated...>
```

```
Last-Time-Cleared
```

```
-----
```

```
Tue Dec 22 1998, 13:42:04
```

```
Console> (enable)
```

Configuring Gigabit Ethernet Port Priority Levels

You can configure the priority level for each port. When two ports simultaneously request access to the switching bus, the switch uses the priority level to determine the order in which the ports get access.

To configure the port priority level, perform this task in privileged mode:

	Task	Command
Step 1	Configure the priority level for a port.	set port level <i>mod_num/port_num</i> { normal high }
Step 2	Verify that the port priority level is configured correctly.	show port [<i>mod_num[/port_num]</i>]

This example shows how to configure the port priority level to high for port 2/1 and verify that the port priority is configured correctly:

```
Console> (enable) set port level 2/1 high
```

```
Port 2/1 level set to high.
```

```
Console> (enable) show port 2/1
```

```
Port  Name              Status      Vlan      Level  Duplex Speed Type
-----
 2/1  Backbone Connectio connected trunk    high    full  1000 1000BASESX
```

```
<...output truncated...>
```

```
Last-Time-Cleared
```

```
-----
Tue Dec 22 1998, 13:42:04
```

```
Console> (enable)
```

Configuring Flow Control on Gigabit Ethernet Ports

To configure flow control on a Gigabit Ethernet port, perform this task in privileged mode:

	Task	Command
Step 1	Configure the flow-control parameters on a Gigabit Ethernet port.	set port flowcontrol { receive send } <i>mod_num/port_num</i> { off on desired }
Step 2	Verify the flow-control configuration.	show port flowcontrol

This example shows how to configure transmit and receive flow control and how to verify the flow-control configuration:

```
Console> (enable) set port flowcontrol send 2/1 on
```

```
Port 2/1 flow control send administration status set to on
```

```
(port will send flowcontrol to far end)
```

```
Console> (enable) set port flowcontrol receive 2/1 on
```

```
Port 2/1 flow control receive administration status set to on
```

```
(port will require far end to send flowcontrol)
```

```
Console> (enable) show port flowcontrol 2/1
```

```
Port  Send FlowControl  Receive FlowControl  RxPause TxPause Unsupported
      admin   oper      admin   oper                  opcodes
-----
 2/1   on     on        on     on                   0       0       0
```

```
Console> (enable)
```

Enabling Port Negotiation on Gigabit Ethernet Ports



Note

You cannot enable port negotiation on 1000BASE-T Gigabit Ethernet ports in this release. If a 1000BASE-T GBIC (Gigabit Interface Converter) is inserted in the port that was previously configured as negotiation disabled, the negotiation disabled setting is ignored and the port operates in negotiation-enabled mode.

To enable port negotiation on a 1000BASE-X Gigabit Ethernet port, perform this task in privileged mode:

	Task	Command
Step 1	Enable Gigabit Ethernet port negotiation.	set port negotiation <i>mod_num/port_num</i> enable
Step 2	Verify the port negotiation configuration.	show port negotiation [<i>mod_num/port_num</i>]

This example shows how to enable port negotiation and verify the configuration:

```
Console> (enable) set port negotiation 2/1 enable
Port 2/1 negotiation enabled
Console> (enable) show port negotiation 2/1
Port    Link Negotiation
-----
 2/1    enabled
Console> (enable)
```

Disabling Port Negotiation

To disable port negotiation on a 1000BASE-X Gigabit Ethernet port, perform this task in privileged mode:

	Task	Command
Step 1	Disable Gigabit Ethernet port negotiation.	set port negotiation <i>mod_num/port_num</i> disable
Step 2	Verify the port negotiation configuration.	show port negotiation [<i>mod_num/port_num</i>]

This example shows how to disable port negotiation and verify the configuration:

```
Console> (enable) set port negotiation 2/1 disable
Port 2/1 negotiation disabled
Console> (enable) show port negotiation 2/1
Port    Link Negotiation
-----
 2/1    disabled
Console> (enable)
```

Configuring errdisable State Gigabit Ethernet Port Timeout Periods

For information on configuring a timeout period for ports in errdisable state, see [Chapter 4, “Configuring Ethernet and Fast Ethernet Switching.”](#)

Checking Gigabit Ethernet Port Connectivity

**Note**

For more detailed information on checking connectivity, see [Chapter 20, “Checking Status and Connectivity.”](#)

Enter the **ping** and **tracert** commands to test connectivity out Gigabit Ethernet ports.

To check connectivity out a port, perform this task in privileged mode:

	Task	Command
Step 1	Ping a remote host that is located out the port you want to test.	ping [-s] <i>host</i> [<i>packet_size</i>] [<i>packet_count</i>]
Step 2	Trace the hop-by-hop route of packets from the switch to a remote host that is located out the port you want to test.	tracert <i>host</i>
Step 3	If the host is unresponsive, check the IP address and default gateway configured on the switch.	show interface show ip route

This example shows how to ping a remote host and how to trace the hop-by-hop path of packets through the network using **tracert**:

```
Console> (enable) ping somehost
somehost is alive
Console> (enable) tracert somehost
tracert to somehost.company.com (10.1.2.3), 30 hops max, 40 byte packets
 1 engineering-1.company.com (173.31.192.206) 2 ms 1 ms 1 ms
 2 engineering-2.company.com (173.31.196.204) 2 ms 3 ms 2 ms
 3 gateway_a.company.com (173.16.1.201) 6 ms 3 ms 3 ms
 4 somehost.company.com (10.1.2.3) 3 ms * 2 ms
Console> (enable)
```

Configuring Fast EtherChannel and Gigabit EtherChannel

This chapter describes how to configure Fast EtherChannel and Gigabit EtherChannel port bundles on the Catalyst enterprise LAN switches. The configuration procedures in this chapter apply to Fast Ethernet and Gigabit Ethernet switch ports on switching modules and fixed-configuration switches, as well as to supervisor engine Fast Ethernet and Gigabit Ethernet uplink ports.

**Note**

For complete information on installing Catalyst 4000 family Fast Ethernet and Gigabit Ethernet modules, refer to the *Catalyst 4000 Family Installation Guide*.

**Note**

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 4500 Series, Catalyst 2948G, and Catalyst 2980G Switches Command Reference*.

This chapter consists of these sections:

- [Understanding How EtherChannel Works, page 6-1](#)
- [PAgP and LACP, page 6-2](#)
- [EtherChannel Configuration Guidelines and Restrictions, page 6-3](#)
- [Understanding the PAgP, page 6-5](#)
- [Configuring EtherChannel Using PAgP, page 6-6](#)
- [EtherChannel Configuration Examples, page 6-12](#)
- [Understanding the LACP, page 6-16](#)
- [Configuring EtherChannel Using LACP, page 6-18](#)

Understanding How EtherChannel Works

These sections describe how EtherChannel works:

- [EtherChannel Overview, page 6-2](#)
- [Understanding Frame Distribution, page 6-2](#)
- [Hardware Support for EtherChannel, page 6-2](#)

CISCO Confidential - DRAFT

EtherChannel Overview

Fast EtherChannel and Gigabit EtherChannel port bundles let you group multiple Fast or Gigabit Ethernet ports into a single logical transmission path between a switch and a router, a host, or another switch. Depending on your hardware, you can form an EtherChannel with up to eight compatibly configured Fast or Gigabit Ethernet ports on the switch. In addition, on the Catalyst 4000 family switches, you can configure an EtherChannel using ports from multiple modules. All ports in an EtherChannel must be the same speed.

The switch distributes frames across the ports in an EtherChannel according to the source and destination MAC addresses. If a port within an EtherChannel fails, traffic previously carried over the failed port switches to the remaining ports within the EtherChannel. A trap is sent when a failure identifies the switch, the EtherChannel, and the failed link.

You can configure both Fast and Gigabit EtherChannel bundles as trunk links. After you have formed a channel, you can configure any port in the channel as a trunk. The configuration is applied to all ports in the channel. You can also configure identical trunk ports as an EtherChannel. For more information, see the [“EtherChannel Configuration Guidelines and Restrictions” section on page 6-3](#) and [Chapter 11, “Configuring VLAN Trunks on Fast Ethernet and Gigabit Ethernet Ports.”](#)

Understanding Frame Distribution

EtherChannel distributes frames across the links in a channel based on the low-order bits of the source and destination MAC addresses of each frame. The frame distribution method is not configurable.

Hardware Support for EtherChannel

EtherChannel support is hardware dependent. You can enter the **show port capabilities** command to determine whether your hardware supports EtherChannel, and to confirm which ports you can bundle into a single EtherChannel.

An EtherChannel bundle can consist of any two to eight ports. Ports in an EtherChannel bundle do not have to be continuous, and they do not have to be on the same module.

Due to the port ID handling by the spanning tree feature, the maximum supported number of channels is 126 for a 6-slot chassis.

PAgP and LACP

Port Aggregation Control Protocol (PAgP) and Link Aggregation Control Protocol (LACP) allow ports with similar characteristics to form a channel through dynamic negotiation with adjoining switches. PAgP is a Cisco-proprietary protocol that can be run only on Cisco switches and those switches released by licensed vendors. LACP, which is defined in IEEE 802.3ad, allows Cisco switches to manage Ethernet channeling with devices that conform to the 802.3ad specification.

**Note**

MAC address notification settings are ignored on PAgP and LACP EtherChannel ports.

To use PAgP, see the [“Understanding the PAgP” section on page 6-5](#). To use LACP, see the [“Understanding the LACP” section on page 6-16](#).

CISCO Confidential - DRAFT

EtherChannel Configuration Guidelines and Restrictions

If improperly configured, some EtherChannel ports are disabled automatically to avoid network loops and other problems. Follow the guidelines below to avoid configuration problems.

**Note**

Except where noted, these guidelines apply to both PAgP and LACP.

Guidelines for Configuring a Port

This section lists the guidelines and restrictions for configuring a port for EtherChannel:

- Ensure that you have a maximum of eight compatibly configured ports per EtherChannel; the ports do not have to be contiguous or on the same module.
- Ensure that all ports in an EtherChannel use the same protocol; you cannot run two protocols on a module.
- PAgP and LACP are not compatible; both ends of a channel must use the same protocol.

**Note**

Switches can be configured manually, with PAgP on one side and LACP on the other side in the **on** mode.

- You can change the protocol at any time, but this change causes all existing EtherChannels to reset to the default channel mode for the new protocol.
- Configure all ports in an EtherChannel to operate at the same speed and duplex mode (full duplex only for LACP mode).
- Enable all ports in an EtherChannel. If you disable a 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.
- You cannot assign a port to more than one channel group at the same time.
- Ports with different port path costs, set by the **set spantree portcost** command, can form an EtherChannel as long as they are otherwise compatibly configured. Setting different port path costs does not, by itself, make ports incompatible for the formation of an EtherChannel.
- PAgP and LACP manage channels differently. When all the ports in a channel get disabled, PAgP removes them from its internal channels list; **show** commands do not display the channel. With LACP, when all the ports in a channel get disabled, LACP does not remove the channel; **show** commands continue to display the channel even though all its ports are down. To determine if a channel is actively sending and receiving traffic with LACP, use the **show port** command to see if the link is up or down.
- LACP does not support half-duplex links. If a port is in active/passive mode and becomes half duplex, the port is suspended (and a syslog message is generated). The port is shown as “connected” using the **show port** command and as “not connected” using the **show spantree** command. This discrepancy exists because the port is physically connected but never joined spanning tree. To get the port to join spanning tree, either set the duplex to full or set the channel mode to off for that port.

With software release 7.3(1) and later releases, LACP behavior for half-duplex links has changed and affected ports are no longer suspended. Instead of suspending a port, LACP PDU transmission (if any) is suppressed. If the port is part of a channel, the port is detached from the channel but still functions as a nonchannel port. A syslog message is generated when this condition occurs. Normal LACP behavior is reenabled automatically when the link is set back to full duplex.

CISCO Confidential - DRAFT

Guidelines for Configuring VLANs and Trunks

This section lists the guidelines and restrictions for configuring VLAN and trunks for EtherChannel:

- Assign all ports in an EtherChannel to the same VLAN, or configure them as trunk ports.
- If you configure the EtherChannel as a trunk, configure the same trunk mode on all the ports in the EtherChannel. Configuring ports in an EtherChannel in different trunk modes can have unexpected results.
- An EtherChannel supports the same allowed range of VLANs on all the ports in a trunking EtherChannel. If the allowed range of VLANs is not the same for a port list, the ports do not form an EtherChannel even when set to the **auto** or **desirable** mode with the **set port channel** command.
- Do not configure the ports in an EtherChannel as dynamic VLAN ports. Doing so can adversely affect switch performance.
- Ports with different VLAN costs or VLAN configurations cannot form a channel.

EtherChannel Interaction with other Features

This section lists the guidelines and restrictions for EtherChannel's interaction with other features:

- An EtherChannel will not form with ports that have different GARP VLAN Registration Protocol (GVRP), GARP Multicast Registration Protocol (GMRP), and quality of service (QoS) configurations.
- An EtherChannel will not form with ports where the port security feature is enabled. Do not enable the port security feature for ports in an EtherChannel.
- An EtherChannel will not form if one of the ports is a SPAN destination port.
- An EtherChannel will not form if protocol filtering is set differently on the ports.
- Cisco Discovery Protocol (CDP) runs on the physical port even after the port is added to a channel.
- VLAN Trunking Protocol (VTP) and Dual Ring Protocol (DRiP) run on the channel.
- During fast switchover to the standby supervisor engine, all channeling ports are cleared on its channeling configuration and state, and the links are pulled down temporarily to cause partner ports to reset. All ports are reset to the nonchanneling state.
- Ports with different dot1q port types cannot form a channel.
- Ports with different jumbo frame configurations cannot form a channel.
- Ports with different dynamic configurations cannot form a channel.
- If one port in an EtherChannel is used by IGMP multicast filtering, you must set the EtherChannel mode for both PAgP and LACP to **off**. No other mode may be used.

**Note**

With software release 6.3(1) and later releases, a PAgP-configured EtherChannel is preserved even if it contains only one port (this does not apply to LACP-configured EtherChannels). In software releases prior to 6.3(1), traffic was disrupted when you removed a 1-port channel from spanning tree and then added it to spanning tree as an individual port.

Understanding the PAgP

Use the information in the following sections if you are configuring EtherChannel using PAgP. If you are using LACP, see the “[Understanding the LACP](#)” section on page 6-16.

PAgP Modes

The Port Aggregation Protocol (PAgP) facilitates the automatic creation of Fast EtherChannel and Gigabit EtherChannel links by exchanging packets between channel-capable ports. The protocol learns the capabilities of port groups dynamically and informs the neighboring ports.

After PAgP identifies correctly paired channel-capable links, it groups the ports into a channel. The channel is then added to the spanning tree as a single bridge port. A given outbound broadcast or multicast packet is transmitted out one port in the channel only, not out every port in the channel. In addition, outbound broadcast and multicast packets that are transmitted on one port in a channel are blocked from returning on any other port of the channel.

There are four user-configurable channel modes: **on**, **off**, **auto**, and **desirable**. PAgP packets are exchanged only between ports in **auto** and **desirable** mode. Ports that are configured in **on** or **off** mode do not exchange PAgP packets. The **auto** and **desirable** modes can be modified with the **silent** and **non-silent** keywords. [Table 6-1](#) describes each mode.

Table 6-1 Channel Modes

Mode	Description
on	Forces the port to channel without negotiation. PAgP packets are not exchanged. The port is channeling regardless of how the peer port is configured. If the peer port is in on mode, a channel is formed. In any other mode, the peer port is placed in the errdisable state due to a channel misconfiguration.
off	Prevents the port from channeling. PAgP packets are not exchanged. The port is not channeling regardless of how the peer port is configured. No channel is formed.
auto	Places a port into a passive negotiating state, in which the port responds to PAgP packets it receives but does not initiate PAgP packet negotiation. A channel is formed only with another port group in desirable mode. (Default)
desirable	Places a port into an active negotiating state, in which the port initiates negotiations with other ports by sending PAgP packets. A channel is formed with another port group in either desirable or auto mode. Use the silent keyword when you are connecting to a “silent partner” (a device that is not generating BPDUs or other traffic). An example of a silent partner is a traffic generator that is not transmitting packets. Use this keyword with the auto or desirable mode. If you do not specify silent or non-silent, silent is assumed. Use the non-silent keyword when you are connecting to a device that will transmit BPDUs or other traffic. Use this keyword with the auto or desirable mode.

Both the **auto** and **desirable** modes allow ports to negotiate with connected ports to determine if they can form a channel, based on criteria such as port speed, trunking state, native VLAN, and so on.

Ports can form an EtherChannel when they are in different channel modes as long as the modes are compatible, as follows:

CISCO Confidential - DRAFT

- A port in **desirable** mode can form an EtherChannel successfully with another port that is in **desirable** or **auto** mode.
- A port in **auto** mode can form an EtherChannel with another port in **desirable** mode.
- A port in **auto** mode cannot form an EtherChannel with another port that is also in **auto** mode, because neither port will initiate negotiation.
- A port in **on** mode can form a channel only with a port in **on** mode, because ports in **on** mode do not exchange PAgP packets.
- A port in **off** mode will not form a channel with any port.

Understanding Administrative Groups and EtherChannel IDs

Configuring an EtherChannel creates an administrative group, designated by an integer between 1 and 1024, inclusive, to which the EtherChannel belongs. You can assign an administrative group number manually or let the system software assign the next available administrative group number automatically.

Forming an EtherChannel without specifying an administrative group number creates a new automatically numbered administrative group consisting of the ports you configure as an EtherChannel. An administrative group can contain a maximum of eight ports.

You can define an EtherChannel administrative group without forming an EtherChannel. Only ports belonging to the same administrative group can form a single EtherChannel.

In addition to the administrative group number, each EtherChannel is automatically assigned a unique EtherChannel ID. Use the **show channel group** command to display the EtherChannel ID.

EtherChannel administrative group numbers are stored in NVRAM and remain the same after the switch is reset or power cycled. EtherChannel IDs are not saved in NVRAM. The ID can change if the EtherChannel is torn down and renegotiated, or if the switch is reset or power cycled.

Configuring EtherChannel Using PAgP

These sections describe how to configure an EtherChannel bundle using PAgP:

- [Creating an EtherChannel, page 6-7](#)
- [Defining an EtherChannel Administrative Group, page 6-7](#)
- [Setting the EtherChannel Spanning Tree Port Cost, page 6-8](#)
- [Setting the EtherChannel Spanning Tree Port VLAN Cost, page 6-9](#)
- [Removing an EtherChannel Bundle, page 6-9](#)
- [Displaying EtherChannel Configuration Information, page 6-10](#)
- [Displaying EtherChannel Traffic Statistics, page 6-11](#)
- [Displaying EtherChannel PAgP Statistics, page 6-12](#)

**Note**

Before you configure the EtherChannel, see the [“EtherChannel Configuration Guidelines and Restrictions” section on page 6-3](#).

Creating an EtherChannel

You create an EtherChannel port bundle by specifying the ports in the channel and the channeling mode. When you create an EtherChannel, an administrative group number is assigned automatically if one is not already assigned to the specified ports. In addition, a channel ID is assigned.

The **silent** and **non-silent** keywords function only with the **auto** and **desirable** modes.

To create an EtherChannel port bundle, perform this task in privileged mode:

	Task	Command
Step 1	If you are unsure which ports you can configure as an EtherChannel, verify the EtherChannel capabilities for the module or switch you are configuring.	show port capabilities [<i>mod_num</i> [/ <i>port_num</i>]]
Step 2	Create an EtherChannel with the desired ports.	set port channel <i>port_list</i> [<i>admin_group</i>] mode { on off desirable auto } [silent non-silent]
Step 3	Verify the EtherChannel configuration.	show port channel [<i>port_list</i>]

This example shows how to create an EtherChannel bundle and verify the configuration:

```

Console> (enable) set port channel 3/5-6 on
Port(s) 3/5-6 are assigned to admin group 57.
Port(s) 3/5-6 channel mode set to on.
Console> (enable) show port channel
Port  Status      Channel      Admin Ch
      Mode                               Group Id
-----
 3/5   connected    on           57    835
 3/6   connected    on           57    835
-----

```

```

Port  Device-ID                               Port-ID      Platform
-----
 3/5   069003103(5500)                           3/5          WS-C4000
 3/6   069003103(5500)                           3/6          WS-C4000
-----

```

```

Console> (enable)

```

Defining an EtherChannel Administrative Group

You can define EtherChannel administrative groups manually to identify groups of ports that are allowed to form an EtherChannel bundle. When you create an EtherChannel port bundle, an administrative group is defined automatically. Administrative group membership is limited by hardware restrictions.

The *admin_group* can be any value between 1 and 1024, inclusive.



Caution

Modifying the EtherChannel administrative group on connected ports causes the specified ports to be removed from and then added to spanning tree (that is, a spanning tree topology change occurs and the ports must enter listening and learning mode before returning to forwarding mode).

To define an EtherChannel administrative group, perform this task in privileged mode:

CISCO Confidential - DRAFT

	Task	Command
Step 1	Define the administrative group by specifying the ports in the group.	set port channel <i>port_list</i> <i>admin_group</i>
Step 2	Verify the administrative group configuration.	show channel group [<i>admin_group</i>]

This example shows how to assign ports to an administrative group and verify the configuration:

```

Console> (enable) set port channel 3/5-6 50
Port(s) 3/5-6 are assigned to admin group 50.
Console> (enable) show channel group 50
Admin Port  Status      Channel      Channel
group      Mode          id
-----
    50  3/5  connected  auto silent          0
    50  3/6  connected  auto silent          0

Admin Port  Device-ID                      Port-ID                      Platform
group
-----
    50  3/5
    50  3/6
Console> (enable)

```

Setting the EtherChannel Spanning Tree Port Cost

To set the spanning tree port cost for an EtherChannel, perform this task in privileged mode:

	Task	Command
Step 1	Determine the EtherChannel ID of the EtherChannel for which you want to set the port cost.	show channel group <i>admin_group</i>
Step 2	Set the spanning tree port cost for an EtherChannel using the EtherChannel ID obtained in Step 1.	set channel cost { <i>channel_id</i> all } <i>cost</i>

This example shows how to set the EtherChannel port path cost for channel ID 768:

```

Console> (enable) show channel group 20
Admin Port  Status      Channel      Channel
group      Mode          id
-----
    20  1/1  notconnect  on           768
    20  1/2  connected   on           768

Admin Port  Device-ID                      Port-ID                      Platform
group
-----
    20  1/1
    20  1/2  066510644(cat26-lnf(NET25))  2/1                      WS-C6009
Console> (enable)

```

CISCO Confidential - DRAFT

```

Console> (enable) set channel cost 768 12
Port(s) 1/1,1/2 port path cost are updated to 31.
Channel 768 cost is set to 12.
Warning:channel cost may not be applicable if channel is broken.
Console> (enable)

```

Setting the EtherChannel Spanning Tree Port VLAN Cost

The spanning tree port VLAN cost provides an alternate cost for some of the VLANs in a trunk channel. Setting the spanning tree port VLAN cost provides load balancing of VLAN traffic across multiple channels configured with trunking because some VLANs in the channel can have port VLAN cost, while the remaining VLANs in the channel have port cost.

To set the spanning tree port VLAN cost for an EtherChannel, perform this task in privileged mode:

	Task	Command
Step 1	Determine the EtherChannel ID of the EtherChannel for which you want to set the port VLAN cost.	show channel group <i>admin_group</i>
Step 2	Set the spanning tree port VLAN cost for an EtherChannel using the EtherChannel ID obtained in Step 1.	set channel vlancost { <i>channel_id</i> all } <i>cost</i>

This example shows how to set the EtherChannel VLAN cost for channel ID 768:

```

Console> (enable) show channel group 20
Admin Port  Status      Channel  Channel
group      Mode        id
-----
   20      1/1 notconnect on         768
   20      1/2 connected on         768

Admin Port  Device-ID                      Port-ID          Platform
group
-----
   20      1/1
   20      1/2 066510644(cat26-lnf(NET25))  2/1             WS-C6009
Console> (enable)

Console> (enable) set channel vlancost 768 12
Channel 768 vlancost set to 12.
Console> (enable)

```

Removing an EtherChannel Bundle

To return a Fast EtherChannel or Gigabit EtherChannel bundle to its default configuration, perform this task in privileged mode:

	Task	Command
Step 1	Return a channel to its default configuration (you must perform this task on both sides of the channel).	set port channel <i>port_list</i> mode auto
Step 2	Verify the configuration.	show port channel [<i>mod_num</i> [/ <i>port_num</i>]]

CISCO Confidential - DRAFT

This example shows how to return a channel to its default configuration and how to verify the configuration:

```
Console> (enable) set port channel 3/5-6 mode auto
Port(s) 3/5-6 channel mode set to auto.
Console> (enable) show port channel
No ports channelling
Console> (enable)
```

Displaying EtherChannel Configuration Information

To display EtherChannel configuration information, perform one of these tasks in privileged mode:

Task	Command
Display EtherChannel configuration information by port.	show port channel [<i>mod_num</i> [/ <i>port_num</i>]] info [spantree trunk protocol gmrp gvrp qos]
Display EtherChannel configuration information by EtherChannel administrative group.	show channel group [<i>admin_group</i>] info [spantree trunk protocol gmrp gvrp qos]
Display EtherChannel configuration information by EtherChannel ID.	show channel [<i>channel_id</i>] info [spantree trunk protocol gmrp gvrp qos]

This example shows how to display EtherChannel configuration information by port:

```
Console> (enable) show port channel info
Switch Frame Distribution Method: mac both
```

Port	Status	Channel mode	Admin Channel group id	Speed	Duplex	Vlan
3/5	connected	on	56	835	a-100	a-full 1
3/6	connected	on	56	835	a-100	a-full 1

Port	ifIndex	Oper-group	Neighbor Oper-group	Oper-Distribution Method	PortSecurity/Dynamic port
3/5	377	1		mac both	
3/6	377	1		mac both	

Port	Device-ID	Port-ID	Platform
3/5	069003103(5500)	3/5	WS-C4000
3/6	069003103(5500)	3/6	WS-C4000

Port	Trunk-status	Trunk-type	Trunk-vlans
3/5	not-trunking	negotiate	1-1005
3/6	not-trunking	negotiate	1-1005

Port	Portvlancost-vlans
3/5	
3/6	

CISCO Confidential - DRAFT

Port	Port priority	Portfast	Port vlanpri	Port vlanpri-vlans
3/5	32	disabled	0	
3/6	32	disabled	0	
Port	IP	IPX	Group	
3/5	on	auto-on	auto-on	
3/6	on	auto-on	auto-on	
Port	GMRP status	GMRP registration	GMRP forwardAll	
3/5	enabled	normal	disabled	
3/6	enabled	normal	disabled	
Port	GVRP status	GVRP registration	GVRP applicant	
3/5	disabled	normal	normal	
3/6	disabled	normal	normal	
Port	Qos-Tx	Qos-Rx	Qos-Trust	Qos-DefCos
3/5	-	-	untrusted	0
3/6	-	-	untrusted	0

Console> (enable)

Displaying EtherChannel Traffic Statistics

To display EtherChannel traffic statistics, perform this task in privileged mode:

Task	Command
Display EtherChannel traffic statistics.	show channel [<i>channel_id</i>] mac

This example shows how to display EtherChannel traffic statistics information for EtherChannel ID 835:

```

Console> show channel 835 mac
Channel  Rcv-Unicast      Rcv-Multicast      Rcv-Broadcast
-----
835              0             119200              0

Channel  Xmit-Unicast      Xmit-Multicast      Xmit-Broadcast
-----
835              0             184171              0

Channel  Rcv-Octet      Xmit-Octet
-----
835          11283708      14942104

Channel  Dely-Excd  MTU-Excd  In-Discard  Lrn-Discrd  In-Lost  Out-Lost

```

```

-----
835                               0           0           0           0           0           0
Console> (enable)
```

Displaying EtherChannel PAgP Statistics

To display EtherChannel PAgP statistics, perform one of these tasks in privileged mode:

Task	Command
Display EtherChannel PAgP statistics by port.	show port channel [<i>mod_num</i> [/ <i>port_num</i>]] statistics
Display EtherChannel PAgP statistics by EtherChannel administrative group.	show channel group [<i>admin_group</i>] statistics
Display EtherChannel PAgP statistics by EtherChannel ID.	show channel [<i>admin_group</i>] statistics

This example shows how to display EtherChannel PAgP statistics information by EtherChannel administrative group:

```

Console> show channel group 58 statistics
Port  Admin   PAgP Pkts   PAgP Pkts PAgP Pkts PAgP Pkts PAgP Pkts PAgP Pkts
      Group   Transmitted Received InFlush RetnFlush OutFlush InError
-----
3/5    58        194      81        0         0         0         0
3/6    58        204      85        0         0         0         0
Console> (enable)
```

EtherChannel Configuration Examples

These sections contain Fast and Gigabit EtherChannel configuration examples:

- [Configuration Example of a Four-Port Fast EtherChannel, page 6-12](#)
- [Configuration Example of Two-Port Gigabit EtherChannel, page 6-14](#)

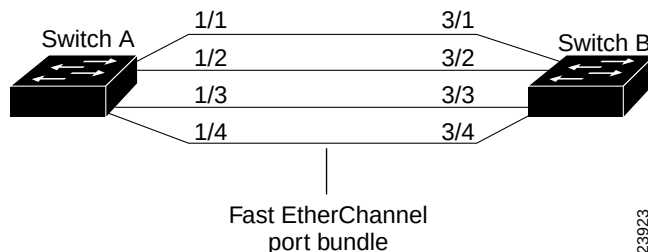


Note

For examples of configuring VLAN trunks on EtherChannel port bundles, see the [“Example VLAN Trunk Configurations”](#) section on page 11-9.

Configuration Example of a Four-Port Fast EtherChannel

This example shows how to configure a four-port Fast EtherChannel link between two switches. [Figure 6-1](#) shows two switches connected through four 100BASE-TX Fast Ethernet ports.

*CISCO Confidential - DRAFT***Figure 6-1 Example of a Fast EtherChannel Port Bundle**

To configure a four-port EtherChannel link between two switches, follow these steps:

- Step 1** Make sure that all ports on Switch A and Switch B have the same port configuration, including VLAN membership, speed, and duplex.

```
Switch_A> (enable) set vlan 50 1/1-4
VLAN 50 modified.
VLAN 1 modified.
VLAN   Mod/Ports
-----
50     1/1-4
        2/1-2
        3/1-3

Switch_A> (enable) set port speed 1/1-4 100
Ports 1/1-4 transmission speed set to 100Mbps.
Switch_A> (enable) set port duplex 1/1-4 full
Ports 1/1-4 set to full-duplex.
Switch_A> (enable)

Switch_B> (enable) set vlan 50 3/1-4
VLAN 50 modified.
VLAN 1 modified.
VLAN   Mod/Ports
-----
50     3/1-4

Switch_B> (enable) set port speed 3/1-4 100
Ports 3/1-4 transmission speed set to 100Mbps.
Switch_B> (enable) set port duplex 3/1-4 full
Ports 3/1-4 set to full-duplex.
Switch_B> (enable)
```

- Step 2** Confirm the channeling status of the switches using the **show port channel** command.

```
Switch_A> (enable) show port channel
No ports channelling
Switch_A> (enable)

Switch_B> (enable) show port channel
No ports channelling
Switch_B> (enable)
```

- Step 3** Configure the ports on Switch A to negotiate a Fast EtherChannel bundle with the neighboring switch. This example assumes that the neighboring ports on Switch B are in EtherChannel **auto** mode. The system logging messages provide information about the formation of the EtherChannel bundle.

```
Switch_A> (enable) set port channel 1/1-4 desirable
Port(s) 1/1-4 channel mode set to desirable.
Switch_A> (enable) %PAGP-5-PORTFROMSTP:Port 1/1 left bridge port 1/1
```

CISCO Confidential - DRAFT

```

%PAGP-5-PORTFROMSTP:Port 1/2 left bridge port 1/2
%PAGP-5-PORTFROMSTP:Port 1/3 left bridge port 1/3
%PAGP-5-PORTFROMSTP:Port 1/4 left bridge port 1/4
%PAGP-5-PORTFROMSTP:Port 1/2 left bridge port 1/2
%PAGP-5-PORTFROMSTP:Port 1/3 left bridge port 1/3
%PAGP-5-PORTFROMSTP:Port 1/4 left bridge port 1/4
%PAGP-5-PORTTOSTP:Port 1/1 joined bridge port 1/1-4
%PAGP-5-PORTTOSTP:Port 1/2 joined bridge port 1/1-4
%PAGP-5-PORTTOSTP:Port 1/3 joined bridge port 1/1-4
%PAGP-5-PORTTOSTP:Port 1/4 joined bridge port 1/1-4

Switch_B> (enable) %PAGP-5-PORTFROMSTP:Port 3/1 left bridge port 3/1
%PAGP-5-PORTFROMSTP:Port 3/2 left bridge port 3/2
%PAGP-5-PORTFROMSTP:Port 3/3 left bridge port 3/3
%PAGP-5-PORTFROMSTP:Port 3/4 left bridge port 3/4
%PAGP-5-PORTFROMSTP:Port 3/2 left bridge port 3/1-4
%PAGP-5-PORTFROMSTP:Port 3/3 left bridge port 3/1-4
%PAGP-5-PORTFROMSTP:Port 3/4 left bridge port 3/1-4
%PAGP-5-PORTTOSTP:Port 3/1 joined bridge port 3/1-4
%PAGP-5-PORTTOSTP:Port 3/2 joined bridge port 3/1-4
%PAGP-5-PORTTOSTP:Port 3/3 joined bridge port 3/1-4
%PAGP-5-PORTTOSTP:Port 3/4 joined bridge port 3/1-4

```

- Step 4** After the EtherChannel bundle is negotiated, enter the **show port channel** command to verify the configuration.

```

Switch_A> (enable) show port channel

```

Port	Status	Channel mode	Channel status	Neighbor device	Neighbor port
1/1	connected	desirable	channel	WS-C4003 JAB023806(Sw	3/1
1/2	connected	desirable	channel	WS-C4003 JAB023806(Sw	3/2
1/3	connected	desirable	channel	WS-C4003 JAB023806(Sw	3/3
1/4	connected	desirable	channel	WS-C4003 JAB023806(Sw	3/4

```

Switch_A> (enable)

Switch_B> (enable) show port channel

```

Port	Status	Channel mode	Channel status	Neighbor device	Neighbor port
3/1	connected	auto	channel	WS-C4012 009979082(Sw	1/1
3/2	connected	auto	channel	WS-C4012 009979082(Sw	1/2
3/3	connected	auto	channel	WS-C4012 009979082(Sw	1/3
3/4	connected	auto	channel	WS-C4012 009979082(Sw	1/4

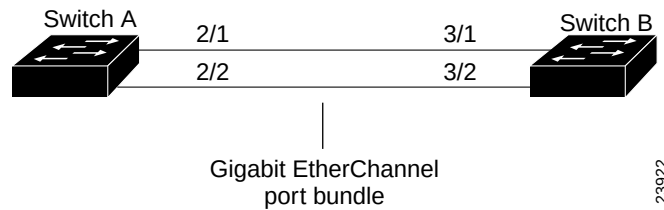
```

Switch_B> (enable)

```

Configuration Example of Two-Port Gigabit EtherChannel

This example shows how to configure a two-port Gigabit EtherChannel link between two switches. [Figure 6-2](#) shows two switches connected through four 1000BASE-SX Gigabit Ethernet ports.

*CISCO Confidential - DRAFT***Figure 6-2 Example of a Gigabit EtherChannel Port Bundle**

To configure a two-port Gigabit EtherChannel link between two switches, follow these steps:

- Step 1** Make sure that all ports on Switch A and Switch B have the same port configuration, such as VLAN membership.
- ```
Switch_A> (enable) set vlan 100 2/1-2
VLAN 100 modified.
VLAN 1 modified.
VLAN Mod/Ports

100 2/1-2

Switch_A> (enable)

Switch_B> (enable) set vlan 100 3/1-2
VLAN 100 modified.
VLAN 1 modified.
VLAN Mod/Ports

100 3/1-2

Switch_B> (enable)
```
- Step 2** Confirm the channeling status of the switches using the **show port channel** command.
- ```
Switch_A> (enable) show port channel
No ports channelling
Switch_A> (enable)

Switch_B> (enable) show port channel
No ports channelling
Switch_B> (enable)
```
- Step 3** In this example, configure EtherChannel as **on** for all ports. If you configure ports **on**, you must configure the ports on both ends of the EtherChannel bundle **on**. The switches will not negotiate an EtherChannel port bundle automatically in **on** mode. The system logging messages provide information about the formation of the EtherChannel bundle.
- ```
Switch_A> (enable) set port channel 2/1-2 on
Port(s) 2/1-2 channel mode set to on.
Switch_A> (enable) %PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1
%PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/2
%PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1-2
%PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/1-2

Switch_B> (enable) set port channel 3/1-2 on
Port(s) 3/1-2 channel mode set to on.
Switch_B> (enable) %PAGP-5-PORTFROMSTP:Port 3/1 left bridge port 3/1
%PAGP-5-PORTFROMSTP:Port 3/2 left bridge port 3/2
%PAGP-5-PORTTOSTP:Port 3/1 joined bridge port 3/1-2
%PAGP-5-PORTTOSTP:Port 3/2 joined bridge port 3/1-2
```

*CISCO Confidential - DRAFT*

**Step 4** After the EtherChannel bundle is negotiated, enter the **show port channel** command to verify the configuration. If you configure only the ports on one side of the link **on**, the **show port channel** command will show that the ports are channeling, but no traffic will pass over the EtherChannel. Spanning tree loops can occur, and eventually the switch will disable the incorrectly configured EtherChannel.

```
Switch_A> (enable) show port channel
Port Status Channel Channel Neighbor
 mode status device

2/1 connected on channel WS-C4003 JAB023806LN(3/1
2/2 connected on channel WS-C4003 JAB023806LN(3/2

Switch_A> (enable)

Switch_B> (enable) show port channel
Port Status Channel Channel Neighbor
 mode status device

3/1 connected on channel WS-C4003 JAB023806JR(2/1
3/2 connected on channel WS-C4003 JAB023806JR(2/2

Switch_B> (enable)
```

# Understanding the LACP

Use the information in these sections if you are configuring EtherChannel using LACP. If you are using PAgP, see the “[Understanding the PAgP](#)” section on page 6-5.

## LACP Modes

You may manually turn on channeling by setting the port channel mode to **on**, and you may turn channeling off by setting the port channel mode to **off**.

If you want LACP to handle channeling, use the **active** and **passive** channel modes. To start automatic EtherChannel configuration with LACP, you need to configure at least one end of the link to **active** mode to initiate channeling, because ports in **passive** mode passively respond to initiation and never initiate the sending of LACP packets.

[Table 6-2](#) describes the EtherChannel modes that use LACP.

**Table 6-2 EtherChannel Modes That Use LACP**

| Mode       | Description                                                                                                                                                                                             |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>on</b>  | Mode that forces the port to channel without LACP. With the <b>on</b> mode, a usable EtherChannel exists only when a port group in <b>on</b> mode is connected to another port group in <b>on</b> mode. |
| <b>off</b> | Mode that prevents the port from channeling.                                                                                                                                                            |

*CISCO Confidential - DRAFT***Table 6-2 EtherChannel Modes That Use LACP (continued)**

| Mode                        | Description                                                                                                                                                         |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>passive</b><br>(Default) | 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 packet negotiation. |
| <b>active</b>               | LACP mode that places a port into an active negotiating state, in which the port initiates negotiations with other ports by sending LACP packets.                   |

## LACP Parameters

LACP uses the following parameters:

- System priority

Each switch running LACP must have a system priority. You can specify the system priority automatically or through the CLI (see the [“Specifying the System Priority” section on page 6-19](#)). The switch uses the MAC address and the system priority to form the system ID and is also used during negotiation with other systems.

- Port priority

Each port in the switch must have a port priority. You can specify the port priority automatically or through the CLI (see the [“Specifying the Port Priority” section on page 6-19](#)). The port priority and the port number form the port identifier. The switch uses the port priority to decide which ports to put in standby mode when a hardware limitation prevents all compatible ports from aggregating.

- Administrative key

Each port in the switch must have an administrative key value. You can specify the administrative key value automatically or through the CLI (see the [“Specifying an Administrative Key Value” section on page 6-19](#)). The administrative key defines the ability of a port to aggregate with other ports. The following factors determine a port’s ability to aggregate with other ports:

- Port physical characteristics, such as data rate, duplex capability, and point-to-point or shared medium
- Configuration constraints that you establish

When enabled, LACP always tries to configure the maximum number of compatible ports in a channel, up to the maximum allowed by the hardware (eight ports). If LACP is not able to aggregate all the ports that are compatible (for example, the remote system might have more restrictive hardware limitations), then the system places all the ports that cannot be actively included in the channel in hot standby state and uses them only if one of the channeled ports fails.

You can configure different channels with ports that have been assigned the same administrative key. For example, if you assign eight ports to the same administrative key, you may configure four ports in a channel using LACP **active** mode and the remaining four ports in a manually configured channel using the **on** mode. An administrative key is meaningful only in the context of the switch that allocates it; there is no global significance to administrative key values.

*CISCO Confidential - DRAFT*

# Configuring EtherChannel Using LACP

These sections describe how to configure EtherChannel using LACP:

- [Specifying the EtherChannel Protocol, page 6-18](#)
- [Specifying the System Priority, page 6-19](#)
- [Specifying the Port Priority, page 6-19](#)
- [Specifying an Administrative Key Value, page 6-19](#)
- [Changing the Channel Mode, page 6-20](#)
- [Specifying the Channel Path Cost, page 6-21](#)
- [Specifying the Channel VLAN Cost, page 6-21](#)
- [Clearing LACP Statistics, page 6-21](#)
- [Displaying EtherChannel Traffic Utilization, page 6-21](#)
- [Disabling an EtherChannel, page 6-22](#)
- [Displaying Spanning Tree-Related Information for EtherChannels, page 6-22](#)

**Note**

Before you configure the EtherChannel, see the “[EtherChannel Configuration Guidelines and Restrictions](#)” section on page 6-3.

## Specifying the EtherChannel Protocol

**Note**

The default protocol is PAgP.

**Note**

You can specify only one protocol, PAgP or LACP, per module.

To specify the EtherChannel protocol, perform this task in privileged mode:

| Task                               | Command                                      |
|------------------------------------|----------------------------------------------|
| Specify the EtherChannel protocol. | <b>set channelprotocol</b> [pagp   lacp] mod |

This example shows how to specify the LACP protocol for modules 2 and 3:

```
Console> (enable) set channelprotocol lacp 2,3
Mod 2 is set to LACP protocol.
Mod 3 is set to LACP protocol.
Console> (enable)
```

Use the **show channelprotocol** command to display the protocols for all modules.

## Specifying the System Priority



### Note

Although the **set lacp-channel system-priority** command is a global option, it applies only to modules on which LACP is enabled; it is ignored on modules running PAgP.

The system priority value must be a number in the range of 1 – 65,535, where higher numbers represent lower priority. The default priority is 32,768.

To specify the system priority, perform this task in privileged mode:

| Task                         | Command                                              |
|------------------------------|------------------------------------------------------|
| Specify the system priority. | <b>set lacp-channel system-priority</b> <i>value</i> |

This example shows how to specify the system priority as 20,000:

```
Console> (enable) set lacp-channel system-priority 20000
LACP system priority is set to 20000
Console> (enable)
```

Use the **show lacp-channel sys-id** command to display the LACP system ID and system priority.

## Specifying the Port Priority

The port priority value must be a number in the range of 1 – 255, where higher numbers represent lower priority. The default priority is 128.

To specify the port priority, perform this task in privileged mode:

| Task                       | Command                                                           |
|----------------------------|-------------------------------------------------------------------|
| Specify the port priority. | <b>set port lacp-channel</b> <i>mod/ports port-priority value</i> |

This example shows how to specify the port priority as 10 for ports 1/1 to 1/4 and 2/6 to 2/8:

```
Console> (enable) set port lacp-channel 1/1-4,2/6-8 port-priority 10
Port(s) 1/1-4,2/6-8 port-priority set to 10.
Console> (enable)
```

Use the **show lacp-channel group admin\_key info** command to display the port priority.

## Specifying an Administrative Key Value



### Note

When the system or module configuration information stored in NVRAM is cleared, the administrative keys are assigned new values automatically. For modules, each group of four consecutive ports, beginning at the 1st, 5th, 9th and so on, are assigned a unique administrative key. Across the module, ports must have unique administrative keys. After NVRAM is cleared, the channel mode of the ports is set to “passive.”

*CISCO Confidential - DRAFT*

You can specify an administrative key value to a set of ports. If you do not specify an administrative key value, the system automatically selects a value. In both cases, the value can range from 1 – 1024.

If you choose a value for the administrative key, and this value has already been used in the system, then the system moves all the ports originally associated with the previously assigned administrative key value to another automatically assigned value, and it assigns the modules and ports you specified in the command to the administrative key value that you specified.

The maximum number of ports to which an administrative key can be assigned is eight.

The default mode for all ports being assigned the administrative key is passive; however, if the channel was previously assigned a particular mode (see the [“Changing the Channel Mode” section on page 6-20](#)), assigning the administrative key will not affect it—that is, the channel mode that you specified previously is maintained.

To specify the administrative key value, perform this task in privileged mode:

| Task                                  | Command                                                            |
|---------------------------------------|--------------------------------------------------------------------|
| Specify the administrative key value. | <b>set port lacp-channel</b> <i>mod/ports</i> [ <i>admin_key</i> ] |

This example assigns ports 4/1 to 4/4 the same administrative key, allowing the system to pick its value:

```
Console> (enable) set port lacp-channel 4/1-4
Port(s) 4/1-4 are assigned to admin key 96.
Console> (enable)
```

This example shows how to assign ports 4/4 to 4/6 the administrative key 96 (you specify the 96). In this example, the administrative key was previously assigned to another group of ports by the system (see the previous example), so those ports will be moved to another administrative key:

```
Console> (enable) set port lacp-channel 4/4-6 96
Port(s) 4/1-3 are moved to admin key 97.
Port(s) 4/4-6 are assigned to admin key 96.
Console> (enable)
```

This example shows the system response when more than eight ports are assigned the same administrative key value:

```
Console> (enable) set port lacp-port channel 2/1-2,4/1-8 123
No more than 8 ports can be assigned to an admin key.
Console> (enable)
```

Use the **show lacp-channel group** command to display administrative key values for ports.

## Changing the Channel Mode

You can change the channel mode for a set of ports that were previously assigned the same administrative key (see the [“Specifying an Administrative Key Value” section on page 6-19](#)).

To change the channel mode, perform this task in privileged mode:

| Task                     | Command                                                                                                               |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Change the channel mode. | <b>set port lacp-channel</b> <i>mod/ports</i> <b>mode</b> [ <b>on</b>   <b>off</b>   <b>active</b>   <b>passive</b> ] |



*CISCO Confidential - DRAFT*

This example shows how to change the channel mode for ports 4/1 and 4/6, setting it to **on**. The administrative key for ports 4/1 and 4/6 is unchanged.

```
Console> (enable) set port lacp-channel 4/1,4/6 mode on
Port(s) 4/1,4/6 channel mode set to on.
Console> (enable)
```

Use the **show lacp-channel group admin\_key** command to display the channel mode for ports.

## Specifying the Channel Path Cost

You can specify the channel path cost by using a global command that configures both LACP and PAgP. For more information, see the [“Setting the EtherChannel Spanning Tree Port Cost” section on page 6-8](#).

## Specifying the Channel VLAN Cost

You can specify the channel VLAN cost with a global command that configures both LACP and PAgP. See the [“Setting the EtherChannel Spanning Tree Port VLAN Cost” section on page 6-9](#) for information.

## Clearing LACP Statistics

To clear LACP statistics, perform this task in privileged mode:

| Task                   | Command                              |
|------------------------|--------------------------------------|
| Clear LACP statistics. | <b>clear lacp-channel statistics</b> |

This example shows how to clear LACP statistics:

```
Console> (enable) clear lacp-channel statistics
LACP channel counters are cleared.
Console> (enable)
```

## Displaying EtherChannel Traffic Utilization

To display the traffic utilization on the EtherChannel ports, perform this task:

| Task                         | Command                          |
|------------------------------|----------------------------------|
| Display traffic utilization. | <b>show lacp-channel traffic</b> |

This example shows how to display traffic utilization on EtherChannel ports:

```
Console> (enable) show lacp-channel traffic
ChanId Port Rx-Ucst Tx-Ucst Rx-Mcst Tx-Mcst Rx-Bcst Tx-Bcst

 808 2/16 0.00% 0.00% 50.00% 75.75% 0.00% 0.00%
 808 2/17 0.00% 0.00% 50.00% 25.25% 0.00% 0.00%
 816 2/31 0.00% 0.00% 25.25% 50.50% 0.00% 0.00%
 816 2/32 0.00% 0.00% 75.75% 50.50% 0.00% 0.00%
Console> (enable)
```

*CISCO Confidential - DRAFT*

## Disabling an EtherChannel

To disable an EtherChannel, perform this task for ports 2/2 to 2/8:

| Task                     | Command                                               |
|--------------------------|-------------------------------------------------------|
| Disable an EtherChannel. | <b>set port lacp-channel <i>mod/port</i> mode off</b> |

This example shows how to disable an EtherChannel:

```
Console> (enable) set port lacp-channel 2/2-8 mode off
Port(s) 2/2-8 channel mode set to off.
Console> (enable)
```

## Displaying Spanning Tree-Related Information for EtherChannels

You can display the channel ID and the truncated port list for all ports that are channeling. Ports that are not channeling are identified by their port number.

To display spanning tree-related information for EtherChannels, perform this task:

| Task                                                         | Command                              |
|--------------------------------------------------------------|--------------------------------------|
| Display spanning-tree related information for EtherChannels. | <b>show spantree <i>mod/port</i></b> |

These examples show how to display spanning tree-related information for EtherChannels:

```
Console> show spantree 4/6
Port Vlan Port-State Cost Priority Portfast Channel_id

4/6 1 not-connected 4 32 disabled 0
Console>
```

```
Console> show spantree 4/7-8
Port Vlan Port-State Cost Priority Portfast Channel_id

4/7-8 1 blocking 3 32 disabled 770
Console>
```

## Configuring Spanning Tree

This chapter describes the IEEE 802.1D bridge Spanning Tree Protocol (STP) and how to use and configure Cisco's proprietary STPs, Per VLAN Spanning Tree + (PVST+), and Multi-Instance Spanning Tree Protocol (MISTP) on the Catalyst enterprise LAN switches.

**Note**

For information on configuring the spanning tree PortFast, UplinkFast, and BackboneFast features, see [Chapter 8, “Configuring Spanning Tree PortFast, BPDU Guard, BPDU Filter, UplinkFast, BackboneFast, and Loop Guard.”](#)

This chapter consists of these sections:

- [Understanding How STPs Work, page 7-2](#)
- [Understanding How PVST+ and MISTP Modes Work, page 7-10](#)
- [Understanding How Bridge Identifiers Work, page 7-12](#)
- [Understanding How MST Works, page 7-13](#)
- [Rate limited at one for every 60 seconds, page 7-21](#)
- [Using MISTP-PVST+ or MISTP, page 7-28](#)
- [Configuring a Root Switch, page 7-36](#)
- [Configuring Spanning Tree Timers, page 7-40](#)
- [Understanding How BPDU Skewing Works, page 7-20](#)
- [Configuring Spanning Tree BPDU Skewing, page 7-53](#)
- [Configuring MST, page 7-42](#)

**Note**

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 4500 Series, Catalyst 2948G, and Catalyst 2980G Switches Command Reference*.

*CISCO Confidential - DRAFT*

## Understanding How STPs Work

This section describes the specific functions that are common to all spanning tree protocols. The Cisco proprietary spanning tree protocols, PVST+ and MISTP, are based on the IEEE 802.1D STP. (See the [“Understanding How PVST+ and MISTP Modes Work”](#) section on page 7-10 for information about PVST+ and MISTP.) The 802.1D STP is a Layer 2 management protocol that provides path redundancy in a network while preventing undesirable loops. All spanning tree protocols use an algorithm that calculates the best loop-free path through the network.

STP uses a distributed algorithm that selects one bridge of a redundantly connected network as the root of a spanning tree connected active topology. STP assigns roles to each port depending on what the port’s function is in the active topology. Port roles are as follows:

- Root—A forwarding port elected for the spanning tree topology
- Designated—A forwarding port elected for every switched LAN segment
- Alternate—A blocked port providing an alternate path to the root port in the spanning tree
- Backup—A blocked port in a loopback configuration

Switches that have ports with these assigned roles are called root or designated switches. For more information, see the [“Understanding How a Topology Is Created”](#) section on page 7-2.

In Ethernet networks, only one active path may exist between any two stations. Multiple active paths between stations can cause loops in the network. When loops occur, some switches recognize stations on both sides of the switch. This situation causes the forwarding algorithm to malfunction allowing duplicate frames to be forwarded.

Spanning tree algorithms provide path redundancy by defining a tree that spans all of the switches in an extended network and then forces certain redundant data paths into a standby (blocked) state. At regular intervals the switches in the network send and receive spanning tree packets which they use to identify the active path. If one network segment becomes unreachable, or if spanning tree costs change, the spanning tree algorithm reconfigures the spanning tree topology and reestablishes the link by activating a standby path.

Spanning tree operation is transparent to end stations, which do not detect whether they are connected to a single LAN segment or a switched LAN of multiple segments.

## Understanding How a Topology Is Created

All switches in an extended LAN participating in a spanning tree gather information about other switches in the network through an exchange of data messages known as bridge protocol data units (BPDUs). This exchange of messages results in the following actions:

- A unique root switch is elected for the spanning tree network topology.
- A designated switch is elected for every switched LAN segment.
- Any loops in the switched network are eliminated by placing redundant switch ports in a backup state; all paths that are not needed to reach the root switch from anywhere in the switched network are placed in STP-blocked mode.

The following three things determine the topology of an active switched network:

- The unique switch identifier (MAC address of the switch) that is associated with each switch
- The path cost to the root associated with each switch port
- The port identifier (MAC address of the port) associated with each switch port

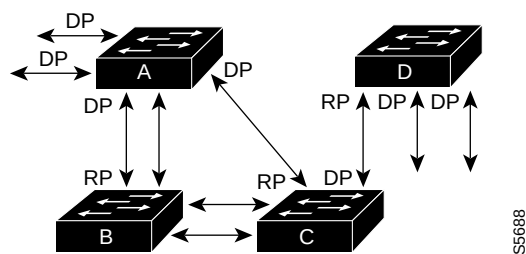
*CISCO Confidential - DRAFT*

In a switched network, the root switch is the logical center of the spanning tree topology. A spanning tree protocol uses BPDUs to elect the root switch and root port for the switched network and the root port and designated port for each switched segment.

## Understanding How a Switch or Port Becomes the Root Switch or Root Port

If all switches in a network are enabled with default settings, the switch with the lowest MAC address becomes the root switch. In the network shown in [Figure 7-1](#), Switch A, with the lowest MAC address, is the root switch. However, due to traffic patterns, number of forwarding ports, or line types, Switch A might not be the ideal root switch. You can force a switch to become the root switch by increasing the priority (that is, lowering the priority number) on the preferred switch. This action causes the spanning tree to recalculate the topology and make the selected switch the root switch.

**Figure 7-1 Configuring a Loop-Free Topology**



RP = Root Port  
DP = Designated Port

You can also change the priority of a port in order to make it the root port. When the spanning tree topology is based on default parameters, the path between the source and the destination stations in a switched network might not be ideal. The goal is to make the fastest link the root port, connecting higher-speed links to a port that has a higher number than the current root port can cause a root-port change.

For example, assume that a port on Switch B is a fiber-optic link. Also, 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 Port Priority parameter for the UTP port to a higher priority (lower numerical value) than the fiber-optic port, the UTP port becomes the root port. You could also accomplish this scenario by changing the port cost parameter for the UTP port to a lower value than that of the fiber-optic port.

## Understanding BPDUs

BPDUs contain configuration information about the transmitting switch and its ports, including switch and port MAC addresses, switch priority, port priority, and port cost. Each configuration BPDU contains this information:

- The unique identifier of the switch that the transmitting switch believes to be the root switch
- The cost of the path to the root from the transmitting port
- The identifier of the transmitting port

*CISCO Confidential - DRAFT*

The switch sends configuration BPDUs to communicate with and compute the spanning tree topology. A MAC frame conveying a BPDU sends the switch group address to the destination address field. All switches connected to the LAN on which the frame is transmitted receive the BPDU. BPDUs are not directly forwarded by the switch, but the receiving switch uses the information in the frame to calculate a BPDU. If the topology changes, the receiving switch initiates a BPDU transmission.

A BPDU exchange results in the following:

- One switch is elected as the root switch.
- The shortest distance to the root switch is calculated for each switch.
- A designated switch is selected. This is the switch that is closest to the root switch through which frames will be forwarded to the root.
- A port for each switch is selected. This is the port that provides the best path from the switch to the root switch.
- Ports included in the STP are selected.

## Understanding Spanning Tree Port States

Topology changes can take place in a switched network due to a link coming up or going down (failing). When a switch port transitions directly from nonparticipation in the topology to the forwarding state, it can create temporary data loops. Ports must wait for new topology information to propagate through the switches in the LAN before they can start forwarding frames. They must also allow the frame lifetime to expire for frames that have been forwarded using the old topology.

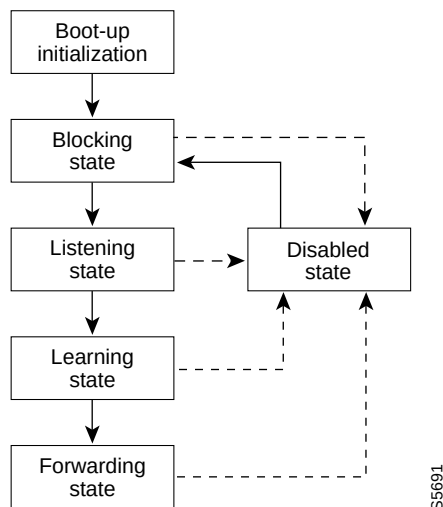
At any given time, each port on a switch using STP is in one of these states:

- Blocking
- Listening
- Learning
- Forwarding
- Disabled

A port moves through these states:

- From initialization to blocking
- From blocking to either listening or disabled
- From listening to either listening or disabled
- From learning to either forwarding or disabled
- From forwarding to disabled

Figure 7-2 illustrates how a port moves through the states.

*CISCO Confidential - DRAFT***Figure 7-2 STP Port States**

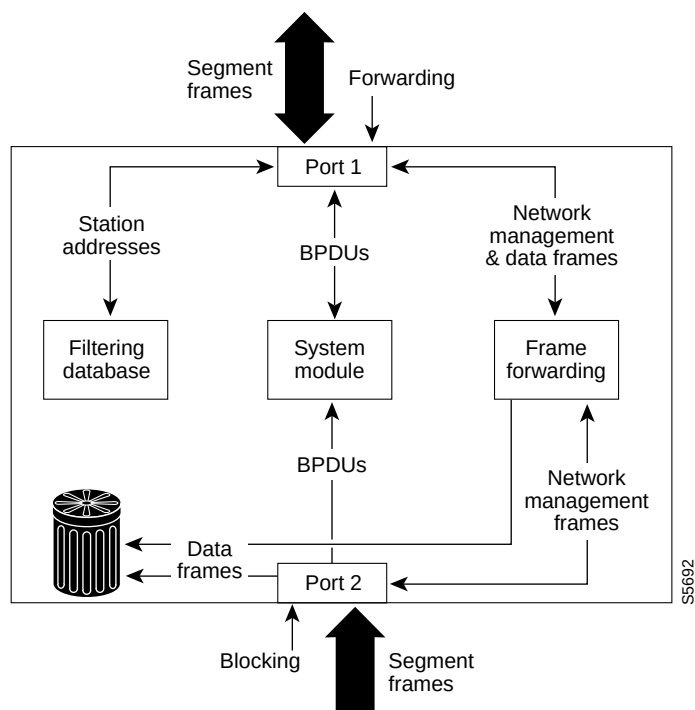
You can modify each port state by using management software, such as the VLAN Trunking Protocol (VTP). When you enable spanning tree, every switch in the network goes through the blocking state and the transitory states of listening and learning at power up. If properly configured, each port stabilizes into the forwarding or blocking state.

When the spanning tree algorithm places a port in the forwarding state, the following occurs:

- The port is put into the listening state while it waits for protocol information that suggests it should go to the blocking state
- The port waits for the expiration of a protocol timer that moves the port to the learning state
- In the learning state, the port continues to block frame forwarding as it learns station location information for the forwarding database
- The expiration of a protocol timer moves the port to the forwarding state, where both learning and forwarding are enabled

## Blocking State

A port in the blocking state, such as Port 2 in [Figure 7-3](#), does not participate in frame forwarding. After initialization, a BPDU is sent to each port in the switch. A switch initially assumes it is the root until it exchanges BPDUs with other switches. This exchange establishes which switch in the network is really the root. If only one switch resides in the network, no exchange occurs, the forward delay timer expires, and the ports move to the listening state. A switch always enters the blocking state following switch initialization.

*CISCO Confidential - DRAFT***Figure 7-3 Port 2 in Blocking State**

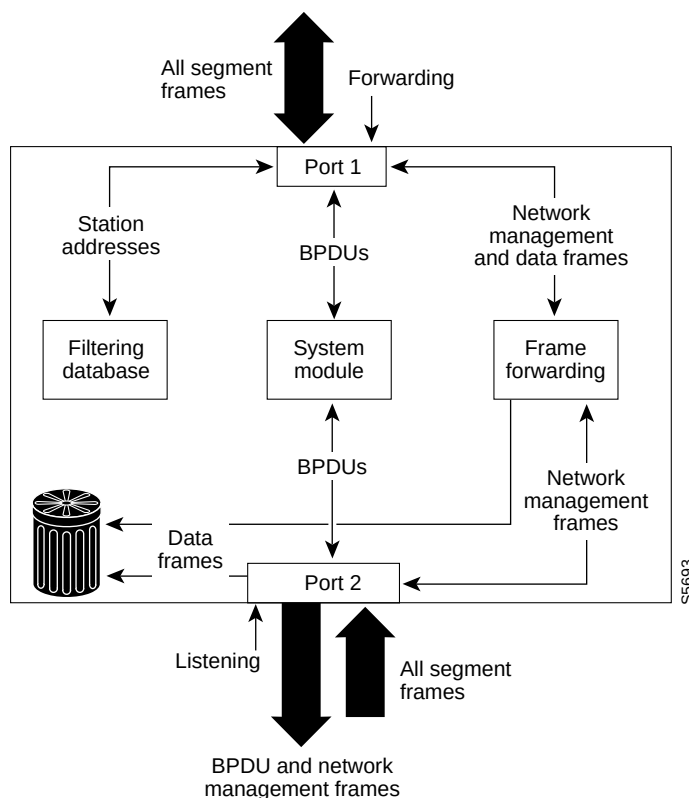
A port in the blocking state performs as follows:

- Discards frames received from the attached segment
- Discards frames switched from another port for forwarding
- Does not incorporate station location into its address database (there is no learning on a blocking 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 port enters after the blocking state. The port enters this state when the spanning tree determines that the port should participate in frame forwarding. Learning is disabled in the listening state. [Figure 7-4](#) shows a port in the listening state.



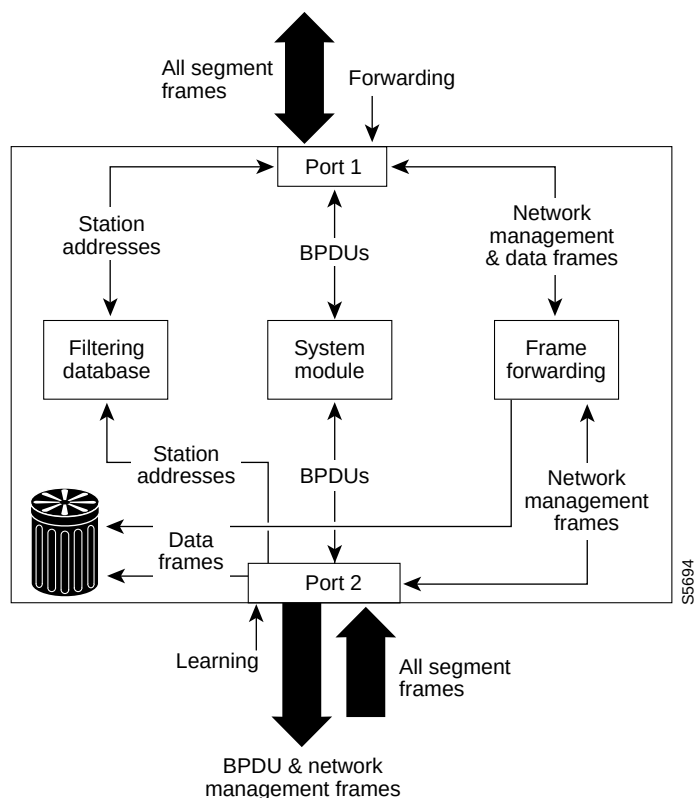
*CISCO Confidential - DRAFT***Figure 7-4 Port 2 in Listening State**

A port in the listening state performs as follows:

- Discards frames received from the attached segment
- Discards frames switched from another port for forwarding
- Does not incorporate 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
- Processes BPDUs received from the system module
- Receives and responds to network management messages

## Learning State

A port in the learning state prepares to participate in frame forwarding. The port enters the learning state from the listening state. [Figure 7-5](#) shows a port in the learning state.

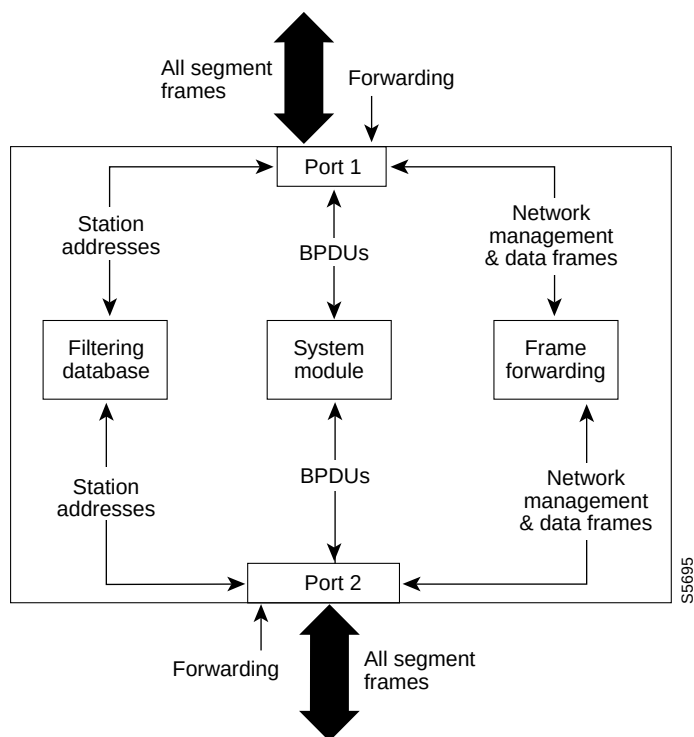
*CISCO Confidential - DRAFT***Figure 7-5 Port 2 in Learning State**

A port in the learning state performs as follows:

- Discards frames received from the attached segment
- Discards frames switched from another port for forwarding
- Incorporates 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 port in the forwarding state forwards frames, as shown in [Figure 7-6](#). The port enters the forwarding state from the learning state.

*CISCO Confidential - DRAFT***Figure 7-6 Port 2 in Forwarding State**

A port in the forwarding state performs as follows:

- Forwards frames received from the attached segment
- Forwards frames switched from another port for forwarding
- Incorporates 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

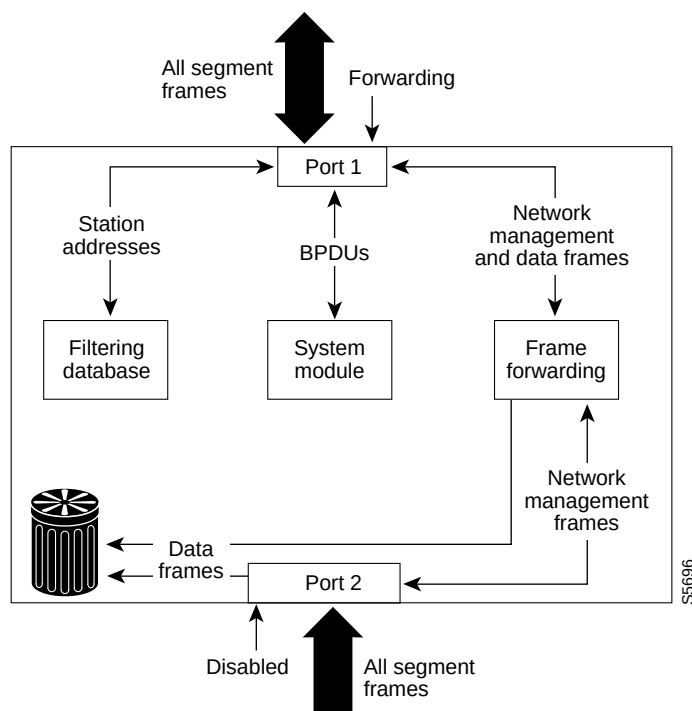
**Caution**

Use spanning tree PortFast mode only on ports directly connected to individual workstations to allow these ports to come up and go directly to the forwarding state, instead of having to go through the entire spanning tree initialization process. To prevent illegal topologies, enable spanning tree on ports connected to switches or other devices that forward messages. For more information on PortFast, see [Chapter 8, “Configuring Spanning Tree PortFast, BPDU Guard, BPDU Filter, UplinkFast, BackboneFast, and Loop Guard.”](#)

*CISCO Confidential - DRAFT***Disabled State**

A port in the disabled state does not participate in frame forwarding or STP, as shown in Figure 7-7. A port in the disabled state is virtually nonoperational.

**Figure 7-7 Port 2 in Disabled State**



A disabled port performs as follows:

- Discards frames received from the attached segment
- Discards frames switched from another port for forwarding
- Does not incorporate station location into its address database (there is no learning, so there is no address database update)
- Receives BPDUs but does not direct them to the system module
- Does not receive BPDUs for transmission from the system module
- Receives and responds to network management messages

## Understanding How PVST+ and MISTP Modes Work

Catalyst 4000 family switches provide two proprietary spanning tree modes based on the IEEE 802.1D standard and one mode that is a combination of the two modes:

- Per VLAN Spanning Tree (PVST+)
- Rapid PVST+
- Multi-Instance Spanning Tree Protocol (MISTP)
- MISTP-PVST+ (combination mode)

*CISCO Confidential - DRAFT*

The following sections provide an overview of each mode.

**Caution**

If your network currently uses PVST+ and you plan to use MISTP on any switch, you must first enable MISTP-PVST+ on the switch and configure an MISTP instance to avoid causing network loops.

## PVST+ Mode

PVST+ is the default STP used on all Ethernet, Fast Ethernet, and Gigabit Ethernet port-based VLANs on Catalyst 4000 family switches. PVST+ runs on each VLAN on the switch, ensuring that each has a loop-free path through the network.

PVST+ provides Layer 2 load balancing for the VLAN on which it runs; you can create different logical topologies using the VLANs on your network to ensure that all of your links will be used but no one link will be oversubscribed.

Each instance of PVST+ on a VLAN has a single root switch. This root switch propagates the spanning tree information associated with that VLAN to all other switches in the network. Because each switch has the same knowledge about the network, this process ensures that the network topology is maintained.

## Rapid PVST+

Rapid PVST+ is the same as PVST+, except that Rapid PVST+ utilizes a Rapid STP based on IEEE 802.1w instead of 802.1D. Rapid PVST+ uses the same configuration as PVST+, and you need only minimal extra configuration. With Rapid PVST+, dynamic CAM entries are flushed immediately on a per-port basis upon any topology change. UplinkFast and BackboneFast are enabled but not active in this mode, because the functionality is built into the rapid STP. This method provides for quick recovery of connectivity following the failure of a bridge, bridge port, or LAN.

## MISTP Mode

MISTP is an optional STP that runs on Catalyst 4000 family switches. MISTP allows you to group multiple VLANs under a single instance of spanning tree (an MISTP instance). MISTP combines the Layer 2 load-balancing benefits of PVST+ with the lower CPU load of IEEE 802.1Q.

An MISTP instance is a virtual logical topology defined by a set of bridge and port parameters; an MISTP instance becomes a real topology when VLANs are mapped to it. Each MISTP instance has its own root switch and a different set of forwarding links (that is different bridge and port parameters).

Each instance of MISTP has a single root switch. This root switch propagates the information associated with that instance of MISTP to all other switches in the network. This process ensures that the network topology is maintained because each switch has the same knowledge about the network.

MISTP builds MISTP instances by exchanging MISTP BPDUs with peer entities in the network. There is only one BPDU for each MISTP instance, rather than for each VLAN as in PVST+. There are fewer BPDUs in an MISTP network; therefore, there is less overhead in the network. MISTP discards any PVST+ BPDUs that it sees.

An MISTP instance can have any number of VLANs mapped to it, but a VLAN can only be mapped to a single MISTP instance. You can easily move a VLAN (or VLANs) in an MISTP topology to another MISTP instance if it has converged. (However, if ports are added at the same time the VLAN is moved, convergence time is required.)

*CISCO Confidential - DRAFT*

## MISTP-PVST+ Mode

MISTP-PVST+ is a transition spanning tree mode that allows you to use the MISTP functionality on Catalyst 4000 family switches while continuing to communicate with the older Catalyst 5000 family and 6500 series switches in your network that use PVST+. A switch using PVST+ mode and a switch using MISTP mode connected together cannot see the BPDUs of the other switch, a condition that can cause loops in the network. MISTP-PVST+ allows interoperability between PVST+ and pure MISTP, because it detects the BPDUs of both modes. If you wish to convert your network to MISTP, you can use MISTP-PVST+ to transition the network from PVST+ to MISTP in order to avoid problems.

MISTP-PVST+ conforms to the limits of PVST+; for example, you can only configure the amount of VLAN ports on your MISTP-PVST+ switches that you configure on your PVST+ switches.

## Understanding How Bridge Identifiers Work

The next two sections explain how MAC addresses are used in PVST+ and MISTP as unique bridge identifiers.

### MAC Address Allocation

Catalyst 4000 series switches have a pool of 1024 MAC addresses that can be used as bridge identifiers for VLANs running under PVST+ or for MISTP instances. The Catalyst 4500 series switches have a pool of only 64 MAC addresses. You can use the **show module** command to view the MAC address range.

MAC addresses are allocated sequentially, with the first MAC address in the range assigned to VLAN 1, the second in the range assigned to VLAN 2, and so forth. The last MAC address in the range is assigned to the supervisor engine in-band (sc0) management interface.

For example, if the MAC address range for the supervisor engine is 00-e0-1e-9b-2e-00 to 00-e0-1e-9b-31-ff, the VLAN 1 bridge ID is 00-e0-1e-9b-2e-00, the VLAN 2 bridge ID is 00-e0-1e-9b-2e-01, the VLAN 3 bridge ID is 00-e0-1e-9b-2e-02, and so forth. The in-band (sc0) interface MAC address is 00-e0-1e-9b-31-ff.

### MAC Address Reduction

The MAC address reduction feature is used on Catalyst 6000 family switches to enable extended-range VLAN identification. If you have a Catalyst 6000 switch in your network and you have MAC address reduction enabled on it, you should also enable MAC address reduction on all your Catalyst 4000 family switches to avoid problems in the spanning tree topology. When MAC address reduction is enabled on Catalyst 4000 family switches, it disables the pool of MAC addresses used for the VLAN spanning tree, leaving a single MAC address that identifies the switch. For detailed information on the MAC address reduction feature, refer to the *Catalyst 6500 Series Software Configuration Guide*.

MAC address reduction is always enabled on the Catalyst 4500 series switches; however, it may or may not be enabled on a Catalyst 4006 switch; this can affect the selection of the root bridge after you migrate your supervisor engine. Here are two scenarios to consider:

- The Catalyst 4006 switch is not a root switch

In this case, the spanning tree topology will not change. If you add to the network a Catalyst 4500 series switch with MAC-reduction enabled and its default spanning tree bridge ID priority set to 32,768, the bridge ID priority of the new switch becomes the bridge ID priority added to the system

## CISCO Confidential - DRAFT

ID extension. The system ID extension is the VLAN number and can vary from 1 to 4094. So if the switch is in VLAN 1, the new bridge ID priority will be 32,769. Because 32,769 is greater than 32,768, this switch cannot become the root switch and poses no problems.

- The Catalyst 4006 is a root switch

In this case, the spanning tree topology might change. If the other switches in the network are not running MAC-reduction, then the topology will change after you replace the chassis with a Catalyst 4500 series switch. The bridge ID priority of the new Catalyst 4500 series switch increments in the same manner as in the previous scenario (bridge ID priority + VLAN number). Therefore, if the switch is in VLAN 1, the new bridge ID will be 32769. Since 32769 is greater than 32768, this switch cannot become the root switch. The network designates a new root switch; the spanning tree topology also changes to reflect the new root switch.

If the bridge priority of the Catalyst 4006 has been lowered administratively and you use the same configuration in the new Catalyst 4500 series switch, then the switch remains the root switch and the spanning tree topology does not change.

For more information on migrating your supervisor engine from a Catalyst 4006 switch to a Catalyst 4500 series switch, see the [“Migrating a Supervisor Engine II from a Catalyst 4006 Switch to a Catalyst 4500 Series Switch” section on page 28-10.](#)

## Understanding How MST Works

The Multiple Spanning Tree (MST) feature is an upcoming IEEE standard: 802.1s for MST is an amendment to 802.1Q. MST extends the 802.1w Rapid Spanning Tree (RST) algorithm to multiple spanning trees. This extension provides for both rapid convergence and load balancing in a VLAN environment. The MST protocol is currently being further developed and the MST feature for this release is based on a draft version of the IEEE standard. The protocol as implemented in this release is backward compatible with 802.1D STP, 802.1w, the Rapid Spanning Tree Protocol (RSTP), and the Cisco PVST+ architecture.

MST allows you to build multiple spanning trees over VLAN 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, having different VLAN-spanning tree instance assignments located in different parts of the network makes it easier to administrate and optimally utilize redundant paths. However, a spanning tree instance can exist only on bridges that have compatible VLAN-instance assignments. Therefore, MST requires that you configure a set of bridges with the same MST configuration information, allowing them to participate in a given 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 a variant of STP (IST) that augments the Common Spanning Tree (CST) information with internal information about the MST region.

*CISCO Confidential - DRAFT*

- IST connects all the MST bridges in the region and appears as a subtree in the CST that encompasses the whole bridged domain. The MST region appears as a virtual bridge to adjacent SST bridges and MST regions.
- The collection of ISTs in each MST region, the CST that interconnects the MST regions, and the SST bridges define Common and Internal Spanning Tree (CIST). 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 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 given 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 part of RSTP.
  - PortFast is supported.
  - BPDU filter and BPDU guard are supported in MST mode.
  - Loop guard and root guard are supported in MST. MST preserves the VLAN 1 disabled functionality except that BPDUs are still transmitted in VLAN 1.
  - MST switches behave as if MAC reduction is enabled.
  - For private VLANs, secondary VLANs are mapped to the same instance as the primary.

Note the following guidelines when using MST:

- Do not disable spanning tree on any VLAN in any of the PVST bridges.
- Ensure that all PVST spanning tree root bridges have lower (numerically higher) priority than the CST root bridge.
- Do not use PVST bridges as the root of CST.
- Ensure that trunks carry all of the VLANs mapped to an instance or do not carry any VLANs at all.
- 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 carried out during the maintenance window. This action should be taken because the complete MST database gets re-initialized for any incremental changes (such as adding new VLANs to instances or moving VLANs across instances).

## Rapid Spanning Tree Protocol

RSTP significantly reduces the time it takes you to reconfigure the active topology of the network when changes to the physical topology or its configurations parameters occur. 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.



## CISCO Confidential - DRAFT

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 through an explicit handshake between them. RSTP allows switch port configuration so the ports can transition to forwarding directly when the switch reinitializes.

RSTP, specified in 802.1w, supersedes STP specified in 802.1D while retaining compatibility with STP. RSTP provides the structure on which the MST operates. You configure RSTP when you configure the MST feature. For more information, see the [“Configuring MST” section on page 7-42](#).

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. RSTP BPDUs are not visible on the port. Only version 3 BPDUs are visible on the 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 7-1](#) provides a comparison between STP port states and RSTP port states.

**Table 7-1 Comparison Between STP and RSTP Port States**

| Operational Status | STP Port State        | RSTP Port State         | Port Included in Active Topology? |
|--------------------|-----------------------|-------------------------|-----------------------------------|
| Enabled            | Blocking <sup>1</sup> | Discarding <sup>2</sup> | No                                |
| Enabled            | Listening             | Discarding              | No                                |
| Enabled            | Learning              | Learning                | Yes                               |

*CISCO Confidential - DRAFT***Table 7-1 Comparison Between STP and RSTP Port States (continued)**

| Operational Status | STP Port State | RSTP Port State | Port Included in Active Topology? |
|--------------------|----------------|-----------------|-----------------------------------|
| Enabled            | Forwarding     | Forwarding      | Yes                               |
| Disabled           | Disabled       | Discarding      | No                                |

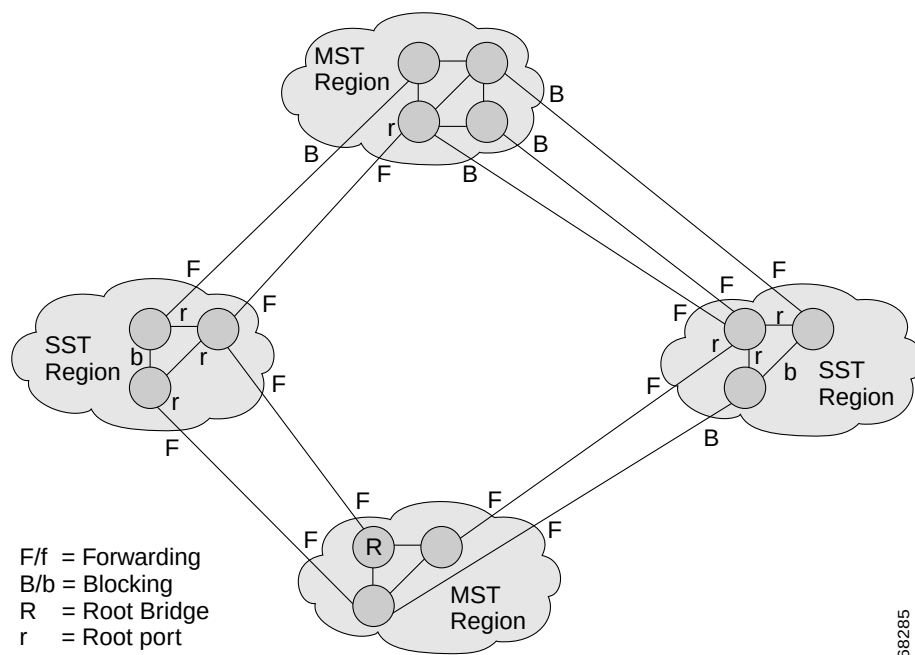
1. IEEE 802.1D port state designation.

2. IEEE 802.1w port state designation. Discarding is analogous with, and the same as blocking in MST in this document.

In a stable topology, RSTP ensures that every root port and designated port transition to forwarding while all alternate ports and backup ports are always in the discarding state.

## MST-to-SST Interoperability

A virtual bridged LAN may contain interconnected regions of SST and MST bridges. [Figure 7-8](#) shows this relationship.

**Figure 7-8 Network with Interconnected SST and MST Regions**

To the spanning tree protocol running in the SST region, an MST region appears as a single SST or pseudobridge. 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.

## CISCO Confidential - DRAFT

- 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 pseudo bridge 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.

## Common Spanning Tree

802.1Q specifies a single spanning tree for all the VLANs called CST. In a Catalyst 4000 family switch running PVST+, the VLAN 1 spanning tree corresponds to CST. In a Catalyst 4000 family switch running MST, IST (instance 0) corresponds to CST.

## MST Instances

This release supports up to 16 instances; each spanning tree instance is identified by an instance ID that ranges from 0 to 15. Instance 0 is mandatory and is always present. Instances 1 through 15 are optional.

## MST Configuration

MST configuration has three parts as follows:

- Name—A 32-character string (null padded and null terminated) identifying the MST region.
- Revision number—An unsigned 16-bit number that increments each time a change is made to the configuration.

**Note**

You must set and update the revision number manually, because it does not auto-increment 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 treated as an SST BPDU.

When you modify an MST configuration through either a console or Telnet connection, the session exits without committing those changes and the edit buffer locks. Further configuration is impossible until you discard the existing edit buffer and acquire a new edit buffer by entering the **set spantree mst config rollback force** command.

*CISCO Confidential - DRAFT*

## MST Region

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 certain delay. We do not recommend partitioning the network into a large number of regions.

## Boundary Ports

A port that connects an MST region to an SST region running RSTP (802.1w), an SST region running STP (802.1D), or another MST region is a boundary port. A boundary port is a port that connects to a LAN, the designated bridge of which, is either an SST bridge or a bridge with a different MST configuration. A designated port knows that it is on the boundary if it detects an STP bridge or receives an agreement message from an RST or MST bridge with a different configuration.

At the boundary, the role of MST ports do not matter; their state is forced to be the same as the IST port state. If the boundary flag is set for the port, the MSTP Port Role selection mechanism assigns a port role to the boundary and the same state as that of the IST port. The IST port at the boundary can take up any port role except a backup port role.

## IST Master

The IST master of an MST region is the bridge with the lowest bridge identifier and the least path cost to the CST root. If an MST bridge is the root bridge for CST, then it is the IST master of that MST region. If the CST root is outside the MST region, then one of the MST bridges at the boundary is selected as the IST master. Other bridges on the boundary that belong to the same region eventually block the boundary ports that lead to the root.

If two or more bridges at the boundary of the region have an identical path to the root, you can set a slightly lower bridge priority to make a specific bridge IST master.

The root path cost and message age inside a region stays constant, but the IST path cost is incremented and the IST remaining hops is decremented at each hop. Enter the **show spantree mst** command to display the information about the IST master, path cost, and remaining hops for the bridge.

## Edge Ports

A port that is connected to a nonbridging device (for example, a host or a router) is an edge port. A port that connects to a hub is also an edge port, provided that the hub or any LAN that is connected by it does not have a bridge. These ports start forwarding as soon as the link is up.

*CISCO Confidential - DRAFT*

MST requires that all ports are configured 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 requires 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.

**Note**

To configure a port as an edge port you enable PortFast on that port. See [Chapter 8, “Configuring Spanning Tree PortFast, BPDU Guard, BPDU Filter, UplinkFast, BackboneFast, and Loop Guard.”](#) When you enter the **show spantree portfast mod/port** command, if the designation for a port is displayed as edge, that port is also a PortFast port.

To prevent a misconfiguration, PortFast turns off operationally if the port receives a BPDU. You can display the configured and operational status of PortFast by using the **show spantree mst mod/port** command.

## Link Type

You can establish rapid connectivity only on point-to-point links. For correct operation of the protocol, you must explicitly configure ports 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. Enter the **set spantree mst link-type** command to configure point-to-point links.

## Message Age and Hop Count

IST and MST instances do not use the Message Age and Maximum Age timer settings in the BPDU. IST and MST use a separate hop count mechanism that is very similar to the IP TTL mechanism. You can configure each MST bridge with a maximum hop count. The root bridge of the instance sends a BPDU (or M-record) with the remaining hop count that is equal to the maximum hop count. When a bridge receives a BPDU (or M-record), it decrements the received remaining hop count by one. The bridge discards the BPDU (M-record) and ages out the information held for the port if the count reaches zero after decrementing. The nonroot bridges propagate the decremented count as the remaining hop count in the BPDUs (M-records) they generate.

The Message Age and Maximum Age timer settings in the RST portion of the BPDU remain the same throughout the region, and the same values are propagated by the region's designated ports at the boundary.

## MST-to-PVST+ Interoperability

These guidelines apply in a topology where you configure MST switches (all in the same region) to interact with PVST+ switches that have VLANs 1–100 set up to span throughout the network:

- Configure the root for all VLANs inside the MST region. The ports that belong to the MST switch at the boundary simulate PVST+ and send PVST+ BPDUs for all the VLANs. This example shows the ports simulating PVST:

```
Console> (enable) show spantree mst 3
Spanning tree mode MST
Instance 3
VLANs Mapped: 31-40

Designated Root 00-10-7b-bb-2f-00
```

*CISCO Confidential - DRAFT*

```

Designated Root Priority 8195 (root priority:8192, sys ID ext:3)
Designated Root Cost 0 Remaining Hops 20
Designated Root Port 1/0

```

```

Bridge ID MAC ADDR 00-10-7b-bb-2f-00
Bridge ID Priority 8195 (bridge priority:8192, sys ID ext:3)

```

| Port           | State      | Role | Cost  | Prio | Type |
|----------------|------------|------|-------|------|------|
| 6/1            | forwarding | BDRY | 10000 | 30   | P2P, |
| Boundary(PVST) |            |      |       |      |      |
| 6/2            | blocking   | BDRY | 20000 | 32   | P2P, |
| Boundary(PVST) |            |      |       |      |      |

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 reenabling 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.

## Understanding How BPDUs Skewing Works

BPDUs skewing is the difference between when the BPDUs are expected to be received and the time BPDUs are actually received. Skewing occurs when the following occurs:

- Spanning tree timers lapse.
- Expected BPDUs are not received.
- Spanning tree detects topology changes.

The skew causes BPDUs to reflood the network to keep the spanning tree topology database current.

The root switch advertises its presence by sending out BPDUs for the configured Hello time interval. The nonroot switches receive and process one BPDU during each configured time period. A VLAN might not receive the BPDU as scheduled. If the BPDU is not received on a VLAN at the configured time interval, the BPDU is skewed.

Spanning tree uses the Hello Time (see [“Configuring the Hello Time” section on page 40](#)) to detect when a connection to the root switch exists through a port and when that connection is lost. This feature applies to both PVST+ and MISTP. In MISTP, the skew detection is on a per-instance basis.

BPDUs skewing detects BPDUs that are not processed in a regular time frame on the nonroot switches in the network. If BPDU skewing occurs, a syslog message is displayed. The syslog applies to both PVST+ and MISTP.

*CISCO Confidential - DRAFT*

The number of syslog messages that are generated may impact the convergence of the network and the CPU utilization of the switch. New syslog messages are not generated as individual messages for every VLAN because the higher the number of syslog messages that are reported, the slower the switching process will be. To reduce the impact on the switch, the syslog messages are as follows:

- Generated 50 percent of the maximum age time (see the [“Configuring the Maximum Aging Time” section on page 41](#))
- Rate limited at one for every 60 seconds

## Using PVST+

PVST+ is the default spanning tree mode for Catalyst 4000 family switches. The following sections describe how to configure PVST+ on Ethernet VLANs.

## Default PVST+ Configuration

[Table 7-2](#) shows the default PVST+ configuration.

**Table 7-2 PVST+ Default Configuration**

| Feature                         | Default Value                                                                                                                                          |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| VLAN 1                          | All ports assigned to VLAN 1                                                                                                                           |
| Enable state                    | PVST+ enabled for all VLANs                                                                                                                            |
| MAC address reduction           | Disabled                                                                                                                                               |
| Bridge priority                 | 32,768                                                                                                                                                 |
| Bridge ID priority              | 32,769 (bridge priority plus system ID extension of VLAN 1)                                                                                            |
| Port priority                   | 32                                                                                                                                                     |
| Port cost                       | <ul style="list-style-type: none"> <li>• Gigabit Ethernet: 4</li> <li>• Fast Ethernet: 10</li> <li>• FDDI/CDDI: 10</li> <li>• Ethernet: 100</li> </ul> |
| Default spantree port cost mode | Short (802.1D)                                                                                                                                         |
| Port VLAN priority              | Same as port priority but configurable on a per-VLAN basis in PVST+                                                                                    |
| Port VLAN cost                  | Same as port cost but configurable on a per-VLAN basis in PVST+                                                                                        |
| Maximum aging time              | 20 sec                                                                                                                                                 |
| Hello time                      | 2 sec                                                                                                                                                  |
| Forward delay time              | 15 sec                                                                                                                                                 |

## Setting the PVST+ Bridge ID Priority

The bridge ID priority is the priority of a VLAN when the switch is in PVST+ mode.

*CISCO Confidential - DRAFT*

When the switch is in PVST+ mode without MAC address reduction enabled, you can enter a bridge priority value between 0–65,535. The VLAN bridge ID priority becomes that value.

When the switch is in PVST+ mode with MAC address reduction enabled, you can enter one of 16 bridge priority values: 0, 4096, 8192, 12,288, 16,384, 20,480, 24,576, 28,672, 32,768, 36,864, 40,960, 45,056, 49,152, 53,248, 57,344, or 61,440.

The switch creates the bridge ID priority by combining the VLAN bridge priority with the system ID extension (that is, the ID of the VLAN).

To set the spanning tree bridge priority for a VLAN, perform this task in privileged mode:

|        | Task                                   | Command                                                                |
|--------|----------------------------------------|------------------------------------------------------------------------|
| Step 1 | Set the bridge ID priority for a VLAN. | <b>set spantree priority</b> <i>bridge_ID_priority</i> [ <i>vlan</i> ] |
| Step 2 | Verify the bridge ID priority.         | <b>show spantree</b> [ <i>vlan</i> ] [ <b>active</b> ]                 |

This example shows how to set the PVST+ bridge ID when MAC address reduction is not enabled (default):

```

Console> (enable) set spantree priority 30000 1
Spantree 1 bridge priority set to 30000.
Console> (enable) show spantree 1
VLAN 1
Spanning tree mode PVST+
Spanning tree type ieee
Spanning tree enabled

Designated Root 00-60-70-4c-70-00
Designated Root Priority 16384
Designated Root Cost 19
Designated Root Port 2/3
Root Max Age 14 sec Hello Time 2 sec Forward Delay 10 sec

Bridge ID MAC ADDR 00-d0-00-4c-18-00
Bridge ID Priority 30000
Bridge Max Age 20 sec Hello Time 2 sec Forward Delay 15 sec

Port Vlan Port-State Cost Prio Portfast Channel_id

1/1 1 not-connected 4 32 disabled 0
1/2 1 not-connected 4 32 disabled 0
2/1 1 not-connected 100 32 disabled 0
2/2 1 not-connected 100 32 disabled 0

```

This example shows how to set the PVST+ the bridge ID priority when MAC reduction is enabled:

```

Console> (enable) set spantree priority 32768 1
Spantree 1 bridge ID priority set to 32769
(bridge priority: 32768 + sys ID extension: 1)
Console> (enable) show spantree 1/1 1
VLAN 1
Spanning tree mode PVST+
Spanning tree type ieee
Spanning tree enabled

Designated Root 00-60-70-4c-70-00
Designated Root Priority 16384
Designated Root Cost 19
Designated Root Port 2/3
Root Max Age 14 sec Hello Time 2 sec Forward Delay 10 sec

```



*CISCO Confidential - DRAFT*

```

Bridge ID MAC ADDR 00-d0-00-4c-18-00
Bridge ID Priority 32769 (bridge priority: 32768, sys ID ext: 1)
Bridge Max Age 20 sec Hello Time 2 sec Forward Delay 15 sec

```

| Port | Vlan | Port-State    | Cost | Prio | Portfast | Channel_id |
|------|------|---------------|------|------|----------|------------|
| 1/1  | 1    | not-connected | 4    | 32   | disabled | 0          |
| 1/2  | 1    | not-connected | 4    | 32   | disabled | 0          |
| 2/1  | 1    | not-connected | 100  | 32   | disabled | 0          |
| 2/2  | 1    | not-connected | 100  | 32   | disabled | 0          |

## Configuring the PVST+ Port Cost

You can configure the port cost of switch ports. Ports with lower port costs are more likely to be chosen to forward frames. Assign lower numbers to ports attached to faster media (such as full duplex), and higher numbers to ports attached to slower media. The possible range of *cost* is 1–65535. The default differs for different media. Path cost is typically  $1000 \div \text{LAN speed in megabits per second}$ .

To configure the port cost for a port, perform this task in privileged mode:

|        | Task                                       | Command                                      |
|--------|--------------------------------------------|----------------------------------------------|
| Step 1 | Configure the port cost for a switch port. | <b>set spantree portcost</b> {mod/port} cost |
| Step 2 | Verify the port cost setting.              | <b>show spantree</b> mod/port                |

This example shows how to configure the port VLAN priority on a port and verify the configuration:

```

Console> (enable) set spantree portcost 2/3 12
Span tree port 2/3 path cost set to 12.
Console> (enable) show spantree 2/3
VLAN 1
.
.

```

| Port | Vlan | Port-State    | Cost | Prio | Portfast | Channel_id |
|------|------|---------------|------|------|----------|------------|
| 1/1  | 1    | not-connected | 4    | 32   | disabled | 0          |
| 1/2  | 1    | not-connected | 4    | 32   | disabled | 0          |
| 2/1  | 1    | not-connected | 100  | 32   | disabled | 0          |
| 2/2  | 1    | not-connected | 100  | 32   | disabled | 0          |
| 2/3  | 1    | forwarding    | 12   | 32   | disabled | 0          |
| 2/4  | 1    | not-connected | 100  | 32   | disabled | 0          |

## Configuring PVST+ Port Priority

You can configure the port priority of switch ports in PVST+ mode. The port with the lowest priority value forwards frames for all VLANs. The possible port priority value is 0–63. The default is 32. If all ports have the same priority value, the port with the lowest port number forwards frames.

To configure the port priority for a port, perform this task in privileged mode:

|        | Task                                           | Command                                               |
|--------|------------------------------------------------|-------------------------------------------------------|
| Step 1 | Configure the port priority for a switch port. | <b>set spantree portpri</b> mod_num/port_num priority |
| Step 2 | Verify the port priority setting.              | <b>show spantree</b> mod/port                         |

*CISCO Confidential - DRAFT*

This example shows how to configure the port priority for a port:

```
Console> (enable) set spantree portpri 2/3 16
```

```
Bridge port 2/3 port priority set to 16.
```

```
Console> (enable) show spantree 2/3
```

```
VLAN 1
```

```
.
.
.
```

| Port | Vlan | Port-State    | Cost | Prio | Portfast | Channel_id |
|------|------|---------------|------|------|----------|------------|
| 1/1  | 1    | not-connected | 4    | 32   | disabled | 0          |
| 1/2  | 1    | not-connected | 4    | 32   | disabled | 0          |
| 2/1  | 1    | not-connected | 100  | 32   | disabled | 0          |
| 2/2  | 1    | not-connected | 100  | 32   | disabled | 0          |
| 2/3  | 1    | forwarding    | 19   | 16   | disabled | 0          |
| 2/4  | 1    | not-connected | 100  | 32   | disabled | 0          |

## Configuring the PVST+ Default Port Cost Mode

If any switch in your network is using a port speed of 10 Gb or over and the network is using PVST+ spanning tree mode, all switches in the network must have the same path cost defaults. You can enter the **set spantree defaultcostmode** command to force all VLANs associated with all the ports to have the same pathcost default set.

There are two default port cost modes available—short and long.

- The short mode has these parameters:
  - Portcost.
  - Portvlancost.
  - When you enable UplinkFast, the actual cost is incremented by 3000.
- The long mode has these parameters:
  - Portcost.
  - Portvlancost.
  - When you enable UplinkFast, the actual cost is incremented by 10,000,000.
  - EtherChannel computes the cost of a bundle using the formula,  $AVERAGE\_COST/NUM\_PORT$ .

The default port cost mode in PVST+ is short. For port speeds of 10 Gb and greater, you must set the default port cost mode to long.

To change the default port cost mode, perform this task in privileged mode:

| Task                                  | Command                                            |
|---------------------------------------|----------------------------------------------------|
| Configure the default port cost mode. | <b>set spantree defaultcostmode {short   long}</b> |

This example shows how to configure the default port cost mode:

```
Console> (enable) set spantree defaultcostmode long
```

```
Portcost and portvlancost set to use long format default values.
```

```
Console> (enable)
```

*CISCO Confidential - DRAFT*

## Configuring the PVST+ Port VLAN Cost

You can configure the port cost for a port on a per-VLAN basis. Ports with a lower port VLAN cost are more likely to be chosen to forward frames. You should assign lower numbers to ports attached to faster media (such as full duplex) and higher numbers to ports attached to slower media. The default cost differs for different media.

You can set a cost value from 1– 65535.

To configure the port VLAN cost for a port, perform this task in privileged mode:

| Task                                                      | Command                                                             |
|-----------------------------------------------------------|---------------------------------------------------------------------|
| Configure the port VLAN cost for a VLAN on a switch port. | <b>set spantree portvlancost</b> {mod/port} [cost cost] [vlan_list] |

This example shows how to configure the port VLAN cost on a port:

```
Console> (enable) set spantree portvlancost 2/3 cost 20000 1-5
Port 2/3 VLANs 6-11,13-1005,1025-4094 have path cost 12.
Port 2/3 VLANs 1-5,12 have path cost 20000.
This parameter applies to trunking ports only.
Console> (enable)
```

## Configuring the PVST+ Port VLAN Priority

When the switch is in PVST+ mode, you can set the port priority for a trunking port in a VLAN. The port with the lowest priority value for a specific VLAN forwards frames for that VLAN. The possible port VLAN priority range is 0–63. The default is 32. If all ports have the same priority value for a particular VLAN, the port with the lowest port number forwards frames for that VLAN.

The port VLAN priority value must be lower than the port priority value.

To configure the port VLAN priority for a port, perform this task in privileged mode:

|        | Task                                                          | Command                                                           |
|--------|---------------------------------------------------------------|-------------------------------------------------------------------|
| Step 1 | Configure the port VLAN priority for a VLAN on a switch port. | <b>set spantree portvlanpri</b> mod_num/port_num priority [vlans] |
| Step 2 | Verify the port VLAN priority.                                | <b>show config all</b>                                            |

This example shows how to configure the port VLAN priority on a port:

```
Console> (enable) set spantree portvlanpri 2/3 16 6
Port 2/3 vlans 6 using portpri 16.
Port 2/3 vlans 1-5,7-800,802-1004,1006-4094 using portpri 32.
Port 2/3 vlans 801,1005 using portpri 4.
This parameter applies to trunking ports only.
Console> (enable) show config all
.
.
.
set spantree portcost 2/12,2/15 19
set spantree portcost 2/1-2,2/4-11,2/13-14,2/16-48 100
set spantree portcost 2/3 12
set spantree portpri 2/1-48 32
```

*CISCO Confidential - DRAFT*

```

set spantree portvlanpri 2/1 0
set spantree portvlanpri 2/2 0
.
.
.
set spantree portvlanpri 2/48 0
set spantree portvlancost 2/1 cost 99
set spantree portvlancost 2/2 cost 99
set spantree portvlancost 2/3 cost 20000 1-5,12

```

## Disabling the PVST+ Mode on a VLAN

When the switch is in PVST+ mode, you can disable spanning tree on individual VLANs or all VLANs. When you disable spanning tree on a VLAN, the switch does not participate in spanning tree and any BPDUs received in that VLAN are flooded on all ports.



### 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 or bridges in a VLAN and leave it enabled on other switches or bridges in the VLAN. Doing so can have unexpected results because switches and bridges with spanning tree enabled will have incomplete information regarding the physical topology of the network.



### 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.

To disable PVST+ mode, perform this task in privileged mode:

| Task                          | Command                                 |
|-------------------------------|-----------------------------------------|
| Disable PVST+ mode on a VLAN. | <b>set spantree disable vlans [all]</b> |

This example shows how to disable PVST+ on a VLAN:

```

Console> (enable) set spantree disable 4
Spantree 4 disabled.
Console> (enable)

```

## Using Rapid PVST+

To configure Rapid PVST+, you need to also configure PVST+ on your switch. You can configure PVST+ either before or after you enable Rapid PVST+.

To configure Rapid PVST+, perform this task in privileged mode:

*CISCO Confidential - DRAFT*

|        | Task                                                                                                          | Command                                                            |
|--------|---------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|
| Step 1 | Enable Rapid PVST+.                                                                                           | <code>set spantree mode rapid-pvst+</code>                         |
| Step 2 | Set the link type to point-to-point mode for the port.                                                        | <code>set spantree link-type <i>mod/port</i> point-to-point</code> |
| Step 3 | If any port on the switch is connected to a port on a PVST+ switch, check for any legacy bridges on the port. | <code>clear spantree detected-protocols <i>mod/port</i></code>     |
| Step 4 | Verify the Rapid PVST+ configuration.                                                                         | <code>show spantree <i>vlan</i></code>                             |

This example shows how to configure Rapid PVST+:

```

Console> (enable) set spantree mode rapid-pvst+
Spanntree mode set to RAPID-PVST+.
Console> (enable) set spantree link-type 3/1 point-to-point
Link type set to point-to-point on port 3/1.
Console> (enable) clear spantree detected-protocols 3/1
Spanning tree protocol detection forced on port 3/1
Console> (enable)

```

This example show how to verify the Rapid PVST+ configuration for VLAN 1. Notice that the first line in the output displays the spanning tree mode:

```

Console> show spantree 1
Spanning tree mode RAPID-PVST+
Spanning tree type ieee
Spanning tree enabled.
.
.
.
Port State Role Cost Prio Type

6/1 forwarding ROOT 20000 16 Shared, PEER(STP)

Console>

```

This example shows how to verify the link type, edge port, and guard type for port 3/6

```

Console> show spantree 3/6
Port 3/6
Edge Port: No, (Configured) Default
Port Guard: Default
Link Type: P2P(Configured) Auto

```

| Port | VLAN | State     | Role | Cost  | Prio | Type |
|------|------|-----------|------|-------|------|------|
| 3/6  | 1    | listening | DESG | 20000 | 32   | P2P  |
| 3/6  | 2    | listening | DESG | 20000 | 32   | P2P  |
| 3/6  | 3    | listening | DESG | 20000 | 32   | P2P  |
| 3/6  | 4    | listening | DESG | 20000 | 32   | P2P  |
| 3/6  | 5    | listening | DESG | 20000 | 32   | P2P  |
| 3/6  | 6    | listening | DESG | 20000 | 32   | P2P  |
| 3/6  | 7    | listening | DESG | 20000 | 32   | P2P  |
| 3/6  | 8    | listening | DESG | 20000 | 32   | P2P  |
| 3/6  | 9    | listening | DESG | 20000 | 32   | P2P  |
| 3/6  | 10   | listening | DESG | 20000 | 32   | P2P  |
| 3/6  | 11   | listening | DESG | 20000 | 32   | P2P  |
| 3/6  | 12   | listening | DESG | 20000 | 32   | P2P  |

*CISCO Confidential - DRAFT*

```

3/6 13 listening DESG 20000 32 P2P
3/6 14 listening DESG 20000 32 P2P
3/6 15 listening DESG 20000 32 P2P
3/6 16 listening DESG 20000 32 P2P
3/6 17 listening DESG 20000 32 P2P
3/6 18 listening DESG 20000 32 P2P
3/6 19 listening DESG 20000 32 P2P

```

Console>

## Using MISTP-PVST+ or MISTP

The default spanning tree mode on Catalyst 4000 family switches is PVST+ mode. If you want to use MISTP mode in your network, we recommend you carefully follow the procedures described in the following sections in order to avoid loss of connectivity in your network.

When you change the spanning tree mode from one mode to another, the current mode stops, the information collected at run-time is used to build the port database for the new mode, and the new spanning tree mode restarts the computation of the active topology. Information about the port states is lost; however, all of the configuration parameters are preserved for the previous mode. If you return to the previous mode, the configuration will still be there.



### Note

We recommend that if you wish to use MISTP mode, you should configure *all* of your Catalyst 4000 family switches to run MISTP.

To use MISTP mode, you first enable an MISTP instance, and then map at least one VLAN to the instance. You must have at least one forwarding port in the VLAN in order for the MISTP instance to be active.

If you are changing a switch from PVST+ mode to MISTP mode and you have other switches in the network that are using PVST+, you must first enable MISTP-PVST+ mode on each switch on which you intend to use MISTP so that PVST+ BPDUs can flow through the switches while you configure them.

When all switches in the network are configured in MISTP-PVST+, you can then enable MISTP on all of the switches.

The following sections describe how to configure PVST+ on Ethernet VLANs.

## Default MISTP Mode Configuration

Table 7-3 shows the default configuration for MISTP and MISTP-PVST+ modes.

**Table 7-3 MISTP Mode Default Configuration**

| Feature               | Default Value                                                             |
|-----------------------|---------------------------------------------------------------------------|
| Enable state          | Disabled until a VLAN is mapped to an MISTP instance                      |
| MAC address reduction | Disabled                                                                  |
| Bridge priority       | 32,768                                                                    |
| Bridge ID priority    | 32,769 (bridge priority plus the system ID extension of MISTP instance 1) |
| Port priority         | 32 (global)                                                               |

*CISCO Confidential - DRAFT***Table 7-3 MISTP Mode Default Configuration (continued)**

| Feature                | Default Value                                                                                                                                  |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| Port cost              | <ul style="list-style-type: none"> <li>Gigabit Ethernet: 4</li> <li>Fast Ethernet: 10</li> <li>FDDI/CDDI: 10</li> <li>Ethernet: 100</li> </ul> |
| Default port cost mode | Short (802.1D)                                                                                                                                 |
| Port VLAN priority     | Same as port priority but configurable on a per-VLAN basis in PVST+                                                                            |
| Port VLAN cost         | Same as port cost but configurable on a per-VLAN basis in PVST+                                                                                |
| Maximum aging time     | 20 sec                                                                                                                                         |
| Hello time             | 2 sec                                                                                                                                          |
| Forward delay time     | 15 sec                                                                                                                                         |

## Setting the MISTP-PVST+ Mode or MISTP Mode

If you enable MISTP in a PVST+ network, you must be very careful to avoid bringing down the network. This section explains how to enable MISTP or MISTP-PVST+ on your network.



**Caution**

If you have more than 4500 VLAN ports that are configured on your switch, your network could crash if you change from MISTP to either PVST+ or MISTP-PVST+ mode. To avoid losing connectivity, reduce the number of configured VLAN ports on your switch to no more than 4500.



**Caution**

If you are working from a Telnet connection to your switch, the first time you enable MISTP-PVST+ or MISTP mode, you must do so from the switch console. Do not use a Telnet connection through the data port or you will lose the connection to the switch. Once you map a VLAN to an MISTP instance, you can Telnet to the switch.

To change from PVST+ to MISTP-PVST+ or MISTP, perform this task in privileged mode:

| Task                      | Command                                                |
|---------------------------|--------------------------------------------------------|
| Set a spanning tree mode. | <b>set spantree mode {mistp   pvst+   mistp-pvst+}</b> |

This example shows how to set a switch to MISTP-PVST+ mode:

```
Console> (enable) set spantree mode mistp-pvst+
PVST+ database cleaned up.
Spanntree mode set to MISTP-PVST+.
Warning!! There are no VLANs mapped to any MISTP instance.
Console> (enable)
```

You can display VLAN-to-MISTP instance mapping information propagated from the root switch at runtime. This display is available only in the MISTP or MISTP-PVST+ mode. When in the PVST+ mode, use the optional keyword **config**, to display the list of mappings configured on the local switch.

*CISCO Confidential - DRAFT***Note**

MAC addresses are not displayed when you specify the keyword **config**.

To display spanning tree mapping, perform this task in privileged mode:

|        | Task                             | Command                               |
|--------|----------------------------------|---------------------------------------|
| Step 1 | Set spanning tree mode to MISTP. | <b>set spantree mode mistp</b>        |
| Step 2 | Show spanning tree mapping.      | <b>show spantree mapping [config]</b> |

This example shows how to display the spanning tree VLAN instance mapping in MISTP mode:

```
Console> (enable) set spantree mode mistp
```

```
PVST+ database cleaned up.
```

```
Spantree mode set to MISTP.
```

```
Console> (enable) show spantree mapping
```

```
Inst Root Mac Vlans

1 00-50-3e-78-70-00 1
2 00-50-3e-78-70-00 -
3 00-50-3e-78-70-00 -
4 00-50-3e-78-70-00 -
5 00-50-3e-78-70-00 -
6 00-50-3e-78-70-00 -
7 00-50-3e-78-70-00 -
8 00-50-3e-78-70-00 -
9 00-50-3e-78-70-00 -
10 00-50-3e-78-70-00 -
11 00-50-3e-78-70-00 -
12 00-50-3e-78-70-00 -
13 00-50-3e-78-70-00 -
14 00-50-3e-78-70-00 -
15 00-50-3e-78-70-00 -
16 00-50-3e-78-70-00 -
```

## Configuring the MISTP Bridge ID Priority

You can set the bridge ID priority for an MISTP instance when the switch is in MISTP or MISTP-PVST+ mode.

The switch combines the bridge priority value with the system ID extension (the ID of the MISTP instance) to create the bridge ID priority. You can set 16 possible bridge priority values: 0, 4096, 8192, 12,288, 16,384, 20,480, 24,576, 28,672, 32,768, 36,864, 40,960, 45,056, 49,152, 53,248, 57,344, and 61,440.

To configure the bridge ID priority for an MISTP instance, perform this task in privileged mode:

|        | Task                                                    | Command                                                                                 |
|--------|---------------------------------------------------------|-----------------------------------------------------------------------------------------|
| Step 1 | Configure the bridge ID priority for an MISTP instance. | <b>set spantree priority <i>bridge_ID_priority</i> [mistp-instance <i>instance</i>]</b> |
| Step 2 | Verify the bridge ID priority.                          | <b>show spantree mistp-instance <i>instance</i> [mod/port] active</b>                   |

The example shows how to configure the bridge ID priority for an MISTP instance:



*CISCO Confidential - DRAFT*

```

Console> (enable) set spantree priority 8192 mistpinstance 1
Spantree 1 bridge ID priority set to 8193
(bridge priority: 8192 + sys ID extension: 1)
Console> (enable) show spantree mistp-instance 1
VLAN 1
Spanning tree mode MISTP
Spanning tree type ieee
Spanning tree enabled
VLAN mapped to MISTP Instance: 1

Bridge ID MAC ADDR 00-d0-00-4c-18-00
Bridge ID Priority 8193 (bridge priority: 8192, sys ID ext: 1)
Bridge Max Age 20 sec Hello Time 2 sec Forward Delay 15 sec

Port Vlan Port-State Cost Prio Portfast Channel_id

1/1 1 not-connected 20000 32 disabled 0
1/2 1 not-connected 20000 32 disabled 0
2/1 1 not-connected 2000000 32 disabled 0
2/2 1 not-connected 2000000 32 disabled 0
2/3 1 forwarding 200000 32 disabled 0

```

## Configuring the MISTP Port Cost

You can configure the port cost of switch ports. When forwarding frames, the switch is more likely to use ports with lower port costs. Assign lower numbers to ports attached to faster media (such as full duplex) and higher numbers to ports attached to slower media. The possible range is 1–65,535. The default differs for different media. Path cost is typically equal to  $1000 \div \text{LAN speed in megabits per second}$ .

To configure the port cost for a port, perform this task in privileged mode:

|        | Task                                       | Command                                                                                          |
|--------|--------------------------------------------|--------------------------------------------------------------------------------------------------|
| Step 1 | Configure the port cost for a switch port. | <b>set spantree portcost</b> <i>mod_num/port_num cost</i>                                        |
| Step 2 | Verify the port cost setting.              | <b>show spantree mistp-instance</b> <i>instance</i><br>[ <i>mod_num/port_num</i> ] <b>active</b> |

This example shows how to configure the port instance priority on an MISTP instance and verify the configuration:

```

Console> (enable) set spantree portcost 2/12 22222222
Spantree port 2/12 path cost set to 22222222.
Console> (enable) show spantree mistp-instance active
Instance 1
Spanning tree mode MISTP-PVST+
Spanning tree type ieee
Spanning tree instance enabled

Designated Root 00-d0-00-4c-18-00
Designated Root Priority 32769 (root priority: 32768, sys ID ext: 1)
Designated Root Cost 0
Designated Root Port none
VLANs mapped: 6
Root Max Age 20 sec Hello Time 2 sec Forward Delay 15 sec

Bridge ID MAC ADDR 00-d0-00-4c-18-00
Bridge ID Priority 32769 (bridge priority: 32768, sys ID ext: 1)
VLANs mapped: 6

```

*CISCO Confidential - DRAFT*

```

Bridge Max Age 20 sec Hello Time 2 sec Forward Delay 15 sec

Port Inst Port-State Cost Prio Portfast Channel_id

 2/12 1 forwarding 22222222 40 disabled 0
Console> (enable)

```

## Configuring the MISTP Port Priority

You can configure the port priority of switch ports. The port with the lowest priority value forwards frames for all VLANs. The possible port priority value is 0–63; the default is 32. If all ports have the same priority value, the port with the lowest port number forwards frames.

To configure the port priority for a port, perform this task in privileged mode:

|        | Task                                           | Command                                                                                       |
|--------|------------------------------------------------|-----------------------------------------------------------------------------------------------|
| Step 1 | Configure the port priority for a switch port. | <b>set spantree portpri</b> <i>mod_num/port_num priority</i> [ <i>instance</i> ]              |
| Step 2 | Verify the port priority setting.              | <b>show spantree mistp-instance</b> <i>instance</i> [ <i>mod_num/port_num</i> ] <b>active</b> |

This example shows how to configure the port priority and verify the configuration:

```

Console> (enable) set spantree portpri 2/12 40
Bridge port 2/12 port priority set to 40.
Console> (enable) show spantree mistp-instance 1
Instance 1
Spanning tree mode MISTP-PVST+
Spanning tree type ieee
Spanning tree instance enabled

Designated Root 00-d0-00-4c-18-00
Designated Root Priority 32769 (root priority: 32768, sys ID ext: 1)
Designated Root Cost 0
Designated Root Port none
VLANs mapped: 6
Root Max Age 20 sec Hello Time 2 sec Forward Delay 15 sec

Bridge ID MAC ADDR 00-d0-00-4c-18-00
Bridge ID Priority 32769 (bridge priority: 32768, sys ID ext: 1)
VLANs mapped: 6
Bridge Max Age 20 sec Hello Time 2 sec Forward Delay 15 sec

Port Inst Port-State Cost Prio Portfast Channel_id

 2/12 1 forwarding 22222222 40 disabled 0
Console> (enable)

```

## Configuring the MISTP Port Instance Cost

You can configure the port instance cost for an instance of MISTP or MISTP-PVST+. Ports with a lower instance cost are more likely to be chosen to forward frames. You should assign lower numbers to ports that are attached to faster media (such as full duplex) and higher numbers to ports that are attached to slower media. The default cost differs for different media. The possible value for port instance cost is 1–268435456.

To configure the port instance cost for a port, perform this task in privileged mode:

*CISCO Confidential - DRAFT*

| Task                                               | Command                                                                                                   |
|----------------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| Configure the port instance cost on a switch port. | <b>set spantree portinstancecost</b> { <i>mod/port</i> } [ <b>cost</b> <i>cost</i> ] [ <i>instances</i> ] |

This example shows how to configure the port instance priority on a port:

```
Console> (enable) set spantree portinstancecost 2/12 cost 110110 2
Port 2/12 instances 1,3-16 have path cost 22222222.
Port 2/12 instances 2 have path cost 110110.
Console> (enable)
```

## Configuring the MISTP Port Instance Priority

You can set the port priority for an instance of MISTP. The port with the lowest priority value for a specific MISTP instance forwards frames for that instance. The possible port instance range is from 0–63. If all ports have the same priority value for an MISTP instance, the port with the lowest port number forwards frames for that instance.

To configure the port instance priority on an MISTP instance, perform this task in privileged mode:

| Task                                                       | Command                                                                                      |
|------------------------------------------------------------|----------------------------------------------------------------------------------------------|
| Configure the port instance priority on an MISTP instance. | <b>set spantree portinstancepri</b> { <i>mod/port</i> } <i>priority</i> [ <i>instances</i> ] |

This example shows how to configure the port instance priority on a port and verify the configuration:

```
Console> (enable) set spantree portinstancepri 2/12 10 2
Port 2/12 instances 2 using portpri 10.
Port 2/12 mistp-instance 1,3-16 using portpri 40.
Console> (enable)
```

## Enabling an MISTP Instance

You can enable up to 16 MISTP instances. Each MISTP instance defines a unique spanning tree topology. MISTP instance 1, the default instance, is enabled by default; however, you must map a VLAN to it in order for it to be active. You can enable a single MISTP instance, a range of instances, or all instances at once using the **all** keyword.



### Note

The software does not display the status of an MISTP instance until it has a VLAN with an active port mapped to it.

To enable an MISTP instance, perform this task in privileged mode:

|        | Task                                 | Command                                                                                   |
|--------|--------------------------------------|-------------------------------------------------------------------------------------------|
| Step 1 | Enable an MISTP instance.            | <b>set spantree enable mistp-instance</b> <i>instance</i> [ <b>all</b> ]                  |
| Step 2 | Verify that the instance is enabled. | <b>show spantree mistp-instance</b> [ <i>instance</i> ] [ <b>active</b> ] <i>mod/port</i> |

*CISCO Confidential - DRAFT***Note**

Enter the **active** keyword to display active ports only.

This example shows how to enable an MISTP instance:

```
Console> (enable) set spantree enable mistp-instance 2
Spantree 2 enabled.
```

```
Console> (enable) show spantree mistp-instance 2
Instance 2
Spanning tree mode MISTP
Spanning tree type ieee
Spanning tree instance enabled
.
.
.
```

## Mapping VLANs to an MISTP Instance

When you are using MISTP-PVST+ or MISTP on a switch, you must map at least one VLAN to an MISTP instance in order for MISTP-PVST+ or MISTP to be active.

**Note**

See [Chapter 10, “Configuring VLANs”](#) for details on using and configuring VLANs.

- You can only map Ethernet VLANs to MISTP instances.
- At least one VLAN in the instance must have an active port in order for MISTP-PVST+ or MISTP to be active.
- You can map as many Ethernet VLANs as you wish to an MISTP instance.
- You cannot map a VLAN to more than one MISTP instance.

To map a VLAN to an MISTP instance, perform this task in privileged mode:

|        | Task                             | Command                                                                     |
|--------|----------------------------------|-----------------------------------------------------------------------------|
| Step 1 | Map a VLAN to an MISTP instance. | <b>set vlan <i>vlan</i> mistp-instance <i>instance</i></b>                  |
| Step 2 | Verify that the VLAN is mapped.  | <b>show spantree mistp-instance [<i>instance</i>] [active]<br/>mod/port</b> |

This example shows how to map a VLAN to an MISTP instance 1 and verify the mapping:

```
Console> (enable) set vlan 6 mistp-instance 1
Vlan 6 configuration successful
Console> (enable) show spantree mist-instance 1
Instance 1
Spanning tree mode MISTP-PVST+
Spanning tree type ieee
Spanning tree instance enabled

Designated Root 00-d0-00-4c-18-00
Designated Root Priority 49153 (root priority: 49152, sys ID ext: 1)
Designated Root Cost 0
Designated Root Port none
VLANs mapped: 6
Root Max Age 20 sec Hello Time 2 sec Forward Delay 15 sec
```

*CISCO Confidential - DRAFT*

```

Bridge ID MAC ADDR 00-d0-00-4c-18-00
Bridge ID Priority 49153 (bridge priority: 49152, sys ID ext: 1)
VLANs mapped: 6
Bridge Max Age 20 sec Hello Time 2 sec Forward Delay 15 sec

Port Inst Port-State Cost Prio Portfast Channel_id

2/12 1 forwarding 22222222 40 disabled 0

```

## Determining an MISTP Instance—VLAN Mapping Conflicts

A VLAN can only be mapped to one MISTP instance. If you attempt to map a VLAN to more than one instance, all of its ports are set to blocking mode. You can use the **show spantree conflicts** command to determine to which MISTP instances you have attempted to map the VLAN.

This command prints a list of the MISTP instances associated with the VLAN, the MAC addresses of the root switches that are sending the BPDUs containing the VLAN mapping information, and the timers associated with the mapping of a VLAN to an MISTP instance. When only one entry is printed or when all the entries are associated to the same instance, the VLAN is mapped to that instance. If two or more entries in the list are associated with different MISTP instances, the VLAN is in conflict.

To clear up the conflict, you must manually remove the incorrect mapping(s) from the root switch. The remaining entry on the list becomes the official mapping.

To determine VLAN mapping conflicts, perform this task in privileged mode:

| Task                              | Command                             |
|-----------------------------------|-------------------------------------|
| Determine VLAN mapping conflicts. | <b>show spantree conflicts vlan</b> |

This example shows that there is an attempt to map VLAN 2 to MISTP instance 1 and to MISTP instance 3 on two different switches as seen from a third switch in the topology:

```

Console> (enable) show spantree conflicts 2
Inst MAC Delay Time left

1 00-30-a3-4a-0c-00 inactive 20
3 00-30-f1-e5-00-01 inactive 10

```

The Delay timer shows the time in seconds remaining before the VLAN will join the instance. The field displays *inactive* if the VLAN is already mapped to an instance (the timer has expired), or the VLAN is in conflict between instances.

The Time Left timer shows the time in seconds left before the entry will expire and be removed from the table. The timer is restarted every time an incoming BPDU confirms the mapping. Entries pertaining to the root switch show *inactive* on the root switch itself.

## Unmapping VLANs from an MISTP Instance

The keyword **none** is used to unmap the specified VLANs from the MISTP instances to which they are currently mapped. When you unmap a VLAN from an MISTP instance, the resulting state of all the ports of the VLAN (if the VLAN exists) is *blocking*.

To unmap a VLAN or all VLANs from an MISTP instance, perform this task in privileged mode:

*CISCO Confidential - DRAFT*

| Task                                 | Command                                         |
|--------------------------------------|-------------------------------------------------|
| Unmap a VLAN from an MISTP instance. | <b>set vlan <i>vlan</i> mistp-instance none</b> |

This example shows how to unmap a VLAN from an MISTP instance:

```
Console> (enable) set vlan 6 mistp none
Vlan 6 configuration successful
```

## Disabling MISTP-PVST+ or MISTP

When the switch is in MISTP mode, you disable spanning tree on an instance, not for the whole switch.

When you disable spanning tree on an MISTP instance, the instance still exists on the switch, all of the VLANs mapped to it have all of their ports forwarding, and the instance BPDUs are flooded.

To disable an MISTP instance, perform this task in privileged mode:

| Task                       | Command                                                          |
|----------------------------|------------------------------------------------------------------|
| Disable an MISTP instance. | <b>set spantree disable mistp-instance <i>instance</i> [all]</b> |

This example shows how to disable an MISTP instance:

```
Console> (enable) set spantree disable mistp-instance 2
MI-STP instance 2 disabled.
```

## Configuring a Root Switch

This section explains how to configure a primary root switch and a secondary root switch, and how to prevent a switch from becoming a root switch using the root guard feature.

### Configuring a Primary Root Switch

You can set a root switch on a VLAN when the switch is in PVST+ mode or on an MISTP instance when the switch is in MISTP mode. Enter the **set spantree root** command to lower the bridge priority (the value associated with the switch) below the default (32,768); the switch can then become the root switch.

When you specify a switch as the primary root, the default bridge priority is modified so that it becomes the root for the specified VLANs. Set the bridge priority to 8192. If this setting does not result in the switch becoming a root, modify the bridge priority to be 1 less or the same as the bridge priority of the current root switch. Because different VLANs could potentially have different root switches, the bridge VLAN-priority chosen makes this switch the root for all the VLANs specified. If reducing the bridge priority as low as 1 still does not make the switch the root switch, the system displays a message.



#### Caution

Enter the **set spantree root** command on backbone switches or distribution switches only, not on access switches.

To configure a switch as the primary root switch, perform this task in privileged mode:

*CISCO Confidential - DRAFT*

| Task                                           | Command                                                                                    |
|------------------------------------------------|--------------------------------------------------------------------------------------------|
| Configure a switch as the primary root switch. | <b>set spantree root</b> [vlans] [ <b>dia</b> network_diameter] [ <b>hello</b> hello_time] |

This example shows how to configure the primary root switch for VLANs 1–10:

```
Console> (enable) set spantree root 1-10 dia 4
VLANs 1-10 bridge priority set to 8192
VLANs 1-10 bridge max aging time set to 14 seconds.
VLANs 1-10 bridge hello time set to 2 seconds.
VLANs 1-10 bridge forward delay set to 9 seconds.
Switch is now the root switch for active VLANs 1-6.
Console> (enable)
```

To configure a switch as the primary root switch for an instance, perform this task in privileged mode:

| Task                                                           | Command                                                                                                    |
|----------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
| Configure a switch as the primary root switch for an instance. | <b>set spantree root mistp-instance</b> instance [ <b>dia</b> network_diameter] [ <b>hello</b> hello_time] |

This example shows how to configure the primary root for an instance:

```
Console> (enable) set spantree root mistp-instance 2-4 dia 4
Instances 2-4 bridge priority set to 8192
VInstances 2-4 bridge max aging time set to 14 seconds.
Instances 2-4 bridge hello time set to 2 seconds.
Instances 2-4 bridge forward delay set to 9 seconds.
Switch is now the root switch for active Instances 1-6.
Console> (enable)
```

## Configuring a Secondary Root Switch

You can set a secondary root switch on a VLAN when the switch is in PVST+ mode or on an MISTP instance when the switch is in MISTP mode.

The **set spantree root secondary** command reduces the bridge priority to 16,384, making it the probable candidate to become the root switch if the primary root switch fails. You can run this command on more than one switch to create multiple backup switches in case the primary root switch fails.

To configure a switch as the secondary root switch, perform this task in privileged mode:

| Task                                             | Command                                                                                              |
|--------------------------------------------------|------------------------------------------------------------------------------------------------------|
| Configure a switch as the secondary root switch. | <b>set spantree root [secondary]</b> vlans [ <b>dia</b> network_diameter] [ <b>hello</b> hello_time] |

This example shows how to configure the secondary root switch for VLANs 22 and 24:

```
Console> (enable) set spantree root secondary 22,24 dia 5 hello 1
VLANs 22,24 bridge priority set to 16384.
VLANs 22,24 bridge max aging time set to 10 seconds.
VLANs 22,24 bridge hello time set to 1 second.
VLANs 22,24 bridge forward delay set to 7 seconds.
```

*CISCO Confidential - DRAFT*

Console> (enable)

To configure a switch as the secondary root switch for an instance, perform this task in privileged mode:

| Task                                                             | Command                                                                                                |
|------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|
| Configure a switch as the secondary root switch for an instance. | <b>set spantree root [secondary] mistp-instance instance [dia network_diameter] [hello hello_time]</b> |

This example shows how to set the secondary root for an instance:

```
Console> (enable) set spantree root secondary mistp-instance 2-4 dia 4
Instances 2-4 bridge priority set to 8192
VlInstances 2-4 bridge max aging time set to 14 seconds.
Instances 2-4 bridge hello time set to 2 seconds.
Instances 2-4 bridge forward delay set to 9 seconds.
Switch is now the root switch for active Instances 1-6.
Console> (enable)
```

## Configuring a Root Switch to Improve Convergence

You can configure the root switch to speed up STP convergence time. To do so, you must reduce the value of the Hello Time, Forward Delay Timer, and Maximum Age Timer parameters. For information on configuring these timers, see the [“Configuring Spanning Tree Timers” section on page 7-40](#).

**Note**

Reduction of the value of the timer parameters is possible only if all of the links are LAN links of 10 Mbps or faster. In this case, the network diameter can reach the maximum value of 7. With WAN connections, it is not possible to reduce the parameters.

When a link failure occurs in a bridged network, network reconfiguration is not immediate. Reconfiguration requires a time of 50 seconds, with the default parameters (specified by IEEE 802.1D) for the Hello Time, Forward Delay Timer, and Maximum Age Timer. The reconfiguration delay depends on the network diameter, which is the maximum number of bridges between any two points of attachment of end stations.

To speed up convergence, we use nondefault parameters values permitted by the IEEE 802.1D standard. Nondefault parameters set for a reconvergence of 14 seconds are as follows:

| Parameter              | Time   |
|------------------------|--------|
| Network Diameter (dia) | 2 hops |
| Hello Time             | 2 sec  |
| Forward Delay Timer    | 4 sec  |
| Maximum Age Timer      | 6 sec  |

You can set these parameters on the Catalyst 4000 family switches without modifying the switches.



*CISCO Confidential - DRAFT***Note**

You can set switch ports for improved convergence in PortFast mode. This setting affects only the transition from disable (link down) to enable (link up), moving the port immediately to the forwarding state. If a port in PortFast mode begins blocking, then it goes through listening and learning before reaching the forwarding state.

To configure the spanning tree bridge to improve convergence, perform this task in privileged mode:

|        | Task                                                           | Command                                                               |
|--------|----------------------------------------------------------------|-----------------------------------------------------------------------|
| Step 1 | Configure the Hello time for a VLAN or MISTP instance.         | <b>set spantree hello interval [vlan] mistp-instance [instances]</b>  |
| Step 2 | Verify the configuration.                                      | <b>show spantree [vlan   mistp-instance instances]</b>                |
| Step 3 | Configure the forward delay time for a VLAN or MISTP instance. | <b>set spantree fwddelay delay [vlan] mistp-instance [instances]</b>  |
| Step 4 | Verify the configuration.                                      | <b>show spantree [mod/port] mistp-instance [instances] [active]</b>   |
| Step 5 | Configure the maximum aging time for a VLAN or MISTP instance. | <b>set spantree maxage agingtime [vlans] mistp-instance instances</b> |
| Step 6 | Verify the configuration.                                      | <b>show spantree [mod/port] mistp-instance [instances] [active]</b>   |

This example shows how to configure the spanning tree Hello Time, Forward Delay Timer, and Maximum Age Timer to 2, 4, and 6 seconds, respectively:

```

Console> (enable) set spantree hello 2 100
Spanntree 100 hello time set to 7 seconds.
Console> (enable)
Console> (enable) set spantree fwddelay 4 100
Spanntree 100 forward delay set to 21 seconds.
Console> (enable)
Console> (enable) set spantree maxage 6 100
Spanntree 100 max aging time set to 36 seconds.
Console> (enable)
Console> (enable) set spantree root 1-10 dia 4
VLANs 1-10 bridge priority set to 8192
VLANs 1-10 bridge max aging time set to 14 seconds.
VLANs 1-10 bridge hello time set to 2 seconds.
VLANs 1-10 bridge forward delay set to 9 seconds.
Switch is now the root switch for active VLANs 1-6.
Console> (enable)

```

## Using Root Guard—Preventing Switches from Becoming Root

You may want to prevent switches from becoming the root switch. The root guard feature forces a port to become a designated port so that no switch on the other end of the link can become a root switch.

When you enable root guard on a per-port basis, it is automatically applied to all of the active VLANs to which that port belongs. When you disable root guard, it is disabled for the specified port(s). If a port goes into the root-inconsistent state, it automatically goes into the listening state.

To prevent switches from becoming root, perform this task in privileged mode:

*CISCO Confidential - DRAFT*

|        | Task                               | Command                                                                           |
|--------|------------------------------------|-----------------------------------------------------------------------------------|
| Step 1 | Enable root guard on a port.       | <b>set spantree guard {root   none} mod/port</b>                                  |
| Step 2 | Verify that root guard is enabled. | <b>show spantree guard {mod/port   vlan} {mistp-instance instance   mod/port}</b> |

## Configuring Spanning Tree Timers

Spanning tree timers affect the spanning tree performance. You can configure the spanning tree timers for a VLAN in PVST+ or an MISTP instance in MISTP mode. If you do not specify a VLAN when the switch is in PVST+ mode, VLAN 1 is assumed. If you do not specify an MISTP instance when the switch is in MISTP mode, MISTP instance 1 is assumed.



### Caution

Exercise care using these commands. For most situations, we recommend that you use the **set spantree root** and **set spantree root secondary** commands to modify the spanning tree performance parameters.

Table 7-4 describes the switch variables that affect spanning tree performance.

**Table 7-4 Switch Variable Descriptions**

| Variable            | Description                                                                                                                                                                                                                                                                        | Default |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
| Hello Time          | Determines how often the switch broadcasts its Hello message to other switches.                                                                                                                                                                                                    | 20 sec  |
| Maximum Age Timer   | Measures the age of the received protocol information recorded for a port and ensures that this information is discarded when its age limit exceeds the value of the maximum age parameter recorded by the switch. The timeout value is the maximum age parameter of the switches. | 2 sec   |
| Forward Delay Timer | Monitors the time spent by a port in learning and listening states. The timeout value is the forward delay parameter of the switches.                                                                                                                                              | 15 sec  |

## Configuring the Hello Time

Enter the **set spantree hello** command to change the Hello time for a VLAN or for an MISTP instance. The possible range for *interval* is 1–10 seconds.

To configure the spanning tree bridge Hello time for a VLAN or an MISTP instance, perform this task in privileged mode:

|        | Task                                                   | Command                                                              |
|--------|--------------------------------------------------------|----------------------------------------------------------------------|
| Step 1 | Configure the Hello time for a VLAN or MISTP instance. | <b>set spantree hello interval [vlan] mistp-instance [instances]</b> |
| Step 2 | Verify the configuration.                              | <b>show spantree [vlan   mistp-instance instances]</b>               |

This example shows how to configure the spanning tree Hello time for VLAN 100 to 7 seconds:

*CISCO Confidential - DRAFT*

```

Console> (enable) set spantree hello 7 100
Spantree 100 hello time set to 7 seconds.
Console> (enable)

```

This example shows how to set the spantree Hello time for an instance to 3 seconds:

```

Console> (enable) set spantree hello 3 mistp-instance 1
Spantree 1 hello time set to 3 seconds.
Console> (enable)

```

## Configuring the Forward Delay Time

Enter the **set spantree fwddelay** command to configure the spanning tree forward delay time for a VLAN. The possible range for *delay* is 4–30 seconds.

To configure the spanning tree forward delay time for a VLAN, perform this task in privileged mode:

|        | Task                                                           | Command                                                                                                 |
|--------|----------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| Step 1 | Configure the forward delay time for a VLAN or MISTP instance. | <b>set spantree fwddelay</b> <i>delay</i> [ <i>vlan</i> ]<br><b>mistp-instance</b> [ <i>instances</i> ] |
| Step 2 | Verify the configuration.                                      | <b>show spantree</b> [ <i>mod/port</i> ] <b>mistp-instance</b> [ <i>instances</i> ] [ <b>active</b> ]   |

This example shows how to configure the spanning tree forward delay time for VLAN 100 to 21 seconds:

```

Console> (enable) set spantree fwddelay 21 100
Spantree 100 forward delay set to 21 seconds.
Console> (enable)

```

This example shows how to set the bridge forward delay for an instance to 16 seconds:

```

Console> (enable) set spantree fwddelay 16 mistp-instance 1
Instance 1 forward delay set to 16 seconds.
Console> (enable)

```

## Configuring the Maximum Aging Time

Enter the **set spantree maxage** command to change the spanning tree maximum aging time for a VLAN or an instance. The possible range for *agingtime* is 6–40 seconds.

To configure the spanning tree maximum aging time for a VLAN or an instance, perform this task in privileged mode:

|        | Task                                                           | Command                                                                                                 |
|--------|----------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| Step 1 | Configure the maximum aging time for a VLAN or MISTP instance. | <b>set spantree maxage</b> <i>agingtime</i> [ <i>vlangs</i> ]<br><b>mistp-instance</b> <i>instances</i> |
| Step 2 | Verify the configuration.                                      | <b>show spantree</b> [ <i>mod/port</i> ] <b>mistp-instance</b> [ <i>instances</i> ] [ <b>active</b> ]   |

This example shows how to configure the spanning tree maximum aging time for VLAN 100 to 36 seconds:

```

Console> (enable) set spantree maxage 36 100

```

*CISCO Confidential - DRAFT*

Spantree 100 max aging time set to 36 seconds.  
 Console> (enable)

This example shows how to set the maximum aging time for an instance to 25 seconds:

Console> (enable) **set spantree maxage 25 mistp-instance 1**  
 Instance 1 max aging time set to 25 seconds.  
 Console> (enable)

## Configuring MST

The following sections describe how to configure MST:

### Enabling MST

To enable and configure MST on the switch, perform this task in privileged mode:

|         | Task                                           | Command                                                                                          |
|---------|------------------------------------------------|--------------------------------------------------------------------------------------------------|
| Step 1  | Begin in PVST+ mode.                           | <b>set spantree mode mst [mistp   pvst+   mistp-pvst+   mst]</b>                                 |
| Step 2  | Display the STP ports.                         | <b>show spantree active</b>                                                                      |
| Step 3  | Configure the MST region.                      | <b>set spantree mst config {[name name]   [revision number]<br/>[commit   rollback   force]}</b> |
| Step 4  | Verify your configuration.                     | <b>show spantree mst config</b>                                                                  |
| Step 5  | Map VLANs to the MST instance.                 | <b>set spantree mst instance vlan vlan</b>                                                       |
| Step 6  | Commit the new region mapping.                 | <b>set spantree mst config commit</b>                                                            |
| Step 7  | Enable MST.                                    | <b>set spantree mode mst [mistp   pvst+   mistp-pvst+   mst]</b>                                 |
| Step 8  | Verify your MST configuration.                 | <b>show spantree mst config</b>                                                                  |
| Step 9  | Verify your MST instance configuration.        | <b>show spantree mst instance</b>                                                                |
| Step 10 | Verify your MST module and port configuration. | <b>show spantree mst mod/port</b>                                                                |

These examples show how to enable MST:

```

Console> (enable)
Console> (enable) set spantree mode pvst
Spantree mode set to PVST+.
Console> (enable) show spantree active
VLAN 1
Spanning tree mode PVST+
Spanning tree type ieee
Spanning tree enabled

Designated Root 00-50-3e-66-d0-00
Designated Root Priority 24576
Designated Root Cost 104
Designated Root Port 6/1
Root Max Age 20 sec Hello Time 2 sec Forward Delay 15 sec

Bridge ID MAC ADDR 00-10-7b-bb-2f-00
Bridge ID Priority 32768

```

*CISCO Confidential - DRAFT*

```

Bridge Max Age 20 sec Hello Time 2 sec Forward Delay 15 sec

Port Vlan Port-State Cost Prio Portfast
Channel_id

6/1 1 forwarding 4 32 disabled 0
6/2 1 blocking 4 32 disabled 0
Console> (enable)
Console> (enable) set spantree mst config name cisco revision 1
Edit Buffer modified. Use 'set spantree mst config commit' to apply the
changes.
Console> (enable) show spantree mst config
Current (NVRAM) MST Region Configuration:
Configuration Name: Revision:0
Instance VLANs

IST 1-4094
1 -
2 -
3 -
4 -
5 -
6 -
7 -
8 -
9 -
10 -
11 -
12 -
13 -
14 -
15 -
=====
NEW MST Region Configuration (Not committed yet)
Configuration Name:cisco Revision:1
Instance VLANs

IST 1-4094
1 -
2 -
3 -
4 -
5 -
6 -
7 -
8 -
9 -
10 -
11 -
12 -
13 -
14 -
15 -
=====
Edit buffer is locked by:Console (pid 142)
Console> (enable)
Console> (enable) set spantree mst 1 vlan 2-10
Edit Buffer modified. Use 'set spantree mst config commit' to apply the
changes.
Console> (enable) set spantree mst 1 vlan 2-20
Edit Buffer modified. Use 'set spantree mst config commit' to apply the
changes.
Console> (enable) set spantree mst 2 vlan 21-30

```

*CISCO Confidential - DRAFT*

Edit Buffer modified. Use 'set spantree mst config commit' to apply the changes.

Console> (enable) **set spantree mst 3 vlan 31-40**

Edit Buffer modified. Use 'set spantree mst config commit' to apply the changes.

Console> (enable) **set spantree mst 4 vlan 41-50**

Edit Buffer modified. Use 'set spantree mst config commit' to apply the changes.

Console> (enable)

Console> (enable) **show spantree mst config**

Current (NVRAM) MST Region Configuration:

Configuration Name:

Revision:0

Instance VLANs

-----

IST 1-4094

1 -  
2 -  
3 -  
4 -  
5 -  
6 -  
7 -  
8 -  
9 -  
10 -  
11 -  
12 -  
13 -  
14 -  
15 -

=====

NEW MST Region Configuration (Not committed yet)

Configuration Name:cisco

Revision:1

Instance VLANs

-----

IST 1,51-4094

1 2-20  
2 21-30  
3 31-40  
4 41-50  
5 -  
6 -  
7 -  
8 -  
9 -  
10 -  
11 -  
12 -  
13 -  
14 -  
15 -

=====

Edit buffer is locked by:Console (pid 142)

Console> (enable)

Console> (enable) **set spantree mst config commit**

Console> (enable)

Console> (enable) **show spantree mst config**

Current (NVRAM) MST Region Configuration:

Configuration Name:cisco

Revision:1

Instance VLANs

-----

IST 1,51-4094

1 2-20  
2 21-30

*CISCO Confidential - DRAFT*

```

3 31-40
4 41-50
5 -
6 -
7 -
8 -
9 -
10 -
11 -
12 -
13 -
14 -
15 -

```

```

=====
Console> (enable)
Console> (enable) set spantree mode mst
PVST+ database cleaned up.
Spantree mode set to MST.
Console> (enable)
Console> (enable)
Console> (enable) show spantree mst 0
Spanning tree mode MST
Instance 0
VLANs Mapped: 1,51-4094

Designated Root 00-50-3e-66-d0-00
Designated Root Priority 24576 (root priority:24576, sys ID ext:0)

Designated Root Cost 20100
Designated Root Port 6/1
Root Max Age 20 sec Hello Time 2 sec Forward Delay 15 sec

IST Master ID MAC ADDR 00-10-7b-bb-2f-00
IST Master ID Priority 32768
IST Master Path Cost 0 Remaining Hops 20

Bridge ID MAC ADDR 00-10-7b-bb-2f-00
Bridge ID Priority 32768 (bridge priority:32768, sys ID ext:
0)
Bridge Max Age 20 sec Hello Time 2 sec Forward Delay 15 sec Max
Hops 20

Port State Role Cost Prio Type

6/1 forwarding ROOT 20000 32 P2P,
Boundary(PVST)
6/2 blocking ALTR 20000 32 P2P,
Boundary(PVST)
Console> (enable) show spantree mst 1
Spanning tree mode MST
Instance 1
VLANs Mapped: 2-20

Designated Root 00-10-7b-bb-2f-00
Designated Root Priority 32769 (root priority:32768, sys ID ext:1)

Designated Root Cost 0 Remaining Hops 20
Designated Root Port 1/0

Bridge ID MAC ADDR 00-10-7b-bb-2f-00
Bridge ID Priority 32769 (bridge priority:32768, sys ID ext:
1)

```

*CISCO Confidential - DRAFT*

```

Port State Role Cost Prio Type

6/1 forwarding BDRY 20000 32 P2P,
Boundary(PVST)
6/2 blocking BDRY 20000 32 P2P,
Boundary(PVST)
Console> (enable)
Console> (enable)
Console> (enable) show spantree mst 6/1
Edge Port: No, (Configured) Default
Link Type: P2P, (Configured) Auto
Port Guard: Default
Boundary: Yes (PVST)

Inst State Role Cost Prio VLANs

0 forwarding ROOT 20000 32 1
1 forwarding BDRY 20000 32 2-20
2 forwarding BDRY 20000 32 21-30
3 forwarding BDRY 20000 32 31-40
4 forwarding BDRY 20000 32 41-50
Console> (enable)
Console> (enable)
Console> (enable) show spantree mst config
Current (NVRAM) MST Region Configuration:
Configuration Name:cisco Revision:1
Instance VLANs

IST 1, 51-4094
1 2-20
2 21-30
3 31-40
4 41-50
5 -
6 -
7 -
8 -
9 -
10 -
11 -
12 -
13 -
14 -
15 -
=====
Console> (enable)

```

## Configuring the MST Bridge ID Priority

You can set the bridge ID priority for an MST instance when the switch is in MST mode. The switch combines the bridge priority value with the system ID extension (the ID of the MST instance) to create the bridge ID priority. You can set 16 possible bridge priority values: 0, 4096, 8192, 12,288, 16,384, 20,480, 24,576, 28,672, 32,768, 36,864, 40,960, 45,056, 49,152, 53,248, 57,344, and 61,440.

To configure the bridge ID priority for an MST instance, perform this task in privileged mode:



*CISCO Confidential - DRAFT*

|        | Task                                                  | Command                                                                            |
|--------|-------------------------------------------------------|------------------------------------------------------------------------------------|
| Step 1 | Configure the bridge ID priority for an MST instance. | <b>set spantree priority</b> <i>bridge_priority</i> <b>mst</b> [ <i>instance</i> ] |
| Step 2 | Verify the bridge ID priority.                        | <b>show spantree mst</b> [ <i>instance</i>   <i>mod/port</i> ]                     |

The example shows how to configure the bridge ID priority for an MST instance:

```

Console> (enable) set spantree priority 8192 mst 3
MST Spantree 3 bridge priority set to 8192.
Console> (enable)
Console> (enable) show spantree mst 3
Spanning tree mode MST
Instance 3
VLANs Mapped: 31-40

Designated Root 00-10-7b-bb-2f-00
Designated Root Priority 8195 (root priority:8192, sys ID ext:3)
Designated Root Cost 0 Remaining Hops 20
Designated Root Port 1/0

Bridge ID MAC ADDR 00-10-7b-bb-2f-00
Bridge ID Priority 8195 (bridge priority:8192, sys ID ext:3)

Port State Role Cost Prio Type

6/1 forwarding BDRY 20000 32 P2P,
Boundary(PVST)
6/2 blocking BDRY 20000 32 P2P,
Boundary(PVST)

```

## Configuring the MST Port Cost

You can configure the port cost of switch ports. The switch uses ports with lower port costs to forward frames. Assign lower numbers to ports attached to faster media (such as full duplex) and higher numbers to ports attached to slower media. The possible range is 1–65,535. The default differs for different media. The path cost is typically  $1000 \div \text{LAN speed in megabits per second}$ .

To configure the port cost for a port, perform this task in privileged mode:

|        | Task                                           | Command                                                                 |
|--------|------------------------------------------------|-------------------------------------------------------------------------|
| Step 1 | Configure the MST port cost for a switch port. | <b>set spantree portcost</b> <i>mod/port</i> <i>cost</i> [ <b>mst</b> ] |
| Step 2 | Verify the port cost setting.                  | <b>show spantree mst</b> [ <i>instance</i>   <i>mod/port</i> ]          |

This example shows how to configure the port cost on an MST instance and verify the configuration:

```

Console> (enable) set spantree portcost 6/1 10000 mst
Spantree port 6/1 path cost set to 10000.
Console> (enable)
Console> (enable) show spantree mst 6/1
Edge Port: No, (Configured) Default
Link Type: P2P, (Configured) Auto
Port Guard: Default
Boundary: Yes (PVST)

```

*CISCO Confidential - DRAFT*

```

Inst State Role Cost Prio VLANs

0 forwarding ROOT 10000 32 1
1 forwarding BDRY 10000 32 2-20
2 forwarding BDRY 10000 32 21-30
3 forwarding BDRY 10000 32 31-40
4 forwarding BDRY 10000 32 41-50
Console> (enable)

```

## Configuring the MST Port Priority

You can configure the port priority of ports. The port with the lowest priority value forwards frames for all VLANs. The possible port priority value is from 0–63; the default is 32. If all ports have the same priority value, the port with the lowest port number forwards frames.

To configure the port priority for a port, perform this task in privileged mode:

|        | Task                                        | Command                                                    |
|--------|---------------------------------------------|------------------------------------------------------------|
| Step 1 | Configure the MST port priority for a port. | <b>set spantree portpri</b> <i>mod/port priority [mst]</i> |
| Step 2 | Verify the port priority setting.           | <b>show spantree mst</b> [ <i>instance   mod/port</i> ]    |

This example shows how to configure the port priority and verify the configuration:

```

Console> (enable) set spantree portpri 6/1 30 mst
Bridge port 6/1 port priority set to 30.
Console> (enable)
Console> (enable) show spantree mst 6/1
Edge Port: No, (Configured) Default
Link Type: P2P, (Configured) Auto
Port Guard: Default
Boundary: Yes (PVST)

```

```

Inst State Role Cost Prio VLANs

0 forwarding ROOT 10000 30 1
1 forwarding BDRY 10000 30 2-20
2 forwarding BDRY 10000 30 21-30
3 forwarding BDRY 10000 30 31-40
4 forwarding BDRY 10000 30 41-50
Console> (enable)

```

## Configuring the MST Port Instance Cost

You can configure the port instance cost for an instance of MST. Ports with a lower instance cost are more likely to be chosen to forward frames. You should assign lower numbers to ports attached to faster media (such as full duplex) and higher numbers to ports attached to slower media. The default cost differs for different media. The possible value for port instance cost is from 1–268,435,456.

To configure the port instance cost for a port, perform this task in privileged mode:

*CISCO Confidential - DRAFT*

|        | Task                                              | Command                                                                                                          |
|--------|---------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | Configure the MST port instance cost on a port.   | <b>set spantree portinstancecost</b> <i>mod/port</i> [ <b>cost</b> <i>cost</i> ] <b>mst</b> [ <i>instances</i> ] |
| Step 2 | Verify the path cost for the instances on a port. | <b>show spantree portinstancecost</b> <i>mod/port</i>                                                            |

This example shows how to configure the MST port instance cost on a port:

```

Console> (enable) set spantree portinstancecost 6/1 cost 5000 mst 4
Port 6/1 MST Instances 0-3,5-15 have path cost 10000.
Port 6/1 MST Instances 4 have path cost 5000.
Console> (enable)
Console> (enable) show spantree mst 4
Spanning tree mode MST
Instance 4
VLANs Mapped: 41-50

Designated Root 00-10-7b-bb-2f-00
Designated Root Priority 32772 (root priority:32768, sys ID ext:4)

Designated Root Cost 0 Remaining Hops 20
Designated Root Port 1/0

Bridge ID MAC ADDR 00-10-7b-bb-2f-00
Bridge ID Priority 32772 (bridge priority:32768, sys ID ext:
4)

Port State Role Cost Prio Type

6/1 forwarding BDRY 5000 30 P2P,
Boundary(PVST)
6/2 blocking BDRY 20000 32 P2P,
Boundary(PVST)
Console> (enable)

```

## Configuring the MST Port Instance Priority

You can set a port priority for an instance of MST. The port with the lowest priority for a specific MST instance forwards frames for that instance. The port instance range is from 0–63. If all ports have the same priority for an MST instance, the port with the lowest port number forwards frames for that instance.

To configure the port instance priority on an MST instance, perform this task in privileged mode:

|        | Task                                                     | Command                                                                                            |
|--------|----------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| Step 1 | Configure the port instance priority on an MST instance. | <b>set spantree portinstancepri</b> <i>mod/port</i> <b>priority</b> <b>mst</b> [ <i>instance</i> ] |
| Step 2 | Verify the port instance priority setting.               | <b>show spantree mst</b> [ <i>instance</i>   <i>mod/port</i> ]                                     |

This example shows how to configure the port instance priority on an MST instance and verify the configuration:

```

Console> (enable) set spantree portinstancepri 6/1 20 mst 2
Port 6/1 MST Instances 2 using portpri 20.
Port 6/1 MST Instances 0-1,3-15 using portpri 30.
Console> (enable)

```

*CISCO Confidential - DRAFT*

```

Console> (enable)
Console> (enable) show spantree mst 2
Spanning tree mode MST
Instance 2
VLANs Mapped: 21-30

Designated Root 00-10-7b-bb-2f-00
Designated Root Priority 32770 (root priority:32768, sys ID ext:2)

Designated Root Cost 0 Remaining Hops 20
Designated Root Port 1/0

Bridge ID MAC ADDR 00-10-7b-bb-2f-00
Bridge ID Priority 32770 (bridge priority:32768, sys ID ext:
2)

Port State Role Cost Prio Type

6/1 forwarding BDRY 10000 20 P2P,
Boundary(PVST)
6/2 blocking BDRY 20000 32 P2P,
Boundary(PVST)
Console> (enable)

```

## Mapping and Unmapping VLANs to an MST Instance



### Note

See [Chapter 10, “Configuring VLANs”](#) for details on using VLANs.

By default, all VLANs are mapped to IST (instance 0). For an MST instance (MSTI) 1 through 15 to be active, you must map at least one VLAN to that MSTI. IST will always be active whether VLANs are mapped to IST or not. There are no VLAN mapping conflicts because of separate regions in MST.

Follow these guidelines for mapping and unmapping VLANs to an MST instance:

- You can only map Ethernet VLANs to MST instances.
- At least one VLAN in the instance must have an active port in order for MST to be active.
- You can map as many Ethernet VLANs as you wish to an MST instance.
- You cannot map a VLAN to more than one MST instance.
- The Hello Time, Maximum Age timer, and Forward Delay timer set for mode and all spanning trees are used globally by MST.

To map a VLAN to an MST instance, perform this task in privileged mode:

|        | Task                                   | Command                                               |
|--------|----------------------------------------|-------------------------------------------------------|
| Step 1 | Map a VLAN to an MST instance.         | <b>set spantree mst instance vlan vlan</b>            |
| Step 2 | Make the new region mapping effective. | set spantree mst config commit                        |
| Step 3 | Verify that the VLAN is mapped.        | <b>show spantree mst [instance] [active] mod/port</b> |

This example shows how to map a VLAN to MST instance 1 and verify the mapping:

```

Console> (enable) show spantree mst config
Current (NVRAM) MST Region Configuration:
Configuration Name:cisco
Revision:1

```

*CISCO Confidential - DRAFT*

## Instance VLANs

```

IST 1,51-4094
 1 2-20
 2 21-30
 3 31-40
 4 41-50
 5 -
 6 -
 7 -
 8 -
 9 -
 10 -
 11 -
 12 -
 13 -
 14 -
 15 -
=====
```

```
Console> (enable)
```

```
Console> (enable) set spantree mst 14 vlan 900-999
```

```
Edit Buffer modified. Use 'set spantree mst config commit' to apply the
changes.
```

```
Console> (enable) show spantree mst config
```

```
Current (NVRAM) MST Region Configuration:
```

```
Configuration Name:cisco
```

```
Revision:1
```

## Instance VLANs

```

IST 1,51-4094
 1 2-20
 2 21-30
 3 31-40
 4 41-50
 5 -
 6 -
 7 -
 8 -
 9 -
 10 -
 11 -
 12 -
 13 -
 14 -
 15 -
=====
```

```
NEW MST Region Configuration (Not committed yet)
```

```
Configuration Name:cisco
```

```
Revision:2
```

## Instance VLANs

```

IST 1,51-899,1000-4094
 1 2-20
 2 21-30
 3 31-40
 4 41-50
 5 -
 6 -
 7 -
 8 -
 9 -
 10 -
 11 -
 12 -
 13 -
 14 900-999
=====
```

*CISCO Confidential - DRAFT*

```

15 -
=====
Edit buffer is locked by:Console (pid 142)
Console> (enable)
Console> (enable) clear spantree mst 14 vlan 900-998
Edit Buffer modified. Use 'set spantree mst config commit' to apply the
changes.
Console> (enable)
Console> (enable) show spantree mst config
Current (NVRAM) MST Region Configuration:
Configuration Name:cisco Revision:1
Instance VLANs

IST 1,51-4094
1 2-20
2 21-30
3 31-40
4 41-50
5 -
6 -
7 -
8 -
9 -
10 -
11 -
12 -
13 -
14 -
15 -
=====
NEW MST Region Configuration (Not committed yet)
Configuration Name:cisco Revision:2
Instance VLANs

IST 1,51-998,1000-4094
1 2-20
2 21-30
3 31-40
4 41-50
5 -
6 -
7 -
8 -
9 -
10 -
11 -
12 -
13 -
14 999
15 -
=====
Edit buffer is locked by:Console (pid 142)
Console> (enable)
Console> (enable) set spantree mst config commit
Console> (enable)
Console> (enable) show spantree mst config
Current (NVRAM) MST Region Configuration:
Configuration Name:cisco Revision:2
Instance VLANs

IST 1,51-998,1000-4094
1 2-20
2 21-30
3 31-40

```

*CISCO Confidential - DRAFT*

```

4 41-50
5 -
6 -
7 -
8 -
9 -
10 -
11 -
12 -
13 -
14 999
15 -
=====
Console> (enable)
Console> (enable) show spantree mst 3
Spanning tree mode MST
Instance 3
VLANs Mapped: 31-40

Designated Root 00-10-7b-bb-2f-00
Designated Root Priority 8195 (root priority:8192, sys ID ext:3)
Designated Root Cost 0 Remaining Hops 20
Designated Root Port 1/0

Bridge ID MAC ADDR 00-10-7b-bb-2f-00
Bridge ID Priority 8195 (bridge priority:8192, sys ID ext:3)

Port State Role Cost Prio Type

6/1 forwarding BDRY 10000 30 P2P,
Boundary(PVST)
6/2 blocking BDRY 20000 32 P2P,
Boundary(PVST)
Console> (enable)

```

## Configuring Spanning Tree BPDU Skewing

Commands that support the spanning tree BPDU skewing feature perform these functions:

- Allow you to enable or disable BPDU skewing. The default is disabled.
- Modify the **show spantree summary** output to show if the skew detection is enabled and for which VLANs or PVST+ or MISTP instances the skew was detected.
- Provide a display of the VLAN or PVST+ or MISTP instance and the port affected by the skew: include this information:
  - The duration (in absolute time) of the last skew
  - The duration (in absolute time) of the worst skew
  - The date and time of the worst duration

To change how spanning tree performs BPDU skewing statistics gathering, enter the **set spantree bpdu-skewing** command. The **bpdu-skewing** command is disabled by default.

To configure the BPDU skewing statistics gathering for a VLAN, perform this task in privileged mode:

*CISCO Confidential - DRAFT*

|        | Task                      | Command                                                                                                                     |
|--------|---------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Configure BPDU skewing.   | <b>set spantree bpdu-skewing</b> [enable   disable]                                                                         |
| Step 2 | Verify the configuration. | <b>show spantree bpdu-skewing</b> vlan [mod/port]<br><b>show spantree bpdu-skewing mistp-instance</b> [instance] [mod/port] |

This example shows how to configure BPDU skewing and view the skewing statistics:

```

Console> (debug-eng) set spantree bpdu-skewing
Usage:set spantree bpdu-skewing <enable|disable>
Console> (debug-eng)
Console> (debug-eng)
Console> (debug-eng) set spantree bpdu-skewing enable
Spantree bpdu-skewing enabled on this switch.
Console> (debug-eng)
Console> (enable)

Console> (enable) show spantree bpdu-skewing 1
Bpdu skewing statistics for vlan 1
Port Last Skew ms Worst Skew ms Worst Skew Time

8/2 5869 108370 Tue Nov 21 2000, 06:25:59
8/4 4050 113198 Tue Nov 21 2000, 06:26:04
8/6 113363 113363 Tue Nov 21 2000, 06:26:05
8/8 4111 113441 Tue Nov 21 2000, 06:26:05
8/10 113522 113522 Tue Nov 21 2000, 06:26:05
8/12 4111 113600 Tue Nov 21 2000, 06:26:05
8/14 113678 113678 Tue Nov 21 2000, 06:26:05
8/16 4111 113755 Tue Nov 21 2000, 06:26:05
8/18 113833 113833 Tue Nov 21 2000, 06:26:05
8/20 4111 113913 Tue Nov 21 2000, 06:26:05
8/22 113917 113917 Tue Nov 21 2000, 06:26:05
8/24 4110 113922 Tue Nov 21 2000, 06:26:05
8/26 113926 113926 Tue Nov 21 2000, 06:26:05
8/28 4111 113931 Tue Nov 21 2000, 06:26:05
Console> (enable)

```

This example shows how to configure BPDU skewing for VLAN 1 on module 8, port 4 and view the skewing statistics:

```

Console> (enable) show spantree bpdu-skewing 1 8/4
Bpdu skewing statistics for vlan 1
Port Last Skew ms Worst Skew ms Worst Skew Time

8/4 5869 108370 Tue Nov 21 2000, 06:25:59

```

You will receive a similar output when MISTP is running.

The **show spantree summary** command shows if BPDU skew detection is enabled and also lists the VLANs or instances affected in the skew. This example shows the output of the **show spantree summary** command:

```

Console> (enable) show spantree summary
Root switch for vlans: 1
BPDU skewing detection enabled for the bridge
BPDU skewed for vlans: 1
Portfast bpdu-guard disabled for bridge.
Portfast bpdu-filter disabled for bridge.
Uplinkfast disabled for bridge.
Backbonefast disabled for bridge.

```



# *CISCO Confidential - DRAFT*

Summary of connected spanning tree ports by vlan

| VLAN     | Blocking | Listening | Learning | Forwarding | STP   | Active |
|----------|----------|-----------|----------|------------|-------|--------|
| -----    | -----    | -----     | -----    | -----      | ----- | -----  |
| 1        | 6        | 4         | 2        | 0          |       | 12     |
|          |          |           |          |            |       |        |
|          | Blocking | Listening | Learning | Forwarding | STP   | Active |
| -----    | -----    | -----     | -----    | -----      | ----- | -----  |
| Total    | 6        | 4         | 2        | 0          |       | 12     |
| Console> | (enable) |           |          |            |       |        |

*CISCO Confidential - DRAFT*

# Configuring Spanning Tree PortFast, BPDU Guard, BPDU Filter, UplinkFast, BackboneFast, and Loop Guard

This chapter describes how to configure the PortFast, BPDU guard, BPDU filter, UplinkFast, BackboneFast, and loop guard spanning tree enhancements on the Catalyst enterprise LAN switches.

**Note**

For information on configuring spanning tree, see [Chapter 7, “Configuring Spanning Tree.”](#)

**Note**

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 4500 Series, Catalyst 2948G, and Catalyst 2980G Switches Command Reference*.

This chapter consists of these sections:

- [Understanding How PortFast Works, page 8-1](#)
- [Understanding How PortFast BPDU Guard Works, page 8-2](#)
- [Understanding How PortFast BPDU Filtering Works, page 8-2](#)
- [Understanding How UplinkFast Works, page 8-3](#)
- [Understanding How BackboneFast Works, page 8-4](#)
- [Understanding How Loop Guard Works, page 8-6](#)
- [Configuring PortFast, page 8-8](#)
- [Configuring PortFast BPDU Guard, page 8-11](#)
- [Configuring PortFast BPDU Filtering, page 8-13](#)
- [Configuring UplinkFast, page 8-14](#)
- [Configuring BackboneFast, page 8-16](#)
- [Configuring Loop Guard, page 8-18](#)

## Understanding How PortFast Works

PortFast causes a switch or trunk port to enter the spanning tree forwarding state immediately, bypassing the listening and learning states.

*CISCO Confidential - DRAFT*

You can use PortFast on switch or trunk ports connected to a single workstation, switch, or server to allow those devices to connect to the network immediately, instead of waiting for the port to transition from the listening and learning states to the forwarding state.

**Caution**

You can use PortFast to connect a single end station or a switch port to a switch port. If you enable PortFast on a port that is connected to another Layer 2 device, such as a switch, you might create network loops.

When the switch powers up, or when a device is connected to a port, the port normally enters the spanning tree listening state. When the Forward Delay timer expires, the port enters the learning state. When the Forward Delay timer expires a second time, the port is transitioned to the forwarding or blocking state.

When you enable PortFast on a switch or trunk port, the port is immediately transitioned to the spanning tree forwarding state.

## Understanding How PortFast BPDU Guard Works

To prevent loops from occurring in a network, the PortFast mode is supported only on nontrunking access ports because these ports typically do not transmit or receive BPDUs. The most secure implementation of PortFast is to enable it only on ports that connect end stations to switches. Because PortFast can be enabled on nontrunking ports connecting two switches, spanning tree loops can occur because BPDUs are still being transmitted and received on those ports.

The PortFast BPDU guard feature prevents loops by moving a nontrunking port into an errdisable state when a BPDU is received on that port. When the BPDU guard feature is enabled on the switch, spanning tree shuts down PortFast-configured interfaces that receive BPDUs, instead of putting them into the spanning tree blocking state. In a valid configuration, PortFast-configured interfaces do not receive BPDUs. If a PortFast-configured interface receives a BPDU, an invalid configuration exists, such as connection of an unauthorized device. The BPDU guard feature provides a secure response to invalid configurations because the administrator must manually put the interface back in service.

**Note**

When enabled on the switch, spanning tree applies the BPDU guard feature to all PortFast-configured interfaces.

## Understanding How PortFast BPDU Filtering Works

BPDU filtering allows you to avoid transmitting BPDUs on PortFast-enabled ports that are connected to an end system. When you enable PortFast on the switch, spanning tree places ports in the forwarding state immediately, instead of going through the listening, learning, and forwarding states.

By default, spanning tree sends BPDUs from all ports regardless of whether PortFast is enabled. BPDU filtering is on a per-switch basis; after you enable BPDU filtering, it applies to all PortFast-enabled ports on the switch.

CISCO Confidential - DRAFT

# Understanding How UplinkFast Works

UplinkFast provides fast convergence using uplink groups in the network access layer after a spanning tree topology change. An uplink group is a set of ports (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 (not including self-looped ports). The uplink group provides an alternate path in case the currently forwarding link fails.

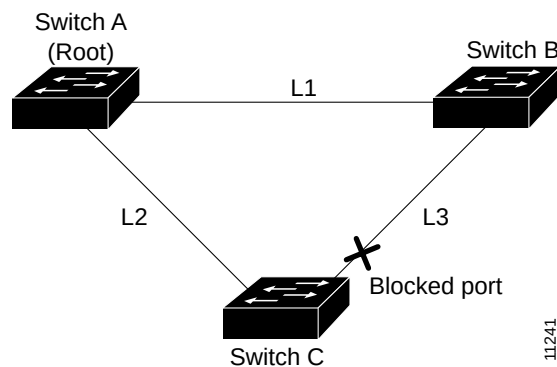


## Note

UplinkFast is most useful in wiring-closet switches that have a limited number of active VLANs. This enhancement might not be useful for other types of applications and should not be enabled on backbone or distribution layer switches.

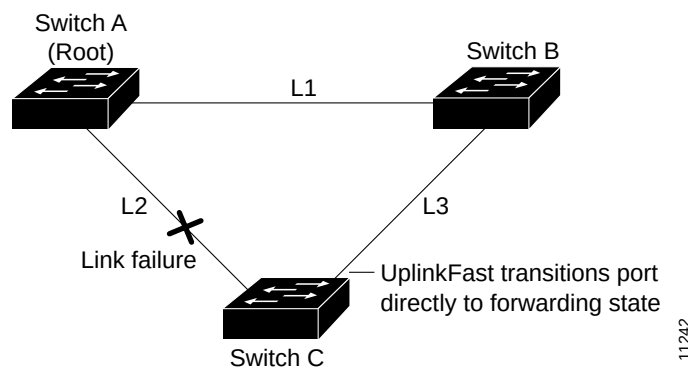
Figure 8-1 shows an example UplinkFast network topology. Switch A, the root switch, is connected directly to Switch B over link L1 and to Switch C over link L2. The port on Switch C that is connected to Switch B over link L3 is in blocking state.

**Figure 8-1 UplinkFast Example Before Direct Link Failure**



If Switch C detects a link failure on the currently active link L2 (a *direct* link failure), UplinkFast unblocks the blocked port on Switch C and transitions it to the forwarding state immediately, without transitioning the port through the listening and learning states (as shown in Figure 8-2). This switchover takes approximately 1 to 5 seconds.

**Figure 8-2 Example of UplinkFast After Direct Link Failure**



*CISCO Confidential - DRAFT*

As soon as the switch transitions the alternate port to the forwarding state, the switch begins transmitting dummy multicast frames on that port, one for each entry in the local Enhanced Address Recognition Logic (EARL) table (except those entries that are associated with the failed root port). By default, approximately 15 dummy multicast frames are transmitted per 100 ms.

Each dummy multicast frame uses the station address in the EARL table entry as its source MAC address and a dummy multicast address (01-00-0C-CD-CD-CD) as the destination MAC address.

Switches receiving these dummy multicast frames immediately update their EARL table entries for each source MAC address to use the new port, allowing the switches to begin using the new path almost immediately.

If connectivity on the original root port is restored, the switch waits for a period equal to twice the forward delay time plus 5 seconds before transitioning the port to the forwarding state to allow the neighbor port enough time to transition through the listening and learning states to the forwarding state.

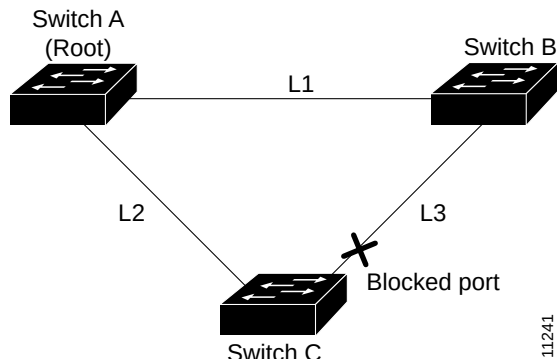
## Understanding How BackboneFast Works

BackboneFast provides fast convergence in the network backbone after a spanning tree topology change occurs. A switch detects an indirect link failure (the failure of a link to which the switch is not directly connected) when the switch receives inferior BPDUs from its designated bridge on its root port or blocked ports. These inferior BPDUs indicate that the designated bridge has lost its connection to the root bridge. An inferior BPDU identifies a single switch as both the root bridge and the designated bridge. Under normal spanning tree rules, the switch ignores inferior BPDUs for the configured maximum aging time (specified by the **set spantree maxage** command).

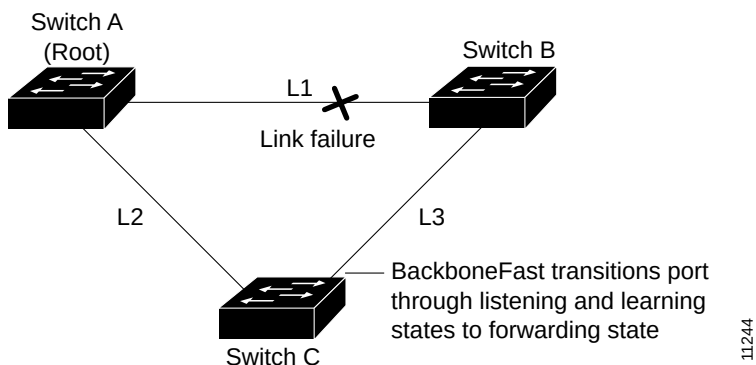
The switch tries to determine if it has an alternate path to the root bridge. If the inferior BPDU arrives on a blocked port, the root port and other blocked ports on the switch become alternate paths to the root bridge. If the inferior BPDU arrives on the root port, all blocked ports become alternate paths to the root bridge. If the inferior BPDU arrives on the root port and there are no blocked ports, the switch assumes that it has lost connectivity to the root bridge, causes the maximum aging time on the root to expire, and becomes the root switch according to normal spanning tree rules.

If the switch 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 out all alternate paths to the root bridge. If the switch determines that it still has an alternate path to the root, it causes the maximum aging time on the ports on which it received the inferior BPDU to expire. If all the alternate paths to the root bridge indicate that the switch has lost connectivity to the root bridge, the switch 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 switch 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.

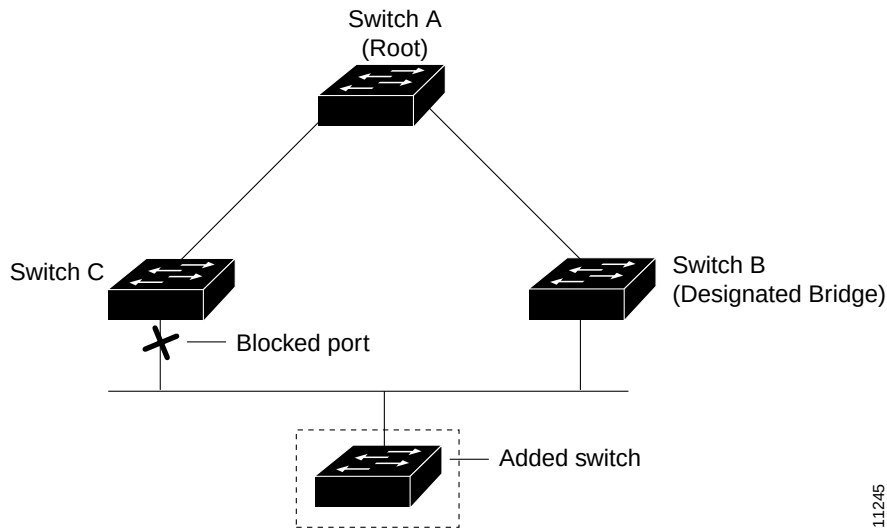
Figure 8-3 shows an example of a BackboneFast network topology. Switch A, the root switch, connects directly to Switch B over link L1 and to Switch C over link L2. The port on Switch C that connects directly to Switch B over link L3 is in the blocking state.

*CISCO Confidential - DRAFT***Figure 8-3 Example of BackboneFast before Indirect Link Failure**

If link L1 fails, Switch C detects this failure as an *indirect* failure, since it is not connected directly to link L1. Switch B no longer has a path to the root switch. 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 port on Switch C to the forwarding state, providing a path from Switch B to Switch A. This switchover takes approximately 30 seconds. [Figure 8-4](#) shows how BackboneFast reconfigures the topology to account for the failure of link L1.

**Figure 8-4 Example of BackboneFast after Indirect Link Failure**

If a new switch is introduced into a shared-medium topology, BackboneFast is not activated. [Figure 8-5](#) shows a shared-medium topology in which a new switch is added. The new switch begins sending inferior BPDUs, which indicate that it is the root switch. However, the other switches ignore these inferior BPDUs and the new switch learns that Switch B is the designated bridge to Switch A, the root switch.

*CISCO Confidential - DRAFT***Figure 8-5 Adding a Switch in a Shared-Medium Topology**

11245

## Understanding How Loop Guard Works

Unidirectional link failures may cause a root port or alternate port to become designated as root if BPDUs are absent. Some software failures may introduce temporary loops in the network. The loop guard feature checks if a root port or an alternate root port receives BPDUs. If the port is receiving BPDUs, the loop guard feature puts the port into an inconsistent state until it starts receiving BPDUs again. Loop guard isolates the failure and lets spanning tree converge to a stable topology without the failed link or bridge.

You can enable loop guard on a per-port basis with the **set spantree guard loop** command.



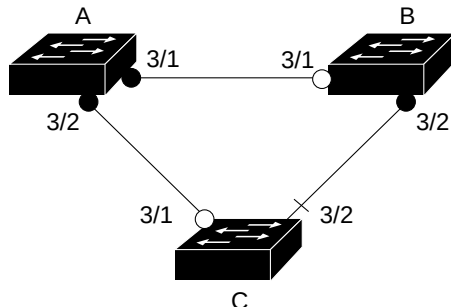
### Note

Provided that you are in MST mode, you can set all the ports on a switch with the **set spantree global-defaults loop-guard** command.

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 8-6](#) shows loop guard in a triangle switch configuration.



*CISCO Confidential - DRAFT***Figure 8-6 Triangle Switch Configuration with Loop Guard**

—● Designated port

—○ Root port

—+ Alternate port

55772

Figure 8-6 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.

Use loop guard only in topologies where there are blocked ports. Topologies that have no blocked ports, which are loop free, do not need to enable this feature. Enabling loop guard on a root switch has no effect but provides protection when a root switch becomes a nonroot switch.

Follow these guidelines when using loop guard:

- Do not enable loop guard on PortFast-enabled or dynamic VLAN ports.
- Do not enable PortFast on loop guard-enabled ports.
- Do not enable loop guard if root guard is enabled.
- Do not enable loop guard on ports that are connected to a shared link.

**Note**

We recommend that you enable loop guard on root ports and alternate root ports on access switches.

Loop guard interacts with other features as follows:

- Loop guard does not affect the functionality of UplinkFast or BackboneFast.
- Root guard forces a port to always be designated as the root port. Loop guard is effective only if the port is a root port or an alternate port. Do not enable loop guard and root guard on a port at the same time.
- PortFast transitions a port into a forwarding state immediately when a link is established. Because a PortFast-enabled port will not be a root port or alternate port, loop guard and PortFast cannot be configured on the same port. Assigning dynamic VLAN membership for the port requires that the port is PortFast enabled. Do not configure a loop guard-enabled port with dynamic VLAN membership.
- If your network has a type-inconsistent port or a PVID-inconsistent port, all BPDUs are dropped until the misconfiguration is corrected. The port transitions out of the inconsistent state after the message age expires. Loop guard ignores the message age expiration on type-inconsistent ports and

*CISCO Confidential - DRAFT*

PVID-inconsistent ports. If the port is already blocked by loop guard, misconfigured BPDUs received on the port make loop guard recover, but the port is moved into the type-inconsistent state or PVID-inconsistent state.

- In high-availability switch configurations, if a port is put into the blocked state by loop guard, it remains blocked even after switchover to the redundant supervisor engine. The newly activated supervisor engine recovers the port only after receiving a BPDU on that port.
- Loop guard uses the ports known to spanning tree. Loop guard can take advantage of logical ports provided by the Port Aggregation Protocol (PAgP). However, to form a channel, all the physical ports grouped in the channel must have compatible configurations. PAgP enforces uniform configurations of root guard or loop guard on all the physical ports to form a channel.

These caveats apply to loop guard:

- Spanning tree always chooses the first operational port in the channel to send the BPDUs. If that link becomes unidirectional, loop guard blocks the channel, even if other links in the channel are functioning properly.
- If a set of ports that are already blocked by loop guard are grouped together to form a channel, spanning tree loses all the state information for those ports and the new channel port may obtain the forwarding state with a designated role.
- If a channel is blocked by loop guard and the channel breaks, spanning tree loses all the state information. The individual physical ports may obtain the forwarding state with the designated role, even if one or more of the links that formed the channel are unidirectional.
- 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.

## Configuring PortFast

The following sections describe how to configure PortFast on the switch.

### Enabling PortFast on an Access Port



#### Caution

You can use PortFast to connect a single end station or a switch port to a switch port. If you enable PortFast on a port that is connected to another Layer 2 device, such as a switch, you might create network loops.

To enable PortFast on a switch port, perform this task in privileged mode:

|        | Task                                                                                   | Command                                                                                |
|--------|----------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| Step 1 | Enable PortFast on a switch port connected to a single workstation, switch, or server. | <b>set spantree portfast</b> <i>mod_num/port_num</i> <b>enable</b><br><b>  disable</b> |
| Step 2 | Verify the PortFast setting on a switch port.                                          | <b>show spantree</b> [ <i>mod_num/port_num</i> ] [ <i>vlan</i> ]                       |

This example shows how to enable PortFast on port 1 of module 4 and verify the configuration (the PortFast status is shown in the “Fast-Start” column):

*CISCO Confidential - DRAFT*

```
Console> (enable) set spantree portfast 4/1 enable
Warning:Connecting Layer 2 devices to a fast start port can cause
temporary spanning tree loops. Use with caution.
```

```
Spantree port 4/1 fast start enabled.
```

```
Console> (enable) show spantree 4/1
```

| Port | Vlan | Port-State    | Cost | Priority | Fast-Start | Group-method |
|------|------|---------------|------|----------|------------|--------------|
| 4/1  | 1    | blocking      | 19   | 20       | enabled    |              |
| 4/1  | 100  | forwarding    | 10   | 20       | enabled    |              |
| 4/1  | 521  | blocking      | 19   | 20       | enabled    |              |
| 4/1  | 522  | blocking      | 19   | 20       | enabled    |              |
| 4/1  | 523  | blocking      | 19   | 20       | enabled    |              |
| 4/1  | 524  | blocking      | 19   | 20       | enabled    |              |
| 4/1  | 1003 | not-connected | 19   | 20       | enabled    |              |
| 4/1  | 1005 | not-connected | 19   | 4        | enabled    |              |

```
Console> (enable)
```

## Enabling PortFast on a Trunk Port



### Caution

You can use PortFast to connect a single end station or a switch port to a switch port. If you enable PortFast on a port that is connected to another Layer 2 device, like a switch, you might create network loops.

To enable PortFast on a trunk port, perform this task in privileged mode:

|        | Task                                                                                          | Command                                                                                                                                                                                                                                     |
|--------|-----------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Enable PortFast on a trunk port that is connected to a single workstation, switch, or server. | <b>set spantree portfast <i>mod_num/port_num</i> enable trunk</b><br><br><b>Note</b> If you enter the <b>set spantree portfast</b> command on a trunk port without entering the <b>trunk</b> keyword, the trunk port stays in disable mode. |
| Step 2 | Verify the PortFast setting on a trunk port.                                                  | <b>show spantree portfast [<i>mod_num/port_num</i>]</b>                                                                                                                                                                                     |

This example shows how to enable PortFast on port 1 of module 4 of a trunk port, bring the trunk port to a forwarding state, and verify the configuration (the PortFast status is shown in the “Fast-Start” column):

```
Console> (enable) set spantree portfast 4/1 enable trunk
Warning:Connecting Layer 2 devices to a fast start port can cause
temporary spanning tree loops. Use with caution.
```

```
Spantree port 4/1 fast start enabled.
```

```
Console> (enable) show spantree 4/1
```

| Port | Vlan | Port-State    | Cost | Prio | Portfast  |
|------|------|---------------|------|------|-----------|
| 4/1  | 1    | blocking      | 4    | 32   | enabled 0 |
| 4/1  | 100  | forwarding    | 4    | 32   | enabled 0 |
| 4/1  | 521  | blocking      | 4    | 32   | enabled 0 |
| 4/1  | 524  | blocking      | 4    | 32   | enabled 0 |
| 4/1  | 1003 | not-connected | 4    | 32   | enabled 0 |
| 4/1  | 1005 | not-connected | 4    | 32   | enabled 0 |

```
Console> (enable) show spantree portfast 4/1
Portfast:enable trunk
```

*CISCO Confidential - DRAFT*

Portfast BPDU guard is disabled.  
 Portfast BPDU filter is disabled.  
 Console>

**Note**

When you enable PortFast between two switches, the system will verify that there are no loops in the network before bringing the blocking trunk to a forwarding state.

## Disabling PortFast

To disable PortFast on a switch or trunk port, perform this task in privileged mode:

|        | Task                               | Command                                                             |
|--------|------------------------------------|---------------------------------------------------------------------|
| Step 1 | Disable PortFast on a switch port. | <b>set spantree portfast</b> <i>mod_num/port_num</i> <b>disable</b> |
| Step 2 | Verify the PortFast setting.       | <b>show spantree</b> <i>mod_num/port_num</i>                        |

This example shows how to disable PortFast on port 1 of module 4:

```
Console> (enable) set spantree portfast 4/1 disable
Spantree port 4/1 fast start disabled.
Console> (enable)
```

To reset PortFast on a switch or trunk port to its default settings, perform this task in privileged mode:

|        | Task                                                | Command                                                             |
|--------|-----------------------------------------------------|---------------------------------------------------------------------|
| Step 1 | Reset PortFast to default setting on a switch port. | <b>set spantree portfast</b> <i>mod_num/port_num</i> <b>default</b> |
| Step 2 | Verify the PortFast setting.                        | <b>show spantree</b> <i>mod_num/port_num</i>                        |

This example shows how to disable PortFast on port 1 of module 4:

```
Console> (enable) set spantree portfast 4/1 default

Spantree port 4/1 fast start set to default.

Console> (enable) show spantree portfast 4/1
Portfast:default
Portfast BPDU guard is disabled.
Portfast BPDU filter is disabled.
Console> (enable)
```

## Resetting PortFast

To reset PortFast on a switch or trunk port to its default settings, perform this task in privileged mode:

|        | Task                                                     | Command                                                             |
|--------|----------------------------------------------------------|---------------------------------------------------------------------|
| Step 1 | Reset PortFast to its default settings on a switch port. | <b>set spantree portfast</b> <i>mod_num/port_num</i> <b>default</b> |
| Step 2 | Verify the PortFast setting.                             | <b>show spantree</b> <i>mod_num/port_num</i>                        |

*CISCO Confidential - DRAFT*

This example shows how to reset PortFast to its default settings on port 1 of module 4:

```
Console> (enable) set spantree portfast 4/1 default
```

```
Spantree port 4/1 fast start set to default.
```

```
Console> (enable) show spantree portfast 4/1
```

```
Portfast:default
```

```
Portfast BPDU guard is disabled.
```

```
Portfast BPDU filter is disabled.
```

```
Console> (enable)
```

## Configuring PortFast BPDU Guard

The following sections describe how to configure PortFast BPDU guard on the switch.

### Enabling PortFast BPDU Guard

The PortFast feature is configured on an individual port, and the PortFast BPDU guard option is configured either globally or on a per-port basis.

When you disable PortFast on a port, PortFast BPDU guard becomes inactive. The port configuration overrides the global configuration unless the port configuration is set to default. If the port configuration is set to default, the global configuration is checked. If the port configuration is enabled, the port configuration is used and the global configuration is not used.

To enable and verify PortFast BPDU guard on a nontrunking switch port, perform this task in privileged mode:

|        | Task                                     | Command                                                                       |
|--------|------------------------------------------|-------------------------------------------------------------------------------|
| Step 1 | Enable BPDU guard on an individual port. | <b>set spantree portfast bpdu-guard mod/port [disable   enable   default]</b> |
| Step 2 | Verify the PortFast BPDU guard setting.  | <b>show spantree summary</b>                                                  |



#### Note

For additional PVST+ information, see [Chapter 7, “Configuring Spanning Tree.”](#)

This example shows how to enable PortFast BPDU guard on module 6 port 1, and verify the configuration in the Per VLAN Spanning Tree + (PVST+) mode:

```
Console> (enable) set spantree portfast bpdu-guard 6/1 enable
```

```
Spantree port 6/1 bpdu guard enabled.
```

```
Console> (enable)
```

```
Console> (enable) show spantree summary
```

```
Root switch for vlans: none.
```

```
Portfast bpdu-guard enabled for bridge.
```

```
Uplinkfast disabled for bridge.
```

```
Backbonefast disabled for bridge.
```

| Vlan | Blocking | Listening | Learning | Forwarding | STP | Active |
|------|----------|-----------|----------|------------|-----|--------|
| 1    | 0        | 0         | 0        | 4          |     | 4      |
| 2    | 0        | 0         | 0        | 4          |     | 4      |

*CISCO Confidential - DRAFT*

```

 3 0 0 0 4 4
 4 0 0 0 4 4
 5 0 0 0 4 4
 6 0 0 0 4 4
 10 0 0 0 4 4
 20 0 0 0 4 4
 .
 .
 .
 999 0 0 0 4 4
 1003 0 0 0 0 0
 1005 0 0 0 0 0

 Blocking Listening Learning Forwarding STP Active

Total 0 0 0 85 85
Console> (enable)

```

## Disabling PortFast BPDU Guard

To disable PortFast BPDU guard, perform this task in privileged mode:

|        | Task                                       | Command                                                                                        |
|--------|--------------------------------------------|------------------------------------------------------------------------------------------------|
| Step 1 | Disable PortFast BPDU guard on the switch. | <b>set spantree portfast bpdu-guard</b> <i>mod/port</i><br><b>[disable   enable   default]</b> |
| Step 2 | Verify the PortFast BPDU guard setting.    | <b>show spantree summary</b>                                                                   |

This example shows how to disable PortFast BPDU guard on the switch and verify the configuration:

```

Console> (enable) set spantree portfast bpdu-guard disable
Spantree portfast bpdu-guard disabled on this switch.
Console> (enable) show spantree summary
Summary of connected spanning tree ports by vlan

```

```

➔ Portfast bpdu-guard disabled for bridge.
Uplinkfast disabled for bridge.
Backbonefast disabled for bridge.

```

```

Vlan Blocking Listening Learning Forwarding STP Active

 1 0 0 0 4 4
 2 0 0 0 4 4
 3 0 0 0 4 4
 4 0 0 0 4 4
 .
 .
 .
 1003 0 0 0 0 0
 1005 0 0 0 0 0

 Blocking Listening Learning Forwarding STP Active

Total 0 0 0 85 85
Console> (enable)

```

*CISCO Confidential - DRAFT*

# Configuring PortFast BPDU Filtering

The following sections describe how to configure PortFast BPDU filtering on the switch.

## Enabling PortFast BPDU Filtering



### Note

Although you can configure PortFast on an individual port, you configure the PortFast BPDU filtering option globally. When you disable PortFast on a port, PortFast BPDU filtering becomes inactive for that port.

To enable PortFast BPDU filtering, perform this task in privileged mode:

|        | Task                                     | Command                                                                               |
|--------|------------------------------------------|---------------------------------------------------------------------------------------|
| Step 1 | Enable BPDU filtering state on the port. | <b>set spantree portfast bpdu-filter</b> <i>mod/port</i> [disable   enable   default] |
| Step 2 | Verify PortFast BPDU filtering setting.  | <b>show spantree summary</b>                                                          |



### Note

For additional PVST+ information, see [Chapter 7, “Configuring Spanning Tree.”](#)

By default, BPDU filtering is set for each port. This example shows how to enable PortFast BPDU filtering on the port and verify the configuration in PVST+ mode:

```
Console> (enable) set spantree portfast bpdu-filter 6/1 enable
Warning:Ports enabled with bpdu filter will not send BPDUs and drop all
received BPDUs. You may cause loops in the bridged network if you misuse
this feature.
```

```
Console> (enable) show spantree summary
Root switch for vlans: none.
Portfast bpdu-filter enabled for bridge.
Uplinkfast disabled for bridge.
Backbonefast disabled for bridge.
```

| Vlan  | Blocking | Listening | Learning | Forwarding | STP | Active |
|-------|----------|-----------|----------|------------|-----|--------|
| 1     | 0        | 0         | 0        | 4          |     | 4      |
| 2     | 0        | 0         | 0        | 4          |     | 4      |
| 3     | 0        | 0         | 0        | 4          |     | 4      |
| 4     | 0        | 0         | 0        | 4          |     | 4      |
| 5     | 0        | 0         | 0        | 4          |     | 4      |
| 6     | 0        | 0         | 0        | 4          |     | 4      |
| .     |          |           |          |            |     |        |
| .     |          |           |          |            |     |        |
| 1003  | 0        | 0         | 0        | 0          |     | 0      |
| 1005  | 0        | 0         | 0        | 0          |     | 0      |
|       |          |           |          |            |     |        |
|       | Blocking | Listening | Learning | Forwarding | STP | Active |
| ----- |          |           |          |            |     |        |
| Total | 0        | 0         | 0        | 85         |     | 85     |

```
Console> (enable)
```

*CISCO Confidential - DRAFT*

## Disabling PortFast BPDU Filtering

To disable PortFast BPDU filtering on a switch, perform this task in privileged mode:

|        | Task                                           | Command                                          |
|--------|------------------------------------------------|--------------------------------------------------|
| Step 1 | Disable PortFast BPDU filtering on the switch. | <b>set spantree portfast bpdu-filter disable</b> |
| Step 2 | Verify the PortFast BPDU filtering setting.    | <b>show spantree summary</b>                     |

This example shows how to disable PortFast BPDU filtering on the switch and verify the configuration:

```
Console> (enable) set spantree portfast bpdu-filter disable
Spanntree portfast bpdu-filter disabled on this switch.
Console> (enable) show spantree summary
Summary of connected spanning tree ports by vlan
```

```
Portfast bpdu-filter disabled for bridge.
Uplinkfast disabled for bridge.
Backbonefast disabled for bridge.
```

| Vlan                                              | Blocking | Listening | Learning | Forwarding | STP | Active |
|---------------------------------------------------|----------|-----------|----------|------------|-----|--------|
| 1                                                 | 0        | 0         | 0        | 4          |     | 4      |
| 2                                                 | 0        | 0         | 0        | 4          |     | 4      |
| 3                                                 | 0        | 0         | 0        | 4          |     | 4      |
| 4                                                 | 0        | 0         | 0        | 4          |     | 4      |
| 5                                                 | 0        | 0         | 0        | 4          |     | 4      |
| 6                                                 | 0        | 0         | 0        | 4          |     | 4      |
| 10                                                | 0        | 0         | 0        | 4          |     | 4      |
| .                                                 |          |           |          |            |     |        |
| .                                                 |          |           |          |            |     |        |
| .                                                 |          |           |          |            |     |        |
| 999                                               | 0        | 0         | 0        | 4          |     | 4      |
| 1003                                              | 0        | 0         | 0        | 0          |     | 0      |
| 1005                                              | 0        | 0         | 0        | 0          |     | 0      |
| Blocking Listening Learning Forwarding STP Active |          |           |          |            |     |        |
| -----                                             |          |           |          |            |     |        |
| Total                                             | 0        | 0         | 0        | 85         |     | 85     |

```
Console> (enable)
```

## Configuring UplinkFast

The following sections describe how to configure the UplinkFast feature on the switch.

### Enabling UplinkFast

When you enable UplinkFast on the switch, UplinkFast processing is enabled and the spanning tree bridge priority for all VLANs is set to 49,152, making it unlikely that the switch will become the root switch. In addition, the spanning tree port cost and port-VLAN cost of all ports on the switch is increased by 3000.

The *station\_update\_rate* value in the UplinkFast command represents the number of dummy multicast packets that are transmitted per 100 ms (the default is 15 packets per 100 ms) in the event of a direct link failure.



*CISCO Confidential - DRAFT*

Enter the **all-protocols on** keywords on switches that have UplinkFast enabled but do not have protocol filtering enabled, and that are connected to upstream switches in the network that have protocol filtering enabled. The **all-protocols on** keywords cause the switch to generate multicasts for each protocol-filtering group.

On switches with both UplinkFast and protocol filtering enabled, or if no other switches have protocol filtering enabled, you do not need to use the **all-protocols on** keywords.

**Note**

When you enable UplinkFast, it affects all VLANs on the switch. You cannot configure UplinkFast on a per-VLAN basis.

To enable UplinkFast, perform this task in privileged mode:

|        | Task                               | Command                                                                                        |
|--------|------------------------------------|------------------------------------------------------------------------------------------------|
| Step 1 | Enable UplinkFast on the switch.   | <b>set spantree uplinkfast enable</b> [rate station_update_rate]<br>[all-protocols {off   on}] |
| Step 2 | Verify that UplinkFast is enabled. | <b>show spantree uplinkfast [vlans]</b>                                                        |

This example shows how to enable UplinkFast with a station-update rate of 40 packets per 100 ms and how to verify that UplinkFast is enabled:

```

Console> (enable) set spantree uplinkfast enable rate 40
VLANs 1-1005 bridge priority set to 49152.
The port cost and portvlancost of all ports set to above 3000.
Station update rate set to 40 packets/100ms.
uplinkfast all-protocols field set to off.
uplinkfast enabled for bridge.
Console> (enable) show spantree uplinkfast
Station update rate set to 40 packets/100ms.
uplinkfast all-protocols field set to off.
VLAN port list

1 1/1(fwd),1/2
100 1/2(fwd)
521 1/1(fwd),1/2
522 1/1(fwd),1/2
523 1/1(fwd),1/2
524 1/1(fwd),1/2
Console> (enable)

```

This example shows how to display the UplinkFast feature settings for all VLANs:

```

Console> show spantree uplinkfast
Station update rate set to 15 packets/100ms.
uplinkfast all-protocols field set to off.
VLAN port list

1-20 1/1(fwd),1/2-1/5
21-50 1/9(fwd), 1/6-1/8, 1/10-1/12
51-100 2/1(fwd), 2/12
Console>

```

*CISCO Confidential - DRAFT*

## Disabling UplinkFast

To disable UplinkFast and restore the default spanning tree bridge priority, port cost, and port-VLAN cost values to their default values, enter the **clear spantree uplinkfast** command.



### Caution

Use caution when entering the **clear spantree uplinkfast** command. This command restores the port-VLAN costs on all ports to the default minus one (18) and the port cost to the default value (19). If you have configured per-VLAN load sharing on redundant trunk links, the load-sharing configuration can be affected by this command.

You can disable only spanning tree UplinkFast processing on the switch using the **set spantree uplinkfast disable** command. This command does not affect the bridge priority, port cost, and port-VLAN cost values on the switch.



### Note

When you disable UplinkFast, it affects all VLANs on the switch. You cannot disable UplinkFast on a per-VLAN basis.

To disable UplinkFast on a switch, perform this task in privileged mode:

|        | Task                                                                                                                                  | Command                                |
|--------|---------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------|
| Step 1 | (Optional) Disable UplinkFast processing on the switch and restore the default bridge priority, port cost, and port-VLAN cost values. | <b>clear spantree uplinkfast</b>       |
| Step 2 | (Optional) Disable UplinkFast processing on the switch without affecting the bridge priority, port cost, and port-VLAN cost values.   | <b>set spantree uplinkfast disable</b> |
| Step 3 | Verify that UplinkFast is enabled.                                                                                                    | <b>show spantree uplinkfast</b>        |

This example shows how to disable UplinkFast on the switch and restore the default bridge priority, port cost, and port-VLAN cost values:

```

Console> (enable) clear spantree uplinkfast
This command will cause all portcosts, portvlancosts, and the
bridge priority on all vlans to be set to default.
Do you want to continue (y/n) [n]? y
VLANs 1-1005 bridge priority set to 32768.
The port cost of all bridge ports set to default value.
The portvlancost of all bridge ports set to default value.
uplinkfast all-protocols field set to off.
uplinkfast disabled for bridge.
Console> (enable) show spantree uplinkfast
uplinkfast disabled for bridge.
Console> (enable)

```

## Configuring BackboneFast

The following sections describe how to configure the BackboneFast feature on the switch.

*CISCO Confidential - DRAFT*

## Enabling BackboneFast



### Note

You must enable BackboneFast on all switches in the network. BackboneFast is not supported on Token Ring VLANs. This feature is supported for use with third-party switches.

To enable BackboneFast on the switch, perform this task in privileged mode:

|        | Task                                 | Command                                 |
|--------|--------------------------------------|-----------------------------------------|
| Step 1 | Enable BackboneFast on the switch.   | <b>set spantree backbonefast enable</b> |
| Step 2 | Verify that BackboneFast is enabled. | <b>show spantree backbonefast</b>       |

This example shows how to enable BackboneFast on the switch and how to verify the configuration:

```
Console> (enable) set spantree backbonefast enable
Backbonefast enabled for all VLANs
Console> (enable) show spantree backbonefast
Backbonefast is enabled.
Console> (enable)
```

## Displaying BackboneFast Statistics

To display BackboneFast statistics, perform this task in privileged mode:

| Task                             | Command                      |
|----------------------------------|------------------------------|
| Display BackboneFast statistics. | <b>show spantree summary</b> |

This example shows how to display BackboneFast statistics:

```
Console> (enable) show spantree summary
Summary of connected spanning tree ports by vlan
```

```
Uplinkfast disabled for bridge.
Backbonefast enabled for bridge.
```

```
Vlan Blocking Listening Learning Forwarding STP Active

 1 0 0 0 1 1

 Blocking Listening Learning Forwarding STP Active

Total 0 0 0 1 1
```

```
BackboneFast statistics

```

```
Number of inferior BPDUs received (all VLANs) : 0
Number of RLQ req PDUs received (all VLANs) : 0
Number of RLQ res PDUs received (all VLANs) : 0
Number of RLQ req PDUs transmitted (all VLANs): 0
Number of RLQ res PDUs transmitted (all VLANs): 0
Console> (enable)
```

*CISCO Confidential - DRAFT*

## Disabling BackboneFast

To disable BackboneFast on the switch, perform this task in privileged mode:

|        | Task                                  | Command                                  |
|--------|---------------------------------------|------------------------------------------|
| Step 1 | Disable BackboneFast on the switch.   | <b>set spantree backbonefast disable</b> |
| Step 2 | Verify that BackboneFast is disabled. | <b>show spantree backbonefast</b>        |

This example shows how to disable BackboneFast on the switch and how to verify the configuration:

```

Console> (enable) set spantree backbonefast disable
Backbonefast enabled for all VLANs
Console> (enable) show spantree backbonefast
Backbonefast is disabled.
Console> (enable)

```

## Configuring Loop Guard

The following sections describe how to configure loop guard.

### Enabling Loop Guard

Enter the **set spantree guard** command to enable the spanning tree loop guard feature on a per-port basis. To set all the ports on the switch, use the **set spantree mst global-defaults loop-guard** command.

To enable loop guard on an individual port, perform this task in privileged mode:

|        | Task                               | Command                                                             |
|--------|------------------------------------|---------------------------------------------------------------------|
| Step 1 | Enable loop guard on a port.       | <b>set spantree guard {root   loop   none} mod/port</b>             |
| Step 2 | Verify that loop guard is enabled. | <b>show spantree guard {mod/port   vlan} mstp-instance instance</b> |

This example shows how to enable loop guard on port 5/1:

```

Console> (enable) set spantree guard loop 5/1
Rootguard is enabled on port 5/1, enabling loopguard will disable rootguard on
this port.
Do you want to continue (y/n) [n]? y
Loopguard on port 5/1 is enabled.
Console> (enable)

```

This example shows how to enable loop guard on all the ports on a switch:

```

Console> (enable) set spantree mst global-defaults loop-guard enable
Spantree global loop-guard state enabled on this switch.

```

*CISCO Confidential - DRAFT*

## Disabling Loop Guard

Enter the **set spantree guard** command to disable the spanning tree loop guard feature on a per-port basis. To disable loop guard on all the ports on a switch, use the **set spantree mst global-defaults loop-guard** command.

To disable loop guard on the switch, perform this task in privileged mode:

|        | Task                                | Command                                                              |
|--------|-------------------------------------|----------------------------------------------------------------------|
| Step 1 | Disable loop guard on a port.       | <b>set spantree guard {root   loop   none} mod/port</b>              |
| Step 2 | Verify that loop guard is disabled. | <b>show spantree guard {mod/port   vlan} mistp-instance instance</b> |

This example shows how to disable loop guard on port 5/1:

```
Console> (enable) set spantree guard none 5/1
Rootguard is disabled on port 5/1, disabling loopguard will disable rootguard on
this port.
Do you want to continue (y/n) [n]? y
Loopguard on port 5/1 is disabled.
Console> (enable)
```

This example shows how to disable loop guard on all the ports on a switch:

```
Console> (enable) set spantree mst global-defaults loop-guard disable
Spantree global loop-guard state disabled on this switch.
```

*CISCO Confidential - DRAFT*

## Configuring VTP

This chapter describes how to configure the VLAN Trunking Protocol (VTP) on the Catalyst enterprise LAN switches.

**Note**

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 4500 Series, Catalyst 2948G, and Catalyst 2980G Switches Command Reference*.

This chapter consists of these sections:

- [Understanding How VTP Works, page 9-1](#)
- [Default VTP Configuration, page 9-5](#)
- [VTP Configuration Guidelines, page 9-5](#)
- [Configuring VTP on the Switch, page 9-5](#)
- [Displaying VTP Statistics, page 9-11](#)

## Understanding How VTP Works

Before you create virtual LANs (VLANs), you must decide whether to use VTP in your network. With VTP, you can make configuration changes centrally on one or more switches and have those changes automatically communicated to all the other switches in the network.

VTP is a Layer 2 messaging protocol that maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs on a network-wide basis. 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.

**Note**

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

The following sections describe how VTP works.

*CISCO Confidential - DRAFT*

## Understanding the VTP Domain

A VTP domain (also called a VLAN management domain) is made up of one or more interconnected switches that share the same VTP domain name. A switch can be configured to be in only one VTP domain. You make global VLAN configuration changes for the domain using either the command-line interface (CLI) or Simple Network Management Protocol (SNMP).

By default, the switch is in VTP server mode and is in the no-management domain state until the switch receives an advertisement for a domain over a trunk link or you configure a management domain. You cannot create or modify VLANs on a VTP server until the management domain name is specified or learned.

If the switch receives a VTP advertisement over a trunk link, it inherits the management domain name and the VTP configuration revision number. The switch remains in the first management domain learned unless changed by the user.

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 switches in the VTP domain. VTP advertisements are transmitted out on all IEEE 802.1Q 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 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 switches in the same VTP domain and synchronize their VLAN configuration with other switches 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 switches do not participate in VTP. A VTP transparent switch does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements. However, in VTP version 2, transparent switches do forward received VTP advertisements out their trunk ports.
- **Off**—In the three modes described above, VTP advertisements are received and transmitted as soon as the switch enters the management domain state. In VTP “off” mode, switches behave the same as in VTP transparent mode, except that VTP advertisements are not forwarded.

## Understanding VTP Advertisements

Each switch in the VTP domain sends periodic advertisements out each trunk port to a reserved multicast address. VTP advertisements are received by neighboring switches, which update their VTP and VLAN configurations as necessary except when in transparent mode.

The following global configuration information is distributed in VTP advertisements:



## *CISCO Confidential - DRAFT*

- VLAN IDs (802.1Q)
- 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. VTP version 2 supports the following features not supported in version 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 nonvolatile RAM (NVRAM).
- **Version-Dependent Transparent Mode**—In VTP version 1, a VTP transparent switch inspects VTP messages for the domain name and version and forwards a message only if the version and domain name match. Since 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.

Before you enable VTP pruning, make sure that all devices in the management domain support it.

[Figure 9-1](#) shows a switched network with VTP pruning disabled. Port 1 on 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 switch in the network receives it, even though Switches 3, 5, and 6 have no ports in the Red VLAN.

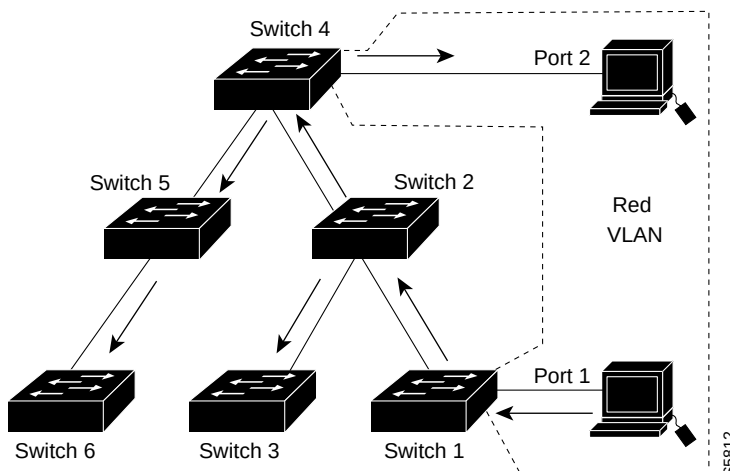
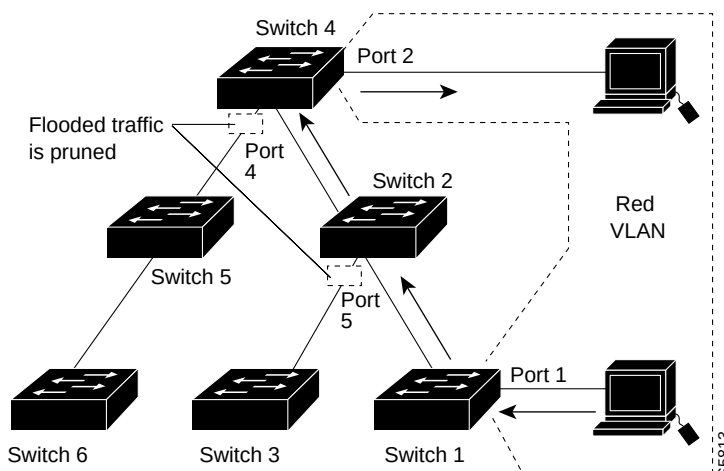
*CISCO Confidential - DRAFT***Figure 9-1 Flooding Traffic Without VTP Pruning**

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 eligible for pruning. VTP pruning does not prune traffic from VLANs that are ineligible for pruning. VLAN 1 is always ineligible for pruning; traffic from VLAN 1 cannot be pruned.

**Note**

You cannot enable VTP pruning on extended-range VLANs.

To make a VLAN ineligible for pruning, enter the **clear vtp pruning** command. To make a VLAN eligible for pruning again, enter the **set vtp pruneeligible** command. You can set VLAN pruning eligibility regardless of whether VTP pruning is enabled or disabled for the domain. Pruning eligibility always applies to the local device only, not for the entire VTP domain.

# Default VTP Configuration

Table 9-1 shows the default VTP configuration.

**Table 9-1 VTP Default Configuration**

| Feature                    | Default               |
|----------------------------|-----------------------|
| 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

This section describes the configuration guidelines for implementing VTP in your network:

- All switches in a VTP domain must run the same VTP version.
- You must configure a password on each switch in the management domain when in VTP 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 switch in the domain.

- A VTP version 2-capable switch can operate in the same VTP domain as a switch running VTP version 1, if that VTP version 2 is disabled on the VTP version 2-capable switch (VTP version 2 is disabled by default).
- Do not enable VTP version 2 on a switch unless all of the switches in the same VTP domain are version 2 capable. When you enable VTP version 2 on a switch, all of the version 2-capable switches in the domain enable VTP version 2.
- Enabling or disabling VTP pruning on a VTP server enables or disables VTP pruning for the entire management domain.
- Making VLANs eligible or ineligible for pruning on a switch affects pruning eligibility for those VLANs on that device only (not on all switches in the VTP domain).
- Extended-range VLANs are not propagated in the VTP domain. For complete information on VLANs, see [Chapter 10, “Configuring VLANs.”](#)

## Configuring VTP on the Switch

The following sections describe how to configure VTP.

*CISCO Confidential - DRAFT*

## Configuring a VTP Server

When a switch is in VTP server mode, you can change the VLAN configuration and have it propagate throughout the network.

To configure the switch as a VTP server, perform this task in privileged mode:

|        | Task                                          | Command                             |
|--------|-----------------------------------------------|-------------------------------------|
| Step 1 | Define the VTP domain name.                   | <b>set vtp domain</b> <i>name</i>   |
| Step 2 | Place the switch in VTP server mode.          | <b>set vtp mode server</b>          |
| Step 3 | (Optional) Set a password for the VTP domain. | <b>set vtp passwd</b> <i>passwd</i> |
| Step 4 | Verify the VTP configuration.                 | <b>show vtp domain</b>              |

This example shows how to configure the switch as a VTP server and verify the configuration:

```

Console> (enable) set vtp domain Lab_Network
VTP domain Lab_Network modified
Console> (enable) set vtp mode server
VTP domain Lab_Network modified
Console> (enable) show vtp domain
Domain Name Domain Index VTP Version Local Mode Password

Lab_Network 1 2 server -
Vlan-count Max-vlan-storage Config Revision Notifications

10 1023 40 enabled
Last Updater V2 Mode Pruning PruneEligible on Vlans

172.20.52.70 disabled disabled 2-1000
Console> (enable)

```

## Configuring a VTP Client

When a switch is in VTP client mode, you cannot change the VLAN configuration on the switch. The client switch receives VTP updates from a VTP server in the management domain and modifies its configuration accordingly.

*CISCO Confidential - DRAFT*

To configure the switch as a VTP client, perform this task in privileged mode:

|        | Task                                 | Command                           |
|--------|--------------------------------------|-----------------------------------|
| Step 1 | Define the VTP domain name.          | <b>set vtp domain</b> <i>name</i> |
| Step 2 | Place the switch in VTP client mode. | <b>set vtp mode client</b>        |
| Step 3 | Verify the VTP configuration.        | <b>show vtp domain</b>            |

This example shows how to configure the switch as a VTP client and verify the configuration:

```

Console> (enable) set vtp domain Lab_Network
VTP domain Lab_Network modified
Console> (enable) set vtp mode client
VTP domain Lab_Network modified
Console> (enable) show vtp domain
Domain Name Domain Index VTP Version Local Mode Password

Lab_Network 1 2 client -
Vlan-count Max-vlan-storage Config Revision Notifications

10 1023 40 enabled
Last Updater V2 Mode Pruning PruneEligible on Vlans

172.20.52.70 disabled disabled 2-1000
Console> (enable)

```

## Configuring VTP Transparent Mode

When you configure the switch as VTP transparent, you disable VTP on the switch. A VTP transparent switch does not send VTP updates and does not act on VTP updates that are received from other switches. However, a VTP transparent switch running VTP version 2 does forward received VTP advertisements out all of its trunk links.

To disable VTP on the switch, perform this task in privileged mode:

|        | Task                                                                    | Command                         |
|--------|-------------------------------------------------------------------------|---------------------------------|
| Step 1 | Place the switch in VTP transparent mode (disabling VTP on the switch). | <b>set vtp mode transparent</b> |
| Step 2 | Verify the VTP configuration.                                           | <b>show vtp domain</b>          |

This example shows how to configure the switch as VTP transparent and verify the configuration:

```

Console> (enable) set vtp mode transparent
VTP domain Lab_Net modified
Console> (enable) show vtp domain
Domain Name Domain Index VTP Version Local Mode Password

Lab_Net 1 2 Transparent -
Vlan-count Max-vlan-storage Config Revision Notifications

10 1023 0 enabled
Last Updater V2 Mode Pruning PruneEligible on Vlans

172.20.52.70 disabled disabled 2-1000
Console> (enable)

```

*CISCO Confidential - DRAFT*

## Disabling VTP Using the Off Mode

When you disable VTP using the **off** mode, the switch behaves the same as in VTP transparent mode with the exception that VTP advertisements are not forwarded.

To disable VTP using the **off** mode, perform this task in privileged mode:

|        | Task                            | Command                 |
|--------|---------------------------------|-------------------------|
| Step 1 | Disable VTP using the off mode. | <b>set vtp mode off</b> |
| Step 2 | Verify the VTP configuration.   | <b>show vtp domain</b>  |

This example shows how to disable VTP using the off mode:

```

Console> (enable) set vtp mode off
VTP domain Lab_Net modified
Console> (enable) show vtp domain
Domain Name Domain Index VTP Version Local Mode Password

Lab_Net 1 2 off -
Vlan-count Max-vlan-storage Config Revision Notifications

10 1023 0 enabled
Last Updater V2 Mode Pruning PruneEligible on Vlans

172.20.52.70 disabled disabled 2-1000
Console> (enable)

```

## Enabling VTP Version 2

VTP version 2 is disabled by default on VTP version 2-capable switches. When you enable VTP version 2 on a switch, every VTP version 2-capable switch in the VTP domain also will enable version 2.



### Caution

VTP version 1 and VTP version 2 are not interoperable on switches in the same VTP domain. Every switch in the VTP domain must use the same VTP version. Do not enable VTP version 2 unless every switch in the VTP domain supports version 2.

To enable VTP version 2, perform this task in privileged mode:

|        | Task                                  | Command                  |
|--------|---------------------------------------|--------------------------|
| Step 1 | Enable VTP version 2 on the switch.   | <b>set vtp v2 enable</b> |
| Step 2 | Verify that VTP version 2 is enabled. | <b>show vtp domain</b>   |

This example shows how to enable VTP version 2 and verify the configuration:

```

Console> (enable) set vtp v2 enable
This command will enable the version 2 function in the entire management domain.
All devices in the management domain should be version2-capable before enabling.
Do you want to continue (y/n) [n]? y
VTP domain Lab_Net modified
Console> (enable) show vtp domain
Domain Name Domain Index VTP Version Local Mode Password

```

*CISCO Confidential - DRAFT*

```

Lab_Net 1 2 server -
Vlan-count Max-vlan-storage Config Revision Notifications

10 1023 1 enabled
Last Updater V2 Mode Pruning PruneEligible on Vlans

172.20.52.70 enabled disabled 2-1000
Console> (enable)

```

## Disabling VTP Version 2

To disable VTP version 2, perform this task in privileged mode:

|        | Task                                   | Command                   |
|--------|----------------------------------------|---------------------------|
| Step 1 | Disable VTP version 2.                 | <b>set vtp v2 disable</b> |
| Step 2 | Verify that VTP version 2 is disabled. | <b>show vtp domain</b>    |

This example shows how to disable VTP version 2:

```

Console> (enable) set vtp v2 disable
This command will disable the version 2 function in the entire management domain.
Warning: trbrf & trcrf vlans will not work properly in this mode.
Do you want to continue (y/n) [n]? y
VTP domain Lab_Net modified
Console> (enable)

```

## Configuring VTP Pruning

To configure VTP pruning, perform this task in privileged mode:

|        | Task                                                                                                                 | Command                                 |
|--------|----------------------------------------------------------------------------------------------------------------------|-----------------------------------------|
| Step 1 | Enable VTP pruning in the management domain.                                                                         | <b>set vtp pruning enable</b>           |
| Step 2 | (Optional) Make specific VLANs pruning ineligible on the device.<br>(By default, VLANs 2–1000 are pruning eligible.) | <b>clear vtp pruning vlan_range</b>     |
| Step 3 | (Optional) Make specific VLANs pruning eligible on the device.                                                       | <b>set vtp pruneeligible vlan_range</b> |
| Step 4 | Verify the VTP pruning configuration.                                                                                | <b>show vtp domain</b>                  |
| Step 5 | Verify that the appropriate VLANs are being pruned on trunk ports.                                                   | <b>show trunk</b>                       |

This example shows how to enable VTP pruning in the management domain and how to make VLANs 2–99, 250–255, and 501–1000 pruning eligible on the particular device:

```

Console> (enable) set vtp pruning enable
This command will enable the pruning function in the entire management domain.
All devices in the management domain should be pruning-capable before enabling.
Do you want to continue (y/n) [n]? y
VTP domain Lab_Network modified
Console> (enable) clear vtp pruneeligible 100-500
Vlans 1,100-500,1001-1005 will not be pruned on this device.
VTP domain Lab_Network modified.
Console> (enable) set vtp pruning 250-255
Vlans 2-99,250-255,501-1000 eligible for pruning on this device.

```

*CISCO Confidential - DRAFT*

VTP domain Lab\_Network modified.

Console> (enable) **show vtp domain**

```

Domain Name Domain Index VTP Version Local Mode Password

Lab_Network 1 2 server -

Vlan-count Max-vlan-storage Config Revision Notifications

8 1023 16 disabled

Last Updater V2 Mode Pruning PruneEligible on Vlans

172.20.52.2 disabled enabled 2-99,250-255,501-1000

```

Console> (enable) **show trunk**

\* - indicates vtp domain mismatch

```

Port Mode Encapsulation Status Native vlan

2/1 on dot1q trunking 1

```

Port Vlans allowed on trunk

```

2/1 1-1005

```

Port Vlans allowed and active in management domain

```

2/1 1

```

Port Vlans in spanning tree forwarding state and not pruned

```

2/1 1

```

Console> (enable)

## Disabling VTP Pruning

To disable VTP pruning, perform this task in privileged mode:

|        | Task                                          | Command                        |
|--------|-----------------------------------------------|--------------------------------|
| Step 1 | Disable VTP pruning in the management domain. | <b>set vtp pruning disable</b> |
| Step 2 | Verify that VTP pruning is disabled.          | <b>show vtp domain</b>         |

This example shows how to disable VTP pruning in the management domain:

Console> (enable) **set vtp pruning disable**

This command will disable the pruning function in the entire management domain.

Do you want to continue (y/n) [n]? **y**

VTP domain Lab\_Network modified

Console> (enable)



*CISCO Confidential - DRAFT*

## Displaying VTP Statistics

To display VTP statistics, including VTP advertisements that are sent and received and VTP errors, perform this task in privileged mode:

| Task                                   | Command                    |
|----------------------------------------|----------------------------|
| Display VTP statistics for the switch. | <b>show vtp statistics</b> |

This example shows how to display VTP statistics on the switch:

```

Console> (enable) show vtp statistics
VTP statistics:
summary advts received 4690
subset advts received 7
request advts received 0
summary advts transmitted 4397
subset advts transmitted 8
request advts transmitted 0
No of config revision errors 0
No of config digest errors 0
VTP pruning statistics:
Trunk Join Transmitted Join Received Summary advts received from

1/1 0 0 0
1/2 0 0 0
non-pruning-capable device
Console> (enable)

```

*CISCO Confidential - DRAFT*

## Configuring VLANs

This chapter describes how to configure virtual LANs (VLANs) on the Catalyst enterprise LAN switches.

**Note**

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 4500 Series, Catalyst 2948G, and Catalyst 2980G Switches Command Reference*.

This chapter contains these sections:

- [Understanding How VLANs Work, page 10-1](#)
- [VLAN Default Configuration, page 10-4](#)
- [VLAN Configuration Guidelines, page 10-4](#)
- [Configuring VLANs on the Switch, page 10-5](#)
- [Configuring Auxiliary VLANs, page 10-12](#)
- [Configuring Private VLANs, page 10-15](#)

## Understanding How VLANs Work

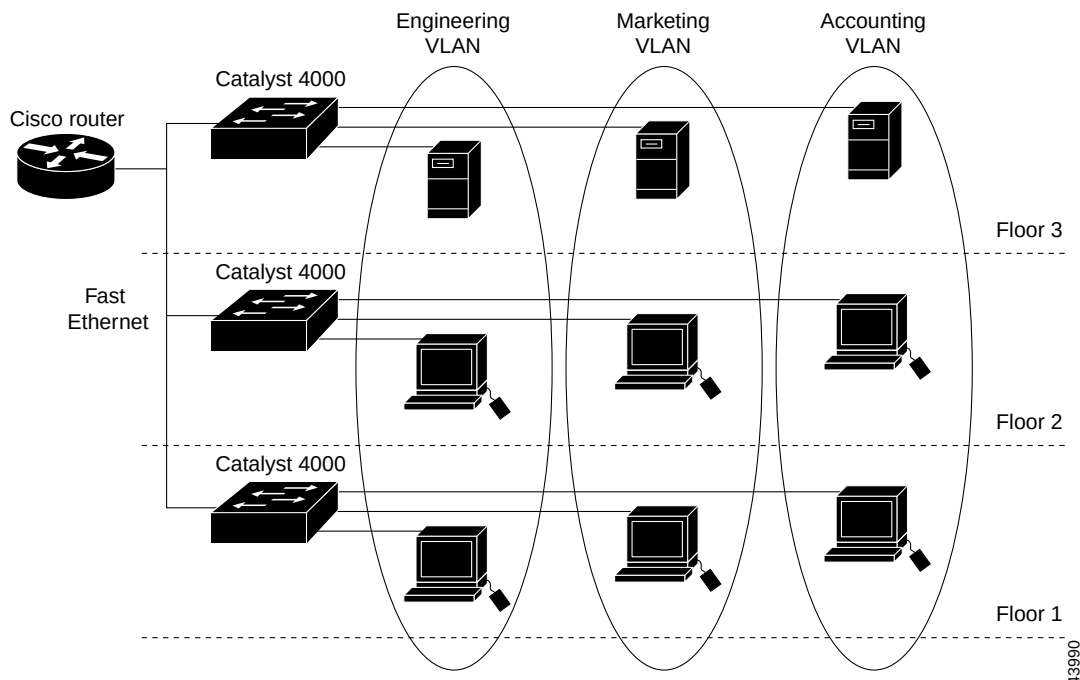
A VLAN is a group of end stations with a common set of requirements, independent of physical location. A VLAN has the same attributes as a physical LAN, but allows you to group end stations even if the VLANs are not located physically on the same LAN segment.

VLANs allow you to group ports on a switch to limit unicast, multicast, and broadcast traffic flooding. Flooded traffic originating from a particular VLAN is only flooded out other ports belonging to that VLAN.

**Note**

Before you create VLANs, you must decide whether to use VTP or VMPS to maintain global VLAN configuration information for your network. For complete information on VTP, see [Chapter 9, “Configuring VTP”](#). For complete information on VMPS, see [Chapter 12, “Configuring Dynamic VLAN Membership with VMPS.”](#)

[Figure 10-1](#) shows an example of VLANs segmented into logically defined networks.

*CISCO Confidential - DRAFT***Figure 10-1 VLANs as Logically Defined Networks**

VLANs are often 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. Port VLAN membership on the switch is assigned manually on a port-by-port basis. When you assign switch ports to VLANs using this method, it is known as port-based, or static, VLAN membership.

The in-band (sc0) interface of a switch can be assigned to any VLAN, so that you can access another switch on the same VLAN directly without a router. Only one IP address at a time can be assigned to the in-band interface. If you change the IP address and assign the interface to a different VLAN, the previous IP address and VLAN assignment are overwritten.

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

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

**Note**

When translating from one VLAN type to another, you must create a different VLAN number for each media type.

*CISCO Confidential - DRAFT*

## VLAN Ranges

Catalyst 4000 family 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 a management protocol, such as the VLAN Trunking Protocol (VTP). Other VLANs are not propagated, and you must configure them on each applicable switch.

There are three ranges of VLANs:

- Normal-range VLANs: 1–1000
- Extended-range VLANs: 1025–4094
- Reserved-range VLANs: 0, 1002–1024, 4095

Table 10-1 describes the VLAN ranges.

**Table 10-1 VLAN Ranges**

| VLAN Number | Range    | Usage                                                                                                                  | Propagated by VTP ? |
|-------------|----------|------------------------------------------------------------------------------------------------------------------------|---------------------|
| 0, 4095     | Reserved | For system use only. You cannot see or use these VLANs.                                                                | N/A                 |
| 1           | Normal   | Cisco default. You can use this VLAN, but you cannot delete it.                                                        | Yes                 |
| 2–1000      | Normal   | Used for Ethernet VLANs; you can create, use, and delete these VLANs.                                                  | Yes                 |
| 1001        | Normal   | You cannot create or use this VLAN.                                                                                    | Yes                 |
| 1002–1005   | Reserved | Cisco defaults for FDDI and Token Ring. Not supported on Catalyst 4000 family switches. You cannot delete these VLANs. | N/A                 |
| 1006–1009   | Reserved | Cisco defaults. Not currently used. You can map nonreserved VLANs to these reserved VLANs when necessary.              | N/A                 |
| 1010–1024   | Reserved | You cannot see or use these VLANs, but you can map nonreserved VLANs to these reserved VLANs when necessary.           | N/A                 |
| 1025–4094   | Extended | For Ethernet VLANs only. You can create, use, and delete these VLANs.                                                  | No                  |

## Configurable VLAN Parameters

When you create VLANs 2–1000 or modify VLANs 2–1005, you can set the parameters as follows:

- VLAN number
- VLAN name
- VLAN type: Ethernet, FDDI, and FDDINET
- VLAN state: active or suspended
- Multi-Instance Spanning Tree Protocol (MISTP) instance
- Private VLAN type: primary, isolated, community, two-way community, or none

*CISCO Confidential - DRAFT*

- SAID
- MTU for the VLAN
- VLAN to use when translating from one VLAN media type to another (VLANs 1–1005 only); requires a different VLAN number for each media type
- Remote Switched Port Analyzer (RSPAN)

**Note**

Ethernet VLANs 1 and 1025–4094 can use the defaults only.

## VLAN Default Configuration

Table 10-2 shows the default VLAN configuration.

**Table 10-2** VLAN Default Configuration

| Feature               | Default Value                                                              |
|-----------------------|----------------------------------------------------------------------------|
| Native (default) VLAN | VLAN 1                                                                     |
| Port VLAN assignments | All ports assigned to VLAN 1                                               |
| VLAN state            | Enabled                                                                    |
| MTU size              | 1500 bytes                                                                 |
| SAID value            | 100,000 plus the VLAN number (for example, the SAID for VLAN 3 is 100,003) |
| Pruning eligibility   | VLANs 2–1000 are eligible for pruning                                      |

## VLAN Configuration Guidelines

This section describes the configuration guidelines for creating and modifying VLANs in your network:

- Before you can create a normal-range VLAN, the switch must be in VTP server mode or VTP transparent mode. If the switch is a VTP server, you must define a VTP domain. For information on configuring VTP, see [Chapter 9, “Configuring VTP.”](#)
- Since VTP does not work on extended-range VLANs, you can create extended-range VLANs (1025–4094) even when the VTP mode is set to client.
- You can create normal-range VLANs one at a time or you can create a range of VLANs.
- You cannot specify a VLAN name when you create a VLAN range, because VLAN names must be unique.
- VLAN numbers are always ISL VLAN identifiers, not 802.1Q VLAN identifiers.
- Always specify a VLAN type when configuring the VLAN. By default, the VLAN will be an Ethernet VLAN.

Consider the following when creating or modifying extended-range VLANs:

- You can create only extended-range Ethernet VLANs.
- You can create and delete only extended-range VLANs from the CLI or SNMP.
- You cannot use VTP to manage these VLANs; they must be statically configured on each switch.

*CISCO Confidential - DRAFT*

- You cannot use extended-range VLANs if you have dot1q-to-isl mappings.
- You can configure private VLAN parameters and RSPAN for extended-range VLANs; however, all other parameters for extended-range VLANs use the system defaults only.

**Note**

The Catalyst 4000 family switch 10/100 Ethernet switching modules support auxiliary VLANs in software release 5.5(1) and later releases. You can plug an externally powered IP phone into a 10/100 port and then add that port to an auxiliary VLAN using the **set port auxiliaryvlan** command. For complete details on configuring auxiliary VLANs, see the [“Configuring Auxiliary VLANs” section on page 12](#).

## Configuring VLANs on the Switch

VLANs are either normal range or extended range. VLANs in the normal range are VLANs 2–1000. VLANs in the extended range are VLANs 1025–4094.

When you configure normal-range VLANs, VLANs 2–1000, you can configure one VLAN at a time or a range of VLANs, all with a single command. If you configure a range of VLANs, you cannot specify a name, because VLAN names must be unique.

**Note**

You cannot configure or modify normal-range VLAN 1.

You can use VTP to manage global normal-range VLAN configuration information on your network, but you cannot manage extended-range VLAN configuration information. In order to use VTP, you must configure it before you create any normal-range VLANs. For more information about configuring VTP, see [Chapter 9, “Configuring VTP.”](#)

Before configuring extended-range VLANs, VLANs 1025–4094, you must first enable MAC address reduction. When you enable MAC address reduction the system commits the IDs for extended-range VLANs. After you enable MAC address reduction you cannot disable it as long as any extended-range VLANs exist.

**Note**

If you wish to use extended-range VLANs and you have existing 802.1Q-to-isl mappings in your system, you must first delete the mappings. See the [“Clearing 802.1Q-to-isl VLAN Mappings” section on page 10-11](#) for more information.

## Creating or Modifying an Ethernet VLAN

To create a new Ethernet VLAN, perform this task in privileged mode:

|        | Task                           | Command                                                                                                                                                  |
|--------|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Create a new Ethernet VLAN.    | <b>set vlan</b> <i>vlan_num</i> [ <b>name</b> <i>name</i> ] [ <b>said</b> <i>said</i> ] [ <b>mtu</b> <i>mtu</i> ] [ <b>translation</b> <i>vlan_num</i> ] |
| Step 2 | Verify the VLAN configuration. | <b>show vlan</b> [ <i>vlan_num</i> ]                                                                                                                     |

*CISCO Confidential - DRAFT***Note**

The default VLAN type is Ethernet; if you do not specify the type, the VLAN is an Ethernet VLAN.

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

```

Console> (enable) set vlan 500 name Engineering
Vlan 500 configuration successful
Console> (enable) show vlan 500
VLAN Name Status IfIndex Mod/Ports, Vlans

500 Engineering active 344
VLAN Type SAID MTU Parent RingNo BrdgNo Stp BrdgMode Trans1 Trans2

500 enet 100500 1500 - - - - - 0 0
VLAN AREHops STEHops Backup CRF

Console> (enable)

```

To modify the VLAN parameters on an existing Ethernet VLAN, perform this task in privileged mode:

|        | Task                              | Command                                                                                                                                                                                                     |
|--------|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Modify an existing Ethernet VLAN. | <b>set vlan</b> <i>vlan_num</i> [ <b>name</b> <i>name</i> ] [ <b>state</b> { <b>active</b>   <b>suspend</b> }] [ <b>said</b> <i>said</i> ] [ <b>mtu</b> <i>mtu</i> ] [ <b>translation</b> <i>vlan_num</i> ] |
| Step 2 | Verify the VLAN configuration.    | <b>show vlan</b> [ <i>vlan_num</i> ]                                                                                                                                                                        |

This example shows how to change the vlan 500 name from Engineering to Development and verify the configuration:

```

Console> (enable) set vlan 500 name Development
Vlan 500 configuration successful
Console> (enable) show vlan 500
VLAN Name Status IfIndex Mod/Ports, Vlans

500 Development active 344
VLAN Type SAID MTU Parent RingNo BrdgNo Stp BrdgMode Trans1 Trans2

500 enet 100500 1500 - - - - - 0 0
VLAN AREHops STEHops Backup CRF

Console> (enable)

```

## Creating or Modifying a Normal-Range Ethernet VLAN

To create a normal-range Ethernet VLAN, perform this task in privileged mode:

|        | Task                                 | Command                                                                                                                                          |
|--------|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Create a normal-range Ethernet VLAN. | <b>set vlan</b> <i>vlan</i> [ <b>name</b> <i>name</i> ] [ <b>said</b> <i>said</i> ] [ <b>mtu</b> <i>mtu</i> ] [ <b>translation</b> <i>vlan</i> ] |
| Step 2 | Verify the VLAN configuration.       | <b>show vlan</b> [ <i>vlan</i> ]                                                                                                                 |



*CISCO Confidential - DRAFT*

This example shows how to create normal-range VLANs when the switch is in per-VLAN spanning tree + (PVST+) mode:

```
Console> (enable) set vlan 500-520
Vlan 500 configuration successful
Vlan 501 configuration successful
Vlan 502 configuration successful
Vlan 503 configuration successful
.
.
.
Vlan 520 configuration successful
Console> (enable)
```

This example shows how to verify that the switch is in PVST+ mode:

```
Console> (enable) show vlan 500-520
VLAN Name Status IfIndex Mod/Ports, Vlans

500 active 342
501 active 343
502 active 344
503 active 345
.
.
.
520 active 362
VLAN Type SAID MTU Parent RingNo BrdgNo Stp BrdgMode Trans1 Trans2

500 enet 100500 1500 - - - - - 0 0
501 enet 100501 1500 - - - - - 0 0
502 enet 100502 1500 - - - - - 0 0
503 enet 100503 1500 - - - - - 0 0
.
.
.
520 enet 100520 1500 - - - - - 0 0
VLAN AREHops STEHops Backup CRF

Console> (enable)
```

To modify VLAN parameters on an existing normal-range VLAN, perform this task in privileged mode:

|        | Task                                  | Command                                                                                                                                                                                             |
|--------|---------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Modify an existing normal-range VLAN. | <b>set vlan</b> <i>vlan</i> [ <b>name</b> <i>name</i> ] [ <b>state</b> { <b>active</b>   <b>suspend</b> }] [ <b>said</b> <i>said</i> ] [ <b>mtu</b> <i>mtu</i> ] [ <b>translation</b> <i>vlan</i> ] |
| Step 2 | Verify the VLAN configuration.        | <b>show vlan</b> [ <i>vlan</i> ]                                                                                                                                                                    |

This example shows how to change the state of an Ethernet VLAN and verify the configuration:

```
Console> (enable) set vlan 500 state suspend
Vlan 500 configuration successful
Console> (enable) show vlan 500
VLAN Name Status IfIndex Mod/Ports, Vlans

500 Engineering suspend 344
VLAN Type SAID MTU Parent RingNo BrdgNo Stp BrdgMode Trans1 Trans2

500 enet 100500 1500 - - - - - 0 0
VLAN AREHops STEHops Backup CRF

Console> (enable)
```

*CISCO Confidential - DRAFT*

## Creating or Modifying an Extended-Range VLAN

To create an extended-range Ethernet VLAN, perform this task in privileged mode:

|        | Task                           | Command                                             |
|--------|--------------------------------|-----------------------------------------------------|
| Step 1 | Enable MAC address reduction.  | <b>set spantree macreduction {enable   disable}</b> |
| Step 2 | Create a VLAN.                 | <b>set vlan vlan</b>                                |
| Step 3 | Verify the VLAN configuration. | <b>show vlan [vlan]</b>                             |

This example shows how to enable MAC address reduction and create an extended-range Ethernet VLAN:

```

Console> (enable) set spantree macreduction enable
MAC address reduction enabled
Console> (enable) set vlan 2000
Vlan 2000 configuration successful
Console> (enable) show vlan 2000
VLAN Name Status IfIndex Mod/Ports, Vlans

2000 VLAN2000 active 61

VLAN Type SAID MTU Parent RingNo BrdgNo Stp BrdgMode Trans1 Trans2

2000 enet 102000 1500 - - - - - 0 0

VLAN Inst DynCreated RSPAN

2000 - static disabled

VLAN AREHops STEHops Backup CRF 1q VLAN

Console> (enable)

```

To modify the VLAN parameters on an existing extended-range VLAN, perform this task in privileged mode:

|        | Task                                    | Command                                                                                              |
|--------|-----------------------------------------|------------------------------------------------------------------------------------------------------|
| Step 1 | Modify an existing extended-range VLAN. | <b>set vlan vlan [name name] [state {active   suspend}] [said said] [mtu mtu] [translation vlan]</b> |
| Step 2 | Verify the VLAN configuration.          | <b>show vlan [vlan]</b>                                                                              |

This example shows how to change the state of an extended-range Ethernet VLAN and verify the configuration:

```

Console> (enable) set vlan 2000 state suspend
Vlan 2000 configuration successful
Console> (enable) show vlan 2000
VLAN Name Status IfIndex Mod/Ports, Vlans

2000 VLAN2000 suspend 61

VLAN Type SAID MTU Parent RingNo BrdgNo Stp BrdgMode Trans1 Trans2

2000 enet 102000 1500 - - - - - 0 0

```

*CISCO Confidential - DRAFT*

```

VLAN Inst DynCreated RSPAN

2000 - static disabled

VLAN AREHops STEHops Backup CRF 1q VLAN

Console> (enable)

```

## Assigning Switch Ports to a VLAN

A VLAN created in a management domain remains unused until you assign one or more switch ports to the VLAN. If you specify a VLAN that does not exist, the VLAN is created and the specified ports are assigned to it.

To assign one or more switch ports to a VLAN, perform this task in privileged mode:

|        | Task                                       | Command                                                                                         |
|--------|--------------------------------------------|-------------------------------------------------------------------------------------------------|
| Step 1 | Assign one or more switch ports to a VLAN. | <b>set vlan</b> <i>vlan_num</i> <i>mod_num/port_num</i>                                         |
| Step 2 | Verify the port VLAN membership.           | <b>show vlan</b> [ <i>vlan_num</i> ]<br><b>show port</b> [ <i>mod_num</i> [/ <i>port_num</i> ]] |

This example shows how to assign switch ports to a VLAN and verify the assignment:

```

Console> (enable) set vlan 500 2/4
VLAN 500 modified.
VLAN 560 modified.
VLAN Mod/Ports

500 2/4
Console> (enable) show vlan 500
VLAN Name Status IfIndex Mod/Ports, Vlans

500 Engineering active 59 2/4

VLAN Type SAID MTU Parent RingNo BrdgNo Stp BrdgMode Trans1 Trans2

500 enet 100500 1500 - - - - - 0 0

VLAN AREHops STEHops Backup CRF

Console> (enable) show port 2/4
Port Name Status Vlan Level Duplex Speed Type

2/4 notconnect 500 normal auto auto 10/100BaseTX

Port Security Secure-Src-Addr Last-Src-Addr Shutdown Trap IfIndex

2/4 disabled No disabled 12

Port Status Channel Channel Neighbor Neighbor
 mode status device port

2/4 notconnect auto not channel

```

## CISCO Confidential - DRAFT

```

Port Align-Err FCS-Err Xmit-Err Rcv-Err UnderSize

2/4 - 0 0 0 0

Port Single-Col Multi-Coll Late-Coll Excess-Col Carri-Sen Runts Giants

2/4 0 0 0 0 0 0 0

Last-Time-Cleared

Wed Jul 26 2000, 19:44:05
Console> (enable)

```

## Mapping 802.1Q VLANs to ISL VLANs

The valid range of user-configurable ISL VLANs is 1–1000. The valid range of VLANs specified in the IEEE 802.1Q standard is 0–4095. In a network environment with non-Cisco devices that are connected to Cisco switches through 802.1Q trunks, you must map 802.1Q VLAN numbers greater than 1000 to ISL VLAN numbers.

802.1Q VLANs in the range 1–1000 are automatically mapped to the corresponding ISL VLAN. 802.1Q VLAN numbers greater than 1000 must be mapped to an ISL VLAN in order to be recognized and forwarded by Cisco switches.

These restrictions apply when mapping 802.1Q VLANs to ISL VLANs:

- You can configure up to seven 802.1Q-to-ISL VLAN mappings on the switch.
- You must 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 2000 to ISL VLAN 200, traffic on 802.1Q VLAN 200 is blocked.
- VLAN mappings are local to each switch. Make sure that you configure the same VLAN mappings on all appropriate switches in the network.
- You cannot use dot1q-to-isl mappings if you have extended-range VLANs.

To map an 802.1Q VLAN to an ISL VLAN, perform this task in privileged mode:

|        | Task                                                                                                                                           | Command                                                             |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------|
| Step 1 | Map an 802.1Q VLAN to an ISL Ethernet VLAN. The valid range for <i>dot1q_vlan</i> is 1001–4095. The valid range for <i>isl_vlan</i> is 1–1000. | <b>set vlan mapping dot1q <i>dot1q_vlan</i> isl <i>isl_vlan</i></b> |
| Step 2 | Verify the VLAN mapping.                                                                                                                       | <b>show vlan mapping</b>                                            |

This example shows how to map 802.1Q VLANs 2000, 3000, and 4000 to ISL VLANs 200, 300, and 400 and how to verify the configuration:

```

Console> (enable) set vlan mapping dot1q 2000 isl 200
802.1q vlan 2000 is existent in the mapping table
Console> (enable) set vlan mapping dot1q 3000 isl 300
Vlan mapping successful
Console> (enable) set vlan mapping dot1q 4000 isl 400
Vlan mapping successful
Console> (enable) show vlan mapping

```

*CISCO Confidential - DRAFT*

| 802.1q vlan | ISL vlan | Effective |
|-------------|----------|-----------|
| 2000        | 200      | true      |
| 3000        | 300      | true      |
| 4000        | 400      | true      |

Console> (enable)

## Clearing 802.1Q-to-ISL VLAN Mappings

To clear an 802.1Q-to-ISL VLAN mapping, perform this task in privileged mode:

|        | Task                                 | Command                                            |
|--------|--------------------------------------|----------------------------------------------------|
| Step 1 | Clear an 802.1Q-to-ISL VLAN mapping. | <b>clear vlan mapping dot1q {dot1q_vlan   all}</b> |
| Step 2 | Verify the VLAN mapping.             | <b>show vlan mapping</b>                           |

This example shows how to clear the VLAN mapping for 802.1Q VLAN 2000:

```
Console> (enable) clear vlan mapping dot1q 2000
Vlan 2000 mapping entry deleted
Console> (enable)
```

This example shows how to clear all 802.1Q-to-ISL VLAN mappings:

```
Console> (enable) clear vlan mapping dot1q all
All vlan mapping entries deleted
Console> (enable)
```

## Deleting a VLAN

When you delete a VLAN in VTP server mode, the VLAN is removed from all switches in the VTP domain. When you delete a VLAN in VTP transparent mode, the VLAN is deleted only on the current switch. When you are on a VTP client, you can only delete a VLAN on the local switch.



### Caution

When you delete a VLAN, any ports that are assigned to that VLAN become inactive. Such ports remain associated with the VLAN (and thus, inactive) until you assign them to a new VLAN.

To delete a VLAN on the switch, perform this task in privileged mode:

| Task           | Command                    |
|----------------|----------------------------|
| Delete a VLAN. | <b>clear vlan vlan_num</b> |

This example shows how to delete a VLAN (in this case, the switch is a VTP server):

```
Console> (enable) clear vlan 500
This command will deactivate all ports on vlan 500
in the entire management domain
Do you want to continue (y/n) [n]?y
Vlan 500 deleted
Console> (enable)
```

*CISCO Confidential - DRAFT*

# Configuring Auxiliary VLANs

The following sections describe how to configure auxiliary VLANs to use with IP phones.

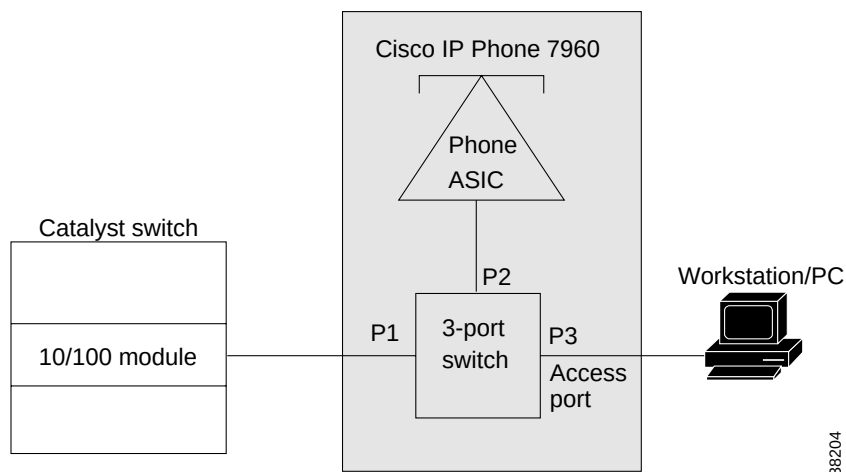
## Understanding Auxiliary VLANs

An IP phone contains an integrated three-port 10/100 switch. The ports, which are dedicated connections, are described as follows:

- Port 1 connects to the Catalyst 4500 series switch or other device that supports voice-over-IP.
- Port 2 is an internal 10/100 interface that carries the phone traffic.
- Port 3 connects to a PC or other device.

Figure 10-2 shows how you can connect a Cisco IP Phone to a Catalyst 4500 series switch.

**Figure 10-2 Switch-to-Phone Connections**



When the IP phone connects to a 10/100 port on the Catalyst 4500 series switch, the *access port* (PC-to-phone jack) of the IP phone can be used to connect a PC.

Packets to and from the PC and to and from the phone share the same physical link to the switch and the same port of the switch.

Introducing IP-based phones into existing switch-based networks raises the following issues:

- The current VLANs might be configured on an IP subnet basis and additional IP addresses might not be available to assign the phone to a port so that it belongs to the same subnet as other devices (PC) that are connected to the same port.
- Data traffic present on the VLAN supporting phones might reduce the quality of VoIP traffic.

You can resolve these issues by isolating the voice traffic onto a separate VLAN on each of the ports that are connected to a phone. The switch port that is configured for connecting a phone would have separate VLANs that are configured for carrying the following:

- Voice traffic to and from the IP phone (auxiliary VLAN)
- Data traffic to and from the PC that is connected to the switch through the access port of the IP phone (native VLAN)

## CISCO Confidential - DRAFT

Isolating the phones on a separate, auxiliary VLAN increases the quality of the voice traffic and allows a large number of phones to be added to an existing network where there are not enough IP addresses. A new VLAN means a new subnet and a new set of IP addresses.

You can configure switch ports to send CDP packets that instruct an attached Cisco IP Phone to transmit voice traffic to the switch in these frame types:

- 802.1Q frames carrying the auxiliary VLAN ID and Layer 2 CoS set to 5 (the switch port drops all 802.1Q frames except those carrying the auxiliary VLAN ID).
  - Reset the Cisco IP Phone if the auxiliary VLAN ID changes.
  - Enter the **set port auxiliaryvlan mod[/port] aux\_vlan\_id** command.



**Note** We recommend that you use 802.1Q frames and a separate VLAN.

- 802.1p frames, which are 802.1Q frames carrying VLAN ID 0 and Layer 2 CoS set to 5 (enter the **set port auxiliaryvlan mod[/port] dot1p** command)
- 802.3 frames, which are untagged and carry no VLAN ID and no Layer 2 CoS value (enter the **set port auxiliaryvlan mod[/port] untagged** command)



**Note** The Cisco IP Phone always sets Layer 3 IP precedence to 5 in voice traffic.

## Auxiliary VLAN Configuration Guidelines

This section describes the guidelines for configuring auxiliary VLANs:

- The IP phone and a device that is attached to the phone are in the same VLAN and must be in the same IP subnet if one of the following occurs:
  - They use the same frame type.
  - The phone uses 802.1p frames and the device uses untagged frames.
  - The phone uses untagged frames and the device uses 802.1p frames.
  - The phone uses 802.1Q frames and the auxiliary VLAN equals the native VLAN.
- The IP phone and a device that is attached to the 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 switch commands to configure a frame type that is used by traffic received from a device attached to the phone's access port.
- With software release 6.2(1) and later releases, dynamic ports can belong to two VLANs—a native VLAN and an auxiliary VLAN. See [Chapter 12, “Configuring Dynamic VLAN Membership with VMPS,”](#) for configuration details for auxiliary VLANs.

## Configuring Auxiliary VLANs

To configure auxiliary VLANs, perform this task in privileged mode:

*CISCO Confidential - DRAFT*

| Task                       | Command                                                                                                         |
|----------------------------|-----------------------------------------------------------------------------------------------------------------|
| Configure auxiliary VLANs. | <b>set port auxiliaryvlan</b> <i>mod[/ports]</i> { <i>vlan</i>   <b>untagged</b>   <b>dot1p</b>   <b>none</b> } |

This example shows how to add voice ports to auxiliary VLANs, specify an encapsulation type, or specify that the VLAN will not send or receive CDP messages with voice-related information:

```

Console> (enable) set port auxiliaryvlan 2/1-3 222
Auxiliaryvlan 222 configuration successful.
AuxiliaryVlan AuxVlanStatus Mod/Ports

222 active 1/2,2/1-3
Console> (enable) set port auxiliaryvlan 5/7 untagged
Port 5/7 allows the connected device send and receive untagged packets and without 802.1p
priority.
Console> (enable) set port auxiliaryvlan 5/9 dot1p
Port 5/9 allows the connected device send and receive packets with 802.1p priority.
Console> (enable) set port auxiliaryvlan 5/12 none
Port 5/12 will not allow sending CDP packets with Voice VLAN information.
Console> (enable)

```

The default setting is **none**. [Table 10-3](#) lists the **set port auxiliaryvlan** command keywords and their descriptions.

**Table 10-3 Keyword Descriptions**

| Keyword         | Action                                                                                             |
|-----------------|----------------------------------------------------------------------------------------------------|
| <b>dot1p</b>    | Specify that the phone send packets with 802.1p priority 5.                                        |
| <b>untagged</b> | Specify that the phone send untagged packets.                                                      |
| <b>none</b>     | Specify that the switch not send any auxiliary VLAN information in the CDP packets from that port. |

## Verifying Auxiliary VLAN Configuration

To verify auxiliary VLAN configuration status, perform this task in privileged mode:

| Task                                        | Command                                                                                       |
|---------------------------------------------|-----------------------------------------------------------------------------------------------|
| Verify auxiliary VLAN configuration status. | <b>show port auxiliaryvlan</b> { <i>vlan</i>   <b>untagged</b>   <b>dot1p</b>   <b>none</b> } |

This example shows how to verify auxiliary VLAN configuration status:

```

Console> show port auxiliaryvlan 123
AuxiliaryVlan AuxVlanStatus Mod/Ports

222 active 1/2,2/1-3
Console>

```



*CISCO Confidential - DRAFT*

## Configuring Private VLANs

A private VLAN is a VLAN that you configure to have some Layer 2 isolation from other ports within the same private VLAN. Ports belonging to a private VLAN are associated with a common set of supporting VLANs that are used to create the private VLAN structure. You can configure private VLANs and normal VLANs from the same Catalyst 4000 family switch.

The three types of private VLAN ports are as follows:

- A promiscuous port communicates with all other private VLAN ports and is the port that you use to communicate with routers, LocalDirector, the CSS11000, backup servers, and administrative workstations.
- An isolated port has complete Layer 2 separation, including broadcasts, from other ports within the same private VLAN with the exception of the promiscuous port.
- Community ports communicate among themselves and with their promiscuous ports. These ports are isolated at Layer 2 from all other ports in other communities or isolated ports within their private VLAN. Broadcasts propagate only between associated community ports and the promiscuous port.

Privacy is granted at the Layer 2 level because the switch blocks outgoing traffic to all isolated ports. You assign all isolated ports to an isolated VLAN where this hardware function occurs. Traffic that is received from an isolated port is forwarded to all promiscuous ports only.

Within a private VLAN are three distinct classifications of VLANs: a single primary VLAN, a single isolated VLAN, and a series of community VLANs.

You must define each supporting VLAN within a private VLAN structure before configuring the private VLAN as follows:

- Primary VLAN—Conveys incoming traffic from the promiscuous port to all other promiscuous, isolated, and community ports.
- Isolated VLAN—Used by isolated ports to communicate to the promiscuous ports. The traffic from an isolated port is blocked on all adjacent ports and can be received only by promiscuous ports.
- Community VLANs—Used by a group of community ports to communicate among themselves and transmit traffic outside the group through the designated promiscuous port.

To create a private VLAN, you assign two or more normal VLANs in the normal VLAN range. One VLAN is designated as a primary VLAN, and a second VLAN is designated as either an isolated VLAN, community VLAN, or two-way community VLAN. You can designate additional VLANs as separate isolated, community, or two-way community VLANs in this private VLAN. After designating the VLANs, you must bind them together and associate them to the promiscuous port.

You can extend private VLANs across multiple Ethernet switches by trunking the primary, isolated, and any community VLANs to other switches that support private VLANs.

In an Ethernet-switched environment, you can assign an individual VLAN and associated IP subnet to each individual or common group of stations. The servers only require the ability to communicate with a default gateway to gain access to end points outside the VLAN itself. By incorporating these stations, regardless of ownership, into one private VLAN, you can do the following:

- Designate the server ports as isolated to prevent any inter-server communication at Layer 2.
- Designate as promiscuous the ports to which the default gateway(s), backup server, or LocalDirector are attached, to allow all stations to have access to these gateways.

*CISCO Confidential - DRAFT*

- Reduce VLAN consumption. You need to allocate only one IP subnet to the entire group of stations, because all stations reside in one common private VLAN.
- Conserve public address space. Servers are now isolated from one another using private VLANs, which eliminates the need to create multiple IP subnets. Multiple IP subnets waste public IP addresses on multiple subnet and broadcast addresses. As a result, all servers can be members of the same IP subnet, but they remain isolated from one another.

## Private VLAN Configuration Guidelines

This section describes the configuration guidelines for configuring private VLANs:

- Designate one VLAN as the primary VLAN.
- Designate one VLAN as an isolated VLAN. If you want to use private VLAN communities, you need to designate a community VLAN for each community.
- Bind the isolated and/or community VLAN(s) to the primary VLAN and assign the isolated or community ports. You will achieve these results:
  - Isolated/community VLAN spanning tree properties are set to those of the primary VLAN.
  - VLAN membership becomes static.
  - Access ports become host ports.
  - BPDU guard protection is activated.
- Set up the automatic VLAN translation that maps the isolated and community VLANs to the primary VLAN on the promiscuous port(s). Set nontrunk ports as promiscuous ports.
- You must set VTP to transparent mode.
- Once you configure a private VLAN, you cannot change the VTP mode to client or server mode, because VTP does not support private VLAN types or mapping propagation.
- You can configure VLANs as primary, isolated, or community only if no access ports are currently assigned to the VLAN. Enter the **show port** command to verify that the VLAN has no access ports assigned to it.
- An isolated or community VLAN can have only one primary VLAN that is associated with it.
- Private VLANs can use VLANs 2–1000 and 1025–4096.
- If you delete either the primary or isolated VLAN, the ports that are associated with the VLAN become inactive.
- When configuring private VLANs, note these hardware and software restrictions:
  - You can use the sc0 interface in a private VLAN that is assigned to either an isolated or community VLAN, but not as a promiscuous port to a primary VLAN.
  - You cannot set private VLAN ports to trunking mode or channeling or have dynamic VLAN memberships. If you attempt such a configuration, a warning message is displayed and the command is rejected.
- Isolated and community ports should run BPDU guard features to prevent spanning tree loops that are caused by misconfigurations.
- Primary VLANs and associated isolated/community VLANs must have the same spanning tree configuration. This configuration maintains consistent spanning tree topologies among associated primary, isolated, and community VLANs and avoids connectivity loss. These priorities and parameters automatically propagate from the primary VLAN to isolated and community VLANs.

*CISCO Confidential - DRAFT*

- You can create private VLANs that run in MISTP mode.
  - If you disable MISTP, any change to the configuration of a private VLAN propagates to all corresponding isolated and community VLANs, and you cannot change the isolated or community VLANs.
  - If you enable MISTP, you can configure only the MISTP instance with the private VLAN. Changes are applied to the primary VLAN and propagate to isolated and community VLANs.
- In networks with some switches 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 double-check the STP configuration to ensure that the primary, isolated, and community VLANs spanning tree topologies match.
- If you enable MAC address reduction on a Catalyst 4000 family switch, you might want to enable MAC address reduction on all the switches in your network to ensure that the STP topologies of the private VLANs match. Otherwise, in a network where private VLANs are configured, if you enable MAC address reduction on some switches and disable it on others (mixed environment), you will have to 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 that are employed by the MAC address reduction feature regardless of whether it is enabled on the system. MAC address reduction allows only discrete levels, and it 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* that is used by any nonroot bridge.
- BPDU guard mode and UplinkFast affect the system and are automatically enabled once the first port is added to a private VLAN.
- You cannot configure a destination SPAN port as a private VLAN port, and vice versa.
- A source SPAN port can belong to a private VLAN.
- You can use VLAN-based SPAN (VSPAN) to span primary, isolated, and community VLANs together, or use SPAN on only one VLAN to separately monitor egress or ingress traffic.
- IGMP snooping and multicast shortcuts are not supported in private VLANs.
- You cannot enable EtherChannel on isolated, community, or promiscuous ports.
- You cannot set a VLAN to a private VLAN if the VLAN has dynamic access control entries (ACEs) that are configured on it.
- You can stop Layer 3 switching on an isolated or community VLAN by destroying the binding of that VLAN with its primary VLAN. Deleting the corresponding mapping is not sufficient.

## Creating a Private VLAN

You can bind isolated or community VLAN(s) to the primary VLAN without associating the isolated or community ports to the private VLAN by using the **set pvlan primary\_vlan\_num {isolated\_vlan\_num | community\_vlan\_num}** command.

You can change the isolated or community ports that are associated to the private VLAN without changing the isolated or community VLANs binding by using the **set pvlan primary\_vlan\_num {isolated\_vlan\_num | community\_vlan\_num} mod/port** command.

Ports do not have to be on the same switch as long as the switches are connected to the trunk and the private VLAN has not been removed from the trunk.

*CISCO Confidential - DRAFT*

You must enter the **set pvlan** command everywhere that a private VLAN needs to be created. This requirement includes entering the command on switches with isolated or community ports, switches with promiscuous ports, and all *intermediate* switches that need to carry private VLANs on their trunks. On the edge switches that do not have any isolated, community, or promiscuous ports (typically, access switches with no private ports), the private VLANs do not need to be created and can be pruned from the trunks for security reasons.

To create a private VLAN, perform this task in privileged mode:

|        | Task                                                                                                                            | Command                                                                                                                    |
|--------|---------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Create the primary VLAN.                                                                                                        | <b>set vlan</b> <i>vlan_num</i> <b>pvlan-type primary</b>                                                                  |
| Step 2 | Set the isolated or community VLAN(s).                                                                                          | <b>set vlan</b> <i>vlan_num</i> <b>pvlan-type</b> { <b>isolated</b>   <b>community</b> }                                   |
| Step 3 | Bind the isolated or community VLAN(s) to the primary VLAN and associate the isolated or community port(s) to the private VLAN. | <b>set pvlan</b> <i>primary_vlan_num</i> { <i>isolated_vlan_num</i>   <i>community_vlan_num</i> } <b>mod/ports</b>         |
| Step 4 | Map the isolated/community VLAN to the primary VLAN on the promiscuous port.                                                    | <b>set pvlan mapping</b> <i>primary_vlan_num</i> { <i>isolated_vlan_num</i>   <i>community_vlan_num</i> } <b>mod/ports</b> |
| Step 5 | Verify the private VLAN configuration.                                                                                          | <b>show pvlan</b> [ <i>vlan_num</i> ]<br><b>show pvlan mapping</b>                                                         |

This example shows how to create a private VLAN using VLAN 7 as the primary VLAN, VLAN 901 as the isolated VLAN, and VLANs 902 and 903 as the community VLANs. VLAN 901 uses module 4, port 3. VLAN 902 uses module 4, ports 4 through 6. VLAN 903 uses module 4, ports 7 through 9. The router is attached to the promiscuous port 3/1.

Before starting, verify that VLANs 7, 901, 902, and 903 have no ports that are assigned to them; do so by using the **show vlan** *vlan\_num* command. If any ports are assigned to one or more of these VLANs, set them to some other VLAN using the **set vlan** *vlan\_num* {*mod/port*} command.

This example shows how to specify VLAN 7 as the primary VLAN:

```
Console> (enable) set vlan 7 pvlan-type primary
Vlan 7 configuration successful
Console> (enable)
```

This example shows how to specify VLAN 901 as the isolated VLAN and VLANs 902 and 903 as the community VLANs:

```
Console> (enable) set vlan 901 pvlan-type isolated
Vlan 901 configuration successful
Console> (enable) set vlan 902 pvlan-type community
Vlan 902 configuration successful
Console> (enable) set vlan 903 pvlan-type community
Vlan 903 configuration successful
Console> (enable)
```

This example shows how to bind VLAN 901 to primary VLAN 7 and assign port 4/3 as the isolated port:

```
Console> (enable) set pvlan 7 901 4/3
Successfully set the following ports to Private Vlan 7,901: 4/3
Console> (enable)
```

*CISCO Confidential - DRAFT*

This example shows how to bind VLAN 902 to primary VLAN 7 and assign ports 4/4 through 4/6 as the community port:

```
Console> (enable) set pvlan 7 902 4/4-6
Successfully set the following ports to Private Vlan 7,902:4/4-6
Console> (enable)
```

This example shows how to bind VLAN 903 to primary VLAN 7 and assign port 4/7 through 4/9 as the community ports:

```
Console> (enable) set pvlan 7 903
Successfully set association between 7 and 903.
Console> (enable) set pvlan 7 903 4/7-9
Successfully set the following ports to Private Vlan 7,903:4/7-9
Console> (enable)
```

This example shows how to map the isolated/community VLAN to the primary VLAN on the promiscuous port, 3/1, for each isolated or community VLAN:

```
Console> (enable) set pvlan mapping 7 901 3/1
Successfully set mapping between 7 and 901 on 3/1
Console> (enable) set pvlan mapping 7 902 3/1
Successfully set mapping between 7 and 902 on 3/1
Console> (enable) set pvlan mapping 7 903 3/1
Successfully set mapping between 7 and 903 on 3/1
```

This example shows how to verify the private VLAN configuration:

```
Console> (enable) show vlan 7
```

| VLAN Name  | Status | IfIndex | Mod/Ports, Vlans |
|------------|--------|---------|------------------|
| 7 VLAN0007 | active | 35      | 4/4-6            |

```

VLAN Type SAID MTU Parent RingNo BrdgNo Stp BrdgMode Trans1 Trans2

7 enet 100010 1500 - - - - - 0 0
VLAN DynCreated RSPAN

7 static disabled
VLAN AREHops STEHops Backup CRF 1q VLAN

Primary Secondary Secondary-Type Ports

7 901 Isolated 4/3
7 902 Community 4/4-6
7 903 Community 4/7-9

```

```
Console> (enable) show vlan 902
```

| VLAN Name    | Status | IfIndex | Mod/Ports, Vlans |
|--------------|--------|---------|------------------|
| 902 VLAN0007 | active | 38      | 4/4-6            |

```

VLAN Type SAID MTU Parent RingNo BrdgNo Stp BrdgMode Trans1 Trans2

7 enet 100010 1500 - - - - - 0 0
VLAN DynCreated RSPAN

7 static disabled
VLAN AREHops STEHops Backup CRF 1q VLAN

Primary Secondary Secondary-Type Ports

7 902 Isolated 4/4-6

```

*CISCO Confidential - DRAFT*

```

Console> (enable) show pvlan
Primary Secondary Secondary-Type Ports

7 901 isolated 4/3
7 902 community 4/4-6
7 903 community 4/7-9
Console> (enable) show pvlan mapping
Port Primary Secondary

3/1 7 901-903
Console> (enable) show port
Port Name Status Vlan Duplex Speed Type

...truncated output...
4/3 notconnect 7,901 half 100 100BaseFX MM
4/4 notconnect 7,902 half 100 100BaseFX MM
4/5 notconnect 7,902 half 100 100BaseFX MM
4/6 notconnect 7,902 half 100 100BaseFX MM
4/7 notconnect 7,903 half 100 100BaseFX MM
4/8 notconnect 7,903 half 100 100BaseFX MM
4/9 notconnect 7,903 half 100 100BaseFX MM
... truncated output...

```

## Viewing the Port Capability of a Private VLAN Port

You can view the port capability of a port in a private VLAN by using the **show pvlan capability** command.

These examples show the port capability for several ports in the following configuration:

```

Console> (enable) set pvlan 10 20
Console> (enable) set pvlan mapping 10 20 3/1
Console> (enable) set pvlan mapping 10 20 5/2
Console> (enable) set trunk 5/1 desirable isl 1-1005,1025-4094
Console> (enable) show pvlan capability 5/20
Port 5/20 can be made a private vlan port.
Console> (enable) show pvlan
Primary Secondary Secondary-Type Ports

10 20 isolated
Console> (enable) show pvlan capability 3/1
Port 3/1 cannot be made a private vlan port due to:

Promiscuous ports cannot be made private vlan ports.

```

## Deleting a Private VLAN

You can delete a private VLAN by deleting the primary VLAN. If you delete a primary VLAN, all bindings to the primary VLAN are broken, all ports in the private VLAN become inactive, and any related mappings on the promiscuous port(s) are deleted.

To delete a private VLAN, perform this task in privileged mode:

| Task                   | Command                        |
|------------------------|--------------------------------|
| Delete a primary VLAN. | <b>clear vlan primary_vlan</b> |

*CISCO Confidential - DRAFT*

This example shows how to delete primary VLAN 7:

```
Console> (enable) clear vlan 7
This command will de-activate all ports on vlan 7
Do you want to continue (y/n) [n]?y
Vlan 7 deleted
Console> (enable)
```

## Deleting an Isolated or Community VLAN

If you delete an isolated or community VLAN, the binding with the primary VLAN is broken, any isolated or community ports that are associated to the VLAN become inactive, and any related mappings on the promiscuous port(s) are deleted.

To delete a VLAN on the switch, perform this task in privileged mode:

| Task                                  | Command                                                    |
|---------------------------------------|------------------------------------------------------------|
| Delete an isolated or community VLAN. | <b>clear vlan</b> {isolated_vlan_num   community_vlan_num} |

This example shows how to delete the community VLAN 902:

```
Console> (enable) clear vlan 902
This command will de-activate all ports on vlan 902
Do you want to continue (y/n) [n]?y
Vlan 902 deleted
Console> (enable)
```

## Deleting a Private VLAN Mapping

If you delete the private VLAN mapping, the connectivity breaks between the isolated or community ports and the promiscuous port. If you delete all the mappings on a promiscuous port, the promiscuous port becomes inactive. When a private VLAN port is set to inactive, it displays “pvlan-” as its VLAN number in the **show port** output.

You might set a private VLAN port to inactive for the following reasons:

- The primary, isolated, or community VLAN to which it belongs is cleared.
- An error occurs during the configuration of a port to be a private VLAN port.

To delete a port mapping from a private VLAN, perform this task in privileged mode:

| Task                                           | Command                                                                    |
|------------------------------------------------|----------------------------------------------------------------------------|
| Delete the port mapping from the private VLAN. | <b>clear pvlan mapping</b> primary_vlan {isolated   community} {mod/ports} |

This example shows how to delete the mapping of VLAN 902 to 901, previously set on ports 3/2 through 3/5:

```
Console> (enable) clear pvlan mapping 901 902 3/2-5
Successfully cleared mapping between 901 and 902 on 3/2-5
Console> (enable)
```

*CISCO Confidential - DRAFT*



# Configuring VLAN Trunks on Fast Ethernet and Gigabit Ethernet Ports

This chapter describes how to configure Fast Ethernet and Gigabit Ethernet virtual LAN (VLAN) trunks on the Catalyst enterprise LAN switches.

**Note**

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

**Note**

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 4500 Series, Catalyst 2948G, and Catalyst 2980G Switches Command Reference*.

This chapter consists of these sections:

- [Understanding How VLAN Trunks Work, page 11-1](#)
- [Default Trunk Configuration, page 11-5](#)
- [Configuring a Trunk Link, page 11-5](#)
- [Disabling VLAN 1 on a Trunk Link, page 11-8](#)
- [Example VLAN Trunk Configurations, page 11-9](#)

## Understanding How VLAN Trunks Work

The following sections describe how VLAN trunks work on the Catalyst enterprise LAN switches.

### Trunking Overview

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

The Catalyst 4000, 2948G, and 2980G switches support IEEE 802.1Q—802.1Q trunking encapsulation.

You can configure a trunk on a single Fast or Gigabit Ethernet port or on a Fast or Gigabit EtherChannel bundle. For more information about Fast and Gigabit EtherChannel, see [Chapter 6, “Configuring Fast EtherChannel and Gigabit EtherChannel.”](#)

*CISCO Confidential - DRAFT*

Fast Ethernet and Gigabit Ethernet trunk ports support five different trunking modes (see [Table 11-1](#)). In addition, on certain Fast Ethernet and Gigabit Ethernet ports, you can specify whether the trunk uses ISL encapsulation, 802.1Q encapsulation, or whether the encapsulation type is autonegotiated.

For autonegotiated trunking on Fast Ethernet and Gigabit Ethernet ports, the ports must be in the same VTP domain. However, you can use the **on** or **nonegotiate** mode to force a port to become a trunk, even if it is in a different domain. For more information on VTP domains, see [Chapter 9, “Configuring VTP.”](#)

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

**Note**

Trunking capabilities are hardware dependent. For example, the Catalyst 4000 family switch modules support only 802.1Q encapsulation. To determine whether your hardware supports trunking, and to determine which trunking encapsulations are supported, see your hardware documentation or use the **show port capabilities** command.

## Trunking Modes and Encapsulation Types

[Table 11-1](#) lists the trunking modes used with the **set trunk** command and describes how they function on Fast Ethernet and Gigabit Ethernet ports.

**Table 11-1 Fast Ethernet and Gigabit Ethernet Trunking Modes**

| Mode               | Function                                                                                                                                                                                                                |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>on</b>          | Puts the port into permanent trunking mode and negotiates to convert the link into a trunk link. The port becomes a trunk port even if the neighboring port does not agree to the change.                               |
| <b>off</b>         | Puts the port into permanent nontrunking mode and negotiates to convert the link into a nontrunk link. The port becomes a nontrunk port even if the neighboring port does not agree to the change.                      |
| <b>desirable</b>   | Makes the port actively attempt to convert the link to a trunk link. The port becomes a trunk port if the neighboring port is set to <b>on</b> , <b>desirable</b> , or <b>auto</b> mode.                                |
| <b>auto</b>        | Enables the port to convert the link to a trunk link. The port becomes a trunk port if the neighboring port is set to <b>on</b> or <b>desirable</b> mode. This is the default mode for Fast and Gigabit Ethernet ports. |
| <b>nonegotiate</b> | Puts the 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.                                |

[Table 11-2](#) lists the encapsulation type used with the **set trunk** command and describes how it functions on Fast Ethernet and Gigabit Ethernet ports. You can use the **show port capabilities** command to determine which encapsulation types a particular port supports.

**Table 11-2 Fast Ethernet and Gigabit Ethernet Trunk Encapsulation Type**

| Mode         | Function                                                                                                                                                                                                                   |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>dot1q</b> | Specifies 802.1Q encapsulation on the trunk link. 802.1Q trunks are supported in Catalyst 4000 family with 802.1Q-capable hardware. Automatic negotiation of 802.1Q trunks is supported in software release 4.2 and later. |

*CISCO Confidential - DRAFT*

The trunking mode, the trunk encapsulation type, and the hardware capabilities of the two connected ports determine whether a trunk link comes up and the type of trunk the link becomes. Table 11-3 shows the result of the possible trunking configurations.

**Table 11-3 Results of Possible Fast Ethernet and Gigabit Ethernet Trunk Configurations**

| Neighbor Port Trunk Mode and Trunk Encapsulation | Local Port Trunk Mode and Trunk Encapsulation |                    |                    |                    |
|--------------------------------------------------|-----------------------------------------------|--------------------|--------------------|--------------------|
|                                                  | off dot1q                                     | on dot1q           | desirable dot1q    | auto dot1q         |
| <b>off dot1q</b>                                 | Local: Nontrunk                               | Local: 1Q trunk    | Local: Nontrunk    | Local: Nontrunk    |
|                                                  | Neighbor: Nontrunk                            | Neighbor: Nontrunk | Neighbor: Nontrunk | Neighbor: Nontrunk |
| <b>on dot1q</b>                                  | Local: Nontrunk                               | Local: 1Q trunk    | Local: 1Q trunk    | Local: 1Q trunk    |
|                                                  | Neighbor: 1Q trunk                            | Neighbor: 1Q trunk | Neighbor: 1Q trunk | Neighbor: 1Q trunk |
| <b>desirable dot1q</b>                           | Local: Nontrunk                               | Local: 1Q trunk    | Local: 1Q trunk    | Local: 1Q trunk    |
|                                                  | Neighbor: Nontrunk                            | Neighbor: 1Q trunk | Neighbor: 1Q trunk | Neighbor: 1Q trunk |
| <b>auto dot1q</b>                                | Local: Nontrunk                               | Local: 1Q trunk    | Local: 1Q trunk    | Local: Nontrunk    |
|                                                  | Neighbor: Nontrunk                            | Neighbor: 1Q trunk | Neighbor: 1Q trunk | Neighbor: Nontrunk |



**Note**

DTP is a point-to-point protocol. However, some internetworking devices might forward DTP frames improperly. To avoid this problem, ensure that trunking is turned **off** on ports connected to nonswitch devices if you do not intend to trunk across those links. When manually enabling trunking on a link to a Cisco router, use the **nonegotiate** keyword to cause the port to become a trunk but not generate DTP frames.

## Trunking Support

Trunking capabilities are hardware dependent. Table 11-4 shows which switches have available hardware that supports the two trunking encapsulations. To determine whether a specific piece of hardware supports trunking, and to determine which trunking encapsulations are supported, see your hardware documentation or use the **show port capabilities** command.

*CISCO Confidential - DRAFT***Table 11-4** *Trunking Encapsulation Support*

| Trunking Method | Catalyst 4000 Family | Catalyst 2948G Catalyst 2980G |
|-----------------|----------------------|-------------------------------|
| ISL             | No                   | No                            |
| 802.1Q          | Yes                  | Yes                           |
| Negotiate       | No                   | No                            |

## 802.1Q Trunk Restrictions

This section lists the configuration guidelines and restrictions for using 802.1Q trunks to impose some limitations on the trunking strategy for a network. These restrictions apply when using 802.1Q trunks:

- For a trunk to come up and work, you must physically connect the trunk port to another network device.
- When using VTP to carry VLANs over the trunk port, you must manually configure extended VLANs on each switch, because VTP carries only VLANs 1–1005.
- When connecting Cisco switches through an 802.1Q trunk, make sure that the native VLAN for an 802.1Q trunk is the same on both ends of the trunk link. If the native VLAN on one end of the trunk is different from the native VLAN on the other end, spanning tree loops can result.
- Disabling spanning tree on the native VLAN of an 802.1Q trunk without disabling spanning tree on every VLAN in the network can cause spanning-tree loops. We recommend that you leave spanning tree enabled on the native VLAN of an 802.1Q trunk. If this is not possible, disable spanning tree on every VLAN in the network. Make sure that your network is free of physical loops before disabling spanning tree.
- When you connect two Cisco switches through 802.1Q trunks, the switches exchange spanning-tree BPDUs on each VLAN 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.
- Make sure 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.

*CISCO Confidential - DRAFT*

- 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.
- You are limited to 64 trunks that use nondefault trunk configurations, unless you use text file configuration mode. See [Chapter 34, “Working With the Flash File System”](#) for more information on text file configuration mode.

## Default Trunk Configuration

Table 11-5 shows the default Fast Ethernet and Gigabit Ethernet trunk configurations.

**Table 11-5 Default Fast Ethernet and Gigabit Ethernet Trunk Configurations**

| Feature             | Default Configuration                                        |
|---------------------|--------------------------------------------------------------|
| Trunk mode          | <b>auto</b>                                                  |
| Trunk encapsulation | <b>dot1q</b> (on hardware supporting 802.1Q only)            |
| Allowed VLAN range  | normal-range VLANs 1–1005 and extended-range VLANs 1025–4094 |

**Note**

A nondefault trunk configuration is a default trunk configuration with one or more extended-range VLANs removed from the trunk configuration.

## Configuring a Trunk Link

The following sections describe how to configure a trunk link on Fast Ethernet and Gigabit Ethernet ports and how to define the allowed VLAN range on a trunk.

### Configuring an 802.1Q Trunk

**Note**

Some hardware does not support 802.1Q encapsulation. To determine whether your hardware supports 802.1Q, see your hardware documentation or use the **show port capabilities** command.

**Caution**

You must configure the ports on both ends of the trunk link as 802.1Q trunks using the **set trunk** command with the **nonegotiate** and **dot1q** keywords. Expect Spanning Tree Protocol (STP) to block the port on the other end of the trunk link until you configure that end of the link as an 802.1Q trunk as well. Do not configure one end of a trunk as an 802.1Q trunk and the other end as an ISL trunk or a nontrunk port. Errors will occur and no traffic can pass over the link. For more information, see the [“Trunking Modes and Encapsulation Types”](#) section on page 11-2.

*CISCO Confidential - DRAFT*

Before configuring an 802.1Q trunk you must set a VTP domain and enter the VLANs that will be used in the trunk or channel. For more information see [Chapter 9, “Configuring VTP,”](#) and [Chapter 10, “Configuring VLANs.”](#)

To configure an 802.1Q trunk, perform this task in privileged mode:

|        | Task                               | Command                                                                                                                   |
|--------|------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Define the VTP domain name.        | <b>set vtp domain</b> <i>name</i>                                                                                         |
| Step 2 | Configure VLANs.                   | <b>set vlan</b> <i>vlan</i>                                                                                               |
| Step 3 | Configure an 802.1Q trunk.         | <b>set trunk</b> <i>mod_num/port_num</i> [ <b>on</b>   <b>desirable</b>   <b>auto</b>   <b>nonegotiate</b> ] <b>dot1q</b> |
| Step 4 | Verify the trunking configuration. | <b>show trunk</b> [ <i>mod_num/port_num</i> ]                                                                             |

This example shows how to configure an 802.1Q trunk and how to verify the trunk configuration:

```

Console> (enable) set vtp domain Lab_Network
VTP domain Lab_Network modified
Console> (enable) set vlan 10,20,100
VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 10,20,100 configuration successful.
Console> (enable) set trunk 2/9 desirable dot1q
Port(s) 2/9 trunk mode set to desirable.
Port(s) 2/9 trunk type set to dot1q.
Console> (enable) 07/02/1998,18:22:25:DTP-5:Port 2/9 has become dot1q trunk

```

```

Console> (enable) show trunk
Port Mode Encapsulation Status Native vlan

2/9 desirable dot1q trunking 1

Port Vlans allowed on trunk

2/9 1,10,20,100

Port Vlans allowed and active in management domain

2/9 1,10,20,100

Port Vlans in spanning tree forwarding state and not pruned

2/9 1,10,20,100
Console> (enable)

```

## Defining the Allowed VLANs on a Trunk

When you configure a trunk port, all VLANs are added to the allowed VLANs list for that trunk. However, you can remove VLANs from the allowed list to prevent traffic for those VLANs from passing over the trunk.

*CISCO Confidential - DRAFT***Note**

When you first configure a port as a trunk, the **set trunk** command always adds all VLANs to the allowed VLAN list for the trunk, even if you specify a VLAN range (any specified VLAN range is ignored). To modify the allowed VLANs list, use the **clear trunk** and **set trunk** commands to specify the allowed VLANs.

To define the allowed VLAN list for a trunk port, perform this task in privileged mode:

|        | Task                                                                 | Command                                                  |
|--------|----------------------------------------------------------------------|----------------------------------------------------------|
| Step 1 | (Optional) Add specific VLANs to the allowed VLANs list for a trunk. | <b>set trunk</b> <i>mod_num/port_num</i> <i>vlan</i> s   |
| Step 2 | Remove VLANs from the allowed VLANs list for a trunk.                | <b>clear trunk</b> <i>mod_num/port_num</i> <i>vlan</i> s |
| Step 3 | Verify the allowed VLAN list for the trunk.                          | <b>show trunk</b> [ <i>mod_num/port_num</i> ]            |

This example shows how to define the allowed VLANs list for trunk port 1/1 to allow VLANs 10, 20, and VLAN 100, and how to verify the allowed VLAN list for the trunk:

```

Console> (enable) set trunk 1/1 10,20,100
Adding vlans 10, 20 to allowed list.
Port(s) 1/1 allowed vlans modified to 10,20,100,1002,1003,1004,1005.
Console> (enable) clear trunk 1/1 1-9,11-19,21-99,101-1001
Removing Vlan(s) 1-9,11-19,21-99,101-100 from allowed list.
Port 1/1 allowed vlans modified to 10,20,100.
Console> (enable) show trunk 1/1
Port Mode Encapsulation Status Native vlan

 1/1 desirable dot1q trunking 1
Port Vlan(s) allowed on trunk

 1/1 1,10,20,100
Port Vlan(s) allowed and active in management domain

 1/1 1,10,20,100
Port Vlan(s) in spanning tree forwarding state and not pruned

 1/1 1,10,20,100
Console> (enable)

```

## Disabling a Trunk Port

To explicitly turn off trunking on a port, perform this task in privileged mode:

|        | Task                               | Command                                             |
|--------|------------------------------------|-----------------------------------------------------|
| Step 1 | Turn off trunking on a port.       | <b>set trunk</b> <i>mod_num/port_num</i> <b>off</b> |
| Step 2 | Verify the trunking configuration. | <b>show trunk</b> [ <i>mod_num/port_num</i> ]       |

To return a port to the default trunk type and mode for that port type, perform this task in privileged mode:

*CISCO Confidential - DRAFT*

|        | Task                                                                      | Command                                       |
|--------|---------------------------------------------------------------------------|-----------------------------------------------|
| Step 1 | Return the port to the default trunking type and mode for that port type. | <b>clear trunk</b> <i>mod_num/port_num</i>    |
| Step 2 | Verify the trunking configuration.                                        | <b>show trunk</b> [ <i>mod_num/port_num</i> ] |

## Disabling VLAN 1 on a Trunk Link

On the Catalyst enterprise LAN switches, VLAN 1 is enabled by default to allow control protocols to transmit and receive packets across the network topology. However, when VLAN 1 is enabled on trunk links in a large complex network topology, the impact of broadcast storms increases. Because spanning tree applies to the entire network topology, the possibility of spanning tree loops also increases when VLAN 1 is enabled on all trunk links. To prevent this situation, you can disable VLAN 1 on trunk interfaces.

When you disable VLAN 1 on a trunk interface, no user traffic is transmitted or received across that trunk interface, but the supervisor engine will continue to transmit and receive packets from control protocols such as Cisco Discovery Protocol (CDP), VLAN Trunking Protocol (VTP), Port Aggregation Protocol (PAgP), Dynamic Trunking Protocol (DTP), and so forth.



### Caution

By default, the sc0 interface management VLAN is VLAN 1. If you disable VLAN 1, you will have to configure another VLAN to be the management VLAN for sc0.

When a trunk port with VLAN 1 disabled becomes a nontrunk port, it is added to the native VLAN. If the native VLAN is VLAN 1, the port is enabled and added to VLAN 1.

To disable VLAN 1 on a trunk interface, perform this task in privileged mode:

|        | Task                                        | Command                                                          |
|--------|---------------------------------------------|------------------------------------------------------------------|
| Step 1 | Disable VLAN 1 on the trunk interface.      | <b>clear trunk</b> <i>mod_num/port_num</i> [ <i>vlan-range</i> ] |
| Step 2 | Verify the allowed VLAN list for the trunk. | <b>show trunk</b> [ <i>mod_num/port_num</i> ]                    |

This example shows how to disable VLAN 1 on a trunk link and verify the configuration:

```

Console> (enable) clear trunk 4/1 1
Removing Vlan(s) 1 from allowed list.
Port 4/1 allowed vlans modified to 2-1005.
Console> (enable) show trunk 4/1
Port Mode Encapsulation Status Native vlan

4/1 on isl trunking 1

Port Vlans allowed on trunk

4/1 2-999, 1025-4094

Port Vlans allowed and active in management domain

4/1 2-6,10,20,50,100,152,200,300,400,500,521,524,570,776,801-802,850,917,999

Port Vlans in spanning tree forwarding state and not pruned

```



*CISCO Confidential - DRAFT*

4/1 2-6, 10, 20, 50, 100, 152, 200, 300, 400, 500, 521, 524, 570, 776, 802, 850, 917, 999  
 Console> (enable)

## Example VLAN Trunk Configurations

The following sections contains examples of a VLAN trunk configurations:



### Note

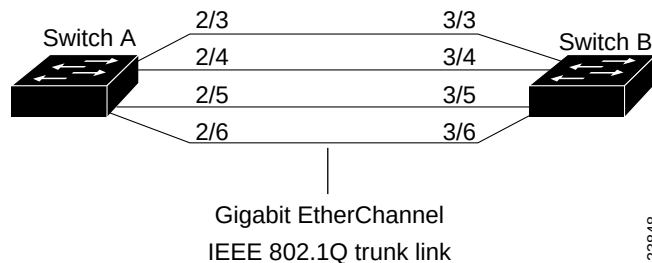
For examples of configuring trunk links between switches and routers, refer to the *Layer 3 Switching Software Configuration Guide—Catalyst 5000 Family, 4000 Family, 2926G Series, 2926 Series, 2948G, and 2980G Switches* publication.

## 802.1Q Trunk over a Gigabit EtherChannel Link Example

This sample configuration shows how to configure an 802.1Q trunk over a Gigabit EtherChannel link between two switches with 802.1Q-capable hardware. (Use the **show port capabilities** command to see if your hardware is 802.1Q-capable.)

Figure 11-1 shows two switches connected through four 1000BASE-SX Gigabit Ethernet ports.

**Figure 11-1 IEEE 802.1Q Trunk over Gigabit EtherChannel Link**



### Note

For complete information on configuring Gigabit EtherChannel, see [Chapter 6, “Configuring Fast EtherChannel and Gigabit EtherChannel.”](#)

To configure the switches to form a four-port Gigabit EtherChannel bundle, and then configure the EtherChannel bundle as an 802.1Q trunk link, follow these steps:

- Step 1** Make sure that all ports on both Switch A and Switch B are assigned to the same VLAN. This VLAN is used as the 802.1Q native VLAN for the trunk. In this example, all ports are configured as members of VLAN 1.

```
Switch_A> (enable) set vlan 1 2/3-6
VLAN Mod/Ports

1 2/3-6
```

```
Switch_A> (enable)
```

```
Switch_B> (enable) set vlan 1 3/3-6
VLAN Mod/Ports

```

*CISCO Confidential - DRAFT*

1 3/3-6

Switch\_B&gt; (enable)

- Step 2** Configure one of the ports in the EtherChannel bundle to negotiate an 802.1Q trunk. The configuration is applied to all of the ports in the bundle. This example assumes that the neighboring ports on Switch B are configured to use **dot1q** or **negotiate** encapsulation and are in **auto** trunk mode. The system logging messages provide information about the formation of the 802.1Q trunk.

```
Switch_A> (enable) set trunk 2/3 desirable dot1q
Port(s) 2/3-6 trunk mode set to desirable.
Port(s) 2/3-6 trunk type set to dot1q.
Switch_A> (enable) %DTP-5-TRUNKPORTON:Port 2/3 has become dot1q trunk
%DTP-5-TRUNKPORTON:Port 2/4 has become dot1q trunk
%ETHC-5-PORTFROMSTP:Port 2/3 left bridge port 2/3-6
%DTP-5-TRUNKPORTON:Port 2/5 has become dot1q trunk
%ETHC-5-PORTFROMSTP:Port 2/4 left bridge port 2/3-6
%ETHC-5-PORTFROMSTP:Port 2/5 left bridge port 2/3-6
%DTP-5-TRUNKPORTON:Port 2/6 has become dot1q trunk
%ETHC-5-PORTFROMSTP:Port 2/6 left bridge port 2/3-6
%ETHC-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
%ETHC-5-PORTTOSTP:Port 2/3 joined bridge port 2/3-6
%ETHC-5-PORTTOSTP:Port 2/4 joined bridge port 2/3-6
%ETHC-5-PORTTOSTP:Port 2/5 joined bridge port 2/3-6
%ETHC-5-PORTTOSTP:Port 2/6 joined bridge port 2/3-6
```

```
Switch_B> (enable) %DTP-5-TRUNKPORTON:Port 3/3 has become dot1q trunk
%DTP-5-TRUNKPORTON:Port 3/4 has become dot1q trunk
%ETHC-5-PORTFROMSTP:Port 3/3 left bridge port 3/3-6
%ETHC-5-PORTFROMSTP:Port 3/4 left bridge port 3/3-6
%ETHC-5-PORTFROMSTP:Port 3/5 left bridge port 3/3-6
%ETHC-5-PORTFROMSTP:Port 3/6 left bridge port 3/3-6
%DTP-5-TRUNKPORTON:Port 3/5 has become dot1q trunk
%DTP-5-TRUNKPORTON:Port 3/6 has become dot1q trunk
%ETHC-5-PORTFROMSTP:Port 3/5 left bridge port 3/3-6
%ETHC-5-PORTFROMSTP:Port 3/6 left bridge port 3/3-6
%ETHC-5-PORTTOSTP:Port 3/3 joined bridge port 3/3-6
%ETHC-5-PORTTOSTP:Port 3/4 joined bridge port 3/3-6
%ETHC-5-PORTTOSTP:Port 3/5 joined bridge port 3/3-6
%ETHC-5-PORTTOSTP:Port 3/6 joined bridge port 3/3-6
```

- Step 3** After the 802.1Q trunk link is negotiated, enter the **show trunk** command to verify the configuration.

Switch\_A&gt; (enable) show trunk

| Port | Mode      | Encapsulation | Status   | Native vlan |
|------|-----------|---------------|----------|-------------|
| 2/3  | desirable | dot1q         | trunking | 1           |
| 2/4  | desirable | dot1q         | trunking | 1           |
| 2/5  | desirable | dot1q         | trunking | 1           |
| 2/6  | desirable | dot1q         | trunking | 1           |

Port Vlans allowed on trunk

|     |                   |
|-----|-------------------|
| 2/3 | 1-1005, 1025-4094 |
| 2/4 | 1-1005, 1025-4094 |
| 2/5 | 1-1005, 1025-4094 |
| 2/6 | 1-1005, 1025-4094 |

Port Vlans allowed and active in management domain

|     |                   |
|-----|-------------------|
| 2/3 | 1-1005, 1025-4094 |
| 2/4 | 1-1005, 1025-4094 |
| 2/5 | 1-1005, 1025-4094 |

*CISCO Confidential - DRAFT*

```

2/6 1-1005, 1025-4094

Port Vlans in spanning tree forwarding state and not pruned

2/3 1-1005, 1025-4094
2/4 1-1005, 1025-4094
2/5 1-1005, 1025-4094
2/6 1-1005, 1025-4094
Switch_A> (enable)

Switch_B> (enable) show trunk
Port Mode Encapsulation Status Native vlan

3/3 auto dot1q trunking 1
3/4 auto dot1q trunking 1
3/5 auto dot1q trunking 1
3/6 auto dot1q trunking 1

Port Vlans allowed on trunk

3/3 1-1005, 1025-4094
3/4 1-1005, 1025-4094
3/5 1-1005, 1025-4094
3/6 1-1005, 1025-4094

Port Vlans allowed and active in management domain

3/3 1-1005, 1025-4094
3/4 1-1005, 1025-4094
3/5 1-1005, 1025-4094
3/6 1-1005, 1025-4094

Port Vlans in spanning tree forwarding state and not pruned

3/3 1-1005, 1025-4094
3/4 1-1005, 1025-4094
3/5 1-1005, 1025-4094
3/6 1-1005, 1025-4094
Switch_B> (enable)

```

**Step 4** Confirm the channeling and trunking status of the switches by entering the **show port channel** and **show trunk** commands.

```

Switch_A> (enable) show port channel
No ports channelling
Switch_A> (enable) show trunk
No ports trunking.
Switch_A> (enable)

```

```

Switch_B> (enable) show port channel
No ports channelling
Switch_B> (enable) show trunk
No ports trunking.
Switch_B> (enable)

```

**Step 5** Configure the ports on Switch A to negotiate a Gigabit EtherChannel bundle with the neighboring switch. This example assumes that the neighboring ports on Switch B are in EtherChannel **auto** mode. The system logging messages provide information about the formation of the EtherChannel bundle.

```

Switch_A> (enable) set port channel 2/3-6 desirable
Port(s) 2/3-6 channel mode set to desirable.
Switch_A> (enable) %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3

```

*CISCO Confidential - DRAFT*

```

%ETHC-5-PORTFROMSTP:Port 2/4 left bridge port 2/4
%ETHC-5-PORTFROMSTP:Port 2/5 left bridge port 2/5
%ETHC-5-PORTFROMSTP:Port 2/6 left bridge port 2/6
%ETHC-5-PORTFROMSTP:Port 2/4 left bridge port 2/4
%ETHC-5-PORTFROMSTP:Port 2/5 left bridge port 2/5
%ETHC-5-PORTFROMSTP:Port 2/6 left bridge port 2/6
%ETHC-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
%ETHC-5-PORTTOSTP:Port 2/3 joined bridge port 2/3-6
%ETHC-5-PORTTOSTP:Port 2/4 joined bridge port 2/3-6
%ETHC-5-PORTTOSTP:Port 2/5 joined bridge port 2/3-6
%ETHC-5-PORTTOSTP:Port 2/6 joined bridge port 2/3-6

Switch_B> (enable) %PAGP-5-PORTFROMSTP:Port 3/3 left bridge port 3/3
%ETHC-5-PORTFROMSTP:Port 3/4 left bridge port 3/4
%ETHC-5-PORTFROMSTP:Port 3/5 left bridge port 3/5
%ETHC-5-PORTFROMSTP:Port 3/6 left bridge port 3/6
%ETHC-5-PORTFROMSTP:Port 3/4 left bridge port 3/4
%ETHC-5-PORTFROMSTP:Port 3/5 left bridge port 3/5
%ETHC-5-PORTFROMSTP:Port 3/6 left bridge port 3/6
%ETHC-5-PORTFROMSTP:Port 3/3 left bridge port 3/3
%ETHC-5-PORTTOSTP:Port 3/3 joined bridge port 3/3-6
%ETHC-5-PORTTOSTP:Port 3/4 joined bridge port 3/3-6
%ETHC-5-PORTTOSTP:Port 3/5 joined bridge port 3/3-6
%ETHC-5-PORTTOSTP:Port 3/6 joined bridge port 3/3-6

```

**Step 6** After the EtherChannel bundle is negotiated, enter the **show port channel** command to verify the configuration.

```

Switch_A> (enable) show port channel

```

| Port | Status    | Channel mode | Channel status | Neighbor device       | Neighbor port |
|------|-----------|--------------|----------------|-----------------------|---------------|
| 2/3  | connected | desirable    | channel        | WS-C4003 JAB023806(Sw | 2/3           |
| 2/4  | connected | desirable    | channel        | WS-C4003 JAB023806(Sw | 2/4           |
| 2/5  | connected | desirable    | channel        | WS-C4003 JAB023806(Sw | 2/5           |
| 2/6  | connected | desirable    | channel        | WS-C4003 JAB023806(Sw | 2/6           |

```

Switch_A> (enable)
Switch_B> (enable) show port channel

```

| Port | Status    | Channel mode | Channel status | Neighbor device       | Neighbor port |
|------|-----------|--------------|----------------|-----------------------|---------------|
| 3/3  | connected | auto         | channel        | WS-C4003 JAB023806(Sw | 2/3           |
| 3/4  | connected | auto         | channel        | WS-C4003 JAB023806(Sw | 2/4           |
| 3/5  | connected | auto         | channel        | WS-C4003 JAB023806(Sw | 2/5           |
| 3/6  | connected | auto         | channel        | WS-C4003 JAB023806(Sw | 2/6           |

```

Switch_B> (enable)

```

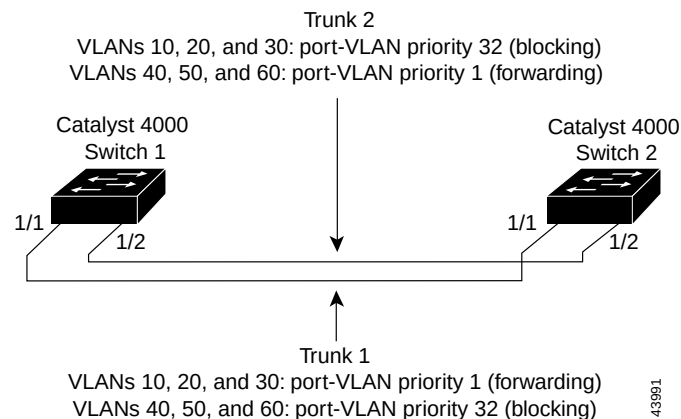
## Load-Sharing VLAN Traffic over Parallel Trunks Example

Using spanning tree port-VLAN priorities, you can load-share VLAN traffic over parallel trunk ports so that traffic from some VLANs travels over one trunk, while traffic from other VLANs travels over the other trunk. This configuration allows traffic to be carried over both trunks simultaneously (instead of keeping one trunk in blocking mode), which reduces the total traffic carried over each trunk while still maintaining a fault-tolerant configuration.

*CISCO Confidential - DRAFT*

Figure 11-2 shows a parallel trunk configuration between two switches, using the Fast Ethernet uplink ports on the supervisor engine.

**Figure 11-2 Parallel Trunk Configuration Before Configuring VLAN-Traffic Load Sharing**



By default, the port-VLAN priority for both trunks is equal (a value of 32). Therefore, STP blocks port 1/2 (Trunk 2) for each VLAN on Switch 1 to prevent forwarding loops. Trunk 2 is not used to forward traffic unless Trunk 1 fails.

To configure the switches so that traffic from multiple VLANs is load balanced over the parallel trunks, follow these steps:

- Step 1** Configure a VTP domain on both Switch 1 and Switch 2 by entering the **set vtp** command so that the VLAN information configured on Switch 1 is learned by Switch 2. Make sure that Switch 1 is a VTP server. You can configure Switch 2 as a VTP client or as a VTP server.

```
Switch_1> (enable) set vtp domain BigCorp mode server
VTP domain BigCorp modified
Switch_1> (enable)
```

```
Switch_2> (enable) set vtp domain BigCorp mode server
VTP domain BigCorp modified
Switch_2> (enable)
```

- Step 2** Create the VLANs on Switch 1 by entering the **set vlan** command. In this example, you see VLANs 10, 20, 30, 40, 50, and 60:

```
Switch_1> (enable) set vlan 10
Vlan 10 configuration successful
Switch_1> (enable) set vlan 20
Vlan 20 configuration successful
Switch_1> (enable) set vlan 30
Vlan 30 configuration successful
Switch_1> (enable) set vlan 40
Vlan 40 configuration successful
Switch_1> (enable) set vlan 50
Vlan 50 configuration successful
Switch_1> (enable) set vlan 60
Vlan 60 configuration successful
Switch_1> (enable)
```

- Step 3** Verify the VTP and VLAN configuration on Switch 1 by entering the **show vtp domain** and **show vlan** commands:

*CISCO Confidential - DRAFT*

```
Switch_1> (enable) show vtp domain
Domain Name Domain Index VTP Version Local Mode Password

BigCorp 1 2 server -

Vlan-count Max-vlan-storage Config Revision Notifications

11 1023 13 disabled

Last Updater V2 Mode Pruning PruneEligible on Vlans

172.20.52.10 disabled enabled 2-1000
Switch_1> (enable) show vlan
VLAN Name Status Mod/Ports, Vlans

1 default active 1/1-2
 2/1-12
 5/1-2
10 VLAN0010 active
11 VLAN0011 active
20 VLAN0020 active
30 VLAN0030 active
40 VLAN0040 active
50 VLAN0050 active
60 VLAN0060 active
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
.
.
.
Switch_1> (enable)
```

- Step 4** Configure the supervisor engine uplinks on Switch 1 as 802.1Q trunk ports by entering the **set trunk** command. Specifying the desirable mode on the Switch 1 ports causes the ports on Switch 2 to negotiate to become trunk links (assuming that the Switch 2 uplinks are in the default **auto** mode).

```
Switch_1> (enable) set trunk 1/1 desirable
Port(s) 1/1 trunk mode set to desirable.
2000 Jul 12 01:56:28 %DTP-5-TRUNKPORTON:Port 1/1 has become dot1q trunk
Switch_1> (enable)
```

```
Switch_1> (enable) set trunk 1/2 desirable
Port(s) 1/2 trunk mode set to desirable.
2000 Jul 12 01:56:52 %DTP-5-TRUNKPORTON:Port 1/2 has become dot1q trunk
Switch_1> (enable)
```

- Step 5** Verify that the trunk links are up by entering the **show trunk** command:

```
Switch_1> (enable) show trunk 1
* - indicates vtp domain mismatch
Port Mode Encapsulation Status Native vlan

1/1 desirable dot1q trunking 1
1/2 desirable dot1q trunking 1

Port Vlans allowed on trunk

1/1 1-1005,1025-4094
1/2 1-1005,1025-4094

Port Vlans allowed and active in management domain

```

*CISCO Confidential - DRAFT*

```
1/1 1,10,20,30,40,50,60
1/2 1,10,20,30,40,50,60
```

```
Port Vlans in spanning tree forwarding state and not pruned
```

```

1/1 1,10,20,30,40,50,60
1/2Switch_1> (enable)
```

- Step 6** When the trunk links come up, VTP passes the VTP and VLAN configuration to Switch 2. Verify that Switch 2 has learned the VLAN configuration by entering the **show vlan** command on Switch 2:

```
Switch_2> (enable) show vlan
```

```
VLAN Name Status Mod/Ports, Vlans
```

```

1 default active
10 VLAN0010 active
20 VLAN0020 active
30 VLAN0030 active
40 VLAN0040 active
50 VLAN0050 active
60 VLAN0060 active
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
```

```
.
.
.
```

```
Switch_2> (enable)
```

- Step 7** Spanning tree takes one to two minutes to converge. After the network stabilizes, check the spanning tree state of each trunk port on Switch 1 by entering the **show spantree** command.
- Trunk 1 is forwarding for all VLANs. Trunk 2 is blocking for all VLANs. On Switch 2, both trunks are forwarding for all VLANs, but no traffic passes over Trunk 2 because port 1/2 on Switch 1 is blocking.

```
Switch_1> (enable) show spantree 1/1
```

```
Port Vlan Port-State Cost Priority Fast-Start Group-method

1/1 1 forwarding 19 32 disabled
1/1 10 forwarding 19 32 disabled
1/1 20 forwarding 19 32 disabled
1/1 30 forwarding 19 32 disabled
1/1 40 forwarding 19 32 disabled
1/1 50 forwarding 19 32 disabled
1/1 60 forwarding 19 32 disabled
1/1 1003 not-connected 19 32 disabled
1/1 1005 not-connected 19 4 disabled
```

```
Switch_1> (enable) show spantree 1/2
```

```
Port Vlan Port-State Cost Priority Fast-Start Group-method

1/2 1 blocking 19 32 disabled
1/2 10 blocking 19 32 disabled
1/2 20 blocking 19 32 disabled
1/2 30 blocking 19 32 disabled
1/2 40 blocking 19 32 disabled
1/2 50 blocking 19 32 disabled
1/2 60 blocking 19 32 disabled
1/2 1003 not-connected 19 32 disabled
1/2 1005 not-connected 19 4 disabled
```

```
Switch_1> (enable)
```

*CISCO Confidential - DRAFT*

- Step 8** Divide the configured VLANs into two groups. You might want traffic from one-half of the VLANs to go over one trunk link and one-half over the other trunk link; or if one VLAN has heavier traffic, you can have traffic from that VLAN go over one trunk and traffic from the other VLANs go over the other trunk link.

VLANs 10, 20, and 30 (Group 1) are forwarded over Trunk 1, and VLANs 40, 50, and 60 (Group 2) are forwarded over Trunk 2.

- Step 9** On Switch 1, enter the **set spantree portvlanpri** command to change the port-VLAN priority for the Group 1 VLANs on Trunk 1 (port 1/1) to an integer value lower than the default of 32:

```
Switch_1> (enable) set spantree portvlanpri 1/1 1 10
Port 1/1 vlans 1-9,11-1004 using portpri 32.
Port 1/1 vlans 10 using portpri 1.
Port 1/1 vlans 1005 using portpri 4.
Switch_1> (enable) set spantree portvlanpri 1/1 1 20
Port 1/1 vlans 1-9,11-19,21-1004 using portpri 32.
Port 1/1 vlans 10,20 using portpri 1.
Port 1/1 vlans 1005 using portpri 4.
Switch_1> (enable) set spantree portvlanpri 1/1 1 30
Port 1/1 vlans 1-9,11-19,21-29,31-1004 using portpri 32.
Port 1/1 vlans 10,20,30 using portpri 1.
Port 1/1 vlans 1005 using portpri 4.
Switch_1> (enable)
```

- Step 10** On Switch 1, change the port-VLAN priority for the Group 2 VLANs on Trunk 2 (port 1/2) to an integer value lower than the default of 32:

```
Switch_1> (enable) set spantree portvlanpri 1/2 1 40
Port 1/2 vlans 1-39,41-1004 using portpri 32.
Port 1/2 vlans 40 using portpri 1.
Port 1/2 vlans 1005 using portpri 4.
Switch_1> (enable) set spantree portvlanpri 1/2 1 50
Port 1/2 vlans 1-39,41-49,51-1004 using portpri 32.
Port 1/2 vlans 40,50 using portpri 1.
Port 1/2 vlans 1005 using portpri 4.
Switch_1> (enable) set spantree portvlanpri 1/2 1 60
Port 1/2 vlans 1-39,41-49,51-59,61-1004 using portpri 32.
Port 1/2 vlans 40,50,60 using portpri 1.
Port 1/2 vlans 1005 using portpri 4.
Switch_1> (enable)
```

- Step 11** On Switch 2, change the port-VLAN priority for the Group 1 VLANs on Trunk 1 (port 1/1) to the same value that you configured for those VLANs on Switch 1:

**Caution**

The port-VLAN priority for each VLAN must be equal on both ends of the link.

```
Switch_2> (enable) set spantree portvlanpri 1/1 1 10
Port 1/1 vlans 1-9,11-1004 using portpri 32.
Port 1/1 vlans 10 using portpri 1.
Port 1/1 vlans 1005 using portpri 4.
Switch_2> (enable) set spantree portvlanpri 1/1 1 20
Port 1/1 vlans 1-9,11-19,21-1004 using portpri 32.
Port 1/1 vlans 10,20 using portpri 1.
Port 1/1 vlans 1005 using portpri 4.
Switch_2> (enable) set spantree portvlanpri 1/1 1 30
Port 1/1 vlans 1-9,11-19,21-29,31-1004 using portpri 32.
Port 1/1 vlans 10,20,30 using portpri 1.
Port 1/1 vlans 1005 using portpri 4.
Switch_2> (enable)
```



*CISCO Confidential - DRAFT*

- Step 12** On Switch 2, change the port-VLAN priority for the Group 2 VLANs on Trunk 2 (port 1/2) to the same value that you configured for those VLANs on Switch 1:

```
Switch_2> (enable) set spantree portvlanpri 1/2 1 40
Port 1/2 vlans 1-39,41-1004 using portpri 32.
Port 1/2 vlans 40 using portpri 1.
Port 1/2 vlans 1005 using portpri 4.
Switch_2> (enable) set spantree portvlanpri 1/2 1 50
Port 1/2 vlans 1-39,41-49,51-1004 using portpri 32.
Port 1/2 vlans 40,50 using portpri 1.
Port 1/2 vlans 1005 using portpri 4.
Switch_2> (enable) set spantree portvlanpri 1/2 1 60
Port 1/2 vlans 1-39,41-49,51-59,61-1004 using portpri 32.
Port 1/2 vlans 40,50,60 using portpri 1.
Port 1/2 vlans 1005 using portpri 4.
Switch_2> (enable)
```

- Step 13** When you have configured the port-VLAN priorities on both ends of the link, the spanning tree converges to use the new configuration.

Check the spanning tree port states on Switch 1 by entering the **show spantree** command. The Group 1 VLANs should be forwarding on Trunk 1 and blocking on Trunk 2. The Group 2 VLANs should be blocking on Trunk 1 and forwarding on Trunk 2.

```
Switch_1> (enable) show spantree 1/1
```

| Port | Vlan | Port-State    | Cost | Priority | Fast-Start | Group-method |
|------|------|---------------|------|----------|------------|--------------|
| 1/1  | 1    | forwarding    | 19   | 32       | disabled   |              |
| 1/1  | 10   | forwarding    | 19   | 1        | disabled   |              |
| 1/1  | 20   | forwarding    | 19   | 1        | disabled   |              |
| 1/1  | 30   | forwarding    | 19   | 1        | disabled   |              |
| 1/1  | 40   | blocking      | 19   | 32       | disabled   |              |
| 1/1  | 50   | blocking      | 19   | 32       | disabled   |              |
| 1/1  | 60   | blocking      | 19   | 32       | disabled   |              |
| 1/1  | 1003 | not-connected | 19   | 32       | disabled   |              |
| 1/1  | 1005 | not-connected | 19   | 4        | disabled   |              |

```
Switch_1> (enable) show spantree 1/2
```

| Port | Vlan | Port-State    | Cost | Priority | Fast-Start | Group-method |
|------|------|---------------|------|----------|------------|--------------|
| 1/2  | 1    | blocking      | 19   | 32       | disabled   |              |
| 1/2  | 10   | blocking      | 19   | 32       | disabled   |              |
| 1/2  | 20   | blocking      | 19   | 32       | disabled   |              |
| 1/2  | 30   | blocking      | 19   | 32       | disabled   |              |
| 1/2  | 40   | forwarding    | 19   | 1        | disabled   |              |
| 1/2  | 50   | forwarding    | 19   | 1        | disabled   |              |
| 1/2  | 60   | forwarding    | 19   | 1        | disabled   |              |
| 1/2  | 1003 | not-connected | 19   | 32       | disabled   |              |
| 1/2  | 1005 | not-connected | 19   | 4        | disabled   |              |

```
Switch_1> (enable)
```

Figure 11-3 shows the network after you configure VLAN traffic load sharing.

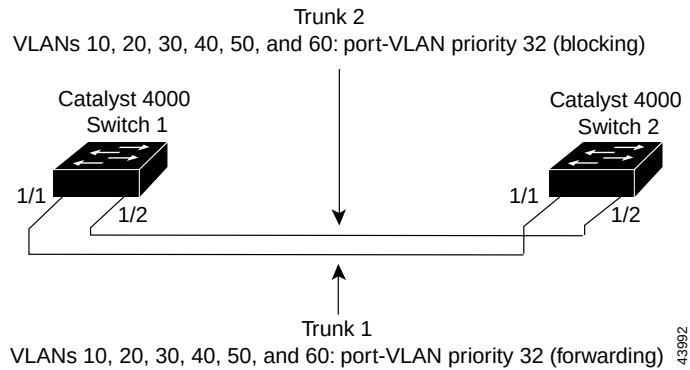
*CISCO Confidential - DRAFT***Figure 11-3 Parallel Trunk Configuration after Configuring VLAN Traffic Load-Sharing**

Figure 11-3 shows that both trunks are utilized when the network is operating normally. If one trunk link fails, the other trunk link acts as an alternate forwarding path for the traffic previously traveling over the failed link.

If Trunk 1 fails in the network shown in Figure 11-3, STP reconverges to use Trunk 2 to forward traffic from all the VLANs, as shown in the following example:

```
Switch_1> (enable) 04/21/1998,03:15:40:ETHC-5:Port 1/1 has become non-trunk
```

```
Switch_1> (enable) show spantree 1/1
```

| Port | Vlan | Port-State    | Cost | Priority | Fast-Start | Group-method |
|------|------|---------------|------|----------|------------|--------------|
| 1/1  | 1    | not-connected | 19   | 32       | disabled   |              |

```
Switch_1> (enable) show spantree 1/2
```

| Port | Vlan | Port-State    | Cost | Priority | Fast-Start | Group-method |
|------|------|---------------|------|----------|------------|--------------|
| 1/2  | 1    | learning      | 19   | 32       | disabled   |              |
| 1/2  | 10   | learning      | 19   | 32       | disabled   |              |
| 1/2  | 20   | learning      | 19   | 32       | disabled   |              |
| 1/2  | 30   | learning      | 19   | 32       | disabled   |              |
| 1/2  | 40   | forwarding    | 19   | 1        | disabled   |              |
| 1/2  | 50   | forwarding    | 19   | 1        | disabled   |              |
| 1/2  | 60   | forwarding    | 19   | 1        | disabled   |              |
| 1/2  | 1003 | not-connected | 19   | 32       | disabled   |              |
| 1/2  | 1005 | not-connected | 19   | 4        | disabled   |              |

```
Switch_1> (enable) show spantree 1/2
```

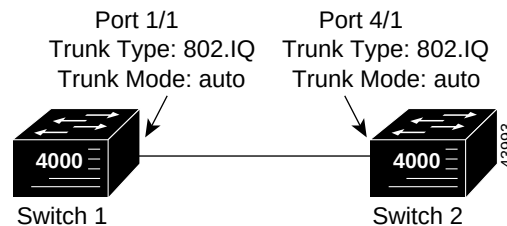
| Port | Vlan | Port-State    | Cost | Priority | Fast-Start | Group-method |
|------|------|---------------|------|----------|------------|--------------|
| 1/2  | 1    | forwarding    | 19   | 32       | disabled   |              |
| 1/2  | 10   | forwarding    | 19   | 32       | disabled   |              |
| 1/2  | 20   | forwarding    | 19   | 32       | disabled   |              |
| 1/2  | 30   | forwarding    | 19   | 32       | disabled   |              |
| 1/2  | 40   | forwarding    | 19   | 1        | disabled   |              |
| 1/2  | 50   | forwarding    | 19   | 1        | disabled   |              |
| 1/2  | 60   | forwarding    | 19   | 1        | disabled   |              |
| 1/2  | 1003 | not-connected | 19   | 32       | disabled   |              |
| 1/2  | 1005 | not-connected | 19   | 4        | disabled   |              |

```
Switch_1> (enable)
```

## 802.1Q Nonegotiate Trunk Configuration Example

This sample configuration shows how to configure an 802.1Q Fast Ethernet trunk between two Catalyst 4000 family switches with 802.1Q-capable hardware. (Use the **show port capabilities** command to see if your hardware is 802.1Q-capable.) The initial network configuration is shown in [Figure 11-4](#). Assume that the native VLAN is VLAN 1 on both ends of the link.

**Figure 11-4 802.1Q Trunking: Initial Network Configuration**



To configure an 802.1Q trunk between port 1/1 on Switch 1 and port 4/1 on Switch 2, follow these steps:

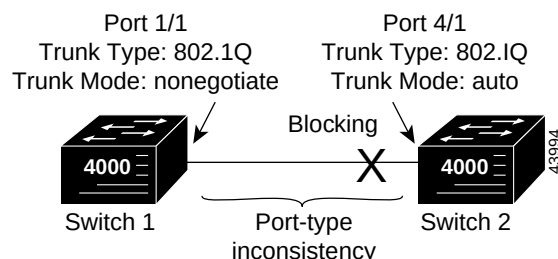
- Step 1** To configure a port as an 802.1Q trunk, enter the **set trunk** command. You must use the **nonegotiate** keyword when configuring a port as an 802.1Q trunk.
- ```
Switch 1> (enable) set trunk 1/1 nonegotiate dot1q
Port(s) 1/1 trunk mode set to nonegotiate.
Port(s) 1/1 trunk type set to dot1q.
Switch 1> (enable) 04/15/1998,22:02:17:DISL-5:Port 1/1 has become dot1q trunk

Switch 2> (enable) 04/15/1998,22:01:42:SPANTREE-2: Rcvd 1Q-BPDU on non-1Q-trunk port 4/1
vlan 1.
04/15/1998,22:01:42:SPANTREE-2: Block 4/1 on rcving vlan 1 for inc trunk port.
04/15/1998,22:01:42:SPANTREE-2: Block 4/1 on rcving vlan 1 for inc peer vlan 2.
Switch 2> (enable)
```



Note After the port on Switch 1 is configured as an 802.1Q trunk, syslog messages are displayed on the Switch 2 console, and port 4/1 on Switch 2 is blocked. STP blocks the port because there is a port-type inconsistency on the trunk link: port 1/1 on Switch 1 is configured as an 802.1Q trunk while port 4/1 on Switch 2 is configured as an ISL trunk (see [Figure 11-5](#)). Port 4/1 would also be blocked if it were configured as a nontrunk port.

Figure 11-5 802.1Q Trunking: Port-Type Inconsistency



- Step 2** Display the problem on Switch 2 by entering the **show spantree** and **show spantree statistics** commands. The configuration mismatch exists until the port on Switch 2 is properly configured.

CISCO Confidential - DRAFT

```
Switch 2> (enable) show spantree 1
VLAN 1
Spanning tree enabled
Spanning tree type          ieee

Designated Root              00-60-09-79-c3-00
Designated Root Priority      32768
Designated Root Cost          0
Designated Root Port          1/0
Root Max Age    20 sec    Hello Time 2 sec    Forward Delay 15 sec

Bridge ID MAC ADDR            00-60-09-79-c3-00
Bridge ID Priority              32768
Bridge Max Age 20 sec    Hello Time 2 sec    Forward Delay 15 sec

Port      Vlan  Port-State      Cost    Priority  Fast-Start  Group-method
-----
1/1       1    not-connected      4        32    disabled
1/2       1    not-connected      4        32    disabled
4/1       1    type-pvid-inconsistent  100      32    disabled
4/2       1    not-connected     100        32    disabled
```

<...output truncated...>

```
Switch 2> (enable) show spantree statistics 4/1
Port 4/1 VLAN 1
```

SpanningTree enabled for vlanNo = 1

```
BPDU-related parameters
port spanning tree          enabled
state                        broken
port_id                      0x8142
port number                   0x142
path cost                     100
message age (port/VLAN)      1(20)
designated_root                00-60-09-79-c3-00
designated_cost                 0
designated_bridge              00-60-09-79-c3-00
designated_port                 0x8142
top_change_ack                FALSE
config_pending                FALSE
port_inconsistency            port_type & port_vlan
```

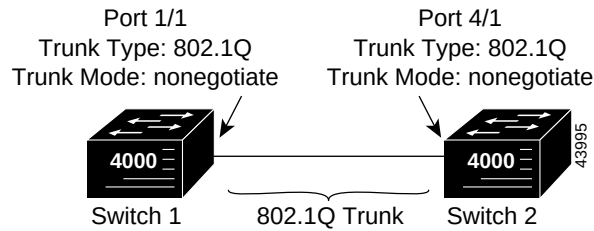
<...output truncated...>

```
Switch 2> (enable)
```

Step 3 Resolve the misconfiguration by completing the 802.1Q configuration on Switch 2:

```
Switch 2> (enable) set trunk 4/1 nonegotiate dot1q
Port(s) 4/1 trunk mode set to nonegotiate.
Port(s) 4/1 trunk type set to dot1q.
Switch 2> (enable) 2/20/1998,23:41:15:DISL-5:Port 4/1 has become dot1q trunk
```

Port 4/1 on Switch 2 changes from blocking mode to forwarding mode once the port-type inconsistency is resolved (see [Figure 11-6](#)). (This assumes that there is no wiring loop present that would cause the port to be blocked normally by spanning tree. In either case, the port state would change from “type-pvid-inconsistent” to “blocking” in the **show spantree** output.)

*CISCO Confidential - DRAFT***Figure 11-6 802.1Q Trunking: Final Network Configuration**

Step 4 Verify the 802.1Q configuration on Switch 1 by entering the **show trunk** and **show spantree** commands:

```
Switch 1> (enable) show trunk 1/1
```

Port	Mode	Encapsulation	Status	Native vlan
1/1	nonegotiate	dot1q	trunking	1

```

Port      Vlans allowed on trunk
-----
1/1      1-1005, 1025-4094

Port      Vlans allowed and active in management domain
-----
1/1      1-3,1003,1005

Port      Vlans in spanning tree forwarding state and not pruned
-----
1/1      1005

```

```
Switch 1> (enable) show spantree 1
```

```

VLAN 1
Spanning tree enabled
Spanning tree type          ieee

Designated Root             00-60-09-79-c3-00
Designated Root Priority     32768
Designated Root Cost         0
Designated Root Port         1/1
Root Max Age 20 sec  Hello Time 2 sec  Forward Delay 15 sec

Bridge ID MAC ADDR           00-10-29-b5-30-00
Bridge ID Priority            49152
Bridge Max Age 20 sec  Hello Time 2 sec  Forward Delay 15 sec

Port      Vlan  Port-State  Cost  Priority  Fast-Start  Group-method
-----
1/1       1    forwarding   4     32     disabled
1/2       1    not-connected 4     32     disabled

```

<...output truncated...>

```
Switch 1> (enable)
```

The output shows that port 1/1 is an 802.1Q trunk port, that its status is “trunking,” and that the port-state is “forwarding.”

Step 5 Verify the configuration on Switch 2 by entering the **show trunk** and **show spantree** commands:

```
Switch 2> (enable) show trunk 4/1
```

Port	Mode	Encapsulation	Status	Native vlan
4/1	nonegotiate	dot1q	trunking	1

CISCO Confidential - DRAFT

```

Port      Vlans allowed on trunk
-----
4/1      1-1005, 1025-4094

Port      Vlans allowed and active in management domain
-----
4/1      1-3,1003,1005

Port      Vlans in spanning tree forwarding state and not pruned
-----
4/1      1005
Switch 2> (enable) show spantree 1
VLAN 1
Spanning tree enabled
Spanning tree type          ieee

Designated Root              00-60-09-79-c3-00
Designated Root Priority      32768
Designated Root Cost          0
Designated Root Port         1/0
Root Max Age    20 sec    Hello Time 2   sec    Forward Delay 15 sec

Bridge ID MAC ADDR            00-60-09-79-c3-00
Bridge ID Priority              32768
Bridge Max Age  20 sec    Hello Time 2   sec    Forward Delay 15 sec

Port      Vlan  Port-State      Cost    Priority  Fast-Start  Group-method
-----
1/1      1      not-connected      4        32    disabled
1/2      1      not-connected      4        32    disabled
4/1      1      forwarding         100       32    disabled
4/2      1      not-connected      100       32    disabled
<...output truncated...>
Switch 2> (enable)

```

The output shows that port 4/1 is an 802.1Q trunk port, that its status is “trunking,” and that the port-state is “forwarding.”

Step 6 Verify connectivity across the trunk using the **ping** command:

```

Switch 1> (enable) ping switch_2
switch_2 is alive
Switch 1> (enable)

```

Configuring Dynamic VLAN Membership with VMPS

This chapter describes how to configure dynamic VLAN membership for ports in your network using the VLAN Management Policy Server (VMPS) on the Catalyst enterprise LAN switches.

**Note**

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 4500 Series, Catalyst 2948G, and Catalyst 2980G Switches Command Reference*.

This chapter consists of these sections:

- [Understanding How VMPS Works, page 12-1](#)
- [VMPS and Dynamic Port Hardware and Software Requirements, page 12-2](#)
- [Default VMPS and Dynamic Port Configuration, page 12-2](#)
- [Configuration Guidelines for Dynamic Ports and VMPS, page 12-3](#)
- [Configuring VMPS, page 12-4](#)
- [Troubleshooting VMPS and Dynamic Port VLAN Membership, page 12-10](#)
- [VMPS Example, page 12-11](#)
- [Dynamic Port VLAN Membership with Auxiliary VLANs, page 12-13](#)

Understanding How VMPS Works

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

When you enable VMPS, a MAC address-to-VLAN mapping database downloads from a Trivial File Transfer Protocol (TFTP) server to the VMPS server, and the VMPS server begins to accept client requests. VMPS remains enabled, regardless whether you reset or power cycle the switch.

The VMPS opens a User Datagram Protocol (UDP) socket to communicate and listen to client requests. When the VMPS server receives a valid request from a client, it searches its database for a MAC address-to-VLAN mapping.

CISCO Confidential - DRAFT

If the assigned VLAN is restricted to a group of ports, VMPS verifies the requesting port against this group. If the VLAN is allowed on the port, the VLAN name is returned to the client. If the VLAN is not allowed on the port and VMPS is in open mode, the host receives an “access denied” response. If VMPS is in secure mode, the port is shut down and you must manually bring the port back up with the **set port** command.

If a VLAN in the database does not match the current VLAN on the port and active hosts are on the port, VMPS sends an access denied or a port shutdown response based on the VMPS secure mode.

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

You can also make an explicit entry in the configuration table to deny access to specific MAC addresses for security reasons by specifying the **--NONE--** keyword for the VLAN name. In this case, VMPS sends an access denied or port shutdown response.

A dynamic port can belong to only one *native* VLAN in software releases prior to software release 6.2(1). With software release 6.2(1), a port can belong to a native VLAN and an auxiliary VLAN. See the “[Dynamic Port VLAN Membership with Auxiliary VLANs](#)” section on page 12-13 for complete details.

When the link comes up, a dynamic port is isolated from its static VLAN. The source MAC address from the first packet of a new host on the dynamic port is sent to the VMPS server, which attempts to match the MAC address to a VLAN in the VMPS database. If there is a match, VMPS provides the VLAN number to assign to the port. If there is no match, VMPS either denies the request or shuts down the port (depending on the VMPS secure mode setting).

You can use up to 50 hosts (MAC addresses) on a dynamic port if they are all authorized for the same VLAN. Each host that comes online through the port is checked against the VMPS database before the host is assigned to a VLAN.

If you move a host from one dynamic port to another, the port remains assigned to the VLAN until another MAC address changes the VLAN. You do not need to do clean up. All clean up is completed by the VMPS database.

VMPS and Dynamic Port Hardware and Software Requirements

VMPS and dynamic port membership requires these software and hardware versions (later software versions might be required depending on the specific hardware):

- Software release 5.1 or later releases—The Catalyst 4000 family switches support only VMPS clients.
- Software release 7.2 or later releases—The Catalyst 4000 family switches support both VMPS servers and clients.
- VMPS-capable hardware—To determine whether a specific piece of hardware supports dynamic port VLAN membership, refer to your hardware documentation or use the **show port capabilities** command. Dynamic port membership is not supported on Gigabit Ethernet ports.

Default VMPS and Dynamic Port Configuration

[Table 12-1](#) shows the default VMPS configurations.

*CISCO Confidential - DRAFT***Table 12-1 Defaults for VMPS Servers and VMPS Clients**

Feature	Default Configuration
VMPS Server	
VMPS enable state	Disabled
VMPS management domain	Null
VMPS TFTP server	None
VMPS database configuration filename	<i>vmpls-config-database.1</i>
VMPS fallback VLAN	Null
VMPS secure mode	Open
VMPS no domain requests	Allow
VMPS Client	
VMPS domain server	None
VMPS reconfirm interval	60 min
VMPS server retry count	3 attempts
Dynamic ports	No dynamic ports configured

Configuration Guidelines for Dynamic Ports and VMPS

This section lists the guidelines for configuring dynamic ports and VMPS:

- You must specify a primary VMPS server; you can specify up to two backup VMPS servers in your network.
- The primary VMPS server and backup VMPS servers do not communicate with each other about the VMPS database. You must enable VMPS on each server, and manually update each VMPS server when you update the VMPS database.
- You must configure VMPS before you configure ports as dynamic.
- When you configure a port as dynamic, spanning tree PortFast is enabled automatically for that port. Automatic enabling of spanning tree PortFast prevents applications on the host from timing out and entering loops caused by incorrect configurations. You can disable spanning tree PortFast mode on a dynamic port.
- If you reconfigure a port from a static port to a dynamic port on the same VLAN, the port connects immediately to that VLAN. However, VMPS checks the legality of the specific host on the dynamic port after a specified period.
- Static secure ports cannot become dynamic ports. You must turn off security on the static secure port before it can become dynamic.
- Static ports that are trunking cannot become dynamic ports. You must turn off trunking on the trunk port before changing it from static to dynamic.


Note

The VTP management domain and the management VLAN of VMPS clients and the VMPS server must be the same. For more information, see [Chapter 9, “Configuring VTP,”](#) and [Chapter 10, “Configuring VLANs.”](#)

CISCO Confidential - DRAFT

Configuring VMPS

To configure VMPS, follow these steps:

-
- Step 1** Create the VMPS Database. See the [“Creating the VMPS Database” section on page 12-4](#).
- Determine the MAC addresses of the hosts that you want assigned to VLANs dynamically.
 - On your workstation or PC, create an ASCII text file that contains the MAC address-to-VLAN mappings.
 - Move the ASCII text file to a TFTP server so it can be downloaded to the switch.
- Step 2** On the VMPS primary and backup servers, do the following:
- Specify the location and name of the VMPS database file.
 - Enable VMPS.
- See the [“Configuring the VMPS Server” section on page 12-7](#) for more information.
- Step 3** On the VMPS clients, do the following:
- Specify the IP addresses for the primary and backup VMSP servers.
 - Configure ports to dynamic mode.
- See the [“Configuring VMPS Clients” section on page 12-7](#) for more information.
- Step 4** Administer and monitor VMPS as necessary. See the [“Monitoring VMPS” section on page 12-8](#).

Creating the VMPS Database

To use VMPS, you first must create a VMPS database and store it on a TFTP server. The VMPS parser is line based. Start each entry in the file on a new line. The example at the end of this section corresponds to the information that is described below.

The VMPS database can have up to five sections:

Section 1, Global settings, lists the settings for the VMPS domain name, security mode, fallback VLAN, and the policy for VMPS and VTP domain name mismatches.

- Begin the configuration file with the word “VMPS,” to prevent other types of configuration files from incorrectly being read by the VMPS server.
- Define the VMPS domain. The VMPS domain should correspond to the VTP domain name configured on the switch.
- Define the security mode. VMPS can operate in open or secure mode. If you set it to open mode, VMPS returns an access denied response for an unauthorized MAC address and returns the fallback VLAN for a MAC address not listed in the VMPS database. In secure mode, VMPS shuts down the port for a MAC address that is unauthorized or that is not listed in the VMPS database.
- (Optional) Define a fallback VLAN. Assign the fallback VLAN if the MAC addresses of the connected host is not defined in the database.

In the example at the end of this section, the VMPS domain name is WBU, the VMPS mode is set to open, the fallback VLAN is set to the VLAN default, and if the VTP domain name does match the VMPS domain name, VMPS sends an access denied response message.

Section 2, MAC addresses, lists MAC addresses and authorized VLAN names for each MAC address.

CISCO Confidential - DRAFT

- Enter the MAC address of each host and the VLAN name to which each should belong.
- Use the **--NONE--** keyword as the VLAN name to deny the specified host network connectivity.
- You can enter up to 21,051 MAC addresses in a VMPS database file for the Catalyst 2948G switch.

In the example at the end of this section, MAC addresses are listed in the MAC table. Notice that the MAC address fedc.ba98.7654 is set to **--NONE--**. This setting explicitly denies this MAC address from accessing the network.

Section 3, Port groups, lists groups of ports on various switches in your network that you want grouped together. You use these port groups when defining VLAN port policies.

- Define a port group name for each port group, and then list all the ports that you want included in the port group.
- A port is identified by the IP address of the switch and the module/port number of the port in the form *mod_num/port_num*. Ranges are not allowed for the port numbers.
- Use the **all-ports** keyword to specify all the ports in the specified switch.

The example at the end of this section has two port groups:

- **WiringCloset1** consists of port 3/2 on the VMPS client 198.92.30.32 and port 2/8 on the VMPS client 172.20.26.141
- **Executive Row** consists of port 1/2 and 1/3 on the VMPS client 198.4.254.222, and all ports on the VMPS client 198.4.254.223

Section 4, VLAN groups, lists groups of VLANs that you want to associate together. You use these VLAN groups when defining VLAN port policies.

- Define the VLAN group name and then list each VLAN name that you want to include in the VLAN group.
- You can enter a maximum of 256 VLANs in a VMPS database file for the Catalyst 2948G switch.

The example at the end of this section has the VLAN group **Engineering**, which consists of the VLANs **hardware** and **software**.

Section 5, VLAN port policies, lists the VLAN port policies, which use the port groups and VLAN groups to further restrict access to the network.

- You can configure a restricted access using MAC addresses and the port groups or VLAN groups.

The example at the end of this section has three VLAN port policies specified:

- In the first VLAN port policy, the VLAN **hardware** or **software** is restricted to port 3/2 on the VMPS client 198.92.30.32 and port 2/8 on the VMPS client 172.20.23.141.
- In the second VLAN port policy, the devices that are specified in VLAN **Green** can connect only to port 4/8 on the VMPS client 198.92.30.32.
- In the third VLAN port policy, the devices that are specified in VLAN **Purple** can connect to only port 1/2 on the VMPS client 198.4.254.22 and the ports that are specified in the port group **Executive Row**.

This example shows a sample VMPS database configuration file:

```
!Section 1: GLOBAL SETTINGS
!VMPS File Format, version 1.1
! Always begin the configuration file with
! the word "VMPS"
!
!vmips domain <domain-name>
! The VMPS domain must be defined.
!vmips mode {open | secure}
```

CISCO Confidential - DRAFT

```

! The default mode is open.
!vmpls fallback <vlan-name>
!vmpls no-domain-req { allow | deny }
!
! The default value is allow.
vmpls domain WBU
vmpls mode open
vmpls fallback default
vmpls no-domain-req deny
!
!Section 2: MAC ADDRESSES
!MAC Addresses
vmpls-mac-addr
!
! address <addr> vlan-name <vlan_name>
!
address 0012.2233.4455 vlan-name hardware
address 0000.6509.a080 vlan-name hardware
address aabb.ccdd.eeff vlan-name Green
address 1223.5678.9abc vlan-name ExecStaff
address fedc.ba98.7654 vlan-name --NONE--
address fedc.ba23.1245 vlan-name Purple
!
!Section 3: PORT GROUPS
!Port Groups
!vmpls-port-group <group-name>
! device <device-id> { port <port-name> | all-ports }
!
vmpls-port-group WiringCloset1
device 198.92.30.32 port 3/2
device 172.20.26.141 port 2/8
vmpls-port-group "Executive Row"
device 198.4.254.222 port 1/2
device 198.4.254.222 port 1/3
device 198.4.254.223 all-ports
!
!Section 4: VLAN GROUPS
!VLAN groups
!
!vmpls-vlan-group <group-name>
! vlan-name <vlan-name>
!
vmpls-vlan-group Engineering
vlan-name hardware
vlan-name software
!
!Section 5: VLAN PORT POLICIES
!VLAN port Policies
!
!vmpls-port-policies {vlan-name <vlan_name> | vlan-group <group-name> }
! { port-group <group-name> | device <device-id> port <port-name> }
!
vmpls-port-policies vlan-group Engineering
port-group WiringCloset1
vmpls-port-policies vlan-name Green
device 198.92.30.32 port 4/8
vmpls-port-policies vlan-name Purple
device 198.4.254.22 port 1/2
port-group "Executive Row"

```

CISCO Confidential - DRAFT

Configuring the VMPS Server

When you enable VMPS on the VMPS server, the switch downloads the VMPS database from the TFTP or RCP server and begins accepting VMPS requests.

You can set one primary and up to two backup VMPS servers. The primary VMPS server and backup VMPS servers do not communicate with each other about the VMPS database. You must enable VMPS on each server and manually update each VMPS server when you update the VMPS database.

To configure a VMPS server, perform this task in privileged mode. You must complete this task for the primary and any backup VMPS servers in your network.

	Task	Command
Step 1	Specify the download method.	set vmps downloadmethod rcp tftp [username]
Step 2	Configure the IP address of the TFTP or RCP server on which the ASCII text VMPS database configuration file resides.	set vmps downloadserver ip_addr [filename]
Step 3	Enable VMPS.	set vmps state enable
Step 4	Verify the VMPS configuration.	show vmps

This example shows how to set the VMPS database as Bldg-G.db on the TFTP server with the IP address 172.20.22.7 and enable VMPS on the switch:

```
Console> (enable) set vmps downloadmethod tftp
vmps download method : TFTP
Console> (enable) set vmps tftpserver 172.20.22.7 Bldg-G.db
IP address of the TFTP server set to 172.20.22.7
VMPS configuration filename set to Bldg-G.db
Console> (enable) set vmps state enable
Vlan Membership Policy Server enable is in progress.
Console> (enable)
```

Configuring VMPS Clients

When you configure a VMPS client, you must configure VMPS on the VMPS client before setting dynamic ports.

You cannot make trunk ports or secure ports a dynamic port. If you attempt to make a trunk port a dynamic port, VMPS disables trunking on the port to make it a dynamic port.

To configure VMPS client switches, perform this task in privileged mode:

	Task	Command
Step 1	Specify the IP address for the primary VMPS server.	set vmps server ip_addr [primary]
Step 2	(Optional) Specify the IP address for the backup VMPS server(s).	set vmps server ip_addr
Step 3	Verify the VMPS server specification.	show vmps server
Step 4	Configure ports on the switch to dynamic mode.	set port membership mod_num/port_num dynamic
Step 5	Verify the dynamic port assignments.	show port [mod_num[/port_num]]

CISCO Confidential - DRAFT

This example shows how to specify the primary VMPS server and two backup VMPS servers, and verify the VMPS server specification:

```

Console> (enable) set vmps server 192.0.0.1 primary
192.0.0.1 added to VMPS table as primary domain server.
Console> (enable) set vmps server 192.0.0.6
192.0.0.6 added to VMPS table as backup domain server.
Console> (enable) set vmps server 192.0.0.9
192.0.0.9 added to VMPS table as backup domain server.

```

```

Console> (enable) show vmps server

```

```

VMPS Client Status:
-----
VMPS VQP Version:      1
Reconfirm Interval:    60 min
Server Retry Count:    3
VMPS domain server:    192.0.0.1 (primary)
                      192.0.0.6
                      192.0.0.9

```

This example shows how to set ports 1 to 3 on module 3 to dynamic mode, disable trunking port 1 on module 2 to make it a dynamic port, and verify the port configuration:

```

Console> (enable) set port membership 3/1-3 dynamic
Ports 3/1-3 vlan assignment set to dynamic.
Console> (enable) set port membership 2/1 dynamic
Spantree port fast start option enabled for ports 2/1.
Trunk mode set to off for ports 2/1.
Console> show port
Port  Name      Status  Vlan   Level  Duplex  Speed  Type
1/1          connect trunk  normal full    100    100 BASE-TX
1/2          connect trunk  normal half    100    100 BASE-TX
2/1          connect dyn   normal full    155    OC3 MMF ATM
3/1          connect dyn-5 normal half    10     10 BASE-T
3/2          connect dyn-5 normal half    10     10 BASE-T
3/3          connect dyn-5 normal half    10     10 BASE-T
.
.
.
Console> (enable)

```



Note

The **show port** command displays dyn- in the Vlan column of the display when a VLAN has not been assigned to a port.

Monitoring VMPS

To display information about MAC address-to-VLAN mappings, perform one of these tasks in privileged mode:

Task	Command
Show the VLAN to which a MAC address is mapped in the database.	show vmps mac [mac_address]

CISCO Confidential - DRAFT

Task	Command
Show the MAC addresses that are mapped to a VLAN in the database.	show vmps vlan <i>vlan_name</i>
Show ports belonging to a restricted VLAN.	show vmps vlanports <i>vlan_name</i>

To show VMPS statistics, perform this task in privileged mode:

Task	Command
Show VMPS statistics.	show vmps statistics

Maintaining VMPS

To clear VMPS statistics, perform this task in privileged mode:

Task	Command
Clear VMPS statistics.	clear vmps statistics

To clear a VMPS server entry from the VMPS client, perform this task in privileged mode:

Task	Command
Clear a VMPS server entry.	clear vmps server <i>ip_addr</i>

To reconfirm the dynamic port VLAN membership assignments, perform this task in privileged mode:

	Task	Command
Step 1	Reconfirm dynamic port VLAN membership.	reconfirm vmps
Step 2	Verify the dynamic VLAN reconfirmation status.	show dvlan statistics

This example shows how to reconfirm dynamic port VLAN membership assignments:

```
Console> (enable) reconfirm vmps
reconfirm process started
Use 'show dvlan statistics' to see reconfirm status
Console> (enable)
```

To download the VMPS database manually and refresh the existing VMPS database, perform this task in privileged mode. If you are updating the VMPS database, you need to download the VMPS database to the primary and backup VMPS servers.

	Task	Command
Step 1	Download the VMPS database from the TFTP server, or specify a different VMPS database configuration file.	download vmps
Step 2	Verify the VMPS database configuration file.	show vmps

CISCO Confidential - DRAFT

To disable VMPS on the VMPS server, perform this task in privileged mode. When you disable the VMPS server, any active dynamic ports in the network will retain the VLAN until the host releases the VLAN or disconnects from the port.

	Task	Command
Step 1	Disable VMPS.	set vmps state disable
Step 2	Verify that VMPS is disabled.	show vmps

This example shows how to disable VMPS on the switch:

```
Console> (enable) set vmps state disable
All the VMPS configuration information will be lost and the resources released on disable.
Do you want to continue (y/n[n]): y
Vlan Membership Policy Server disabled.
Console> (enable)
```

Configuring Static Ports

To return a port to the static mode, perform this task in privileged mode:

	Task	Command
Step 1	Configure to static mode.	set port membership mod_num/port_num static
Step 2	Verify the static port assignments.	show port [mod_num[/port_num]]

This example shows how to return port 1 on module 3 to static mode:

```
Console> (enable) set port membership 3/1 static
Port 3/1 vlan assignment set to static.
Spantree port fast start option set to default for ports 3/1.
Console> (enable)
```

Troubleshooting VMPS and Dynamic Port VLAN Membership

The next two sections describe how to troubleshoot VMPS and dynamic port VLAN membership.

Troubleshooting VMPS

Table 12-2 shows the VMPS error messages that you might see when you enter the **set vmps state enable** or the **download vmps** command.

*CISCO Confidential - DRAFT***Table 12-2 VMPS Error Messages**

VMPS Error Message	Recommended Action
TFTP server IP address is not configured.	Specify the TFTP server address using the set vmps tftpserver ip_addr [filename] command.
Unable to contact the TFTP server 172.16.254.222.	Enter a static route (using the set ip route command) to the TFTP server.
File "vmips_configuration.db" not found on the TFTP server 172.16.254.222.	Check the filename of the VMPS database configuration file on the TFTP server. Verify that the permissions are set correctly.
Failed to download VMPS configuration file. Out of memory.	The VMPS database file might have more than 256 different VLANs specified. Reduce the number of VLANs that are used in the file.
Download aborted. File size larger than download buffer	The VMPS database file is longer than 21051 lines. If possible, shorten the file.

After VMPS successfully downloads the VMPS database configuration file, it parses the existing file on the VMPS server and builds a database. When the parsing is complete, VMPS displays statistics about the total number of lines parsed and the number of parsing errors.

To obtain more information on VMPS parsing errors, set the syslog level for VMPS to 3 using the **set logging level vmips** command.

Troubleshooting Dynamic Ports

A dynamic port might shut down under these circumstances:

- VMPS is in secure mode, and it is illegal for the host to connect to the port. The port shuts down to prevent the host from connecting to the network.
- More than 50 active hosts reside on a dynamic port.

To reenab a dynamic port that has been shut down, enter the **set port enable** command.

When you move a PC from a hub connected to the switch to a direct port on the VMPS client, both ports remain assigned to the same VLAN.

The VMPS query and response messages are multicast packets with a destination address of 01000CCCCCD.

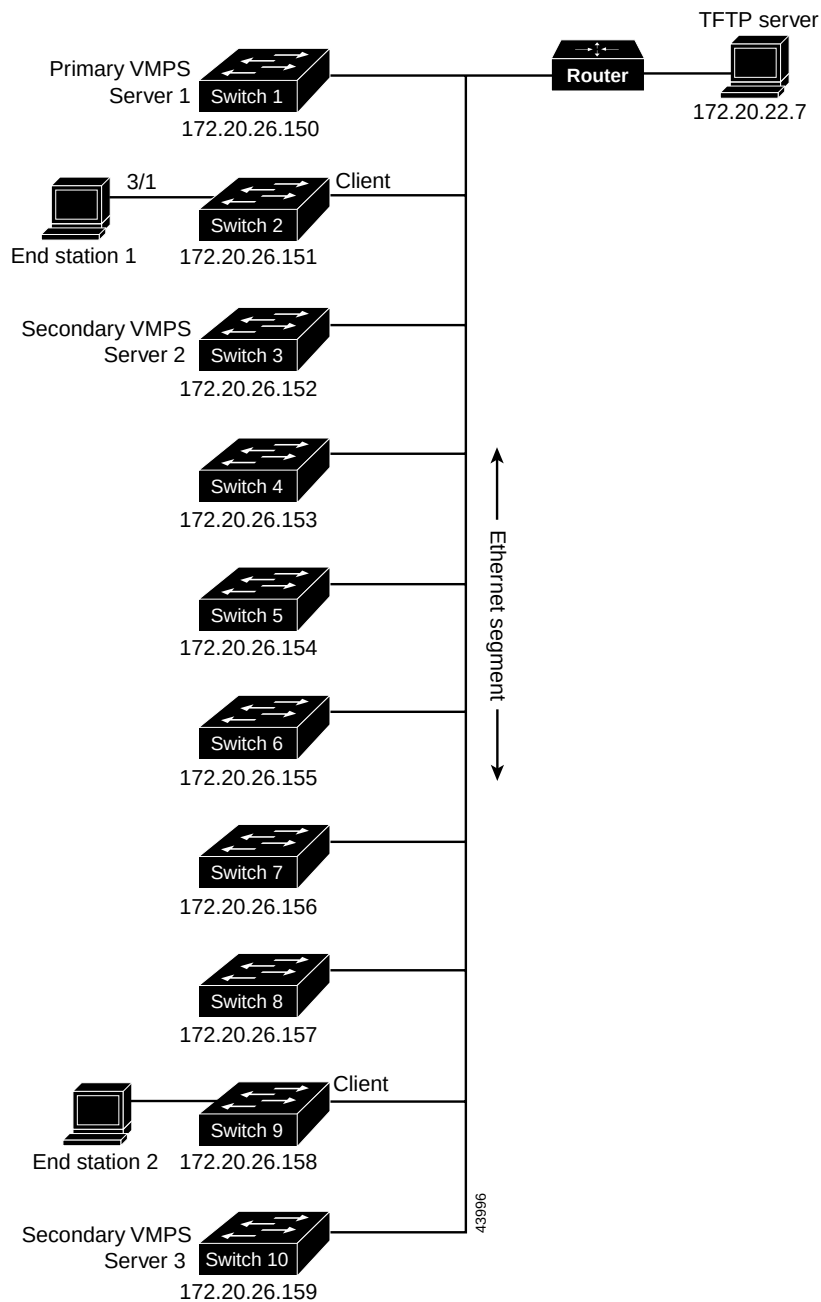
VMPS Example

Figure 12-1 shows a network with a VMPS server switch, two backup VMPS servers, and VMPS client switches with dynamic ports. In this example, the following assumptions apply:

- The VMPS server and the VMPS client are separate switches.
- Switch 1 is the primary VMPS server.
- Switch 3 and Switch 10 are secondary VMPS servers.
- End stations are connected to these clients:
 - Switch 2

CISCO Confidential - DRAFT

- Switch 9
- The database configuration file is called **Bldg-G.db** and is stored on a TFTP server with IP address 172.20.22.7.

Figure 12-1 Dynamic Port VLAN Membership Configuration

To configure VMPS and dynamic ports, follow these steps:

CISCO Confidential - DRAFT

-
- Step 1** Configure Switch 1 as the primary VMPS server.
- a. Configure the IP address of the TFTP server on which the ASCII file resides:
Console> (enable) **set vmps tftpserver 172.20.22.7 Bldg-G.db**
 - b. Enable VMPS:
Console> (enable) **set vmps state enable**
- After entering these commands, the file **Bldg-G.db** is downloaded to Switch 1. Switch 1 becomes the VMPS server.
- Step 2** Configure Switch 2 and Switch 3 as backup VMPS servers.
- a. Configure the IP address of the TFTP server on which the ASCII file resides:
Console> (enable) **set vmps tftpserver 172.20.26.152 Bldg-G.db**
 - b. Enable VMPS:
Console> (enable) **set vmps state enable**
 - c. Repeat Steps a and b for switch 3.
- After you enter these commands, the file **Bldg-G.db** is downloaded to each switch.
- Step 3** Configure the VMPS server addresses on each VMPS client.
- a. Configure the IP address for the primary VMPS server:
Console> (enable) **set vmps server 172.20.26.150 primary**
 - b. Configure the IP addresses for the backup VMPS servers:
Console> (enable) **set vmps server 172.20.26.152**
Console> (enable) **set vmps server 172.20.26.159**
 - c. Verify the VMPS server addresses:
Console> (enable) **show vmps server**
- Step 4** Configure port 3/1 on Switch 2 as dynamic.
Console> (enable) **set port membership 3/1 dynamic**
- Step 5** Connect End Station 2 on port 3/1.
- When End Station 2 sends a packet, Switch 2 sends a query to the primary VMPS server, Switch 1. Switch 1 responds with a message to assign port 3/1 to the VLAN specified in the VMPS database. Because spanning tree PortFast mode is enabled by default on dynamic ports, port 3/1 connects immediately and enters forwarding mode.
- Step 6** Repeat Steps 2 and 3 to configure the VMPS server addresses and assign dynamic ports on each VMPS client switch.
-

Dynamic Port VLAN Membership with Auxiliary VLANs

This section describes how to configure a dynamic port to belong to two VLANs—a native VLAN and an auxiliary VLAN. This section uses the following terminology:

CISCO Confidential - DRAFT

- Auxiliary VLAN—Separate VLAN for IP phones
- Native VLAN—Traditional VLAN for data
- Auxiliary VLAN ID—VLAN ID of an auxiliary VLAN
- Native VLAN ID—VLAN ID of a native VLAN

Prior to software release 6.2(1), dynamic ports could only belong to one VLAN. You could not enable the dynamic port VLAN feature on ports that carried a native VLAN and an auxiliary VLAN.

With software release 6.2(1) and later releases, the dynamic ports can belong to two VLANs. The switch port configured for connecting an IP phone can have separate VLANs configured for carrying the following:

- Voice traffic to and from the IP phone (auxiliary VLAN)
- Data traffic to and from the PC that is connected to the switch through the *access port* of the IP phone (native VLAN)

Configuration Guidelines

This section lists the guidelines for configuring dynamic port VLAN membership for auxiliary VLANs:

- Read the “[Configuration Guidelines for Dynamic Ports and VMPS](#)” section on page 12-3 before you begin the configuration.
- Configuration of the native VLAN ID is dynamic for the PC that is connected to the access port of the IP phone. Configuration of the auxiliary VLAN ID is not dynamic, you need to configure it manually. As you manually configure the auxiliary VLAN ID, the VMPS server is queried for packets coming from the PC, but not for packets coming from the IP phone.
- All packets, except CDP packets from the IP phone, are tagged with the auxiliary VLAN ID. All such tagged packets are considered to be packets from the phone, and all other packets are considered to be packets from the PC.
- When configuring the auxiliary VLAN ID with untagged frames, you need to configure the VMPS server with the IP phone’s MAC address (see the “[VMPS Example](#)” section on page 12-11 for information on configuring VMPS).
- For dynamic ports, the auxiliary VLAN ID cannot be the same as the native VLAN ID that is assigned by VMPS for the dynamic port.

Configuring Dynamic Port VLAN Membership with Auxiliary VLANs

This example shows how to add voice ports to auxiliary VLANs and specify an encapsulation type:

```

Console> (enable) set port auxiliaryvlan 5/9 222
Auxiliaryvlan 222 configuration successful.
AuxiliaryVlan AuxVlanStatus Mod/Ports
-----
222          active          5/9
Console> (enable)

Console> (enable) set port auxiliaryvlan 5/9 untagged
Port 2/48 allows the connected device send and receive untagged packets and without 802.1p
priority.
Console> (enable)

```

This example shows how to specify port 5/9 as a dynamic port:

CISCO Confidential - DRAFT

```
Console> (enable) set port membership 5/9 dynamic  
Warning: Auxiliary Vlan set to dot1p|untagged on dynamic port. VMPS will be queried for IP  
phones.  
Port 5/9 vlan assignment set to dynamic.  
Spantree port fast start option enabled for ports 5/9.  
Console> (enable)
```

This example shows that the auxiliary VLAN ID specified cannot be the same as the native VLAN ID:

```
Console> (enable) set port auxiliaryvlan 5/10 223  
Auxiliary vlan cannot be set to 223 as PVID=223.  
Console> (enable)
```

CISCO Confidential - DRAFT

Configuring GVRP

This chapter describes how to configure the Generic Attribute Registration Protocol (GARP) VLAN Registration Protocol (GVRP) on the Catalyst enterprise LAN switches.

**Note**

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 4500 Series, Catalyst 2948G, and Catalyst 2980G Switches Command Reference*.

This chapter consists of these sections:

- [Understanding How GVRP Works, page 13-1](#)
- [GVRP Hardware and Software Requirements, page 13-1](#)
- [Default GVRP Configuration, page 13-2](#)
- [GVRP Configuration Guidelines, page 13-2](#)
- [Configuring GVRP on the Switch, page 13-2](#)

Understanding How GVRP Works

GARP and GVRP are industry-standard protocols described in IEEE 802.1p.

GVRP is a GARP application that provides 802.1Q-compliant VLAN pruning and dynamic VLAN creation on 802.1Q trunk ports.

With GVRP, the switch can exchange VLAN configuration information with other GVRP switches, prune unnecessary broadcast and unknown unicast traffic, and dynamically create and manage VLANs on switches connected through 802.1Q trunk ports.

GVRP Hardware and Software Requirements

GVRP requires these software and hardware versions:

- Supervisor engine software release 5.1 or later releases
- IEEE 802.1Q-capable switching modules (refer to the documentation for your hardware, or use the **show port capabilities** command)

CISCO Confidential - DRAFT

Default GVRP Configuration

Table 13-1 shows the default GVRP configuration.

Table 13-1 GVRP Default Configuration

Feature	Default Value
GVRP global enable state	Disabled
GVRP per-trunk enable state	Disabled on all ports
GVRP dynamic creation of VLANs	Disabled
GVRP registration mode	normal , with VLAN 1 set to fixed , for all ports
GVRP applicant state	normal (ports do not declare VLANs when in STP ¹ blocking state)
GARP timers	- Join time: 200 ms - Leave time: 600 ms - Leaveall time: 10,000 ms

1. STP = Spanning Tree Protocol

GVRP Configuration Guidelines

This section lists the guidelines for configuring GVRP:

- You can configure the per-port GVRP state only on 802.1Q-capable ports.
- You must enable GVRP on both ends of an 802.1Q trunk link.
- The GVRP registration mode for VLAN 1 is always **fixed** and is not configurable. VLAN 1 is always carried by 802.1Q trunks on which GVRP is enabled.
- When VTP pruning is enabled, it runs on all GVRP-disabled 802.1Q trunk ports.

Configuring GVRP on the Switch

The following sections describe how to configure GVRP.

Enabling GVRP Globally

You must enable GVRP globally before any GVRP will process on the switch. Enabling GVRP globally enables GVRP to perform VLAN pruning on 802.1Q trunk links. Pruning occurs only on GVRP-enabled trunks. For information on setting the per-trunk port GVRP enable state, see the [“Enabling GVRP on Individual 802.1Q Trunk Ports”](#) section on page 13-3.

To enable dynamic VLAN creation, you must explicitly enable dynamic VLAN creation globally on the switch as well. For information on enabling dynamic VLAN creation, see the [“Enabling GVRP Dynamic VLAN Creation”](#) section on page 13-4.

To enable GVRP globally on the switch, perform this task in privileged mode:

CISCO Confidential - DRAFT

	Task	Command
Step 1	Enable GVRP on the switch.	set gvrp enable
Step 2	Verify the configuration.	show gvrp configuration

This example shows how to enable GVRP and verify the configuration:

```

Console> (enable) set gvrp enable
GVRP enabled
Console> (enable) show gvrp configuration
Global GVRP Configuration:
GVRP Feature is currently enabled on the switch.
GVRP dynamic VLAN creation is disabled.
GVRP Timers(milliseconds)
Join = 200
Leave = 600
LeaveAll = 10000

Port based GVRP Configuration:
Port                                     GVRP Status Registration
-----
2/1-2,3/1-8,7/1-24,8/1-24             Enabled      Normal

GVRP Participants running on 3/7-8.
Console>

```

Enabling GVRP on Individual 802.1Q Trunk Ports



Note

You can change the per-trunk GVRP configuration regardless of whether GVRP is enabled globally. However, GVRP will not function on any ports until you enable it globally. For information on configuring GVRP globally on the switch, see the [“Enabling GVRP Globally” section on page 13-2](#).

There are two per-port GVRP states:

- The static GVRP state configured in the CLI and stored in NVRAM
- The actual GVRP state of the ports (active GVRP participants)

You can configure the static GVRP port-state on any 802.1Q-capable switch ports, regardless of the global GVRP enable state or whether the port is an 802.1Q trunk. However, in order for the port to become an active GVRP participant, you must enable GVRP globally and the port must be an 802.1Q trunk port, either through CLI configuration or Dynamic Trunking Protocol (DTP) negotiation.

To enable GVRP on individual 802.1Q-capable ports, perform this task in privileged mode:

	Task	Command
Step 1	Enable GVRP on an individual 802.1Q-capable port.	set port gvrp enable mod_num/port_num
Step 2	Verify the configuration.	show gvrp configuration

This example shows how to enable GVRP on 802.1Q-capable port 1/1:

```

Console> (enable) set port gvrp enable 1/1
GVRP enabled on 1/1.
Console> (enable)

```

CISCO Confidential - DRAFT

Enabling GVRP Dynamic VLAN Creation

You can enable GVRP dynamic VLAN creation only if these conditions are met:

- The switch is in VTP transparent mode
- All trunk ports on the switch are 802.1Q trunks
- GVRP is enabled on all trunk ports

**Note**

Dynamic VLAN creation supports all VLAN types.

If you enable dynamic VLAN creation, these configuration restrictions are imposed:

- You cannot change the switch to VTP server or client mode
- You cannot disable GVRP on a trunk port running GVRP

If any port on the switch becomes an ISL trunk (either by CLI configuration or negotiated using DTP while dynamic VLAN creation is enabled), dynamic VLAN creation is automatically disabled until the conditions for enabling dynamic VLAN creation are restored.

**Note**

VLANs can only be created dynamically on 802.1Q trunks in the **normal** registration mode.

To enable GVRP dynamic VLAN creation on the switch, perform this task in privileged mode:

	Task	Command
Step 1	Enable dynamic VLAN creation on the switch.	set gvrp dynamic-vlan-creation enable
Step 2	Verify the configuration.	show gvrp configuration

This example shows how to enable dynamic VLAN creation on the switch:

```
Console> (enable) set gvrp dynamic-vlan-creation enable
Dynamic VLAN creation enabled.
Console> (enable)
```

Configuring GVRP Registration

The following sections describe how to configure GVRP registration modes on switch ports.

Setting GVRP Normal Registration

Configuring an 802.1Q trunk port in **normal** registration mode allows dynamic creation (if dynamic VLAN creation is enabled), registration, and deregistration of VLANs on the trunk port. Normal mode is the default.

To configure GVRP normal registration on an 802.1Q trunk port, perform this task in privileged mode:

CISCO Confidential - DRAFT

	Task	Command
Step 1	Configure normal registration on an 802.1Q trunk port.	set gvrp registration normal <i>mod_num/port_num</i>
Step 2	Verify the configuration.	show gvrp configuration

This example shows how to configure normal registration on an 802.1Q trunk port:

```
Console> (enable) set gvrp registration normal 1/1
Registrar Administrative Control set to normal on port 1/1.
Console> (enable)
```

Setting GVRP Fixed Registration

Configuring an 802.1Q trunk port in **fixed** registration mode allows manual creation and registration of VLANs, prevents VLAN deregistration, and registers all known VLANs on other ports on the trunk port.

To configure GVRP fixed registration on an 802.1Q trunk port, perform this task in privileged mode:

	Task	Command
Step 1	Configure fixed registration on an 802.1Q trunk port.	set gvrp registration fixed <i>mod_num/port_num</i>
Step 2	Verify the configuration.	show gvrp configuration

This example shows how to configure fixed registration on an 802.1Q trunk port:

```
Console> (enable) set gvrp registration fixed 1/1
Registrar Administrative Control set to fixed on port 1/1.
Console> (enable)
```

Setting GVRP Forbidden Registration

Configuring an 802.1Q trunk port in **forbidden** registration mode deregisters all VLANs (except VLAN 1) and prevents any further VLAN creation or registration on the trunk port.

To configure GVRP forbidden registration on an 802.1Q trunk port, perform this task in privileged mode:

	Task	Command
Step 1	Configure forbidden registration on an 802.1Q trunk port.	set gvrp registration forbidden <i>mod_num/port_num</i>
Step 2	Verify the configuration.	show gvrp configuration

This example shows how to configure forbidden registration on an 802.1Q trunk port:

```
Console> (enable) set gvrp registration forbidden 1/1
Registrar Administrative Control set to forbidden on port 1/1.
Console> (enable)
```

CISCO Confidential - DRAFT

Sending GVRP VLAN Declarations from Blocking Ports

To prevent undesirable Spanning Tree Protocol (STP) topology reconfiguration on a port that is connected to a device that does not support per-VLAN STP, configure the GVRP active applicant state on the port. Ports in the GVRP active applicant state send GVRP VLAN declarations when they are in the STP blocking state, which prevents the STP bridge protocol data units (BPDUs) from being pruned from the other port.

**Note**

Configuring fixed registration on the other device's port would also prevent undesirable STP topology reconfiguration.

To configure an 802.1Q trunk port to send VLAN declarations when in the blocking state, perform this task in privileged mode:

Task	Command
Configure an 802.1Q trunk port to send VLAN declarations when in the blocking state.	set gvrp applicant state {normal active} mod_num/port_num

This example shows how to configure a group of 802.1Q trunk ports to send VLAN declarations when in the blocking state:

```
Console> (enable) set gvrp applicant active 4/2-3,4/9-10,4/12-24  
Applicant was set to active on port(s) 4/2-3,4/9-10,4/12-24.  
Console> (enable)
```

Use the **normal** keyword to return to the default state (active mode disabled).

Setting the GARP Timers

**Note**

The commands **set gvrp timer** and **show gvrp timer** are aliases for **set garp timer** and **show garp timer**. The aliases may be used if desired.

**Note**

Modifying the GARP timer values affects the behavior of *all* GARP applications running on the switch, not just GVRP. (For example, GMRP uses the same timers.)

You can modify the default GARP timer values on the switch.

When you set the timer values, the value for **leave** must be greater than three times the **join** value (**leave** >= **join** * 3). The value for **leaveall** must be greater than the value for **leave** (**leaveall** > **leave**).

If you attempt to set a timer value that does not adhere to these rules, an error message is displayed. For example, if you set the **leave** timer to 600 ms and you attempt to configure the **join** timer to 350 ms, an error message is displayed. Set the **leave** timer to at least 1050 ms, and then set the **join** timer to 350 ms.

CISCO Confidential - DRAFT**Caution**

Set the same GARP timer values on all Layer 2-connected devices. If the GARP timers are set differently on Layer 2-connected devices, GARP applications (for example, GMRP and GVRP) do not operate successfully.

To adjust the GARP timer values, perform this task in privileged mode:

	Task	Command
Step 1	Set the GARP timer values.	set garp timer {join leave leaveall} timer_value
Step 2	Verify the configuration.	show garp timer

This example shows how to set GARP timers and verify the configuration:

```

Console> (enable) set garp timer leaveall 10000
GMRP/GARP leaveAll timer value is set to 10000 milliseconds.
Console> (enable) set garp timer leave 600
GMRP/GARP leave timer value is set to 600 milliseconds.
Console> (enable) set garp timer join 200
GMRP/GARP join timer value is set to 200 milliseconds.
Console> (enable) show garp timer
Timer      Timer Value (milliseconds)
-----
Join       200
Leave       600
LeaveAll    10000
Console> (enable)

```

Displaying GVRP Statistics

To display GVRP statistics on the switch, perform this task:

Task	Command
Display GVRP statistics.	show gvrp statistics [mod_num/port_num]

This example shows how to display GVRP statistics for port 1/1:

```

Console> (enable) show gvrp statistics 1/1
Join Empty Received:      0
Join In Received:        0
Empty Received:          0
LeaveIn Received:         0
Leave Empty Received:     0
Leave All Received:       40
Join Empty Transmitted: 156
Join In Transmitted:     0
Empty Transmitted:       0
Leave In Transmitted:     0
Leave Empty Transmitted:  0
Leave All Transmitted:    41
VTP Message Received:    0
Console> (enable)

```

CISCO Confidential - DRAFT

Clearing GVRP Statistics

To clear all GVRP statistics on the switch, perform this task in privileged mode:

Task	Command
Clear GVRP statistics.	clear gvrp statistics { <i>mod_num/port_num</i> all }

This example shows how to clear all GVRP statistics on the switch:

```
Console> (enable) clear gvrp statistics all
GVRP Statistics cleared for all ports.
Console> (enable)
```

Disabling GVRP on Individual 802.1Q Trunk Ports

To disable GVRP on individual 802.1Q trunk ports, perform this task in privileged mode:

	Task	Command
Step 1	Disable GVRP on an individual 802.1Q trunk port.	set port gvrp disable <i>mod_num/port_num</i>
Step 2	Verify the configuration.	show gvrp configuration

This example shows how to disable GVRP on 802.1Q trunk port 1/1:

```
Console> set gvrp disable 1/1
GVRP disabled on 1/1.
Console>
```

Disabling GVRP Globally

To disable GVRP globally on the switch, perform this task in privileged mode:

Task	Command
Disable GVRP on the switch.	set gvrp disable

This example shows how to disable GVRP globally on the switch:

```
Console> (enable) set gvrp disable
GVRP disabled
Console> (enable)
```

Configuring QoS

This chapter describes how to configure quality of service (QoS) on Catalyst enterprise LAN switches.

**Note**

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 4500 Series, Catalyst 2948G, and Catalyst 2980G Switches Command Reference*.

This chapter consists of these sections:

- [Understanding How QoS Works, page 14-1](#)
- [Software Requirements, page 14-4](#)
- [QoS Default Configuration, page 14-4](#)
- [Configuring QoS on the Switch, page 14-4](#)

Understanding How QoS Works

These sections describe how QoS works:

- [QoS Overview, page 14-1](#)
- [Understanding QoS Terminology, page 14-2](#)
- [Understanding Classification and Marking at the Ingress Port, page 14-3](#)
- [Understanding Scheduling, page 14-3](#)

QoS Overview

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, prioritizes it according to its relative importance, and provides priority-indexed treatment through congestion-avoidance techniques. Implementing QoS in your network makes network performance more predictable and bandwidth utilization more effective.

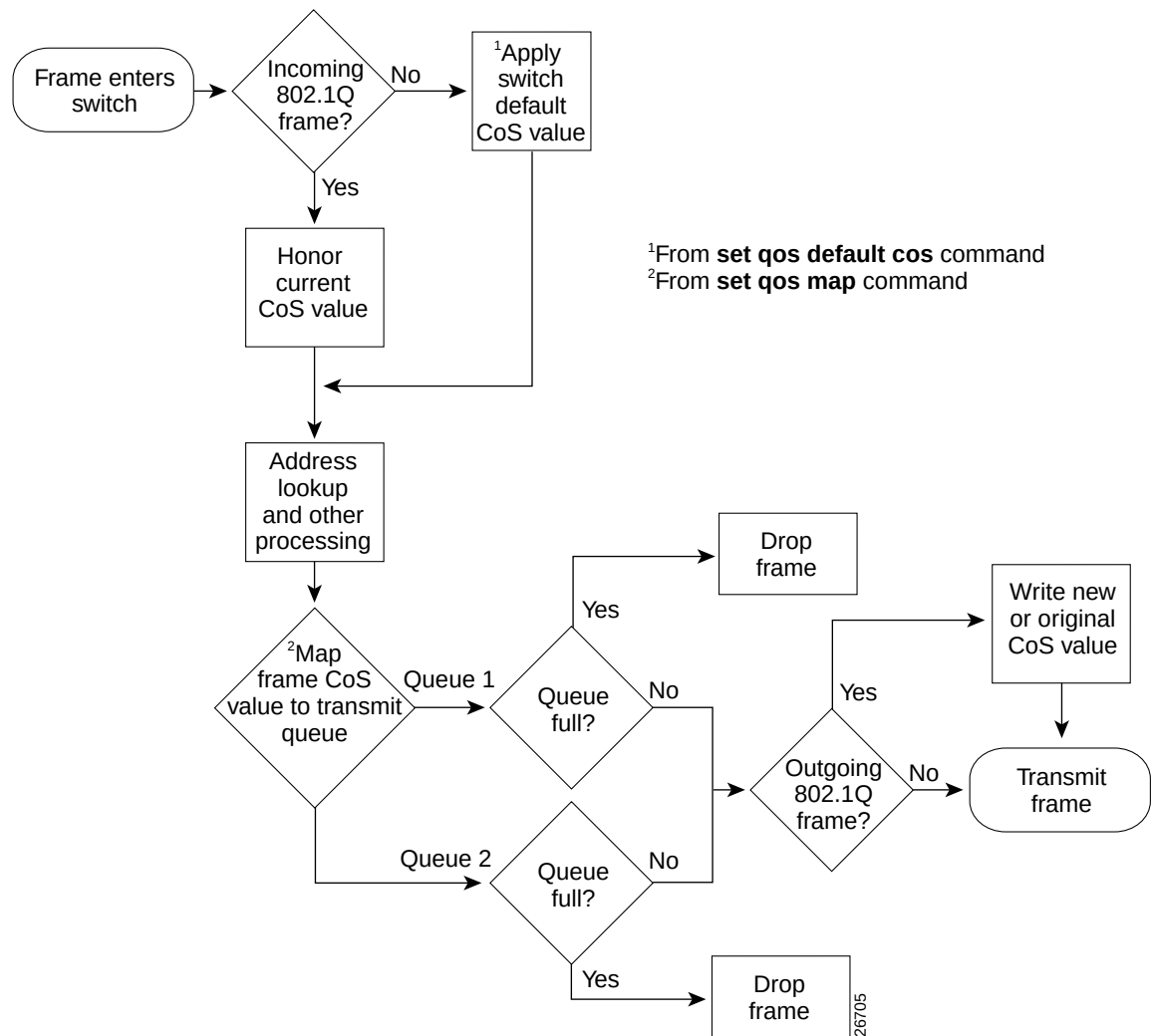
QoS classifies traffic by assigning priority-indexed 802.1p class of service (CoS) values to frames at ingress ports. If traffic is tagged with a CoS value at the ingress port, the switch forwards the value. If traffic is native, then the switch can rewrite the CoS tag.

■ Understanding How QoS Works

QoS implements scheduling on supported egress ports with transmit queue drop thresholds and multiple transmit queues that use the 802.1p CoS values to give preference to higher-priority traffic.

Figure 14-1 shows how QoS affects the traffic flow.

Figure 14-1 Traffic Flow Through the Switch with QoS Enabled—Catalyst 4000 Family, Catalyst 2948G, and Catalyst 2980G Switches



Understanding QoS Terminology

The following QoS terminology is used in this chapter:

- QoS *labels* are used to prioritize traffic:
 - Layer 2 CoS values—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 (the User Priority bits). Other frame types cannot carry CoS values. CoS values range between 0 (low priority) and 7 (high priority).
- *Classification* is the selection of traffic to be marked.

CISCO Confidential - DRAFT

- *Marking* is the application of QoS labels to traffic.
- *Scheduling* is the assignment of traffic to a queue. QoS assigns traffic based on CoS values.
- *Congestion avoidance* is the process by which QoS reserves ingress and egress port capacity for traffic with high-priority CoS values. QoS implements congestion avoidance with CoS value-based drop thresholds and transmit queues. A drop threshold is the percentage of buffer utilization at which traffic with a specified CoS value is dropped, leaving the buffer available for traffic with higher-priority CoS values. A transmit queue is a queue on the egress port where outgoing frames are stored before transmission. With multiple transmit queues, traffic with higher-priority CoS values can be placed in a reserved transmit queue.
- *Policing* is the process by which the switch limits the bandwidth consumed by a flow of traffic. Policing can mark or drop traffic.

Understanding Classification and Marking at the Ingress Port

ISL or 802.1Q frames are not classified or marked at the ingress port; the existing CoS value is honored. When an 802.1Q frame enters the switch through a supported ingress port, QoS accepts the User Priority bits as the CoS value.

QoS classifies and marks all other frame types that enter the switch with the default CoS value configured for the entire switch. You cannot mark traffic on a per-port basis.



Note

The Catalyst 4000 family, 2948G, and 2980G switches support frame classification and marking only on unclassified frames entering the switch.

Understanding Scheduling

There are two user-configurable transmit queues and one non-user-configurable transmit queue drop threshold for each port. You can specify such ports using the **2q1t** keyword in QoS-related commands.

QoS uses the transmit queues to schedule transmission of network traffic from the switch through egress ports. By default, all traffic is assigned to queue 1 and threshold 1 when QoS is enabled. All traffic that is destined for a transmit queue, regardless of classification, is subject to tail drop when the queue is full (that is, frames at the end of the queue are dropped).



Caution

When you disable QoS, the switch assigns unicast traffic to queue 1 and broadcast, multicast, and unknown traffic to queue 2. If you enable QoS but do not modify the CoS-to-transmit queue mappings, switch performance could be affected because *all* traffic is assigned to queue 1. If you enable QoS, we recommend that you modify the CoS-to-transmit queue mappings.



Note

To configure the CoS values that are mapped to each transmit queue, see the [“Mapping CoS Values to Transmit Queues and Drop Thresholds”](#) section on page 14-6.

Software Requirements

QoS requires supervisor engine software release 5.2 or later releases. Use the **show port capabilities** command to determine the specific QoS support for a module.

QoS Default Configuration

Table 14-1 shows the QoS default configuration.

Table 14-1 QoS Default Configuration

Feature	Default Value
QoS global enable state	Disabled
Switch CoS value	0
Transmit queue drop threshold percentages	Threshold 1:100%¹
CoS value-to-drop threshold mapping	Transmit queue drop threshold 1: CoS 0–7¹.
CoS value-to-transmit queue mapping	- Transmit queue 1: CoS 0–7 - Transmit queue 2: None configured

1. Not user-configurable

Configuring QoS on the Switch

These sections describe how to configure QoS:

- [Enabling QoS Globally, page 14-5](#)
- [Configuring the Default CoS Value for the Switch, page 14-5](#)
- [Reverting to the Default Switch CoS Value, page 14-5](#)
- [Mapping CoS Values to Transmit Queues and Drop Thresholds, page 14-6](#)
- [Reverting to the Default CoS-to-Transmit Queue and Drop Threshold Mapping, page 14-6](#)
- [Displaying QoS Information, page 14-7](#)
- [Reverting to QoS Defaults, page 14-7](#)
- [Disabling QoS, page 14-7](#)

**Note**

Because entering some QoS commands disables and then reenables ports (which can cause spanning tree topology changes), enter QoS commands only when necessary.

CISCO Confidential - DRAFT

Enabling QoS Globally

To enable QoS globally on the switch, perform this task in privileged mode:

Task	Command
Enable QoS globally.	set qos enable

This example shows how to enable QoS globally:

```
Console> (enable) set qos enable
QoS is enabled.
Console> (enable)
```

Configuring the Default CoS Value for the Switch

QoS assigns a CoS value to unclassified frames that are received on a port. The default CoS value is zero.

To set the default CoS value on the switch, perform this task in privileged mode:

	Task	Command
Step 1	Set the CoS value.	set qos defaultcos <i>cos-value</i>
Step 2	Verify the CoS value.	show qos info [runtime config]

This example shows how to set CoS equal to 7 in all unclassified frames that are received on the switch and verify the configuration:

```
Console> (enable) set qos defaultcos 7
qos defaultcos set to 7
Console> (enable)
```

Reverting to the Default Switch CoS Value

To revert to the default switch CoS value on the switch, perform this task in privileged mode:

	Task	Command
Step 1	Revert to the default CoS value.	clear qos defaultcos
Step 2	Verify that the default CoS value was restored.	show qos info [runtime config]

This example shows how to revert to the default CoS value for port 8/1 and verify the configuration:

```
Console> (enable) clear qos defaultcos
qos defaultcos setting cleared.
Console> (enable)
```

CISCO Confidential - DRAFT

Mapping CoS Values to Transmit Queues and Drop Thresholds

Enter the **set qos map** command to associate CoS values to transmit queue drop thresholds.

The *port_type* is hardware dependent. Enter the **show port capabilities** command to determine the *port_type* for your hardware. The port type is defined by the number of transmit queues and the number of drop thresholds that are supported on the port. For example, the **2q1t** port type supports two transmit queues and one drop threshold.

The *q#* is the transmit queue number. The *threshold#* is the drop threshold number for the specified queue. The *cos_list* is the list of CoS values to map to the specified transmit queue and drop threshold. CoS values must be specified in pairs (0–1, 2–3, 4–5, and 6–7).

To associate CoS values to a transmit queue and drop threshold, perform this task in privileged mode:

Task	Command
Associate a CoS value to a transmit queue and drop threshold.	set qos map <i>port_type</i> <i>q#</i> <i>threshold#</i> cos <i>cos_list</i>

This example shows how to map CoS values 4 through 7 to the second transmit queue and the first drop threshold for that queue on a **2q1t** port:

```
Console> (enable) set qos map 2q1t 2 1 cos 4-7
Qos tx priority queue and threshold mapped to cos successfully.
Console> (enable)
```

Reverting to the Default CoS-to-Transmit Queue and Drop Threshold Mapping

Enter the **clear qos map** command to revert to the default CoS-to-transmit queue and drop threshold mappings. The *port_type* is hardware dependent. Enter the **show port capabilities** command to determine the *port_type* for your hardware.

To revert to default CoS-to-transmit queue and drop threshold mappings, perform this task in privileged mode:

Task	Command
Revert to default CoS-to-transmit queue and drop threshold mappings.	clear qos map <i>port_type</i>

This example shows how to revert the CoS-to-transmit queue and drop threshold mappings to the default values on **2q1t** ports:

```
Console> (enable) clear qos map 2q1t
Qos map setting cleared.
Console> (enable)
```

CISCO Confidential - DRAFT

Displaying QoS Information

To display QoS information, perform this task:

Task	Command
Display QoS information.	show qos info [runtime config]

This example shows how to display the current QoS configuration information for the switch:

```

Console> show qos info config
QoS setting in NVRAM:
QoS is enabled
All ports have 2 transmit queues with 1 drop thresholds (2q1t).
Default CoS = 4
Queue and Threshold Mapping:
Queue Threshold CoS
-----
1      1      0 1 2 3
2      1      4 5 6 7
Console>

```

Reverting to QoS Defaults

To revert to QoS defaults, perform this task in privileged mode:

Task	Command
Revert to QoS defaults.	clear qos config

This example shows how to revert to QoS defaults:

```

Console> (enable) clear qos config
This command will disable QoS and take values back to factory default.
Do you want to continue (y/n) [n]? y
QoS config cleared.
Console> (enable)

```


Note

Reverting to defaults disables QoS, because QoS is disabled by default.

Disabling QoS

To disable QoS, perform this task in privileged mode:

Tas	Command
Disable QoS on the switch.	set qos disable

CISCO Confidential - DRAFT

This example shows how to disable QoS:

```
Console> (enable) set qos disable  
QoS is disabled.  
Console> (enable)
```

Configuring Multicast Services

This chapter describes how to configure multicast services, including Cisco Group Management Protocol (CGMP), Internet Group Management Protocol (IGMP) snooping, and GARP Multicast Registration Protocol (GMRP) on the Catalyst enterprise LAN switches.

**Note**

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 4500 Series, Catalyst 2948G, and Catalyst 2980G Switches Command Reference*.

This chapter consists of these sections:

- [Understanding How Multicasting Works, page 15-1](#)
- [Configuring CGMP, page 15-3](#)
- [Configuring GMRP, page 15-8](#)
- [Configuring Multicast Router Ports and Group Entries, page 15-15](#)
- [Filtering IGMP Traffic, page 15-17](#)

Understanding How Multicasting Works

The following sections describe how multicasting works on the Catalyst enterprise LAN switches.

Understanding Multicasting and Multicast Services Operation

CGMP, IGMP snooping, and GMRP manage multicast traffic in switches by allowing directed switching of IP multicast traffic. Switches can use CGMP, IGMP snooping, or GMRP to dynamically configure switch ports so that IP multicast traffic is forwarded only to ports that are associated with IP multicast hosts.

**Note**

For more information on IP multicast and IGMP, see RFC 1112. GMRP is described in IEEE 802.1p.

CGMP and IGMP software components run on the Cisco router and the switch. A CGMP/IGMP-capable IP multicast router sees all IGMP packets and can inform the switch when specific hosts join or leave IP multicast groups.

CISCO Confidential - DRAFT

When the CGMP/IGMP-capable router receives an IGMP control packet, it creates a CGMP or IGMP packet that contains the request type (either join or leave), the multicast group address, and the MAC address of the host. The router sends the packet to a well-known address to which all switches listen. When a switch receives the packet, the supervisor engine module interprets the packet and modifies the forwarding table automatically.

You can statically configure multicast groups using the **set cam static** command. Multicast groups that are learned through CGMP or IRPM snooping are dynamic. If you specify group membership for a multicast group address, your static setting supersedes any automatic manipulation by CGMP or IGMP. Multicast group membership lists can consist of both user-defined and CGMP/IGMP-learned settings.

**Note**

If a spanning tree VLAN topology changes, the CGMP/IGMP-learned multicast groups on the VLAN are purged and the CGMP/IGMP-capable router generates new multicast group information.

If a CGMP/IGMP-learned port link is disabled for any reason, that port is removed from any multicast group memberships. We recommend that you enable the spanning tree PortFast feature on ports to which hosts are directly connected if you are using CGMP. For information on configuring spanning tree PortFast, see [Chapter 8, “Configuring Spanning Tree PortFast, BPDU Guard, BPDU Filter, UplinkFast, BackboneFast, and Loop Guard.”](#)

Joining a Multicast Group

When a host wants to join an IP multicast group, it sends an IGMP join message specifying its MAC address and the IP multicast group it wants to join. The CGMP/IGMP-capable router then builds a CGMP/IGMP join message and multicasts the join message to the well-known address to which the switches listen.

Upon receipt of the join message, each switch searches its Enhanced Address Recognition Logic (EARL) table to determine if it contains the MAC address of the host asking to join the multicast group. If a switch finds the MAC address of the host in its EARL table associating the MAC address with a nontrunking port, the switch creates a multicast forwarding entry in the EARL forwarding table. The host that is associated with that port receives multicast traffic for that multicast group. In this way, the EARL automatically learns the MAC addresses and port numbers of the IP multicast hosts.

Leaving a Multicast Group

The CGMP/IGMP-capable router sends periodic multicast group queries. If a host wants to remain in a multicast group, it responds to the query from the router. In this case, the router does nothing. If a host does not want to remain in the multicast group, it does not respond to the router query. After a number of queries, if the router receives no reports from any host in a multicast group, the router sends a CGMP/IGMP command to the switch and requests that the switch remove the multicast group from its forwarding tables.

**Note**

If other hosts in the same multicast group *do* respond to the multicast group query, the router does not ask the switch to remove the group from its forwarding tables. The router does not remove a multicast group from the forwarding tables until all the hosts in the group ask to leave the group.

CISCO Confidential - DRAFT

CGMP leave-processing allows the switch to detect IGMP version 2 leave messages that were sent to the all-routers multicast address by hosts on any of the supervisor engine module ports. When the supervisor engine module receives a leave message, it starts a query-response timer. If this timer expires before a CGMP join message is received, the port is pruned from the multicast tree for the multicast group that is specified in the original leave message. CGMP leave processing optimizes bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously.

When CGMP fast-leave processing is enabled, the switch does not start a query response timer. The switch immediately prunes the port from the multicast tree for the multicast group by deleting the multicast MAC address from the port that received an IGMP leave message.

Understanding GMRP Operation

GARP Multicast Registration Protocol (GMRP) is a Generic Attribute Registration Protocol (GARP) application that provides a constrained multicast flooding facility similar to IGMP snooping and CGMP. GMRP and GARP are industry-standard protocols that are defined by the IEEE. For detailed protocol operational information, refer to IEEE 802.1p.

GMRP can register and deregister multicast group addresses at the MAC layer throughout the Layer 2-connected network. GMRP is Layer 3-protocol independent, which allows it to support the multicast traffic of any Layer 3 protocol (such as IP, IPX, and so forth).

GMRP software components run on both the switch and on the host (Cisco is not a source for GMRP host software). On the host, GMRP is typically used with IGMP: the host GMRP software generates Layer 2 GMRP versions of the host's Layer 3 IGMP control packets. The switch receives both the Layer 2 GMRP and the Layer 3 IGMP traffic from the host. The switch uses the received GMRP traffic to constrain multicasts at Layer 2 in the host's VLAN.

**Note**

In all cases, you can use CGMP or IGMP snooping to constrain multicasts at Layer 2 without the need to install or configure software on hosts.

When a host wants to join an IP multicast group, it sends an IGMP join message, which creates a corresponding GMRP join message. When the switch receives the GMRP join message, it adds the port through which the join message was received to the appropriate multicast group. The switch propagates the GMRP join message to all other hosts in the VLAN, one of which is typically the multicast source. When the source is multicasting to the group, the switch forwards the multicast only to the ports from which it received join messages for the group.

The switch sends periodic GMRP queries. If a host wants to remain in a multicast group, it responds to the query. In this case, the switch does nothing. If a host does not want to remain in the multicast group, it can either send a leave message or not respond to the periodic queries from the switch. If the switch receives a leave message or receives no response from the host for the duration of the leaveall timer, the switch removes the host from the multicast group.

**Note**

To use GMRP in a routed environment, enable the GMRP forward-all option on all ports where routers are attached.

Configuring CGMP

The following sections describe how to configure CGMP.

CGMP Hardware and Software Requirements

CGMP requires these hardware and software versions:

- Software release 2.2 or later releases
- Router running CGMP

Default CGMP Configuration

Table 15-1 shows the default CGMP configuration.

Table 15-1 CGMP Default Configuration

Feature	Default Value
CGMP enable state	Disabled
Multicast routers	None configured

Enabling CGMP



Note

You cannot enable CGMP if IGMP snooping or GMRP is enabled.

To enable CGMP on the switch, perform this task in privileged mode:

	Task	Command
Step 1	Enable CGMP.	set cgmp enable
Step 2	Verify that CGMP is enabled.	show cgmp statistics [vlan_num]

This example shows how to enable CGMP and verify the configuration:

```
Console> (enable) set cgmp enable
CGMP support for IP multicast enabled.
Console> (enable) show cgmp statistics 1
CGMP enabled

CGMP statistics for vlan 1:
valid rx pkts received          211915
invalid rx pkts received        0
valid cgmp joins received       211729
valid cgmp leaves received      186
valid igmp leaves received      0
valid igmp queries received     3122
igmp gs queries transmitted     0
igmp leaves transmitted         0
failures to add GDA to EARL     0
topology notifications received 80
number of CGMP packets dropped 2032227
Console> (enable)
```

CISCO Confidential - DRAFT

Enabling CGMP Leave Processing

To enable CGMP leave processing on the switch, perform this task in privileged mode:

	Task	Command
Step 1	Enable CGMP leave processing.	set cgmp leave enable
Step 2	Verify that CGMP leave processing is enabled.	show cgmp leave

This example shows how to enable CGMP leave processing and verify the configuration:

```

Console> (enable) set cgmp leave enable
CGMP leave processing enabled.
Console> (enable)
Console> (enable) show cgmp leave

CGMP:                enabled
CGMP leave:           enabled
CGMP FastLeave:        disabled
Console> (enable)

```

Enabling CGMP Fast-Leave Processing

To enable CGMP fast-leave processing on the switch, perform this task in privileged mode:

	Task	Command
Step 1	Enable CGMP fast-leave processing.	set cgmp fastleave enable
Step 2	Verify that CGMP fast-leave processing is enabled.	show cgmp leave

This example shows how to enable CGMP fast-leave processing and verify the configuration:

```

Console> (enable) set cgmp fastleave enable
CGMP fastleave processing enabled.
Console> (enable)
Console> (enable) show cgmp leave

CGMP:                enabled
CGMP leave:           enabled
CGMP FastLeave:        enabled
Console> (enable)

```

Displaying Multicast Router Information

When you enable CGMP, the switch automatically learns to which ports a multicast router is connected.

To display dynamically learned multicast router information, perform one of these tasks in privileged mode:

- Display information on dynamically learned and manually configured multicast router ports—**show multicast router** [*mod_num/port_num*] [*vlan_id*]
- Display information only on those multicast router ports that are learned dynamically using CGMP—**show multicast router cgmp** [*mod_num/port_num*] [*vlan_id*]

CISCO Confidential - DRAFT

This example shows how to display information on all multicast router ports (the asterisk [*] next to the multicast router on port 3/1 indicates that the entry was configured manually):

```

Console> (enable) show multicast router
CGMP enabled
IGMP disabled

```

```

Port      Vlan
-----
2/1       99
2/2       255
3/1       * 1

```

```

Total Number of Entries = 4
'*' - Configured
Console> (enable)

```

This example shows how to display only those multicast router ports that were learned dynamically through CGMP:

```

Console> (enable) show multicast router cgmp
CGMP enabled
IGMP disabled

```

```

Port      Vlan
-----
2/1       99
2/2       255

```

```

Total Number of Entries = 3
'*' - Configured
Console> (enable)

```

Displaying Multicast Group Information

To display information about multicast groups, perform one of these tasks:

Task	Command
Display information about multicast groups.	show multicast group [mac_addr] [vlan_id]
Display only information about multicast groups that are learned dynamically through CGMP.	show multicast group cgmp [mac_addr] [vlan_id]
Display the total number of multicast addresses (groups) in each VLAN.	show multicast group count [vlan_id]
Display the total number of multicast addresses (groups) in each VLAN that were learned dynamically through CGMP.	show multicast group count cgmp [vlan_id]

This example shows how to display information about all multicast groups on the switch:

```

Console> (enable) show multicast group
CGMP enabled
IGMP disabled

```

```

VLAN  Dest MAC/Route Des  Destination Ports or VCs / [Protocol Type]
-----
1      01-00-11-22-33-44*  2/6-12

```

CISCO Confidential - DRAFT

```
1      01-11-22-33-44-55*  2/6-12
1      01-22-33-44-55-66*  2/6-12
1      01-33-44-55-66-77*  2/6-12
```

```
Total Number of Entries = 4
Console> (enable)
```

Displaying CGMP Statistics

To check CGMP statistics on the switch, perform this task:

Task	Command
Display CGMP statistics.	show cgmp statistics [vlan_id]

This example shows how to display CGMP statistics:

```
Console> (enable) show cgmp statistics
CGMP enabled

CGMP statistics for vlan 1:
valid rx pkts received          211915
invalid rx pkts received        0
valid cgmp joins received       211729
valid cgmp leaves received      186
valid igmp leaves received      0
valid igmp queries received     3122
igmp gs queries transmitted     0
igmp leaves transmitted         0
failures to add GDA to EARL     0
topology notifications received 80
number of CGMP packets dropped 2032227
Console> (enable)
```

Disabling CGMP Leave Processing

To disable CGMP leave processing on the switch, perform this task in privileged mode:

Task	Command
Disable CGMP leave processing.	set cgmp leave disable

This example shows how to disable CGMP leave processing on the switch:

```
Console> (enable) set cgmp leave disable
CGMP leave processing disabled.
Console> (enable)
```

Disabling CGMP Fast-Leave Processing

To disable CGMP fast-leave processing on the switch, perform this task in privileged mode:

CISCO Confidential - DRAFT

Task	Command
Disable CGMP fast-leave processing.	set cgmp fastleave disable

This example shows how to disable CGMP fast-leave processing:

```
Console> (enable) set cgmp fastleave disable
CGMP FastLeave processing disabled.
Console> (enable)
```

Disabling CGMP

To disable CGMP on the switch, perform this task in privileged mode:

Task	Command
Disable CGMP.	set cgmp disable

This example shows how to disable CGMP:

```
Console> (enable) set cgmp disable
CGMP support for IP multicast disabled.
Console> (enable)
```

Configuring GMRP

The following sections describe how to configure the GARP Multicast Registration Protocol (GMRP).

GMRP Software Requirements

GMRP requires software release 5.1 or later releases.

Default GMRP Configuration

[Table 15-2](#) shows the default GMRP configuration.

Table 15-2 GMRP Default Configuration

Feature	Default Value
GMRP enable state	Disabled
GMRP per-port enable state	Disabled
GMRP forward all	Disabled on all ports

*CISCO Confidential - DRAFT***Table 15-2 GMRP Default Configuration (continued)**

Feature	Default Value
GMRP registration	Normal on all ports
GARP/GMRP timers	- Join time: 200 ms - Leave time: 600 ms - Leaveall time: 10,000 ms

Enabling GMRP Globally

**Note**

You cannot enable GMRP if CGMP is enabled.

To enable GMRP globally on the switch, perform this task in privileged mode:

	Task	Command
Step 1	Enable GMRP globally.	set gmrp enable
Step 2	Verify the configuration.	show gmrp configuration

This example shows how to enable GMRP globally and verify the configuration:

```

Console> (enable) set gmrp enable
GMRP enabled.
Console> (enable) show gmrp configuration
Global GMRP Configuration:
GMRP Feature is currently enabled on this switch.
GMRP Timers (milliseconds):
Join = 200
Leave = 600
LeaveAll = 10000
Port based GMRP Configuration:
Port                                     GMRP Status Registration ForwardAll
-----
1/1-2,3/1,6/1-48                       Enabled      Normal      Disabled
Console> (enable)

```

Enabling GMRP on Individual Switch Ports

**Note**

You can change the per-port GMRP configuration regardless of whether GMRP is enabled globally. However, GMRP will not function until you enable it globally. For information on configuring GMRP globally on the switch, see the [“Enabling GMRP Globally” section on page 15-9](#).

To enable GMRP on individual switch ports, perform this task in privileged mode:

CISCO Confidential - DRAFT

	Task	Command
Step 1	Enable GMRP on an individual switch port.	set port gmrp enable <i>mod_num/port_num</i>
Step 2	Verify the configuration.	show gmrp configuration

This example shows how to enable GMRP on port 6/12 and verify the configuration:

```

Console> (enable) set port gmrp enable 6/12
GMRP enabled on port 6/12.
Console> (enable) show gmrp configuration
Global GMRP Configuration:
GMRP Feature is currently enabled on this switch.
GMRP Timers (milliseconds):
Join = 200
Leave = 600
LeaveAll = 10000
Port based GMRP Configuration:
Port
-----
1/1-2,3/1,6/1-9,6/12,6/15-48      Enabled      Normal      Disabled
6/10-11,6/13-14                  Disabled     Normal      Disabled
Console> (enable)

```

Disabling GMRP on Individual Switch Ports



Note

You can change the per-port GMRP configuration regardless of whether GMRP is enabled globally. However, GMRP will not function until you enable it globally. For information on configuring GMRP globally on the switch, see the [“Enabling GMRP Globally”](#) section on page 15-9.

To disable GMRP on individual switch ports, perform this task in privileged mode:

	Task	Command
Step 1	Disable GMRP on individual switch ports.	set port gmrp disable <i>mod_num/port_num</i>
Step 2	Verify the configuration.	show gmrp configuration

This example shows how to disable GMRP on ports 6/10–14 and verify the configuration:

```

Console> (enable) set port gmrp disable 6/10-14
GMRP disabled on ports 6/10-14.
Console> (enable) show gmrp configuration
Global GMRP Configuration:
GMRP Feature is currently enabled on this switch.
GMRP Timers (milliseconds):
Join = 200
Leave = 600
LeaveAll = 10000
Port based GMRP Configuration:
Port
-----
1/1-2,3/1,6/1-9,6/15-48      Enabled      Normal      Disabled
6/10-14                      Disabled     Normal      Disabled
Console> (enable)

```


CISCO Confidential - DRAFT

Enabling GMRP Forward-All Option

When you enable GMRP forward-all on a port, a copy of all multicast traffic that is registered on the switch is forwarded to the port. We recommend enabling this option on any port that is connected to a router. Forward-all can also forward all registered multicast traffic to a port with a network analyzer or probe attached.

To forward a copy of all GMRP multicast packets that are registered on the switch to a port, perform this task in privileged mode:

Task	Command
Enable the GMRP forward-all option on a switch port.	set gmrp fwdall enable <i>mod_num/port_num</i>

This example shows how to enable the GMRP forward-all option on port 1/1:

```
Console> (enable) set gmrp fwdall enable 1/1  
GMRP Forward All groups option enabled on port 1/1.  
Console> (enable)
```

Disabling GMRP Forward-All Option

To disable the GMRP forward-all option on a port, perform this task in privileged mode:

Task	Command
Disable the GMRP forward-all option on a port.	set gmrp fwdall disable <i>mod_num/port_num</i>

This example shows how to disable the GMRP forward-all option on port 1/1:

```
Console> (enable) set gmrp fwdall disable 1/1  
GMRP Forward All groups option disabled on port 1/1.  
Console> (enable)
```

Configuring GMRP Registration

The following sections describe how to configure GMRP registration modes on switch ports.

Setting Normal Registration Mode

Configuring a port in **normal** registration mode allows dynamic GMRP multicast registration and deregistration on the port. Normal mode is the default on all switch ports.

To configure GMRP normal registration on a port, perform this task in privileged mode:

	Task	Command
Step 1	Configure normal registration on a port.	set gmrp registration normal <i>mod_num/port_num</i>
Step 2	Verify the configuration.	show gmrp configuration

CISCO Confidential - DRAFT

This example shows how to configure normal registration on port 2/10:

```
Console> (enable) set gmrp registration normal 2/10
GMRP Registration is set normal on port 2/10.
Console> (enable)
```

Setting Fixed Registration Mode

When you configure a port in **fixed** registration mode, all multicast groups that are currently registered on all ports are registered on the port, but the port ignores any subsequent registrations or deregistrations on other ports. A port in fixed registration mode continues to register multicast groups that are specific to the port. You must return the port to **normal** registration mode to deregister multicast groups on the port.

To configure GMRP fixed registration on a port, perform this task in privileged mode:

	Task	Command
Step 1	Configure fixed registration on a port.	set gmrp registration fixed <i>mod_num/port_num</i>
Step 2	Verify the configuration.	show gmrp configuration

This example shows how to configure fixed registration on port 2/10 and verify the configuration:

```
Console> (enable) set gmrp registration fixed 2/10
GMRP Registration is set fixed on port 2/10.
Console> (enable) show gmrp configuration
Global GMRP Configuration:
GMRP Feature is currently enabled on this switch.
GMRP Timers (milliseconds):
Join = 200
Leave = 600
LeaveAll = 10000
Port based GMRP Configuration:
GMRP-Status Registration ForwardAll Port(s)
-----
Enabled      Normal      Disabled  1/1-4
                                           2/1-9, 2/11-48
                                           3/1-24
                                           5/1
Enabled      Fixed      Disabled  2/10
Console> (enable)
```

Setting Forbidden Registration Mode

Configuring a port in **forbidden** registration mode deregisters all GMRP multicasts and prevents any further GMRP multicast registration on the port.

To configure GMRP forbidden registration on a port, perform this task in privileged mode:

	Task	Command
Step 1	Configure forbidden registration on a port.	set gmrp registration forbidden <i>mod_num/port_num</i>
Step 2	Verify the configuration.	show gmrp configuration

This example shows how to configure forbidden registration on port 2/10 and verify the configuration:

```
Console> (enable) set gmrp registration forbidden 2/10
```

CISCO Confidential - DRAFT

GMRP Registration is set forbidden on port 2/10.

```
Console> (enable) show gmrp configuration
```

Global GMRP Configuration:

GMRP Feature is currently enabled on this switch.

GMRP Timers (milliseconds):

Join = 200

Leave = 600

LeaveAll = 10000

Port based GMRP Configuration:

GMRP-Status Registration ForwardAll Port(s)

```
-----
Enabled      Normal      Disabled  1/1-4
                                           2/1-9,2/11-48
                                           3/1-24
                                           5/1
Enabled      Forbidden  Disabled  2/10
Console> (enable)
```

Setting the GARP Timers



Note

The commands **set gmrp timer** and **show gmrp timer** are aliases for **set garp timer** and **show garp timer**.



Note

Modifying the GARP timer values affects the behavior of *all* GARP applications running on the switch, not just GMRP. (For example, GVRP uses the same timers.)

You can modify the default GARP timer values on the switch.

When you set the timer values, the value for **leave** must be equal to or greater than three times the **join** value (**leave** $\geq$ **join** * 3). The value for **leaveall** must be greater than the value for **leave** (**leaveall** $>$ **leave**). The more registered attributes there are on the switch, the greater you should configure the difference between the **leave** value and the **join** value.

For better performance on switches with many registered multicast groups, increase the timer values to the order of seconds.

If you attempt to set a timer value that does not adhere to these rules, an error is returned. For example, if you set the **leave** timer to 600 ms and you attempt to configure the **join** timer to 350 ms, an error is returned. Set the **leave** timer to at least 1050 ms, and then set the **join** timer to 350 ms.



Caution

Set the same GARP timer values on all Layer 2-connected devices. If the GARP timers are set differently on the Layer 2-connected devices, GARP applications (for example, GMRP and GVRP) will not operate successfully.

To adjust the GARP timer values, perform this task in privileged mode:

	Task	Command
Step 1	Set the GARP timer values.	set garp timer {join leave leaveall} timer_value
Step 2	Verify the configuration.	show garp timer

CISCO Confidential - DRAFT

This example shows how to set GARP timers and verify the configuration:

```

Console> (enable) set garp timer leaveall 12000
GMRP/GARP leaveAll timer value is set to 12000 milliseconds.
Console> (enable) set garp timer leave 650
GMRP/GARP leave timer value is set to 650 milliseconds.
Console> (enable) set garp timer join 300
GMRP/GARP join timer value is set to 300 milliseconds.
Console> (enable) show garp timer
Timer      Timer Value (milliseconds)
-----
Join       300
Leave       650
LeaveAll    12000
Console> (enable)

```

Displaying GMRP Statistics

To display GMRP statistics on the switch, perform this task in privileged mode:

Task	Command
Display GMRP statistics.	show gmrp statistics [<i>vlan_id</i>]

This example shows how to display GMRP statistics for VLAN 23:

```

Console> show gmrp statistics 23
GMRP Statistics for vlan <23>:
Total valid GMRP Packets Received:500
Join Empties:200
Join INs:250
Leaves:10
Leave Alls:35
Empties:5
Fwd Alls:0
Fwd Unregistered:0
Total valid GMRP Packets Transmitted:600
Join Empties:200
Join INs:150
Leaves:45
Leave Alls:200
Empties:5
Fwd Alls:0
Fwd Unregistered:0
Total valid GMRP Packets Received:0
Total GMRP packets dropped:0
Total GMRP Registrations Failed:0
Console> (enable)

```

Clearing GMRP Statistics

To clear all GMRP statistics on the switch, perform this task in privileged mode:

Task	Command
Clear GMRP statistics.	clear gmrp statistics { <i>vlan_id</i> all }

CISCO Confidential - DRAFT

This example shows how to clear the GMRP statistics for all VLANs:

```
Console> (enable) clear gmrp statistics all
Console> (enable)
```

Disabling GMRP

To disable GMRP globally on the switch, perform this task in privileged mode:

Task	Command
Disable GMRP globally.	set gmrp disable

This example shows how to disable GMRP globally:

```
Console> (enable) set gmrp disable
GMRP disabled.
Console> (enable)
```

Configuring Multicast Router Ports and Group Entries

The following sections describe how to manually specify multicast router ports and configure multicast group entries.

Specifying Multicast Router Ports

When you enable CGMP or GMRP, the switch automatically learns to which ports a multicast router is connected. However, you can manually specify multicast router ports.

To specify multicast router ports manually, perform this task in privileged mode:

	Task	Command
Step 1	Manually specify a multicast router port.	set multicast router <i>mod_num/port_num</i>
Step 2	Verify the configuration.	show multicast router [<i>mod_num/port_num</i>] [<i>vlan_id</i>]

This example shows how to specify a multicast router port manually and verify the configuration (the asterisk [*] next to the multicast router on port 3/1 indicates that the entry was configured manually):

```
Console> (enable) set multicast router 3/1
Port 3/1 added to multicast router port list.
Console> (enable) show multicast router
CGMP enabled
IGMP disabled
```

```
Port      Vlan
-----
2/1      99
2/2      255
3/1      * 1
```

```
Total Number of Entries = 4
'*' - Configured
```

CISCO Confidential - DRAFT

```
Console> (enable)
```

Configuring Multicast Groups

To configure a multicast group manually, perform this task in privileged mode:

	Task	Command
Step 1	Add one or more multicast MAC addresses to the CAM table.	set cam {static permanent} multicast_mac mod_num/port_num [vlan]
Step 2	Verify the multicast group configuration.	show multicast group [mac_addr] [vlan_id]

This example shows how to configure multicast groups manually and verify the configuration (the asterisks indicate that the entry was manually configured):

```
Console> (enable) set cam static 01-00-11-22-33-44 2/6-12
Static multicast entry added to CAM table.
Console> (enable) set cam static 01-11-22-33-44-55 2/6-12
Static multicast entry added to CAM table.
Console> (enable) set cam static 01-22-33-44-55-66 2/6-12
Static multicast entry added to CAM table.
Console> (enable) set cam static 01-33-44-55-66-77 2/6-12
Static multicast entry added to CAM table.
Console> (enable) show multicast group
CGMP enabled
IGMP disabled
```

```
VLAN  Dest MAC/Route Des  Destination Ports or VCs / [Protocol Type]
----  -
1      01-00-11-22-33-44*  2/6-12
1      01-11-22-33-44-55*  2/6-12
1      01-22-33-44-55-66*  2/6-12
1      01-33-44-55-66-77*  2/6-12
```

```
Total Number of Entries = 4
Console> (enable)
```

Disabling Multicast Router Ports

To disable manually configured multicast router ports, perform one of these tasks in privileged mode:

Task	Command
Disable a specific manually configured multicast router port.	clear multicast router mod_num/port_num
Disable all manually configured multicast router ports.	clear multicast router all

This example shows how to disable a manually configured multicast router port entry:

```
Console> (enable) clear multicast router 2/12
Port 2/12 cleared from multicast router port list.
Console> (enable)
```

Disabling Multicast Group Entries

To disable manually configured multicast group entries, perform this task in privileged mode:

Task	Command
Disable a multicast group entry from the CAM table.	clear cam mac_addr [vlan]

This example shows how to disable a multicast group entry from the CAM table:

```
Console> (enable) clear cam 01-11-22-33-44-55 1
CAM entry cleared.
Console> (enable)
```

Filtering IGMP Traffic

Internet Group Management Protocol (IGMP) filtering allows an administrator to configure IP multicast group profiles consisting of one or more ranges of IP multicast addresses. The administrator associates these profiles with a filtering and monitoring action. These actions apply to IGMP packets, are configured on a per-switch-port basis, and are available to all VLANs that are associated with the physical port.

If a port is set to permit, only matching IPs are forwarded; all others are dropped. If a filtering action permits a particular IGMP packet, only that packet is forwarded for processing, and all others are dropped.

If a port is set to deny, matched IPs are dropped; all others are forwarded. If the filtering action causes an IGMP packet to be dropped, the switch port requesting the stream of IP multicast traffic cannot receive IP multicast traffic for that group.



Note

IGMP filtering actions do not direct IP multicast traffic forwarding. For example, IGMP filtering does not know if CGMP is used to allow IP multicast traffic forwarding.

The following sections describe IGMP traffic filtering usage, requirements, and configurations.

Using IGMP Traffic Filtering

You can use IGMP filters in video service deployment of Ethernet to the Home (ETTH).

IGMP transmits video channels as IP multicast traffic using MPEG encoding. In access switches, filters specify which video channels (multicast addresses) are allowed to be received by every customer.

In ETTH, a typical access switch has two high-speed uplink ports. The other ports are user ports, each connected to a different end subscriber who has a box that generates IGMP report and leave messages. You can define which channels (IP multicast addresses) to monitor and the minimum monitoring interval. If an end subscriber is looking at a channel for more than the minimum monitoring interval, an entry is created in a monitoring table. IGMP monitoring creates statistics about channel changing patterns of which channels are viewed when and for how long.

IGMP Software Requirements

IGMP requires software release 7.1(1) or later releases and has the following physical restrictions for filtering through software:

- A threshold of 1024 profiles available on the Catalyst 4000 family switch
- A limit of 512 Class D multicast IP addresses which can be filtered in all profiles
- One (1) profile per port

Default IGMP Filter Configuration

Table 15-3 shows the default IGMP traffic filter configuration.

Table 15-3 IGMP Default Configuration

Feature	Default Value
IGMP filtering	None
IGMP enable state	Disabled
IGMP match-action state	Deny

IGMP Multicast Filter Activation

IGMP multicast filters associate with each physical switch port.

The following sections show configurations for controlling IGMP multicast filter activation/deactivation on the switch.

Enabling and Verifying IGMP Multicast Filtering

To enable IGMP traffic filtering on the switch, perform this task in privileged mode:

	Task	Command
Step 1	Enable IGMP filtering.	set igmp filter enable
Step 2	Verify the configuration.	show igmp filter

This example shows how to enable IGMP multicast filtering:

```
Console> (enable) set igmp filter enable
igmp filter set to enable
Console> (enable)
```

This example shows how to verify the enable configuration status of IGMP multicast filtering on the switch:

```
Console> (enable) show igmp filter
igmp filter is enabled
Console> (enable)
```


CISCO Confidential - DRAFT

Disabling and Verifying IGMP Multicast Filtering

To disable IGMP traffic filtering on the switch, perform this task in privileged mode:

Step 1	Disable IGMP filtering.	set igmp filter disable
Step 2	Verify the configuration.	show igmp filter

This example shows how to disable IGMP multicast filtering:

```
Console> (enable) set igmp filter disable
igmp filter set to disable
Console> (enable)
```

This example shows how to verify the disable configuration status of IGMP multicast filtering:

```
Console> (enable) show igmp filter
igmp filter is disabled
Console> (enable)
```

Configuring Port IP Multicast Filtering

IP multicast group profiles consist of one or more ranges of IP multicast addresses that are associated with a filtering and monitoring action and are configured on a per-switch-port basis. Given a particular profile that is associated with a switch port, you can configure the filter action.

- If the filter action is to permit, the matching IGMP packet is forwarded for normal processing.
- If the filter action is to deny, the matching IGMP packet is dropped, discontinuing normal processing.

The following sections provide switch port IP multicast filtering configurations.

Adding and Listing an IGMP Multicast Filter Profile

To add a multicast address or a range of addresses to an IGMP multicast filter profile, perform this task in privileged mode:

	Task	Command
Step 1	Add a multicast IP address or a range of IP addresses to an IGMP multicast filter profile.	set igmp filter profile <i>profile_id</i> <i>ip_addr</i> [- <i>ip_addr</i>]
Step 2	List an IGMP multicast filter profile.	show igmp filter profile <i>profile_id</i>

This example shows how to add the multicast IP address 226.1.1.1 to IGMP multicast filter profile 1:

```
Console> (enable) set igmp filter profile 1 226.1.1.1
Successfully add ip(s) to profile
Console> (enable)
```

This example shows how to list an IP address for profile 1 when the IGMP multicast filter match-action is denied:

```
Console> (enable) show igmp filter profile 1
ProfileId 1: FilterMode deny, IP Range
-----
```

```
226.1.1.1
Console> (enable)
```

Permitting and Verifying an IGMP Multicast Filter Match-Action

To specify an IGMP multicast filter profile on a switch to permit an IP address or a range of IP addresses, perform this task in privileged mode:

	Task	Command
Step 1	Permit an IP address or range of IP addresses.	set igmp filter profile <i>profile_id</i> match-action permit
Step 2	Verify the permit configuration.	show igmp filter profile <i>profile_id</i> match-action

This example shows how to permit an IP address or range of IP addresses:

```
Console> (enable) set igmp filter profile 1 match-action permit
igmp filter match-action set to permit
Console> (enable)
```

This example shows how to verify the status of an IGMP multicast filter profile to accept IP addresses:

```
Console> (enable) show igmp filter profile 1 match-action
igmp filter match action is permit
Console> (enable)
```

Denying and Verifying an IGMP Multicast Filter Match-Action

To specify an IGMP multicast filter profile on a switch deny an IP address or range of IP addresses, perform this task in privileged mode:

	Task	Command
Step 1	Deny an IP address or range of IP addresses.	set igmp filter profile <i>profile_id</i> match-action deny
Step 2	Verify the deny configuration.	show igmp filter profile <i>profile_id</i> match-action

This example shows how to deny an IP address or range of IP addresses:

```
Console> (enable) set igmp filter profile 1 match-action deny
igmp filter match-action set to deny
Console> (enable)
```

This example shows how to verify the status of an IGMP multicast filter profile to deny IP addresses:

```
Console> (enable) show igmp filter profile 1 match-action
igmp filter match action is denied
Console> (enable)
```

Removing an IGMP Multicast Filter Profile

To remove a multicast address from an IGMP multicast filter profile or to remove the filter profile, perform this task in privileged mode:

CISCO Confidential - DRAFT

	Task	Command
Step 1	Remove a multicast address from an IGMP multicast filter profile or to remove the filter profile.	clear igmp filter profile <i>profile_id</i> { <i>ip_addr</i> [- <i>ip_addr</i>] all }
Step 2	Verify that an IGMP multicast filter profile was removed.	show igmp filter profile <i>profile_id</i>

**Note**

When you remove a filter, all associations between the filter and associated ports are removed.

This example shows how to remove an IP address (226.1.1.1) from an IGMP multicast filter profile (1):

```
Console> (enable) clear igmp filter profile 1 226.1.1.1
Console> (enable)
```

This example shows how to verify that an IGMP multicast filter profile 1 was deleted:

```
Console> (enable) show igmp filter profile 1
Console> (enable)
```

Listing or Removing All IGMP Multicast Filters

To list, remove, and verify all IGMP multicast filter profiles, perform this task in privileged mode:

	Task	Command
Step 1	Display all IGMP multicast filter profiles.	show igmp filter all
Step 2	Remove all IGMP multicast filter profiles.	clear igmp filter all

**Note**

When you remove a filter, all associations between the filter and associated ports are removed.

This example shows how to display all IGMP multicast filter profiles:

```
Console> (enable) show igmp filter all
ProfileId 1: FilterMode deny, IP Range
-----
226.1.1.1
Console> (enable)
```

This example shows how to remove all IGMP multicast filter profiles:

```
Console> (enable) clear igmp filter all
Successfully remove all the profile(s)
Console> (enable)
```

This example shows how to verify that all IGMP multicast filter profiles were deleted:

```
Console> (enable) show igmp filter all
Console> (enable)
```

Assigning and Displaying Port Filter Associations

To assign and display IGMP multicast filter associations to a port or port list, perform this task in privileged mode:

	Task	Command
Step 1	Assign IGMP multicast filters to a port or port list.	set igmp filter map <i>profile_id port_list</i>
Step 2	Display all IGMP multicast port filter associations.	show igmp filter map { <i>port_list</i> all }

This example shows how to assign an association of module 2/port 1 to IGMP multicast filter profile 1:

```

Console> (enable) set igmp filter map 1 2/1
Console> (enable)

```

This example shows how to display the association of IGMP multicast filter profiles with module 2/port 48:

```

Console> (enable) show igmp filter map 2/48
Port      Profile
----      -
2/48      -

```

This example shows how to display the association of IGMP multicast filter profiles for all ports:

```

Console> (enable) show igmp filter map all
Port      Profile
----      -
2/1       1
2/2       -
2/3       -
2/4       -
2/5       -
2/6       -
2/7       -
2/8       -
2/9       -
2/10      -
2/11      -
2/12      -
2/13      -
2/14      -
2/15      -
2/16      -
.
.
.
2/46      -
2/47      -
2/48      -
Console> (enable)

```

Removing IGMP Multicast Port Filter Associations

To remove the association of IGMP multicast filters with ports, perform this task in privileged mode:

CISCO Confidential - DRAFT

Task	Command
Remove IGMP multicast port filter associations.	clear igmp filter map { <i>port_list</i> all }

**Note**

The filter is not removed when the association is removed.

This example shows how to remove the association of IGMP multicast filter profiles with a port or list of ports:

```
Console> (enable) clear igmp filter map all
Console> (enable)
```

CISCO Confidential - DRAFT

Configuring Port Security

This chapter describes how to configure port security on the Catalyst enterprise LAN switches.

**Note**

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 4500 Series, Catalyst 2948G, and Catalyst 2980G Switches Command Reference*.

This chapter consists of these sections:

- [Understanding How Port Security Works, page 16-1](#)
- [Port Security Configuration Guidelines, page 16-3](#)
- [Configuring Port Security on the Switch, page 16-3](#)
- [Monitoring Port Security, page 16-10](#)

Understanding How Port Security Works

You can use port security to block input to an Ethernet, Fast Ethernet, or Gigabit Ethernet port when the MAC address of the station attempting to access the port is different from any of the MAC addresses that are specified for that port. Alternatively, you can use port security to filter traffic that is destined to or received from a specific host that is based on the host MAC address.

Allowing Traffic Based on the Host MAC Address

The total number of MAC addresses that can be specified per port is limited to the global resource of 1024 plus 1 default MAC address. That is, the total number of MAC addresses on any port cannot exceed 1025.

The maximum number of MAC addresses that you can allocate for each port depends on your network configuration. The following combinations are valid allocations:

- 1025 (1 + 1024) addresses on one port and 1 address each on the rest of the ports
- 513 (1 + 512) each on two ports in a system and 1 address each on the rest of the ports
- 901 (1 + 900) on one port, 101 (1 + 100) on another port, 25 (1 + 24) on a third port, and 1 address on each of the rest of the ports

CISCO Confidential - DRAFT

After you allocate the maximum number of MAC addresses on a port, you can either specify the secure MAC address for the port manually or have the port dynamically configure the MAC address of the connected devices. Out of a maximum allocated number of MAC addresses on a port, you can manually configure all, allow all to be autoconfigured, or configure some manually and allow the rest to be autoconfigured. Once you manually configure or autoconfigure the addresses, they are stored in nonvolatile RAM (NVRAM) and are maintained after a reset.

When you manually change the maximum number of MAC addresses that are associated to a port greater than the default value and then manually enter the authorized MAC addresses, any remaining MAC addresses are automatically configured. For example, if you configure the port security for a port to have a maximum of ten MAC addresses but add only two MAC addresses, the next eight new source MAC addresses that are received on that port are added to the secured MAC address list for the port.

After you allocate a maximum number of MAC addresses on a port, you can also specify how long the addresses on the port will remain secure. After the age time expires, the MAC addresses on the port become insecure. By default, all addresses on a port are secured permanently.

If a security violation occurs, you can configure the port to go either into shutdown mode or restrictive mode. The shutdown mode option allows you to specify whether the port is to be permanently disabled or disabled for only a specified time. The default is for the port to shut down permanently. The restrictive mode allows you to configure the port to remain enabled during a security violation and drop only packets that are coming in from insecure hosts.

**Note**

If you configure a secure port in restrictive mode, and a station is connected to the port whose MAC address is already configured as a secure MAC address on another port on the switch, the port in restrictive mode shuts down instead of restricting traffic from that station. For example, if you configure MAC-1 as the secure MAC address on port 2/1 and MAC-2 as the secure MAC address on port 2/2 and then connect the station with MAC-1 to port 2/2 when port 2/2 is configured for restrictive mode, port 2/2 shuts down instead of restricting traffic from MAC-1.

When a secure port receives a packet, the source MAC address of the packet is compared to the list of secure source addresses that were manually configured or autoconfigured (learned) on the port. If a MAC address of a device that is attached to the port differs from the list of secure addresses, the port either shuts down permanently (default mode), shuts down for the time that you have specified, or drops incoming packets from the insecure host.

The behavior of a port depends on how you configure it to respond to a security violation. If a security violation occurs, the LED labeled Link for that port turns orange, and a link-down trap is sent to the Simple Network Management Protocol (SNMP) manager. An SNMP trap is not sent if you configure the port for restrictive violation mode. A trap is sent only if you configure the port to shut down during a security violation.

Restricting Traffic Based on the Host MAC Address

You can filter traffic based on a host MAC address, so that packets tagged with a specific source MAC address are discarded. When you specify a MAC address filter with the **set cam filter** command, incoming traffic from that host MAC address is dropped, and packets that are addressed to that host are not forwarded. You cannot filter traffic for multicast addresses with this command.

**Note**

The **set cam filter** command allows filtering for unicast addresses only.

CISCO Confidential - DRAFT

Blocking Unicast Flood Packets on Secure Ports

You can block unicast flood packets on a secure Ethernet port by disabling the unicast flood feature. If you disable unicast flood on a port, the port will drop unicast flood packets when the port reaches the allowed maximum number of MAC addresses.

The port automatically restarts unicast flood packet learning when the number of MAC addresses drops below the maximum number that is allowed. The learned MAC address count decreases when a configured MAC address is removed or a time to live counter (TTL) is reached.

Port Security Configuration Guidelines

This section lists the guidelines for configuring port security:

- Do not configure port security on a SPAN destination port.
- Do not configure SPAN destination on a secure port.
- Do not configure dynamic, static, or permanent CAM entries on a secure port.

Configuring Port Security on the Switch

The following sections describe how to configure port security.

Enabling Port Security

When you enable port security on a port, any static or dynamic CAM entries that are associated with the port are cleared; any currently configured permanent CAM entries are treated as secure.

To enable port security, perform this task in privileged mode:

	Task	Command
Step 1	Enable port security on the desired ports. If desired, specify the secure MAC address.	set port security <i>mod_num/port_num</i> enable [<i>mac_addr</i>]
Step 2	You can add MAC addresses to the list of secure addresses.	set port security <i>mod_num/port_num</i> <i>mac_addr</i>
Step 3	Verify the configuration.	show port [<i>mod_num[/port_num]</i>]

This example shows how to enable port security using the learned MAC address on a port:

```
Console> (enable) set port security 2/1 enable
Port 2/1 port security enabled with the learned mac address.
Trunking disabled for Port 2/1 due to Security Mode
```

This example shows how to verify the port security:

```
Console> (enable) show port 2/1
Port  Name              Status      Vlan      Level Duplex Speed Type
-----
2/1              connected  522       normal   half   100   100BaseTX
```

CISCO Confidential - DRAFT

```

Port  Security  Secure-Src-Addr  Last-Src-Addr  Shutdown  Trap  IfIndex
-----
2/1  enabled  00-90-2b-03-34-08  00-90-2b-03-34-08  No        disabled  1081

Port      Broadcast-Limit  Broadcast-Drop
-----
2/1      -                0

Port  Align-Err  FCS-Err  Xmit-Err  Rcv-Err  UnderSize
-----
2/1      0        0        0        0        0

Port  Single-Col  Multi-Coll  Late-Coll  Excess-Col  Carri-Sen  Runts  Giants
-----
2/1      0          0          0          0          0        0      0

Last-Time-Cleared
-----
Fri Jul 10 1998, 17:53:38

```

This example shows how to enable port security on a port and manually specify the secure MAC address:

```

Console> (enable) set port security 2/1 enable 00-90-2b-03-34-08
Port 2/1 port security enabled with 00-90-2b-03-34-08 as the secure mac address
Trunking disabled for Port 2/1 due to Security Mode
Console> (enable)

```

Setting the Maximum Number of Secure MAC Addresses

You can set the number of MAC addresses to secure on a port. By default, at least one MAC address per port can be secured. In addition to this default, a global resource of up to 1024 MAC addresses is available to be shared by the ports. This means that if the entire global resource of 1024 MAC addresses is used on some ports, you can still enable port security on the rest of the ports with a maximum of one MAC per port.

If you reduce the maximum number of MAC addresses, the system clears the specified number of MAC addresses and displays the list of removed addresses.

To set the number of MAC addresses to be secured on a port, perform this task in privileged mode:

Task	Command
Set the number of MAC addresses to be secured on a port.	set port security <i>mod_num/port_num maximum num_of_mac</i>

This example shows how to set the number of MAC addresses to be secured:

```

Console> (enable) set port security 4/7 maximum 20
Maximum number of secure addresses set to 20 for port 4/7.
Console> (enable)

```

This example shows how to reduce the number of MAC addresses; it also shows how to display the list of cleared MAC addresses:

```

Console> (enable) set port security 4/7 maximum 18
Maximum number of secure addresses set to 18 for port 4/7
00-11-22-33-44-55 cleared from secure address list for port 4/7
00-11-22-33-44-66 cleared from secure address list for port 4/7
Console> (enable)

```

Setting the Port Security Age Time

The age time on a port specifies how long all addresses on that port will be secured. This age time is activated when a MAC address initiates traffic on the port. After the age time expires for a MAC address, the entry for that MAC address on the port is removed from the secure address list. The valid range is from 1–1440 minutes. Setting the age time to zero disables aging of secure addresses.

To set the age time on a port, perform this task in privileged mode:

Task	Command
Set the age time for which addresses on a port will be secured.	set port security <i>mod_num/port_num</i> <i>age time</i>

```
Console> (enable) set port security 4/7 age 600
Secure address age time set to 600 minutes for port 4/7.
Console> (enable)
```

Clearing MAC Addresses

Enter the **clear port security** command to clear MAC addresses from a list of secure addresses on a port.



Note

If you enter the **clear** command on a MAC address that is in use, the network may relearn that MAC address and make the MAC address secure again. We recommend that you disable port security before you clear the MAC addresses.

To clear all of the MAC addresses or one particular address from the list of secure MAC addresses, perform this task in privileged mode:

Task	Command
Clear all of the MAC addresses or one particular address from the list of secure MAC addresses.	clear port security <i>mod_num/port_num</i> <i>{mac_addr all}</i>

This example removes one MAC address from the secure address list on port 4/7:

```
Console> (enable) clear port security 4/7 00-11-22-33-44-55
00-11-22-33-44-55 cleared from secure address list for port 4/7
Console> (enable)
```

This example removes all MAC addresses from ports 4/5–7:

```
Console> (enable) clear port security 4/5-7 all
All addresses cleared from secure address list for ports 4/5-7
Console> (enable)
```

Configuring Unicast Flood Blocking on Secure Ports

To configure unicast flood blocking, you must disable the unicast flood feature.

CISCO Confidential - DRAFT**Note**

The port disables unicast flooding once the MAC address limit is reached.

To configure unicast flood blocking on a secure port, perform this task in privileged mode:

	Task	Command
Step 1	Disable unicast flood blocking on the desired secure ports.	set port security mod/port unicast-flood disable
Step 2	Verify the configuration of unicast flood blocking.	show port security mod/port
Step 3	Verify the status of unicast flood blocking.	show port unicast-flood mod/port

This example shows how to configure the switch to disable unicast flood packets on a port and how to verify its configuration:

```

Console> (enable) set port security 4/1 unicast-flood disable
Port 4/1 security flood mode set to disable.
Console> (enable) show port security 4/1
Port  Security Violation Shutdown-Time Age-Time Max-Addr Trap      IfIndex
-----
4/1   disabled  shutdown          0          0          1 disabled      50

Port  Num-Addr Secure-Src-Addr  Age-Left Last-Src-Addr  Shutdown/Time-Left
-----
4/1      0          -          -          -          -          -

Port Flooding on Address Limit
-----
4/1          Disabled
Console> (enable) show port unicast-flood 4/1
Port      Unicast Flooding
----      -
4/1      Disabled
Console> (enable)

```

**Note**

The **show port unicast-flood** command displays the run-time status of unicast flood blocking. The output can show unicast flooding as either enabled or disabled depending upon if the port has exceeded its address limitation.

Enabling MAC Address Notification

Enabling MAC address notification allows you to monitor MAC addresses at the module and port level that were added by the switch or removed from the CAM table.

A new MAC address is added when either of the following occurs:

- When a packet is received from a new device on one of the ports of the switch with a new source address
- When the MAC address is added to the CAM table by the CLI

A MAC address is removed from the CAM table when one of the following is true:

- When the MAC address receives no packets during the time-out period

CISCO Confidential - DRAFT

- When the switch invalidates a CAM table entry and replaces the entry with a new one
- When the MAC address is removed from the CAM table by the CLI

**Note**

MAC address notification settings are ignored on PAGP and LACP EtherChannel ports.

To enable MAC address notification globally, perform this task in privileged mode:

	Task	Command
Step 1	Enable MAC address notification globally.	set cam notification {enable disable}
Step 2	Set the history log size.	set cam notification historysize <i>log_size</i>
Step 3	Enable notification of added MAC addresses.	set cam notification added {enable disable} <i>mod/port</i>
Step 4	Enable notification of removed MAC addresses.	set cam notification removed {enable disable} <i>mod/port</i>
Step 5	Verify the configuration.	show cam notification all

MAC addresses are stored in memory between notifications. To set the interval time between notifications and verify the configuration, perform this task in privileged mode:

	Task	Command
Step 1	Set the interval time between notifications.	set cam notification interval <i>time</i>
Step 2	Verify the configuration.	show cam notification all

If the **set cam notification interval** is set to 0, the switch will send notification immediately. If the notifications are sent immediately, they will have an impact on the performance of the switch.

You can generate SNMP traps whenever a MAC address change occurs; do so by enabling the commands **set snmp trap enable macnotification**, **set cam notification**, and **set cam notification historysize**.

To set the SNMP trap MAC address notification, perform this task in privileged mode:

Task	Command
Set the SNMP traps on the system.	set snmp trap enable macnotification

This example shows how to enable MAC address notification globally, how to enable notification of added and removed MAC addresses, and how to set interval time between notifications:

```

Console> (enable) set cam notification enable
MAC address change detection globally enabled
Be sure to specify which ports are to detect MAC address changes
with the 'set cam notification [added|removed] enable <m/p>' command.
SNMP traps will be sent if 'set snmp trap enable macnotification' has been set.
Console> (enable) set cam notification historysize 300
MAC address change history log size set to 300 entries
Console> (enable) set cam notification added enable 3/1-4
MAC address change notifications for added addresses are
enabled on port(s) 3/1-4
Console> (enable) set cam notification removed enable 3/3-6
MAC address change notifications for removed addresses are

```

CISCO Confidential - DRAFT

```
enabled on port(s) 3/3-6
Console> (enable) set cam notification interval 10
MAC address change notification interval set to 10 seconds
Console> (enable) show cam notification all
MAC address change detection enabled
CAM notification interval = 10 second(s).
MAC address change history log size = 300
MAC addresses added = 3
MAC addresses removed = 5
MAC addresses added overflowed = 0
MAC addresses removed overflowed = 0
MAC address SNMP traps generated = 0
Console> (enable) set snmp trap enable macnotification
SNMP MAC notification trap enabled.
Console> (enable)
```

Setting the Security Violation Action

You can set a port to the following two modes to handle a security violation:

- **Shutdown**—Shuts down the port permanently or for a specified time. Permanent shutdown is the default mode.
- **Restrict**—Drops all packets from insecure hosts, but remains enabled.

To set the security violation action to be taken, perform this task in privileged mode:

Task	Command
Set the security violation action on a port.	set port security <i>mod_num/port_num</i> violation {shutdown restrict}

This example sets the port to drop all packets that are coming in on the port from insecure hosts:

```
Console> (enable) set port security 4/7 violation restrict
Port security violation on port 4/7 will cause insecure packets to be dropped.
Console> (enable)
```

**Note**

If you restrict the number of secure MAC addresses on a port to one, and additional hosts attempt to connect to that port, port security prevents these additional hosts from being connected to that port and to any other port in the same VLAN for the duration of the VLAN aging time. By default, the VLAN aging time is 5 minutes. If a host is blocked from joining a port in the same VLAN as the secured port, allow the VLAN aging time to expire before you attempt to connect the host to the port again.

Setting the Shutdown Time

You can specify how long a port is to remain disabled in the event of a security violation. By default, the port is shut down permanently. The valid range is from 1–1440 minutes.

If you set the time to zero, the shutdown is disabled for this port.

**Note**

When the shutdown timeout expires, the port is reenabled and all port security-related configuration is maintained.

CISCO Confidential - DRAFT

To set the shutdown timeout, perform this task in privileged mode:

Task	Command
Set the shutdown timeout on a port.	set port security <i>mod_num/port_num</i> shutdown time

This example shows how to set the shutdown time to 600 minutes on port 4/7:

```
Console> (enable) set port security 4/7 shutdown 600
Secure address shutdown time set to 600 minutes for port 4/7.
Console> (enable)
```

Disabling Port Security

To disable port security, perform this task in privileged mode:

	Task	Command
Step 1	Disable port security on the desired ports.	set port security <i>mod_num/port_num</i> disable
Step 2	Verify the configuration.	show port security [<i>mod_num/port_num</i>]

This example shows how to disable security on a port:

```
Console> (enable) set port security 2/1 disable
Port 2/1 port security disabled.
Console> (enable) show port security 2/1
Port  Security Violation Shutdown-Time Age-Time Max-Addr Trap      IfIndex
-----
 3/24 disabled restrict          20      300      10 disabled    921

Port  Num-Addr Secure-Src-Addr  Age-Left Last-Src-Addr  Shutdown/Time-Left
-----
 3/24      1 00-e0-4f-ac-b4-00      -          -          -          -
Console> (enable)
```

Restricting Traffic for a Host MAC Address

To restrict incoming or outgoing traffic for a specific MAC address, perform this task in privileged mode:

	Task	Command
Step 1	Restrict traffic that is destined to or originating from a specific MAC address.	set cam { static permanent } filter <i>unicast_mac</i> <i>vlan</i>
Step 2	Clear the filter.	clear cam { static permanent } clear cam <i>mac_address</i> <i>vlan</i>
Step 3	Verify the configuration.	show cam <i>mac_address</i> <i>vlan</i> show cam { static permanent }

This example shows how to create a filter for a specific MAC address:

CISCO Confidential - DRAFT

```

Console> (enable) set cam static filter 00-02-03-04-05-06 1
Filter entry added to CAM table.
Console> (enable)

```

This example shows how to clear the filter:

```

Console> (enable) clear cam 00-02-03-04-05-06 1
CAM entry cleared.
Console> (enable)

```

This example shows how to display the static CAM entries:

```

Console> show cam static

VLAN  Dest MAC/Route Des      [CoS]  Destination Ports or VCs / [Protocol Type]
-----
3      04-04-05-06-07-08  *      FILTER
Console> (enable)

```

Monitoring Port Security

You can view the following port security information:

- List of secure MAC addresses for a port
- Maximum number of secure addresses that are allowed on a port
- Total number of secure MAC addresses
- Age and shutdown timeout
- Shutdown and security mode
- Statistics data related to port security

To display port security configuration information and statistics, perform this task in privileged mode:

	Task	Command
Step 1	Display the configuration.	show port security [statistics] <i>mod_num/ port_num</i>
Step 2	Display the port security statistics.	show port security [statistics] [system] [<i>mod_num/port_num</i>]

These examples show how to display port security configuration information and statistics:

```

Console> (enable) show port security 3/24
Port  Security Violation Shutdown-Time Age-Time Max-Addr Trap      IfIndex
-----
3/24  enabled  shutdown          300      60      10 disabled  921

Port  Num-Addr Secure-Src-Addr  Age-Left Last-Src-Addr  Shutdown/Time-Left
-----
3/24      4 00-e0-4f-ac-b4-00      60 00-e0-4f-ac-b4-00      no      -
      00-11-22-33-44-55      0
      00-11-22-33-44-66      0
      00-11-22-33-44-77      0

Console> (enable) show port security statistics 3/24
Port  Total-Addrs Maximum-Addrs
-----
3/24      4          10

```


CISCO Confidential - DRAFT

```

Console> (enable)
Port  Total-Addrs  Maximum-Addrs
-----
  3/24          1          10
Console> (enable)

```

This example shows how to display port security statistics on a module:

```

Console> (enable) show port security statistics 3
Port  Total-Addrs  Maximum-Addrs
-----
  3/1          0          1
  3/2          0          1
  3/3          0          1
  3/4          0          1
  3/5          0          1
  3/6          0          1
Module 3:
  Total ports: 6
  Total secure ports: 0
  Total MAC addresses: 6
  Total global address space used (out of 1024): 0
  Status: installed
Console> (enable)

```

This example shows how to display port security statistics on the system:

```

Console> (enable) show port security statistics system
Module 1:
  Total ports: 2
  Total MAC address(es): 2
  Total global address space used (out of 1024): 0
  Status: installed
Module 3:
  Module does not support port security feature
Module 6:
  Total ports: 48
  Total MAC address(es): 48
  Total global address space used (out of 1024): 0
  Status: installed
Console> (enable)

```

CISCO Confidential - DRAFT

Configuring Unicast Flood Blocking

This chapter describes how to configure unicast flood blocking on the Catalyst enterprise LAN switches.

**Note**

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 4500 Series, Catalyst 2948G, and Catalyst 2980G Switches Command Reference*.

This chapter consists of these sections:

- [Understanding How Unicast Flood Blocking Works, page 17-1](#)
- [Configuration Guidelines for Unicast Flood Blocking, page 17-2](#)
- [Configuring Unicast Flood Blocking on the Switch, page 17-2](#)

Understanding How Unicast Flood Blocking Works

You can enable unicast flood blocking on any Ethernet port on a per-port basis. Unicast flood blocking allows you to drop unicast flood packets on an Ethernet port that has only one host that is connected to the port. All Ethernet ports on a switch are configured to allow unicast flooding. With unicast flood blocking, you can drop unicast flood packets before they reach the port.

**Caution**

You must have a static CAM entry that is associated with the Ethernet port before you enable unicast flood blocking. If you do not have a static CAM entry that is associated with the port, you will lose network connectivity if you enable unicast flood blocking. You can verify that a static CAM entry exists by entering the **show cam static** command.

**Note**

If you are configuring unicast flood blocking on a secure port; see [Chapter 16, “Configuring Port Security.”](#)

CISCO Confidential - DRAFT

Configuration Guidelines for Unicast Flood Blocking

This section lists the guidelines for configuring unicast flood blocking:

- Only Ethernet ports can block unicast flood traffic.
- If the Ethernet port is part of an IPX network, you must manually enter a static CAM entry in the CAM table before you disable unicast flood on the port.
- You cannot configure unicast flood blocking on SPAN destination ports.
- You cannot configure a SPAN destination on a unicast flood blocking port.
- You cannot configure unicast flood blocking on a trunk port. If you attempt to configure unicast flood blocking on a trunk port, you will see an error message.
- You cannot configure unicast flood blocking on a port channel.
- You cannot configure a port channel on a unicast flood blocking port.
- Unicast flood blocking and GARP VLAN Registration Protocol (GVRP) are mutually exclusive. You cannot configure the port to block unicast flood packets and exchange VLAN configuration information with GVRP switches at the same time.

Configuring Unicast Flood Blocking on the Switch

These sections describe how to configure unicast flood blocking:

- [Enabling Unicast Flood Blocking, page 17-2](#)
- [Disabling Unicast Flood Blocking, page 17-3](#)
- [Displaying Unicast Flood Blocking, page 17-3](#)

**Note**

It is important to remember that the unicast flood blocking feature is given priority over other features, such as protocol filtering.

Enabling Unicast Flood Blocking

To configure the switch to drop unicast flood packets on a port, you must disable unicast flood blocking.

**Note**

The port disables unicast flooding once the MAC address limit is reached.

To configure unicast flood blocking, perform this task in privileged mode:

Task	Command
Enable unicast flood blocking on the desired Ethernet ports to disable unicast flooding.	set port unicast-flood <i>mod/port</i> disable

CISCO Confidential - DRAFT

This example shows how to disable unicast flood packets on a port:

```
Console> (enable) set port unicast-flood 4/1 disable  
WARNING: Trunking & Channelling will be disabled on the port.  
Unicast Flooding is successfully disabled on the port 4/1.  
Console> (enable)
```

Disabling Unicast Flood Blocking

To configure the switch to receive unicast flood packets on a port, you must enable unicast flood blocking.

To configure unicast flood blocking, perform this task in privileged mode:

Task	Command
Disable unicast flood blocking on the desired Ethernet ports to enable unicast flooding.	set port unicast-flood <i>mod/port</i> enable

This example shows how to disable unicast flood blocking on a port:

```
Console> (enable) set port unicast-flood 4/1 enable  
Unicast Flooding is successfully enabled on the port 4/1.  
Console> (enable)
```

Displaying Unicast Flood Blocking

To display unicast flood blocking information, perform this task in privileged mode:

Task	Command
Display unicast flood blocking information on a per-port basis.	show port unicast-flood <i>mod/port</i>

This example shows how to display unicast flood block information for port 1 on module 4:

```
Console> (enable) show port unicast-flood 4/1  
Port      Unicast Flooding  
----      -  
4/1       Disabled  
Console> (enable)
```

CISCO Confidential - DRAFT

Configuring the IP Permit List

This chapter describes how to configure the IP permit list on the Catalyst enterprise LAN switches.

**Note**

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 4500 Series, Catalyst 2948G, and Catalyst 2980G Switches Command Reference*.

This chapter consists of these sections:

- [Understanding How the IP Permit List Works, page 18-1](#)
- [IP Permit List Default Configuration, page 18-2](#)
- [Configuring the IP Permit List on the Switch, page 18-2](#)

Understanding How the IP Permit List Works

The IP permit list prevents inbound Telnet and SNMP access to the switch from unauthorized source IP addresses. All other TCP/IP services (such as IP traceroute and IP ping) continue to work normally when you enable the IP permit list. Outbound Telnet, Trivial File Transfer Protocol (TFTP), and other IP-based services are unaffected by the IP permit list.

Telnet attempts from unauthorized source IP addresses are denied a connection. SNMP requests from unauthorized IP addresses receive no response; the request times out. If you want to log unauthorized access attempts to the console or a syslog server, you must change the logging severity level for IP, as described in the [“Enabling the IP Permit List” section on page 18-3](#). If you want to generate SNMP traps when unauthorized access attempts are made, you must enable IP permit list (ippermit) SNMP traps, as described in the [“Enabling the IP Permit List” section on page 18-3](#). Multiple access attempts from the same unauthorized host only trigger notifications every 10 minutes.

You can configure up to 100 entries in the permit list. Each entry consists of an IP address and subnet mask pair in dotted decimal format and information on whether the IP address is part of the SNMP permit list, Telnet permit list, or both lists. The bits set to one in the mask are checked for a match with the source IP address of incoming packets, while the bits set to zero are not checked. This process allows wildcard addresses to be specified.

If you do not specify the mask for an IP permit list entry, or if you enter a host name instead of an IP address, the mask has an implicit value of all bits set to one (255.255.255.255 or 0xffffffff), which matches only the IP address of that host.

If you do not specify SNMP or Telnet for the type of permit list for the IP address, the IP address is added to both the SNMP and Telnet permit lists.

CISCO Confidential - DRAFT

You can specify the same IP address in more than one entry in the permit list if the masks are different. The mask is applied to the address before it is stored in NVRAM, so that entries that have the same effect (but different addresses) are not stored. When you add such an address to the IP permit list, the system displays the address after the mask is applied.

IP Permit List Default Configuration

Table 18-1 shows the default IP permit list configuration.

Table 18-1 IP Permit List Default Configuration

Feature	Default Value
IP permit list enable state	Disabled
Permit list entries	None configured
IP syslog message severity level	2
SNMP IP permit trap (ippermit)	Disabled

Configuring the IP Permit List on the Switch

The following sections describe how to configure IP permit list.

Adding IP Addresses to the IP Permit List

You can add an IP address to the SNMP permit list, the Telnet permit list, or both lists. To add IP addresses to an IP permit list, perform this task in privileged mode:

	Task	Command
Step 1	Specify the IP addresses to add to the IP permit list.	set ip permit <i>ip_address</i> [<i>mask</i>] [all snmp telnet ssh]
Step 2	Verify the IP permit list configuration.	show ip permit

	
Note	You can use the set security acl command to set permit lists more efficiently.

This example shows how to add IP addresses to IP permit list and verify the configuration:

```

Console> (enable) set ip permit 172.16.0.0 255.255.0.0 telnet
172.16.0.0 with mask 255.255.0.0 added to Telnet permit list.
Console> (enable) set ip permit 172.20.52.32 255.255.0.0 snmp
172.20.52.32 with mask 255.255.0.0 added to Snmp permit list.
Console> (enable) set ip permit 172.20.52.3 all
172.20.52.3 added to IP permit list.
Console> (enable) set ip permit 172.20.52.31 255.255.255.224 ssh
172.20.52.31 with mask 255.255.255.224 added to Ssh permit list.
Console> (enable) show ip permit
Telnet permit list disabled.
```


CISCO Confidential - DRAFT

```

Ssh permit list disabled.
Snmp permit list disabled.
Permit List      Mask      Access-Type
-----
172.16.0.0      255.255.0.0    telnet
172.20.0.0      255.255.0.0    snmp
172.20.52.0     255.255.255.224 ssh
172.20.52.3     telnet ssh snm
Denied IP Address  Last Accessed Time Type      Telnet Count  SNMP Count
-----
172.100.101.104   01/20/97,07:45:20 SNMP      14            1430
172.187.206.222   01/21/97,14:23:05 Telnet     7             236

Console> (enable)

```

Enabling the IP Permit List

You can enable either the SNMP permit list, the Telnet permit list, or both lists. If you do not specify a permit list, both the SNMP and Telnet permit lists are enabled.



Caution

Before enabling the IP permit list, make sure that you add the IP address of your workstation or network management system to the permit list, especially when configuring through SNMP. Failure to do so could result in your connection being dropped by the switch that you are configuring. We recommend that you disable the IP permit list before clearing IP permit entries or host addresses.

To enable the IP permit list on the switch, perform this task in privileged mode:

	Task	Command
Step 1	Enable the IP permit list.	set ip permit enable [ssh snmp telnet]
Step 2	If desired, enable the IP permit trap to generate traps for unauthorized access attempts.	set snmp trap enable ippermit
Step 3	If desired, configure the logging level to see syslog messages for unauthorized access attempts.	set logging level ip 4 default
Step 4	Verify the IP permit list configuration.	show ip permit show snmp

This example shows how to enable the IP permit list and verify the configuration:

```

Console> (enable) set ip permit enable
Telnet, Snmp and Ssh permit list enabled
Console> (enable) set snmp trap enable ippermit
SNMP IP Permit traps enabled.
Console> (enable) set logging level ip 4 default
System logging facility <ip> set to severity 4(warnings)
Console> (enable) show ip permit
Telnet permit list enabled.
Ssh permit list enabled.
Snmp permit list enabled.
Permit List      Mask      Access-Type
-----
172.16.0.0      255.255.0.0    telnet
172.20.0.0      255.255.0.0    snmp
172.20.52.0     255.255.255.224 ssh
172.20.52.3     telnet ssh snmp

```

CISCO Confidential - DRAFT

```
Denied IP Address Last Accessed Time Type
-----
Denied IP Address   Last Accessed Time Type   Telnet Count   SNMP Count
-----
172.100.101.104     01/20/97,07:45:20  SNMP           14             1430
172.187.206.222     01/21/97,14:23:05  Telnet          7              236

Console> (enable) show snmp
RMON:                               Disabled
Extended RMON Netflow:             Disabled
Traps Enabled:
ippermit
Port Traps Enabled: None

Community-Access   Community-String
-----
read-only          public
read-write         private
read-write-all    secret

Trap-Rec-Address   Trap-Rec-Community
-----
Console> (enable)
```

Disabling the IP Permit List

To disable the IP permit list on the switch, perform this task in privileged mode:

	Task	Command
Step 1	Disable the IP permit list.	set ip permit disable [ssh snmp telnet]
Step 2	Verify the IP permit list configuration.	show ip permit

This example shows how to disable the IP permit list:

```
Console> (enable) set ip permit disable
IP permit list disabled.
Console> (enable)
```

Clearing an IP Permit List Entry

You can clear an IP address from the SNMP permit list, SSH permit list, the Telnet permit list, or all lists. If you do not specify which permit list to clear the IP address from, the IP address is deleted from both permit lists.



Caution

Disable the IP permit list before clearing IP permit entries or host addresses. This action prevents your connection from being dropped by the switch you are configuring in case you clear your current IP address.

To clear an IP permit list entry, perform this task in privileged mode:

CISCO Confidential - DRAFT

	Task	Command
Step 1	Disable the IP permit list.	set ip permit disable [ssh snmp telnet]
Step 2	Specify the IP address to remove from the IP permit list.	clear ip permit { <i>ip_address</i> [<i>mask</i>] all } [ssh snmp telnet]
Step 3	Verify the IP permit list configuration.	show ip permit

This example shows how to clear an IP permit list entry:

```
Console> (enable) set ip permit disable
IP permit list disabled.
Console> (enable) clear ip permit 172.100.101.102
172.100.101.102 cleared from IP permit list.
Console> (enable) clear ip permit 172.160.161.0 255.255.192.0 snmp
172.160.128.0 with mask 255.255.192.0 cleared from snmp permit list.
Console> (enable) clear ip permit 172.100.101.102 telnet
172.100.101.102 cleared from telnet permit list.
Console> (enable) clear ip permit all
IP permit list cleared.
Console> (enable)
```

CISCO Confidential - DRAFT

Configuring Protocol Filtering

This chapter describes how to configure protocol filtering on Ethernet, Fast Ethernet, and Gigabit Ethernet ports on the Catalyst enterprise LAN switches. The configuration procedures in this chapter apply to Ethernet, Fast Ethernet, and Gigabit Ethernet switch ports on switching modules and fixed-configuration switches, in addition to supervisor engine Fast and Gigabit Ethernet uplink ports.

**Note**

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 4500 Series, Catalyst 2948G, and Catalyst 2980G Switches Command Reference*.

This chapter consists of these sections:

- [Understanding How Protocol Filtering Works, page 19-1](#)
- [Default Protocol Filtering Configuration, page 19-2](#)
- [Configuring Protocol Filtering on the Switch, page 19-2](#)

Understanding How Protocol Filtering Works

Protocol filtering prevents certain protocol traffic from being forwarded out switch ports. Broadcast and unicast flood traffic is filtered based on the membership of ports in different protocol groups. This filtering is in addition to the filtering that is provided by port-VLAN membership.

Protocol filtering identifies ports on a protocol basis. A port can be a member of one or more of the protocol groups. Flood traffic for each protocol group is forwarded out a port only if that port belongs to the appropriate protocol group.

Layer 2 protocols, such as Spanning Tree Protocol (STP) and Cisco Discovery Protocol (CDP), are not affected by protocol filtering. Dynamic VLAN ports and ports that have port security enabled are members of all protocol groups.

You can configure a port with any one of these modes for each protocol group: **on**, **off**, or **auto**. If the configuration is set to **on**, the port receives all the flood traffic for that protocol. If the configuration is set to **off**, the port does not receive any flood traffic for that protocol. If the configuration is set to **auto**, a port becomes a member of the protocol group only after the device that is connected to the port transmits packets of the specific protocol group. The switch detects the traffic, adds the port to the protocol group, and begins forwarding flood traffic for that protocol group to that port. Autoconfigured ports are removed from the protocol group if the attached device does not transmit packets for that protocol within 60 minutes. Ports are also removed from the protocol group when the supervisor engine detects that the link is down on the port.

CISCO Confidential - DRAFT

For example, if a host that supports both IP and Internetwork Packet Exchange (IPX) is connected to a switch port that is configured as **auto** for IPX, and the host is transmitting only IP traffic, the port to which the host is connected will not forward any IPX flood traffic to the host. However, if the host transmits an IPX packet, the supervisor engine software detects the protocol traffic and the port is added to the IPX group, allowing the port to receive IPX flood traffic. If the host does not send any IPX traffic for more than 60 minutes, the port is removed from the IPX protocol group.

By default, ports are configured as **on** for the IP protocol group. Typically, you should configure a port to **auto** for IP only if there is a directly connected end station that is connected to the port. The default port configuration for IPX and Group is **auto**.

Packets are classified into these protocol groups:

- IP (**ip**)
- IPX (**ipx**)
- AppleTalk and DECnet (**group**)
- Packets not belonging to any of these protocols

Default Protocol Filtering Configuration

Table 19-1 shows the default protocol filtering configuration.

Table 19-1 Protocol Filtering Default Configuration

Feature	Default Value
Protocol filtering	Disabled
ip mode	on
ipx mode	auto
group mode	auto

Configuring Protocol Filtering on the Switch

The next two sections describe how to configure and disable protocol filtering on Ethernet, Fast Ethernet, and Gigabit Ethernet ports.

Configuring Protocol Filtering

To configure protocol filtering on Ethernet, Fast Ethernet, and Gigabit Ethernet ports, perform this task in privileged mode:

	Task	Command
Step 1	Enable protocol filtering.	set protocolfilter enable
Step 2	Set the protocol membership of the desired ports.	set port protocol <i>mod_num/port_num</i> {ip ipx group} {on off auto}
Step 3	Verify the port filtering configuration.	show port protocol [<i>mod_num</i>[/<i>port_num</i>]]

CISCO Confidential - DRAFT

This example shows how to enable protocol filtering, set the protocol membership of ports, and verify the configuration:

```

Console> (enable) set protocolfilter enable
Protocol filtering enabled on this switch.
Console> (enable) set port protocol 3/1-4 ip on
IP protocol set to on mode on ports 3/1-4.
Console> (enable) set port protocol 3/1-4 ipx off
IPX protocol disabled on ports 3/1-4.
Console> (enable) set port protocol 3/1-4 group auto
Group protocol set to auto mode on ports 3/1-4.
Console> (enable) show port protocol 3/1-4

```

Port	Vlan	IP	IP Hosts	IPX	IPX Hosts	Group	Group Hosts
3/1	4	on	1	off	0	auto-off	0
3/2	5	on	1	off	0	auto-on	1
3/3	2	on	1	off	0	auto-off	0
3/4	4	on	1	off	0	auto-on	1

```

Console> (enable)

```

Disabling Protocol Filtering

To disable protocol filtering, perform this task in privileged mode:

Task	Command
Disable protocol filtering.	set protocolfilter disable

This example shows how to disable protocol filtering:

```

Console> (enable) set protocolfilter disable
Protocol filtering disabled on this switch.
Console> (enable)

```

CISCO Confidential - DRAFT

Checking Status and Connectivity

This chapter describes how to check switch status and connectivity on the Catalyst enterprise LAN switches.

**Note**

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 4500 Series, Catalyst 2948G, and Catalyst 2980G Switches Command Reference*.

This chapter consists of these sections:

- [Checking Module Status, page 20-1](#)
- [Checking Port Status, page 20-2](#)
- [Displaying the Port MAC Address, page 20-4](#)
- [Displaying Port Capabilities, page 20-5](#)
- [Using Telnet, page 20-6](#)
- [Changing the Login Timer, page 20-6](#)
- [Using Secure Shell Encryption for Telnet Sessions, page 20-7](#)
- [Monitoring User Sessions, page 20-7](#)
- [Using Ping, page 20-9](#)
- [Using Layer 2 Traceroute, page 20-11](#)
- [Using IP Traceroute, page 20-12](#)

Checking Module Status

The Catalyst enterprise LAN switches are multimodule systems. You can see what modules are installed, as well as the MAC address ranges and version numbers for each module, by using the **show module** command. You can use the `[mod_num]` argument to specify a particular module number to see detailed information on that module.

The Catalyst 4912G, 2948G, and 2980G switches are fixed-configuration switches, but are logically modular. You must apply configuration commands to the appropriate module. For example, on a Catalyst 2948G series switch, the 24 Fast Ethernet ports belong logically to module 2.

CISCO Confidential - DRAFT

This example shows how to check module status on a Catalyst 2948G switch:

```

Console> (enable) show module
Mod Slot Ports Module-Type           Model           Status
-----
1  1    0    Switching Supervisor      WS-X2948        ok
2  1    50    10/100/1000 Ethernet      WS-X2948G       ok

Mod Module-Name      Serial-Num
-----
1  Supervisor        JAB023807H1
2  Switch Ports      JAB023807H1

Mod MAC-Address(es)           Hw    Fw    Sw
-----
1  00-50-73-12-09-00 to 00-50-73-12-0c-ff 1.0    4.4(1)  5.1(1)
2  00-50-73-12-0c-9e to 00-50-73-12-0c-fd 1.0
Console> (enable)

```

This example shows how to check module status on a specific module:

```

Console> (enable) show module 3
Mod Slot Ports Module-Type           Model           Sub Status
-----
3  3    6    1000BaseX Ethernet      WS-X4306        no  ok

Mod Module-Name      Serial-Num
-----
3                      JAB024000YY

Mod MAC-Address(es)           Hw    Fw    Sw
-----
3  00-10-7b-f6-b2-1a to 00-10-7b-f6-b2-1f 0.2
Console> (enable)

```

Checking Port Status

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

The Catalyst 4912G, 2948G, and 2980G switches are fixed-configuration switches but are logically modular. To apply configuration commands to a particular port, you must specify the appropriate logical module. For more information, see the [“Checking Module Status” section on page 20-1](#).

This example shows how to display information about the ports on a specific module only:

```

Console> (enable) show port 3
Port  Name              Status      Vlan      Level  Duplex  Speed  Type
-----
3/1                      connected   10        normal   full    1000   1000BaseSX
3/2                      connected   10        normal   full    1000   1000BaseSX
3/3                      connected   20        normal   full    1000   1000BaseSX
3/4                      connected   40        normal   full    1000   1000BaseSX
3/5                      notconnect  1         normal   full    1000   No GBIC
3/6                      notconnect  1         normal   full    1000   No GBIC

Port  Security Secure-Src-Addr  Last-Src-Addr  Shutdown  Trap  IfIndex
-----
3/1   disabled
3/2   disabled

```

CISCO Confidential - DRAFT

3/3	disabled	No	disabled 17
3/4	disabled	No	disabled 18
3/5	disabled	No	disabled 19
3/6	disabled	No	disabled 20

Port	Send FlowControl admin oper	Receive FlowControl admin oper	RxPause	TxPause	Unsupported opcodes
3/1	desired on	desired on	0	0	0
3/2	desired on	desired on	0	0	0
3/3	desired on	desired on	0	0	0
3/4	desired on	desired on	0	0	0
3/5	desired off	off off	0	0	0
3/6	desired off	off off	0	0	0

Port	Status	Channel mode	Channel status	Neighbor device	Neighbor port
3/1	connected	off	not channel		
3/2	connected	off	not channel		
3/3	connected	off	not channel		
3/4	connected	off	not channel		
3/5	notconnect	off	not channel		
3/6	notconnect	off	not channel		

Port	Align-Err	FCS-Err	Xmit-Err	Rcv-Err	UnderSize
3/1	-	0	0	0	0
3/2	-	0	0	0	0
3/3	-	0	0	0	0
3/4	-	0	0	0	0
3/5	-	0	0	0	0
3/6	-	0	0	0	0

Port	Single-Col	Multi-Coll	Late-Coll	Excess-Col	Carri-Sen	Runts	Giants
3/1	0	0	0	0	0	0	0
3/2	0	0	0	0	0	0	0
3/3	0	0	0	0	0	0	0
3/4	0	0	0	0	0	0	0
3/5	0	0	0	0	0	0	0
3/6	0	0	0	0	0	0	0

Last-Time-Cleared

 Fri Apr 30 1999, 18:54:17
 Console> (enable)

This example shows how to display information on an individual port:

Console> (enable) **show port 2/1**

Port	Name	Status	Vlan	Level	Duplex	Speed	Type
2/1		inactive	100	normal	auto	auto	10/100BaseTX

Port	AuxiliaryVlan	AuxVlan-Status	InlinePowered Admin Oper	PowerAllocated Detected	mWatt	mA	@51V
2/1	none	none	-	-	-	-	-

Port	Security Violation	Shutdown-Time	Age-Time	Max-Addr	Trap	IfIndex
2/1	disabled	shutdown	0	0	1 disabled	15

CISCO Confidential - DRAFT

```

Port  Num-Addr  Secure-Src-Addr  Age-Left  Last-Src-Addr  Shutdown/Time-Left
-----
2/1      0          -          -          -          -

Port  Status      Channel      Admin Ch      Group Id
-----
2/1  inactive    auto silent          1      0

Port  Align-Err  FCS-Err  Xmit-Err  Rcv-Err  UnderSize
-----
2/1      -          0        998      1012      0

Port  Single-Col  Multi-Coll  Late-Coll  Excess-Col  Carri-Sen  Runts      Giants
-----
2/1      0          0          0          0          0        1012      0

Last-Time-Cleared
-----
Mon Jun 11 2001, 07:26:48
Console> (enable)

```

Displaying the Port MAC Address

In addition to displaying the MAC address range for a module using the **show module** command, you can display the MAC address of a specific port in the switch using the **show port mac-address** command.

To display the MAC address for a specific port, perform this task in privileged mode:

Task	Command
Display the MAC address for a specific port.	show port mac-address [<i>mod[/port]</i>]

This example shows you how to display the MAC address of a specific port:

```

Console> show port mac-address 4/1
Port  Mac address
-----
4/1  00-50-54-bf-59-64

```

This example shows you how to display the MAC addresses of all ports on a module:

```

Console> show port mac-address 4
Port  Mac address
-----
4/1  00-50-54-bf-59-64
4/2  00-50-54-bf-59-65
4/3  00-50-54-bf-59-66
4/4  00-50-54-bf-59-67
.
.
.
4/47 00-50-54-bf-59-92
4/48 00-50-54-bf-59-93

```

CISCO Confidential - DRAFT

Displaying Port Capabilities

You can display the capabilities of any port in a switch using the **show port capabilities** command. This example shows you how to display the port capabilities for ports on module 2:

```
Console> (enable) show port capabilities 2
Model          WS-X4148
Port           2/1
Type           10/100BaseTX
Speed          auto,10,100
Duplex         half,full
Trunk encap type 802.1Q
Trunk mode     on,off,desirable,auto,nonegotiate
Channel        2/1-48
Flow control   no
Security       yes
Membership     static,dynamic
Fast start     yes
QOS scheduling rx-(none),tx-(2q1t)
CoS rewrite    no
ToS rewrite    no
Rewrite        no
UDLD          yes
Inline power   no
AuxiliaryVlan  1..1000,untagged,none
SPAN           source,destination
```

```
-----
Model          WS-X4148
Port           2/2
Type           10/100BaseTX
Speed          auto,10,100
Duplex         half,full
Trunk encap type 802.1Q
Trunk mode     on,off,desirable,auto,nonegotiate
Channel        2/1-48
Flow control   no
Security       yes
Membership     static,dynamic
Fast start     yes
QOS scheduling rx-(none),tx-(2q1t)
CoS rewrite    no
ToS rewrite    no
Rewrite        no
UDLD          yes
Inline power   no
AuxiliaryVlan  1..1000,untagged,none
SPAN           source,destination
.
.
.
```

This example shows you how to display the port capabilities for port 5 on module 3:

```
Console> (enable) show port capabilities 3/5
Model          WS-X4148
Port           3/5
Type           10/100BaseTX
Speed          auto,10,100
Duplex         half,full
Trunk encap type 802.1Q
Trunk mode     on,off,desirable,auto,nonegotiate
Channel        3/1-48
```

CISCO Confidential - DRAFT

```
Flow control          no
Security              yes
Membership            static,dynamic
Fast start            yes
QoS scheduling        rx-(none), tx-(2q1t)
CoS rewrite           no
ToS rewrite           no
Rewrite              no
UDLD                  yes
Inline power          no
AuxiliaryVlan         1..1000, untagged, none
SPAN                  source,destination
```

```
Console> (enable)
```

Using Telnet

You can access the switch CLI using Telnet. In addition, you can use Telnet from the switch to access other devices in the network. Up to eight simultaneous Telnet sessions are possible.

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

To open a Telnet session to another device on the network from the switch, perform this task in privileged mode:

Task	Command
Open a Telnet session to a remote host.	telnet <i>host</i> [<i>port</i>]

This example shows how to open a Telnet session from the switch to the remote host labsparc:

```
Console> (enable) telnet labsparc
Trying 172.16.10.3...
Connected to labsparc.
Escape character is '^]'.

UNIX(r) System V Release 4.0 (labsparc)

login:
```

Changing the Login Timer

The login timer is the number of minutes after which an idle session is disconnected. To change the logout timer value, perform this task in privileged mode:

Task	Command
Change the logout timer value (a timeout value of 0 prevents idle sessions from being disconnected automatically).	set logout <i>timeout</i>

This example shows how to set the logout timer value to 10 minutes:

CISCO Confidential - DRAFT

```
Console> (enable) set logout 10
Sessions will be automatically logged out after 10 minutes of idle time.
Console> (enable)
```

This example shows how to set the logout timer value to 0, preventing idle sessions from being disconnected automatically:

```
Console> (enable) set logout 0
Sessions will not be automatically logged out.
Console> (enable)
```

Using Secure Shell Encryption for Telnet Sessions

**Note**

To use the secure shell encryption (SSH) feature commands, you must be running an encryption image. Encryption commands are **set crypto key rsa**, **clear crypto key rsa**, and **show crypto key**. See [Chapter 33, “Working with System Software Images,”](#) for the software image naming conventions that are used for the encryption images.

The SSH feature provides security for Telnet sessions to the switch. SSH is supported for remote logins to the switch only. Telnet sessions that are initiated from the switch cannot be encrypted. To use this feature, you must install the application on the client accessing the switch and you must configure SSH the switch.

The current implementation of SSH supports version 1, both the data encryption standard (DES) and 3DES encryption methods, and can be used with RADIUS and TACACS+ authentication. To support authentication for Telnet with secure shell encryption, enter the **telnet** keyword in the **set authentication** commands.

**Note**

If you are using Kerberos to authenticate to the switch, you will not be able to use the secure shell encryption feature.

To enable SSH on the switch, perform this task in privileged mode:

Task	Command
Create the RSA host key.	set crypto key rsa nbits [force]

This example shows how to create the RSA host key:

```
Console> (enable) set crypto key rsa 1024
Generating RSA keys.... [OK]
Console> (enable)
```

The *nbits* value specifies the RSA key size; the valid key size range is from 512 to 2048 bits. A key size with a larger number provides higher security but takes longer to generate.

Monitoring User Sessions

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

CISCO Confidential - DRAFT

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

Task	Command
Display the currently active user sessions on the switch.	show users [noalias]

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

```
Console> (enable) show users
  Session  User              Location
  -----
  console
  telnet           sam-pc.bigcorp.com
  * telnet         jake-mac.bigcorp.com
Console> (enable)
```

This example shows the output of the **show users** command when TACACS+ authentication is enabled for console and Telnet sessions:

```
Console> (enable) show users
  Session  User              Location
  -----
  console  sam
  telnet   jake              jake-mac.bigcorp.com
  telnet   tim              tim-nt.bigcorp.com
  * telnet  suzy              suzy-pc.bigcorp.com
Console> (enable)
```

This example shows how to display information about user sessions using the **noalias** keyword to display the IP addresses of connected hosts:

```
Console> (enable) show users noalias
  Session  User              Location
  -----
  console
  telnet           10.10.10.12
  * telnet         10.10.20.46
Console> (enable)
```

To disconnect an active user session, perform this task in privileged mode:

Task	Command
Disconnect an active user session on the switch.	disconnect { console ip_addr }

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

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


CISCO Confidential - DRAFT

```

Console> (enable) show users
  Session  User                Location
  -----  -
telnet    jake                jake-mac.bigcorp.com
* telnet  suzy                suzy-pc.bigcorp.com
Console> (enable)

```

Using Ping

The next two sections describe how to use IP ping.

Understanding How Ping Works

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

The **ping** command is configurable from normal executive and privileged executive mode. In normal executive mode, the **ping** command supports the **-s** parameter, which allows you to specify the packet size and packet count. In privileged executive mode, the **ping** command allows you to specify the packet size, packet count, and the wait time.

Table 20-1 lists the default values that apply to the **ping-s** command.

Table 20-1 Ping Default Values

	Ping	Ping-s
Number of Packets	5	0=continuous ping
Packet Size	56	56
Wait Time	2	2
Source Address	Host IP Address	—

Ping will return one of the following responses:

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

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

CISCO Confidential - DRAFT

Executing Ping

To ping another device on the network from the switch, perform one of these tasks in normal or privileged mode:

Task	Command
Ping a remote host.	ping <i>host</i>
Ping a remote host using ping options.	ping -s <i>host</i> [<i>packet_size</i>] [<i>packet_count</i>]

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

```

Console> ping labsparc
labsparc is alive
Console> ping 72.16.10.3
72.16.10.3 is alive
Console>

```

This example shows how to ping a remote host using the **-s** option:

```

Console> ping -s 12.20.5.3 800 10
PING 12.20.2.3: 800 data bytes
808 bytes from 12.20.2.3: icmp_seq=0. time=2 ms
808 bytes from 12.20.2.3: icmp_seq=1. time=3 ms
808 bytes from 12.20.2.3: icmp_seq=2. time=2 ms
808 bytes from 12.20.2.3: icmp_seq=3. time=2 ms
808 bytes from 12.20.2.3: icmp_seq=4. time=2 ms
808 bytes from 12.20.2.3: icmp_seq=5. time=2 ms
808 bytes from 12.20.2.3: icmp_seq=6. time=2 ms
808 bytes from 12.20.2.3: icmp_seq=7. time=2 ms
808 bytes from 12.20.2.3: icmp_seq=8. time=2 ms
808 bytes from 12.20.2.3: icmp_seq=9. time=3 ms

---17.20.2.3 PING Statistics---
10 packets transmitted, 10 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 2/2/3
Console>

```

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

```

Console> (enable) ping
Target IP Address []: 12.20.5.19
Number of Packets [5]: 10
Datagram Size [56]: 100
Timeout in seconds [2]: 10
Source IP Address [12.20.2.18]: 12.20.2.18
!!!!!!!!!!!!

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

```

Using Layer 2 Traceroute

The Layer 2 Traceroute utility allows you to identify the physical path that a packet takes from a source to a destination. This utility determines the path by looking at the forwarding engine tables of the switches in the path.

Information is displayed about all Catalyst 4000 family, Catalyst 5000 family, and Catalyst 6500 series switches that are in the path from the source to the destination.

Layer 2 Traceroute Usage Guidelines

This section lists the guidelines for the Layer 2 Traceroute utility:

- The Layer 2 Traceroute utility works for unicast traffic only.
- You must enable CDP on all of the Catalyst 4000 family, Catalyst 5000 family, and Catalyst 6500 series switches in the network. (See [Chapter 21, “Configuring CDP,”](#) for information about enabling CDP.) If any devices in the path are transparent to CDP, **l2trace** will not be able to trace the Layer 2 path through those devices.
- You can use this utility from a switch that is not in the Layer 2 path between the source and the destination; however, all of the switches in the path, including the source and destination, must be reachable from the switch.
- All switches in the path must be reachable from each other.
- You can trace a Layer 2 path by specifying the source and destination IP addresses (or IP aliases) or the MAC addresses. If the source and destination belong to multiple VLANs and you specify MAC addresses, you can also specify a VLAN.
- The source and destination switches must belong to the same VLAN.
- The maximum number of hops an **l2trace** query will try is 10; this includes hops involved in source tracing.
- The Layer 2 Traceroute utility does not work with Token Ring VLANs, when multiple devices are attached to one port through hubs, or when multiple neighbors are on a port.

Identifying a Layer 2 Path

To identify a Layer 2 path, perform one of these tasks in privileged mode:

Task	Command
Trace a Layer 2 path using MAC addresses.	l2trace {src-mac-addr} {dest-mac-addr} [vlan] [detail]
Trace a Layer 2 path using IP addresses or IP aliases.	l2trace {src-ip-addr} {dest-ip-addr} [detail]

This example shows the source and destination MAC addresses specified, with no VLAN specified but with the detail option specified. For each Catalyst 4000 family, 5000 family, and 6500 series switch found in the path, the output shows the device type, device name, device IP address, in port name, in port speed, in port duplex mode, out port name, out port speed, and out port duplex mode.

```
Console> (enable) l2trace 00-01-22-33-44-55 10-22-33-44-55-66 detail
```

CISCO Confidential - DRAFT

```
l2trace vlan number is 10.
```

```
00-01-22-33-44-55 found in C4000 named wiring-1 on port 4/1 10Mb half duplex
C4000:wiring-1:192.168.242.10:4/1 10Mb half duplex -> 5/2 100MB full duplex
C4000:backup-wiring-1:192.168.242.20:1/1 100Mb full duplex -> 3/1 100MB full duplex
C5000:backup-core-1:192.168.242.30:4/1 100 MB full duplex -> 1/1 100MB full duplex
C6000:core-1:192.168.242.40:1/1 100MB full duplex -> 2/1 10MB half duplex.
10-22-33-44-55-66 found in C4000 named core-1 on port 2/1 10MB half duplex.
Console> (enable)
```

Using IP Traceroute

The next two sections describe how to use IP traceroute.

Understanding How IP Traceroute Works

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

Switches can participate as the source or destination of the **traceroute** command but will not appear as a hop in the **traceroute** command output.

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

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

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

Executing IP Traceroute

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

Task	Command
Execute IP traceroute to trace the path packets take through the network.	traceroute [-n] [-w <i>wait_time</i>] [-i <i>initial_ttl</i>] [-m <i>max_ttl</i>] [-p <i>dest_port</i>] [-q <i>nqueries</i>] [-t <i>tos</i>] <i>host</i> [<i>data_size</i>]

CISCO Confidential - DRAFT

This example shows the basic usage of the **traceroute** command:

```
Console> (enable) traceroute 10.1.1.100  
traceroute to 10.1.1.100 (10.1.1.100), 30 hops max, 40 byte packets  
 1 10.1.1.1 (10.1.1.1)  1 ms  2 ms  1 ms  
 2 10.1.1.100 (10.1.1.100)  2 ms  2 ms  2 ms  
Console> (enable)
```

This example shows how to perform a **traceroute** with six queries to each hop with packets of 1400 bytes each:

```
Console> (enable) traceroute -q 6 10.1.1.100 1400  
traceroute to 10.1.1.100 (10.1.1.100), 30 hops max, 1440 byte packets  
 1 10.1.1.1 (10.1.1.1)  2 ms  2 ms  2 ms  1 ms  2 ms  2 ms  
 2 10.1.1.100 (10.1.1.100)  2 ms  4 ms  3 ms  3 ms  3 ms  3 ms  
Console> (enable)
```

CISCO Confidential - DRAFT

Configuring CDP

This chapter describes how to configure the Cisco Discovery Protocol (CDP) on the Catalyst enterprise LAN switches.

**Note**

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 4500 Series, Catalyst 2948G, and Catalyst 2980G Switches Command Reference*.

This chapter consists of these sections:

- [Understanding How CDP Works, page 21-1](#)
- [Default CDP Configuration, page 21-2](#)
- [Configuring CDP on the Switch, page 21-2](#)

Understanding How CDP Works

CDP is a media- and protocol-independent protocol that runs on all Cisco-manufactured equipment including routers, bridges, access and communication servers, and switches. Using CDP, you can view information about all the Cisco devices that are directly attached to the switch. In addition, CDP detects native VLAN and port duplex mismatches.

Network management applications can retrieve the device type and SNMP-agent address of neighboring Cisco devices using CDP. This allows applications to send SNMP queries to neighboring devices. CDP allows network management applications to discover Cisco devices that are neighbors of already known devices, in particular, neighbors running lower-layer, transparent protocols.

CDP runs on all media that support Subnetwork Access Protocol (SNAP). CDP runs over the data link layer only.

Cisco devices do not forward CDP packets. When new CDP information is received, old information is discarded.

CISCO Confidential - DRAFT

Default CDP Configuration

Table 21-1 shows the default CDP configuration.

Table 21-1 CDP Default Configuration

Feature	Default Value
CDP global enable state	Enabled
CDP port enable state	Enabled on all ports
CDP message interval	60 sec
CDP holdtime	180 sec

Configuring CDP on the Switch

The following sections describe how to configure CDP.

Setting the CDP Global Enable State

To set the CDP global enable state on the switch, perform this task in privileged mode:

	Task	Command
Step 1	Set the CDP global enable state.	set cdp {enable disable}
Step 2	Verify the CDP configuration.	show cdp

This example shows how to enable CDP globally and verify the configuration:

```
Console> (enable) set cdp enable
CDP enabled globally
Console> (enable) show cdp
CDP                : enabled
Message Interval   : 60
Hold Time          : 180
Console> (enable)
```

This example shows how to disable CDP globally and verify the configuration:

```
Console> (enable) set cdp disable
CDP disabled globally
Console> (enable) show cdp
CDP                : disabled
Message Interval   : 60
Hold Time          : 180
Console> (enable)
```

Setting the CDP Enable State on a Port

You can enable or disable CDP on a per-port basis. You must enable CDP globally before the switch can transmit CDP messages on any ports.

CISCO Confidential - DRAFT

To set the CDP enable state on a per-port basis, perform this task in privileged mode:

	Task	Command
Step 1	Set the CDP enable state on individual ports.	set cdp {enable disable} [mod_num/port_num]
Step 2	Verify the CDP configuration.	show cdp port [mod_num[/port_num]]

This example shows how to disable CDP on ports 3/1–6 and verify the configuration:

```
Console> (enable) set cdp disable 3/1-6
CDP disabled on ports 3/1-6.
Console> (enable) show cdp port 3
CDP                : enabled
Message Interval   : 60
Hold Time          : 180
```

```
Port      CDP Status
-----
3/1       disabled
3/2       disabled
3/3       disabled
3/4       disabled
3/5       disabled
3/6       disabled
3/7       enabled
3/8       enabled
3/9       enabled
3/10      enabled
3/11      enabled
3/12      enabled
Console> (enable)
```

This example shows how to enable CDP on ports 3/1–2 and verify the configuration:

```
Console> (enable) set cdp enable 3/1-2
CDP enabled on ports 3/1-2.
Console> (enable) show cdp port 3
CDP                : enabled
Message Interval   : 60
Hold Time          : 180
```

```
Port      CDP Status
-----
3/1       enabled
3/2       enabled
3/3       disabled
3/4       disabled
3/5       disabled
3/6       disabled
3/7       enabled
3/8       enabled
3/9       enabled
3/10      enabled
3/11      enabled
3/12      enabled
Console> (enable)
```

CISCO Confidential - DRAFT

Setting the CDP Message Interval

The CDP message interval specifies how often the switch will transmit CDP messages to directly connected Cisco devices.

To set the default CDP message interval, perform this task in privileged mode:

	Task	Command
Step 1	Set the default CDP message interval. The allowed range is 5–900 seconds.	set cdp interval <i>interval</i>
Step 2	Verify the CDP configuration.	show cdp

This example shows how to set the default CDP message interval to 100 seconds and verify the configuration:

```
Console> (enable) set cdp interval 100
CDP message interval set to 100 seconds for all ports.
Console> (enable) show cdp
CDP                : enabled
Message Interval   : 100
Hold Time          : 180
Console> (enable)
```

Setting the CDP Holdtime

The CDP holdtime specifies how much time can pass between CDP messages from neighboring devices before the device is no longer considered connected and the neighbor entry is aged out.

To set the default CDP holdtime, perform this task in privileged mode:

	Task	Command
Step 1	Set the default CDP holdtime. The allowed range is 10–255 seconds.	set cdp holdtime <i>interval</i>
Step 2	Verify the CDP configuration.	show cdp

This example shows how to set the default CDP holdtime to 225 seconds and verify the configuration:

```
Console> (enable) set cdp holdtime 225
CDP holdtime set to 225 seconds.
Console> (enable) show cdp
CDP                : enabled
Message Interval   : 100
Hold Time          : 225
Console> (enable)
```

Displaying CDP Neighbor Information

To display information about directly connected Cisco devices, enter the **show cdp neighbors** command.

To display specific information, use the following keywords:

- To display the native VLAN for the connected ports, enter the **vlan** keyword.
- To display the duplex mode for the connected ports, enter the **duplex** keyword.
- To display the device capability codes for the connected device, enter the **capabilities** keyword.
- To display the device capability codes for the connected device, enter the **detail** keyword.

To display information about directly connected Cisco devices, perform this task in privileged mode:

Task	Command
View information about CDP neighbors.	show cdp neighbors [<i>mod_num</i> [/ <i>port_num</i>]] [vlan duplex capabilities detail]

This example shows how to display CDP neighbor information for connected Cisco devices:

```
Console> (enable) show cdp neighbors
```

```
* - indicates vlan mismatch.
```

```
# - indicates duplex mismatch.
```

Port	Device-ID	Port-ID	Platform
2/3	JAB023807H1(2948)	2/2	WS-C2948
3/1	JAB023806JR(4003)	2/1	WS-C4003
3/2	JAB023806JR(4003)	2/2	WS-C4003
3/5	JAB023806JR(4003)	2/5	WS-C4003
3/6	JAB023806JR(4003)	2/6	WS-C4003

```
Console> (enable)
```

This example shows how to display the native VLAN for each port that is connected on the neighboring device (there is a native VLAN mismatch between port 3/6 on the local switch and port 2/6 on the neighbor device, as indicated by the asterisk [*]):

```
Console> (enable) show cdp neighbors vlan
```

```
* - indicates vlan mismatch.
```

```
# - indicates duplex mismatch.
```

Port	Device-ID	Port-ID	NativeVLAN
2/3	JAB023807H1(2948)	2/2	522
3/1	JAB023806JR(4003)	2/1	100
3/2	JAB023806JR(4003)	2/2	100
3/5	JAB023806JR(4003)	2/5	1
3/6	JAB023806JR(4003)	2/6*	1

```
Console> (enable)
```

This example shows how to display detailed information about the neighboring device:

```
Console> (enable) show cdp neighbors 2/3 detail
```

```
Port (Our Port): 2/3
```

```
Device-ID: JAB023807H1(2948)
```

```
Device Addresses:
```

```
IP Address: 172.20.52.36
```

```
Holdtime: 132 sec
```

```
Capabilities: TRANSPARENT_BRIDGE SWITCH
```

```
Version:
```

```
WS-C2948 Software, Version MpsW: 5.1(57) NmpSW: 5.1(1)
```

```
Copyright (c) 1995-1999 by Cisco Systems, Inc.
```

CISCO Confidential - DRAFT

```
Platform: WS-C2948
Port-ID (Port on Neighbors's Device): 2/2
VTP Management Domain: Lab_Network
Native VLAN: 522
Duplex: full
Console> (enable)
```

Using Switch TopN Reports

This chapter describes how to use the Switch TopN Reports utility on the Catalyst enterprise LAN switches.

**Note**

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 4500 Series, Catalyst 2948G, and Catalyst 2980G Switches Command Reference*.

This chapter consists of these sections:

- [Understanding How Switch TopN Reports Works, page 22-1](#)
- [Running and Viewing Switch TopN Reports, page 22-3](#)

Understanding How Switch TopN Reports Works

The Switch TopN Reports utility allows you to collect and analyze data for each physical port on a switch.

The Switch TopN Reports utility collects the following data for each physical port:

- Port utilization (**util**)
- Number of in and out bytes (**bytes**)
- Number of in and out packets (**pkts**)
- Number of in and out broadcast packets (**bcst**)
- Number of in and out multicast packets (**mcst**)
- Number of in errors (**in-errors**)
- Number of buffer-overflow errors (**buf-ovflw**)

When the Switch TopN Reports utility starts, it gathers data from the appropriate hardware counters and then goes into sleep mode for a user-specified period. When the sleep time ends, the utility gathers the current data from the same hardware counters, compares the current data from the earlier data, and stores the difference. The switch sorts data for each port using a user-specified metric that is selected from the types listed in [Table 22-1](#).

*CISCO Confidential - DRAFT***Table 22-1 Valid Switch TopN Reports Data Types**

Data Type	Definition
util	Utilization
bytes	Input/output bytes
pkts	Input/output packets
bcst	Input/output broadcast packets
mcst	Input/output multicast packets
errors	Input errors
overflow	Buffer overflows

Running Switch TopN Reports Without the Background Option

If you enter the **show top** command without specifying the **background** option, processing begins but the system prompt does not reappear on the screen and you cannot enter other commands while the report is being generated.

You can terminate the Switch TopN process before it finishes by pressing **Ctrl-C** from the same console or Telnet session, or by opening a separate console or Telnet session and entering the **clear top** [report_num] command. After the Switch TopN Reports utility finishes processing the data, it displays the output on the screen immediately. The output is not saved.

Running Switch TopN Reports with the Background Option

If you enter the **show top** command and specify the **background** option, processing begins and the system prompt reappears immediately. When processing completes, Switch TopN reports do not display immediately on the screen but are saved for later viewing.

The system notifies you when the Switch TopN reports are complete by sending a syslog message to the screen. Enter the **show top report** [report_num] command to view the completed Switch TopN reports. The system displays only those reports that are completed. For reports that are not completed, the system displays a short description of the Switch TopN process information.

You can terminate a Switch TopN process invoked with the **background** option only by entering the **clear top** [report_num] command. Pressing **Ctrl-C** does not terminate the process. Completed Switch TopN reports remain available for viewing until you remove them using the **clear top {all | report_num}** command.

CISCO Confidential - DRAFT

Running and Viewing Switch TopN Reports

To run a Switch TopN Report in the background and view the results, perform this task in privileged mode:

	Task	Command
Step 1	Run the Switch TopN Reports utility in the background.	show top [N] [metric] [interval interval] [port_type] background
Step 2	View the generated report when it is complete.	show top report [report_num]



Note

You must enter the **background** keyword to the Switch TopN Reports utility to use the **show top report** command to view the completed report contents. Otherwise, the report is displayed immediately upon completion of the process, and the results are not saved.

If you specify the *report_num* variable with the **show top report** command, the associated Switch TopN report is displayed. Each process is associated with a unique report number.

If you do not specify the *report_num* variable, all active Switch TopN processes and all available Switch TopN reports for the switch are displayed. All Switch TopN processes (both with and without the **background** option) are shown in the list.

This example shows how to run the Switch TopN Reports utility with the **background** option:

```

Console> (enable) show top 5 pkts background
Console> (enable) 06/16/1998,17:21:08:MGMT-5:TopN report 4 started by Console//.
Console> (enable) 06/16/1998,17:21:39:MGMT-5:TopN report 4 available.
Console> (enable) show top report 4
Start Time:      06/16/1998,17:21:08
End Time:        06/16/1998,17:21:39
PortType:        all
Metric:          pkts (Tx + Rx)

```

Port	Band- width	Uti %	Bytes (Tx + Rx)	Pkts (Tx + Rx)	Bcst (Tx + Rx)	Mcst (Tx + Rx)	Error (Rx)	Over flow
1/1	100	0	7950	81	0	81	0	0
2/1	100	0	2244	29	0	23	0	0
1/2	100	0	1548	12	0	12	0	0
2/10	100	0	0	0	0	0	0	0
2/9	100	0	0	0	0	0	0	0

```

Console> (enable)

```

To run the Switch TopN Reports utility in the foreground and view the results immediately, perform this task in privileged mode:

Task	Command
Run the Switch TopN Reports utility in the foreground.	show top [N] [metric] [interval interval] [port_type]

This example shows how to run the Switch TopN Reports utility in the foreground:

```

Console> (enable) show top 5 pkts
Start Time:      06/16/1998,17:26:38
End Time:        06/16/1998,17:27:09

```

CISCO Confidential - DRAFT

```

PortType:      all
Metric:        pkts (Tx + Rx)
Port  Band-  Uti  Bytes          Pkts          Bcst          Mcst          Error  Over
       width %  (Tx + Rx)      (Tx + Rx)      (Tx + Rx)      (Tx + Rx)      (Rx)  flow
-----
2/1    100    0          10838          94            2            26            0      0
1/1    100    0           7504          79            0            79            0      0
1/2    100    0          2622           21            0            21            0      0
2/10   100    0            0            0            0            0            0      0
2/9    100    0            0            0            0            0            0      0
Console> (enable)

```

To display stored and pending Switch TopN reports, perform this task in privileged mode:

Task	Command
Display a Switch TopN report. To display all stored and pending reports, do not specify a <i>report number</i> .	show top report [<i>report_num</i>]

This example shows how to display a specific report and how to display all stored and pending reports:

```

Console> (enable) show top report 5
Start Time:      06/16/1998,17:29:40
End Time:        06/16/1998,17:30:11
PortType:        all
Metric:           overflow
Port  Band-  Uti  Bytes          Pkts          Bcst          Mcst          Error  Over
       width %  (Tx + Rx)      (Tx + Rx)      (Tx + Rx)      (Tx + Rx)      (Rx)  flow
-----
1/1    100    0          7880           83            0            83            0      0
2/12   100    0            0            0            0            0            0      0
2/11   100    0            0            0            0            0            0      0
2/10   100    0            0            0            0            0            0      0
2/9    100    0            0            0            0            0            0      0
Console> (enable) show top report
Rpt  Start time      Int N  Metric      Status  Owner (type/machine/user)
-----
  1  06/16/1998,17:05:00 30  20  Util      done    telnet/172.16.52.3/
  2  06/16/1998,17:05:59 30   5  Util      done    telnet/172.16.52.3/
  3  06/16/1998,17:08:06 30   5  Pkts      done    telnet/172.16.52.3/
  4  06/16/1998,17:21:08 30   5  Pkts      done    Console//
  5  06/16/1998,17:29:40 30   5  Overflow  pending Console//
Console> (enable)

```

To remove stored Switch TopN reports, perform this task in privileged mode:

Task	Command
Remove Switch TopN reports. Enter the all keyword to remove all completed Switch TopN reports.	clear top { all <i>report_num</i> }

**Note**

The **clear top all** command does not clear pending Switch TopN reports. Only the reports that have completed are cleared.

CISCO Confidential - DRAFT

This example shows how to remove a specific Switch TopN report and how to remove all stored reports:

```
Console> (enable) clear top 4
Console> (enable) 06/16/1998,17:36:45:MGMT-5:TopN report 4 killed by Console//.
Console> (enable) clear top all
06/16/1998,17:36:52:MGMT-5:TopN report 1 killed by Console//.
06/16/1998,17:36:52:MGMT-5:TopN report 2 killed by Console//.
Console> (enable) 06/16/1998,17:36:52:MGMT-5:TopN report 3 killed by Console//.
06/16/1998,17:36:52:MGMT-5:TopN report 5 killed by Console//.
Console> (enable)
```

CISCO Confidential - DRAFT

Configuring UDLD

This chapter describes how to configure the UniDirectional Link Detection (UDLD) protocol on the Catalyst enterprise LAN switches.

**Note**

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 4500 Series, Catalyst 2948G, and Catalyst 2980G Switches Command Reference*.

This chapter consists of these sections:

- [Understanding How UDLD Works, page 23-1](#)
- [UDLD Software and Hardware Requirements, page 23-2](#)
- [Default UDLD Configuration, page 23-2](#)
- [Configuring UDLD on the Switch, page 23-3](#)

Understanding How UDLD Works

The UDLD protocol allows devices that are connected through fiber-optic or copper Ethernet cables (for example, Category 5 cabling) to monitor the physical configuration of the cables and detect when a unidirectional link exists. When a unidirectional link is detected, UDLD shuts down the affected 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 Layer 1 mechanisms, such as autonegotiation, to determine the physical status of a link. At Layer 1, autonegotiation handles physical signaling and fault detection. UDLD also performs tasks that autonegotiation cannot perform such as detecting the identities of neighbors and shutting down misconnected ports. When both autonegotiation and UDLD are enabled, Layer 1 and Layer 2 detection features can work together to prevent physical and logical unidirectional connections and malfunctioning of other protocols.

A unidirectional link occurs whenever traffic that is transmitted by the local device over a link is received by the neighbor, but traffic that is transmitted from the neighbor is not received by the local device. For example, 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 situation, the logical link is undetermined, and UDLD does not take any actions. 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 is a Layer 1 feature.

CISCO Confidential - DRAFT

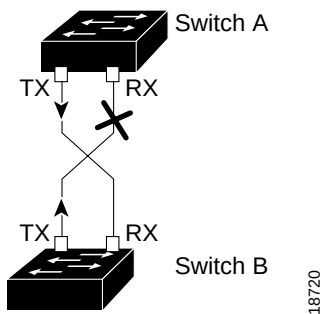
The switch periodically transmits UDLD messages (packets) to neighbor devices on ports with UDLD enabled. If the messages are echoed back to the sender within a specific time frame and they are lacking a specific acknowledgment (echo), the link is flagged as unidirectional and the port is shut down. Devices on both ends of the link must support UDLD in order for the protocol to successfully identify and disable unidirectional links.

**Note**

With software release 5.4(3) and later releases, you can specify the message interval between UDLD messages. Previously, the message interval was fixed at 60 seconds. With a configurable message interval, UDLD reacts much faster to link failures.

Figure 23-1 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 23-1 Unidirectional Link



UDLD Software and Hardware Requirements

UDLD requires the following hardware and software:

- For fiber-optic links:
 - Software release 5.1 or later releases
 - Ethernet, Fast Ethernet, or Gigabit Ethernet fiber-optic switching modules
- For copper links:
 - Software release 5.2 or later releases
 - Ethernet or Fast Ethernet copper switching modules

Default UDLD Configuration

Table 23-1 shows the default UDLD configuration.

*CISCO Confidential - DRAFT***Table 23-1 UDLD Default Configuration**

Feature	Default Value
UDLD global enable state	Globally disabled
UDLD per-port enable state	- Enabled on all Ethernet, Fast Ethernet, and Gigabit Ethernet ports using fiber-optic media - Disabled on all Ethernet and Fast Ethernet ports using copper media
UDLD message interval	15 sec
UDLD aggressive mode	Disabled

Configuring UDLD on the Switch

These sections describe how to configure UDLD:

- [Enabling UDLD Globally, page 23-3](#)
- [Enabling UDLD on Individual Ports, page 23-4](#)
- [Disabling UDLD on Individual Ports, page 23-4](#)
- [Disabling UDLD Globally, page 23-4](#)
- [Specifying the UDLD Message Interval, page 23-5](#)
- [Enabling UDLD Aggressive Mode, page 23-5](#)
- [Displaying the UDLD Configuration, page 23-6](#)

Enabling UDLD Globally

You must enable UDLD globally before any port can use UDLD.

To enable UDLD globally on the switch, perform this task in privileged mode:

	Task	Command
Step 1	Enable UDLD globally.	set udld enable
Step 2	Verify the configuration.	show udld

This example shows how to enable UDLD globally and verify the configuration:

```
Console> (enable) set udld enable
UDLD enabled globally
Console> (enable) show udld
UDLD      : enabled
Console> (enable)
```

CISCO Confidential - DRAFT

Enabling UDLD on Individual Ports

To enable UDLD on individual ports, perform this task in privileged mode:

	Task	Command
Step 1	Enable UDLD on a specific port.	set udld enable <i>mod_num/port_num</i>
Step 2	Verify the configuration.	show udld port [<i>mod_num[/port_num]</i>]

This example shows how to enable UDLD on port 4/1 and verify the configuration:

```

Console> (enable) set udld enable 4/1
UDLD enabled on port 4/1
Console> (enable) show udld port 4/1
UDLD      : enabled
Message Interval: 15 seconds
Port      Admin Status  Aggressive Mode  Link State
-----
4/1       enabled        disabled         bidirectional
Console> (enable)

```

Disabling UDLD on Individual Ports

To disable UDLD on individual ports, perform this task in privileged mode:

	Task	Command
Step 1	Disable UDLD on a specific port.	set udld disable <i>mod_num/port_num</i>
Step 2	Verify the configuration.	show udld port [<i>mod_num[/port_num]</i>]

This example shows how to disable UDLD on port 4/1:

```

Console> (enable) set udld disable 4/1
UDLD disabled on port 4/1.
Console> (enable)

```

Disabling UDLD Globally

To disable UDLD globally on the switch, perform this task in privileged mode:

	Task	Command
Step 1	Disable UDLD globally.	set udld disable
Step 2	Verify the configuration.	show udld

This example shows how to disable UDLD globally:

```

Console> (enable) set udld disable
UDLD disabled globally
Console> (enable)

```

Specifying the UDLD Message Interval

To specify the UDLD message interval, perform this task in privileged mode:

	Task	Command
Step 1	Specify the UDLD message interval.	set udld interval <i>interval</i>
Step 2	Verify the configuration.	show udld

This example shows how to specify the UDLD message interval:

```
Console> (enable) set udld interval 10
UDLD message interval set to 10 seconds
Console> (enable)
```

This example shows how to verify the message interval:

```
Console> (enable) show udld
UDLD                : enabled
Message Interval    : 10 seconds
Console> (enable)
```

Enabling UDLD Aggressive Mode

Software release 5.4(3) and later releases support UDLD aggressive mode. UDLD aggressive mode is disabled by default and its use is recommended only for point-to-point links between Cisco switches running software release 5.4(3) or later releases. With aggressive mode enabled, when a port on a bidirectional link stops receiving UDLD packets, UDLD tries to reestablish the connection with the neighbor. After eight failed retries, the port is put into errdisable state.

To prevent spanning tree loops, normal UDLD with a 15-second message interval is fast enough to shut down a unidirectional link before a blocking port transitions to forwarding state (when default spanning tree parameters are used).

Enabling UDLD aggressive mode provides additional benefits in the following cases:

- 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 error disables one of the ports on the link and stops the loss of traffic. Even with aggressive mode disabled, there is no risk for a broadcast storm due to a spanning tree loop in this situation, because one port cannot pass traffic in both directions.

To enable UDLD aggressive mode on module ports, perform this task in privileged mode:

	Task	Command
Step 1	Enable UDLD aggressive mode.	set udld aggressive-mode enable <i>mod_num/port_num</i>
Step 2	Verify the configuration.	show udld

This example shows how to enable UDLD aggressive mode:

```
Console> (enable) set udld aggressive-mode enable 4/1
Aggressive UDLD enabled on port 4/1.
Console> (enable)
```

CISCO Confidential - DRAFT

This example shows how to verify that UDLD aggressive mode is enabled:

```

Console> (enable) show udld port 4/1
UDLD      : enabled
Message Interval: 10 seconds
Port      Admin Status  Aggressive Mode Link State
-----
4/1       enabled       Enabled         bidirectional
Console> (enable)

```

Displaying the UDLD Configuration

To display the UDLD enable state, perform this task in privileged mode:

Task	Command
Display the UDLD enable state.	show udld

This example shows how to display the UDLD enable state:

```

Console> (enable) show udld
UDLD      : enabled
Message Interval : 10 seconds
Console> (enable)

```

To display UDLD configuration for a module or port, perform this task in privileged mode:

Task	Command
Display the UDLD configuration for a module or port.	show udld port [mod_num] [mod/port_num]

This example shows how to display the UDLD configuration for ports on module 4:

```

Console> (enable) show udld port 4
UDLD      : enabled
Message Interval: 10 seconds
Port      Admin Status  Aggressive Mode Link State
-----
4/1       enabled       disabled         bidirectional
4/2       enabled       disabled         bidirectional
4/3       enabled       disabled         undetermined
4/4       enabled       disabled         bidirectional
.
.

```

```

Console> (enable)

```

[Table 23-2](#) describes the fields in the **show udld** command output.

Table 23-2 show udld Command Output Fields

Field	Description
UDLD	Status of whether UDLD is enabled or disabled.
Message Interval	Message interval, in seconds.

*CISCO Confidential - DRAFT***Table 23-2** *show udld Command Output Fields (continued)*

Field	Description
Port	Module and port numbers.
Admin Status	Status of whether administration status is enabled or disabled.
Aggressive Mode	Status of whether aggressive mode is enabled or disabled.
Link State	Status of the link: undetermined (detection in progress, neighboring UDLD has been disabled), not applicable (UDLD has been disabled), shutdown (unidirectional link has been detected and the port is disabled), or bidirectional (bidirectional link has been detected and the port is disabled).

CISCO Confidential - DRAFT

Configuring SNMP

This chapter describes how to configure Simple Network Management Protocol (SNMP) on Catalyst enterprise LAN switches.

**Note**

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 4500 Series, Catalyst 2948G, and Catalyst 2980G Switches Command Reference*.

This chapter consists of these sections:

- [SNMP Terminology, page 24-1](#)
- [Understanding How SNMP Works, page 24-3](#)
- [Understanding How SNMPv1 and SNMPv2c Work, page 24-5](#)
- [SNMPv1 and SNMPv2c Default Configuration, page 24-6](#)
- [Configuring SNMPv1 and SNMPv2c from an NMS, page 24-6](#)
- [Configuring SNMPv1 and SNMPv2c from the CLI, page 24-6](#)
- [Understanding SNMPv3, page 24-11](#)
- [Configuring SNMPv3 from an NMS, page 24-14](#)
- [Configuring SNMPv3 from the CLI, page 24-14](#)
- [Using CiscoWorks2000, page 24-17](#)

SNMP Terminology

[Table 24-1](#) lists the terms used in SNMP technology.

*CISCO Confidential - DRAFT***Table 24-1 SNMP Terminology**

Term	Definition
authentication	The process of ensuring message integrity and protection against message replays, including data integrity and data origin authentication.
authoritative SNMP engine	One of the SNMP copies that is used in network communication is designated as the allowed SNMP engine which protects against message replay, delay, and redirection. The security keys that are used for authenticating and encrypting SNMPv3 packets are generated as a function of the authoritative SNMP engine's engine ID and user passwords. When an SNMP message expects a response (for example, get exact, get next, set request), the <i>receiver</i> of these messages is authoritative. When an SNMP message does not expect a response, the <i>sender</i> is authoritative.
community string	A text string used to authenticate messages between a management station and an SNMPv1 or SNMPv2c engine.
data integrity	A condition or state of data in which a message packet has not been altered or destroyed in an unauthorized manner.
data origin authentication	The ability to verify the identity of a user on whose behalf the message is supposedly sent. This ability protects users against both message capture and replay by a different SNMP engine, and against packets that are received or sent to a particular user that uses an incorrect password or security level.
encryption	A method of hiding data from an unauthorized user by scrambling the contents of an SNMP packet.
group	A set of users belonging to a particular security model. A group defines the access rights for all the users belonging to it. Access rights define the SNMP objects that can be read, written to, or created. In addition, the group defines the notifications that a user is allowed to receive.
notification host	An SNMP entity to which notifications (traps) are to be sent.
notify view	A view name (not to exceed 64 characters) for each group; the view name defines the list of notifications that can be sent to each user in the group.
privacy	An encrypted state of the contents of an SNMP packet; in this state, the contents are prevented from being disclosed on a network. Encryption is performed with an algorithm called CBC-DES (DES-56).
read view	A view name (not to exceed 64 characters) for each group; the view name defines the list of object identifiers (OIDs) that can be read by users belonging to the group.
security level	A type of security algorithm that is performed on each SNMP packet. There are three levels: noauth, auth, and priv. The noauth level authenticates a packet by a string match of the username. The auth level authenticates a packet by using either the HMAC MD5 or SHA algorithms. The priv level authenticates a packet by using either the HMAC MD5 or SHA algorithms and encrypts the packet using the CBC-DES (DES-56) algorithm.
security model	The security strategy that is used by the SNMP agent. Currently, software supports three security models: SNMPv1, SNMPv2c, and SNMPv3.
Simple Network Management Protocol (SNMP)	A network management protocol that provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

*CISCO Confidential - DRAFT***Table 24-1** *SNMP Terminology (continued)*

Term	Definition
SNMP Version 2c (SNMPv2c)	This second version of SNMP supports centralized and distributed network management strategies and includes improvements in the Structure of Management Information (SMI), protocol operations, management architecture, and security.
SNMP engine	A copy of SNMP that can reside on the local or remote device.
SNMP group	A collection of SNMP users that belong to a common SNMP list that defines an access policy, in which object identification numbers (OIDs) are both read-accessible and write-accessible. Users belonging to a particular SNMP group inherit all of these attributes that are defined by the group.
SNMP user	A person for which an SNMP management operation is performed. The user is the person on a remote SNMP engine who receives the inform messages.
SNMP view	A mapping between SNMP objects and the access rights available for those objects. An object can have different access rights in each view. Access rights indicate whether the object is accessible by either a community string or a user.
trap	A message sent by an SNMP agent to a console or terminal indicates that a significant event occurred.
write view	A view name (not to exceed 64 characters) for each group; the view name defines the list of object identifiers (OIDs) that are able to be created or modified by users of the group.

Understanding How SNMP Works

SNMP is an application-layer protocol that facilitates the exchange of management information between network devices. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

There are three versions of SNMP:

- Version 1 (SNMPv1)—This is the initial implementation of SNMP. Refer to RFC 1157 for a full description of functionality. See the [“Understanding How SNMPv1 and SNMPv2c Work” section on page 24-5](#) for more information on SNMPv1.
- Version 2 (SNMPv2c)—The second release of SNMP, described in RFC 1902, has additions and enhancements to data types, counter size, and protocol operations. See the [“Understanding How SNMPv1 and SNMPv2c Work” section on page 24-5](#) for more information on SNMPv2.
- Version 3 (SNMPv3)—This is the most recent version of SNMP and is fully described in RFC 2571, RFC 2572, RFC 2573, RFC 2574, and RFC 2575. The SNMP functionality on the Catalyst enterprise LAN switches for SNMPv1 and SNMPv2c remain intact; however, SNMPv3 has significant enhancements to administration and security. See the [“Understanding SNMPv3” section on page 24-11](#) for more information on SNMPv3.

CISCO Confidential - DRAFT

Security Models and Levels

A security model is an authentication strategy that is set up for a user and the group in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level will determine which security mechanism is employed when handling an SNMP packet. Three security models are available: SNMPv1, SNMPv2c, and SNMPv3. [Table 24-2](#) identifies what the combinations of security models and levels mean.

Table 24-2 Security Model Combinations

Model	Level	Authentication	Encryption	What Happens
v1	noAuthNoPriv	Community String	No	Uses a community string match for authentication.
v2c	noAuthNoPriv	Community String	No	Uses a community string match for authentication.
v3	noAuthNoPriv	Username	No	Uses a username match for authentication.
v3	authNoPriv	MD5 or SHA	No	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.
v3	authPriv	MD5 or SHA	DES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard.

Note the following about SNMPv3 objects:

- Each user belongs to a group.
- A group defines the access policy for a set of users.
- SNMP objects refer to an access policy for reading, writing, and creating.
- A group determines the list of notifications its users can receive.
- A group also defines the security model and security level for its users.

SNMP ifindex Persistence Feature

The SNMP ifIndex persistence feature is always enabled. With the ifIndex persistence feature, the ifIndex value of the port and VLAN is always retained and used after the following occurrences:

- Switch reboot
- High-availability switchover
- Software upgrade
- Module reset
- Module removal and insertion of the same type of module

For Fast EtherChannel and Gigabit EtherChannel interfaces, the ifIndex value is only retained and used after a high-availability switchover.

CISCO Confidential - DRAFT

Understanding How SNMPv1 and SNMPv2c Work

The components of SNMPv1 and SNMPv2c network management fall into three categories:

- Managed devices (such as a switch)
- SNMP agents and MIBs, including Remote Monitoring (RMON) MIBs, which run on managed devices
- SNMP management applications, such as CiscoWorks2000, which communicate with agents to get statistics and alerts from the managed devices



Note An SNMP management application, together with the computer it runs on, is called a network management system (NMS).

SNMP network management uses these SNMP agent functions:

- Accessing a MIB variable—This function is initiated by the SNMP agent in response to a request from the NMS. The agent retrieves the value of the requested MIB variable and responds to the NMS with that value.
- Setting a MIB variable—This function is also initiated by the SNMP agent in response to an NMS message. The SNMP agent changes the MIB variable value to the value that is requested by the NMS.
- SNMP trap—This function is used to notify an NMS that a significant event has occurred at an agent. When a trap condition occurs, the SNMP agent sends an SNMP trap message to any NMS that is specified as a trap receiver, under the following conditions:
 - When a port or module goes up or down
 - When temperature limitations are exceeded
 - When there are spanning tree topology changes
 - When there are authentication failures
 - When power supply errors occur
- SNMP community strings—SNMP community strings authenticate access to MIB objects and function as embedded passwords:
 - Read-only—Gives *only* read access to all objects in the MIB except the community strings
 - Read-write—Gives read and write access to all objects in the MIB; does not allow access to community strings
 - Read-write-all—Gives read and write access to all objects in MIB, including community strings



Note

The community string definitions on your NMS must match at least one of the three community string definitions on the switch.

Catalyst enterprise LAN switches are managed devices that support SNMP network management with the following features:

- SNMP traps (see the [“Configuring SNMPv1 and SNMPv2c from the CLI”](#) section on page 24-6)
- RMON in the supervisor engine module software (see [Chapter 25, “Configuring RMON”](#))
- RMON and RMON2 on an external SwitchProbe device

CISCO Confidential - DRAFT**Note**

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

SNMPv1 and SNMPv2c Default Configuration

Table 24-3 describes the SNMP default configuration.

Table 24-3 *SNMP Default Configuration*

Feature	Default Setting
SNMP community strings	• Read-Only: Public • Read-Write: Private • Read-Write-all: Secret
SNMP trap receiver	None configured
SNMP traps	None enabled

Configuring SNMPv1 and SNMPv2c from an NMS

To configure SNMP from a Network Management System (NMS), refer to the NMS documentation (see the “[Using CiscoWorks2000](#)” section on page 24-17).

The switch supports up to 20 trap receivers through the RMON2 trap destination table. Configure the RMON2 trap destination table from the NMS.

Configuring SNMPv1 and SNMPv2c from the CLI

**Note**

This section provides basic SNMPv1 and SNMPv2c configuration information. For detailed information on the SNMP commands supported by the Catalyst enterprise LAN switches, refer to the *Catalyst 4500 Series, Catalyst 2948G, and Catalyst 2980G Switches Command Reference*.

**Note**

For enhanced SNMP features in software release 7.5(1), see the “[SNMPv1 and SNMPv2c Enhancements in Software Release 7.5\(1\)](#)” section on page 24-7.

To configure SNMPv1 and SNMPv2c from the command-line interface (CLI), perform this task in privileged mode:

CISCO Confidential - DRAFT

	Task	Command
Step 1	Define the SNMP community strings for each access type.	set snmp community read-only <i>community_string</i> set snmp community read-write <i>community_string</i> set snmp community read-write-all <i>community_string</i>
Step 2	Assign a trap receiver and community. You can specify up to ten trap receivers.	set snmp trap rcvr_address rcvr_community [port <i>rcvr_port</i>] [owner <i>rcvr_owner</i>] [index <i>rcvr_index</i>]
Step 3	Specify the SNMP traps to send to the trap receiver.	set snmp trap enable [all auth bridge chassis config entity entityfru envfan envpower envshutdown envtemp flashinsert flashremove ippermit module stpx syslog system vlancreate vlandelete vmpps vtp]
Step 4	Verify the SNMP configuration.	show snmp

This example shows how to define community strings, assign a trap receiver, and specify which traps to send to the trap receiver:

```

Console> (enable) set snmp community read-only Everyone
SNMP read-only community string set to 'Everyone'.
Console> (enable) set snmp community read-write Administrators
SNMP read-write community string set to 'Administrators'.
Console> (enable) set snmp community read-write-all Root
SNMP read-write-all community string set to 'Root'.
Console> (enable) set snmp trap 172.16.10.10 read-write
SNMP trap receiver added.
Console> (enable) set snmp trap 172.16.10.20 read-write-all
SNMP trap receiver added.
Console> (enable) set snmp trap enable all
All SNMP traps enabled.
Console> (enable) show snmp
RMON:                               Disabled
Extended RMON:                       Extended RMON module is not present
Traps Enabled:
Port,Module,Chassis,Bridge,Repeater,Vtp,Auth,ippermit,Vmps,config,entity,stpx
Port Traps Enabled: 1/1-2,4/1-48,5/1

```

```

Community-Access      Community-String
-----
read-only             Everyone
read-write            Administrators
read-write-all        Root
Trap-Rec-Address      Trap-Rec-Community
-----
172.16.10.10          read-write
172.16.10.20          read-write-all
Console> (enable)

```

**Note**

To disable access for an SNMP community, set the community string for that community to the null string (do not enter a value for the community string).

SNMPv1 and SNMPv2c Enhancements in Software Release 7.5(1)

The following sections describe enhancements that were added to software release 7.5(1).

*CISCO Confidential - DRAFT***Setting Multiple SNMP Community Strings**

You can set multiple SNMP community strings using the **community-ext** keyword. Community strings that are defined with the **community-ext** keyword cannot be duplicates of existing community strings. When you add a new community string using the **community-ext** keyword, appropriate entries are created in the vacmAccessTable (if a view is specified), snmpCommunityTable, and the vacmSecurityToGroup table.

To set multiple SNMP community strings from the CLI, perform this task in privileged mode:

	Task	Command
Step 1	Set multiple SNMP community strings.	set snmp community-ext <i>community_string</i> { read-only read-write read-write-all } [view <i>view_oid</i>] [access <i>access_number</i>]
Step 2	Verify the SNMP configuration.	show snmp

This example shows how to set an additional SNMP community string:

```
Console> (enable) set snmp community-ext public1 read-only
```

```
Community string public1 is created with access type as read-only
Console> (enable)
```

This example shows how to restrict the community string to an access number:

```
Console> (enable) set snmp community-ext private1 read-write access 2
```

```
Community string private1 is created with access type as read-write access number 2
Console> (enable)
```

This example shows how to change the access number to the community string:

```
Console> (enable) set snmp community-ext private1 read-write access 3
```

```
Community string private1 is updated with access type as read-write access
number 3
Console> (enable)
```

This example shows how to display the SNMP configuration:

```
Console> (enable) show snmp
```

```
SNMP:Enabled
RMON:Disabled
Extended RMON Netflow Enabled :None.
Memory usage limit for new RMON entries:85 percent
Traps Enabled:None
Port Traps Enabled:None
```

```
Community-Access Community-String
```

```
-----
read-only      public
read-write     private
read-write-all secret
```

```
Additional-          Access-          Access-
Community-String     Type            Number  View
-----
public1              read-only          1
public2              read-only          1
```

CISCO Confidential - DRAFT

```

private1          read-write      2          1.3.6
secret1           read-write-all 500        1.3.6.1.4.1.9.9

Trap-Rec-Address Trap-Rec-Community Trap-Rec-Port Trap-Rec-Owner Trap-Rec-Index
-----
Console> (enable)

```

Clearing SNMP Community Strings

You can clear community strings using the **clear snmp community-ext** command. When you use this command to clear a community string, corresponding entries in the vacmAccessTable and vacmSecurityToGroup tables are also removed.

To clear an SNMP community string from the CLI, perform this task in privileged mode:

	Task	Command
Step 1	Clear an SNMP community string.	clear snmp community-ext <i>community-string</i>
Step 2	Verify the SNMP configuration.	show snmp

This example shows how to clear an SNMP community string:

```

Console> (enable) clear snmp community-ext public1
Community string public1 has been removed
Console> (enable)

```

Specifying Access Numbers for Hosts

You can specify a list of access numbers that are associated with one or more hosts to limit which hosts can use a specific community string to access the system. You can specify more than one IP address that is associated with an access number by separating each IP address with a space. If the new IP address uses an existing access number, the switch adds the new IP addresses to the list.

To specify an access number for a host from the CLI, perform this task in privileged mode:

	Task	Command
Step 1	Specify an access number for a host.	set snmp access-list <i>access_number IP_address</i> [<i>ipmask maskaddr</i>]
Step 2	Verify the SNMP configuration.	show snmp access-list

These examples show how to specify an access number for a host:

```

Console> (enable) set snmp access-list 1 172.20.60.100
Access number 1 has been created with new IP Address 172.20.60.100

```

```

Console> (enable) set snmp access-list 2 172.20.60.100 mask 255.0.0.0
Access number 2 has been created with new IP Address 172.20.60.100 mask 255.0.0.0

```

```

Console> (enable) set snmp access-list 2 172.20.60.7
Access number 2 has been updated with new IP Address 172.20.60.7

```

```

Console> (enable) set snmp access-list 2 172.20.60.7 mask 255.255.255.0
Access number 2 has been updated with existing IP Address 172.20.60.7 mask 255.255.255.0
Console> (enable)

```

CISCO Confidential - DRAFT

This example shows how to display the SNMP configuration:

```

Console> (enable) show snmp access-list
Access-Number    IP-Addresses/IP-Mask
-----
1                172.20.60.100/255.0.0.0
                1.1.1.1/-
2                172.20.60.7/-
                2.2.2.2/-
3                2.2.2.2/155.0.0.0
4                1.1.1.1/2.1.2.4
                2.2.2.2/-
                2.2.2.5/-
Console> (enable)

```

Clearing IP Addresses Associated with Access Numbers

To clear IP addresses that are associated with access numbers from the CLI, perform this task in privileged mode:

	Task	Command
Step 1	Clear IP addresses that are associated with access numbers.	clear snmp access-list <i>access_number</i> <i>IP_address</i> [[<i>IP_address</i>] ...]
Step 2	Verify the SNMP configuration.	show snmp access-list

These examples show how to clear IP addresses that are associated with access numbers:

```

Console> (enable) clear snmp access-list 101
All IP addresses associated with access-number 101 have been cleared.
Console> (enable)

Console> (enable) clear snmp access-list 2 172.20.60.8
Access number 2 no longer associated with 172.20.60.8
Console> (enable)

```

Specifying and Displaying an Interface Alias

You can specify and display an interface alias. The length of the alias can be up to 64 characters.

To specify and display an interface alias, perform this task in privileged mode:

	Task	Command
Step 1	Specify an interface alias.	set snmp ifalias { <i>ifIndex</i> } [<i>ifAlias</i>]
Step 2	Display the interface alias.	show snmp ifalias [<i>ifIndex</i>]

These examples show how to specify and display an interface alias:

```

Console> (enable) set snmp ifalias 1 Inband port

ifIndex 1 alias set
Console> (enable)

Console> (enable) show snmp ifalias 1
ifIndex    ifName          ifAlias
-----

```

CISCO Confidential - DRAFT

```
1          sc0          Inband port
Console> (enable)
```

Understanding SNMPv3

SNMPv3 contains all the functionality of SNMPv1 and SNMPv2, but SNMPv3 has significant enhancements to administration and security. SNMPv3 is an interoperable standards-based protocol. SNMPv3 provides secure access to devices by authenticating and encrypting packets over the network. The security features provided in SNMPv3 are as follows:

- Message integrity—Ensuring that a packet has not been tampered with in transit
- Authentication—Determining that the message is from a valid source
- Encryption—Scrambling contents of packet to prevent it from being seen by an unauthorized source

Benefits of SNMPv3

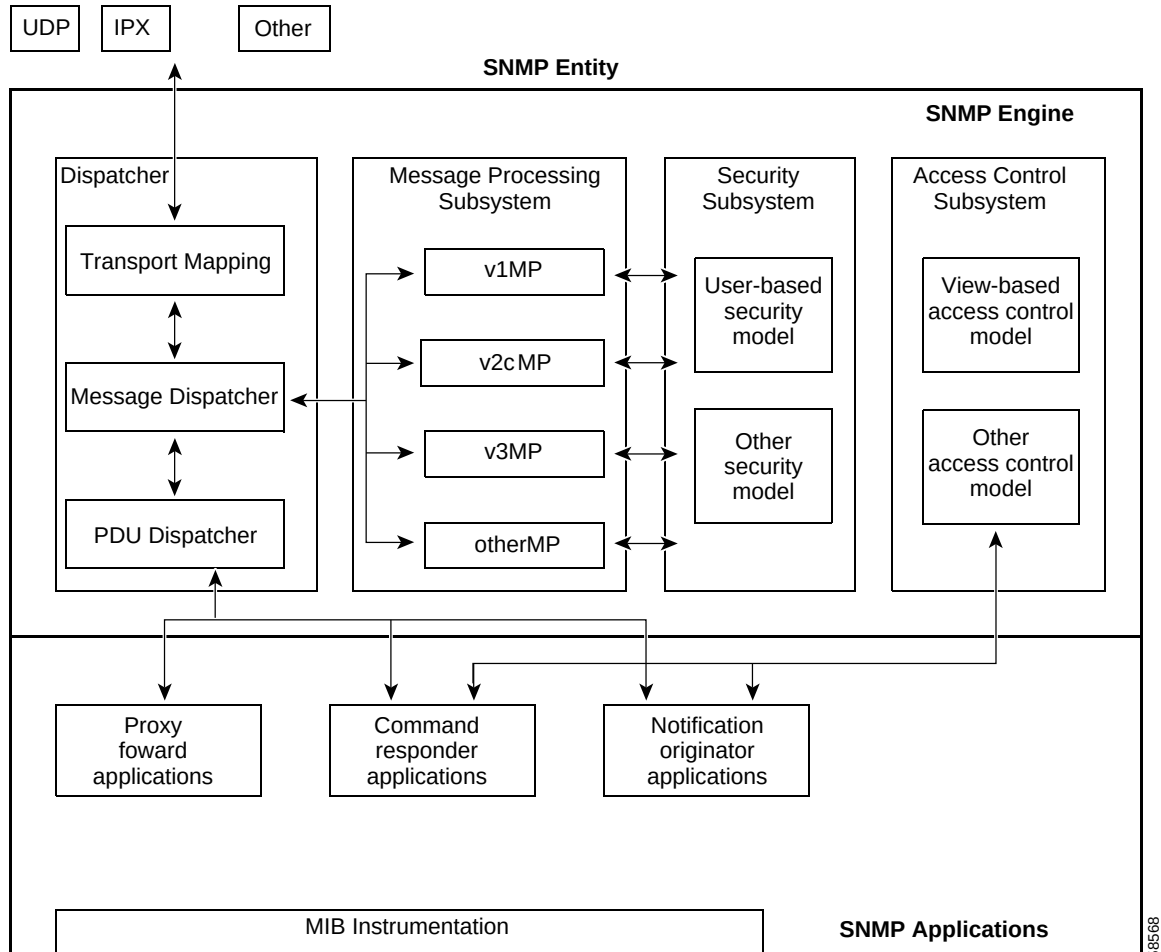
SNMPv3 provides the following benefits for managing your network:

- SNMP devices can collect data securely without being tampered with or corrupted.
- You can encrypt confidential information (such as SNMP **set** commands that change a router's configuration) to prevent the contents from being exposed on the network.

SNMP Entity

In SNMPv3, the terms SNMP Agents and SNMP Managers are no longer used. These concepts have been combined into what is called an SNMP entity. An SNMP entity is made up of an SNMP engine and SNMP applications. An SNMP engine is made up of these four components ([Figure 24-1](#)):

- Dispatcher
- Message Processing Subsystem
- Security Subsystem
- Access Control Subsystem

*CISCO Confidential - DRAFT***Figure 24-1 SNMP Entity for Traditional SNMP Agents**

Dispatcher

The Dispatcher is a simple traffic manager that sends and receives messages. After receiving a message, the Dispatcher tries to determine the version number of the message and then passes the message to the appropriate Message Processing Model. The Dispatcher is also responsible for dispatching protocol data units (PDUs) to applications and for selecting the appropriate transports for sending messages.

Message Processing Subsystem

The Message Processing Subsystem accepts outgoing PDUs from the Dispatcher and prepares them for transmission by wrapping them in a message header and returning them to the Dispatcher. The Message Processing Subsystem also accepts incoming messages from the Dispatcher, processes each message header, and returns the enclosed PDU to the Dispatcher. An implementation of the Message Processing Subsystem may support a single message format corresponding to a single version of SNMP (SNMPv1, SNMPv2c, SNMPv3), or it may contain a number of modules, each supporting a different version of SNMP.

CISCO Confidential - DRAFT

Security Subsystem

The Security Subsystem authenticates and encrypts messages. Each outgoing message is passed to the Security Subsystem from the Message Processing Subsystem. Depending on the services required, the Security Subsystem may encrypt the enclosed PDU and some fields in the message header. In addition, the Security Subsystem may generate an authentication code and insert it into the message header. After encryption, the message is returned to the Message Processing Subsystem.

Each incoming message is passed to the Security Subsystem from the Message Processing Subsystem. If required, the Security Subsystem checks the authentication code and performs decryption. The processed message is returned to the Message Processing Subsystem. An implementation of the Security Subsystem may support one or more distinct security models. So far, the only defined security model is the User-Based Security Model (USM) for SNMPv3, that is specified in RFC 2274.

The USM protects SNMPv3 messages from the following potential security threats:

- An authorized user sending a message that gets modified in transit by an unauthorized SNMP entity
- An unauthorized user trying to masquerade as an authorized user
- Anyone modifying the message stream
- Anyone eavesdropping

The USM currently defines the use of HMAC-MD5-96 and HMAC-SHA-96 as the possible authentication protocols and CBC-DES as the privacy protocol.

SNMPv1 and SNMPv2c security models provide only weak authentication (community names) and no privacy.

Access Control Subsystem

The responsibility of the Access Control Subsystem is straightforward. It determines whether access to a managed object should be allowed. Currently, one access control model, the View-Based Access Control Model (VACM), has been defined. With VACM, you can control which users and which operations can have access to which managed objects.

Applications

SNMPv3 applications refer to internal applications within an SNMP entity. These internal applications can generate SNMP messages, respond to received SNMP messages, generate notifications, receive notifications, and forward messages between SNMP entities. Currently, there are five types of applications:

- Command generators—Generate SNMP commands to collect or set management data.
- Command responders—Provide access to management data. For example, **processing get**, **get-next**, **get-bulk**, and **set pdus** are used in a command responder application.
- Notification originators—Initiate Trap or Inform messages.
- Notification receivers—Receive and process Trap or Inform messages.
- Proxy forwarders—Forward messages between SNMP entities.

CISCO Confidential - DRAFT

Configuring SNMPv3 from an NMS

To configure SNMP from a Network Management System (NMS), refer to your NMS documentation (also see the “Using CiscoWorks2000” section on page 24-17).

The switch supports up to 20 trap receivers through the RMON2 trap destination table. Configure the RMON2 trap destination table from the NMS.

Configuring SNMPv3 from the CLI



Note

This section provides very basic SNMP v3 configuration information. For detailed information on the SNMP commands that are supported by the Catalyst enterprise LAN switches, refer to the *Catalyst 4500 Series, Catalyst 2948G, and Catalyst 2980G Switches Command Reference*.

To configure SNMPv3 from the command-line interface (CLI), perform this task in privileged mode:

	Task	Command
Step 1	Set the SNMP-Server EngineID name for the local SNMP engine.	set snmp engineid <i>engineid</i>
Step 2	Configure the MIB views.	set snmp view [-hex] {viewname} {subtree} [mask] [included excluded] [volatile nonvolatile]
Step 3	Set the access rights for a group with a certain security model in different security levels.	set snmp access [-hex] {groupname} {security-model v3} {noauthentication authentication privacy} [read [-hex] {readview}] [write [-hex] {writeview}] [notify [-hex] {notifyview}] [context [-hex] {contextname} [exact prefix]] [volatile nonvolatile]
Step 4	Specify the target addresses for notifications.	set snmp notify [-hex] {notifyname} tag [-hex] {notifytag} [trap inform] [volatile nonvolatile]
Step 5	Set the snmpTargetAddrEntry in the target address table.	set snmp targetaddr [-hex] {addrname} param [-hex] {paramsname} {ipaddr} [udpport {port}] [timeout {value}] [retries {value}] [volatile nonvolatile] [taglist [{-hex} tag] [{-hex} tag]]
Step 6	Set the SNMP parameters that are used to generate a message to a target.	set snmp targetparams [-hex] {paramsname} user [-hex] {username} {security-model v3} {message-processing v3} {noauthentication authentication privacy} [volatile nonvolatile]
Step 7	Configure a new user.	set snmp user [-hex] {username} [remote {engineid}] [{authentication [md5 sha] {authpassword}}] [privacy {privpassword}] [volatile nonvolatile]
Step 8	Relate a user to a group using a specified security model.	set snmp group [-hex] {groupname} user [-hex] {username} {security-model v1 v2 v3} [volatile nonvolatile]
Step 9	Configure the community table for the system default part, which maps community strings of previous versions of SNMP to SNMPv3.	set snmp community {access_type} [community_string] (access_type = read-only read-write read-write-all)

CISCO Confidential - DRAFT

	Task	Command
Step 10	Configure the community table for mappings between different community strings and security models with full permissions.	set snmp community index {index_name} name [community_string] security {security_name} context {context_name} transporttag {tag_value} [volatile nonvolatile]
Step 11	Verify the SNMP configuration.	show snmp

This example shows how to set a MIB view name to interfacesMibView:

```
Console> (enable) set snmp view interfacesMibView 1.3.6.1.2.1.2 included
Snmp view name was set to interfacesMibView with subtree 1.3.6.1.2.1.2 included,
nonvolatile.
```

This example shows how to set the access rights for a group called guestgroup to SNMPv3 authentication read mode:

```
Console> (enable) set snmp access guestgroup security-model v3 authentication read
interfacesMibView
Snmp access group was set to guestgroup version v3 level authentication,
readview interfacesMibView, context match:exact, nonvolatile.
```

This example shows how to specify the target addresses:

```
Console> (enable) set snmp notify notifytable1 tag routers trap
Snmp notify name was set to notifytable1 with tag routers notifyType trap, and storageType
nonvolatile.
```

These examples show how to set the snmpTargetAddrEntry in the target address table:

```
Console> (enable) set snmp targetaddr router_1 param p1 172.20.21.1
Snmp targetaddr name was set to router_1 with param p1
ipAddr 172.20.21.1, udpport 162, timeout 1500, retries 3, storageType nonvolatile.
```

```
Console> (enable) set snmp targetaddr router_2 param p2 172.20.30.1
Snmp targetaddr name was set to router_2 with param p2
ipAddr 172.20.30.1, udpport 162, timeout 1500, retries 3, storageType nonvolatile.
```

These examples show how to set SNMP target parameters:

```
Console> (enable) set snmp targetparams p1 user guestuser1 security-model v3
message-processing v3 authentication
Snmp target params was set to p1 v3 authentication, message-processing v3,
user guestuser1 nonvolatile.
```

```
Console> (enable) set snmp targetparams p2 user guestuser2 security-model v3
message-processing v3 privacy
Snmp target params was set to p2 v3 privacy, message-processing v3,
user guestuser2 nonvolatile.
```

These examples show how to configure guestuser1 and guestuser2 as users:

```
Console> (enable) set snmp user guestuser1 authentication md5 guestuser1password privacy
privacypasswd1
Snmp user was set to guestuser1 authProt md5 authPasswd guestuser1password privProt des
privPasswd
privacypasswd1 with engineid 00:00:00:09:00:10:7b:f2:82:00:00:00 nonvolatile.
```

```
Console> (enable) set snmp user guestuser2 authentication sha guestuser2password
Snmp user was set to guestuser2 authProt sha authPasswd guestuser2password privProt
no-priv with engineid
00:00:00:09:00:10:7b:f2:82:00:00:00 nonvolatile.
```

CISCO Confidential - DRAFT

These examples show how to set guestuser1 and guestuser2 as members of the groups guestgroup and mygroup:

```
Console> (enable) set snmp group guestgroup user guestuser1 security-model v3
Snmp group was set to guestgroup user guestuser1 and version v3, nonvolatile.
```

```
Console> (enable) set snmp group mygroup user guestuser1 security-model v3
Snmp group was set to mygroup user guestuser1 and version v3, nonvolatile.
```

```
Console> (enable) set snmp group mygroup user guestuser2 security-model v3
Snmp group was set to mygroup user guestuser2 and version v3, nonvolatile.
```

This example shows how to verify the SNMPv3 setup for guestuser1 from a workstation:

```
workstation% getnext -v3 10.6.4.201 guestuser1 ifDescr.0
Enter Authentication password :guestuser1password
Enter Privacy password      :privacypasswd1
ifDescr.1 = sc0
```

This example shows how to verify the SNMPv3 setup for guestuser1 in the snmpEngineID MIB from a workstation:

```
workstation% getnext -v3 10.6.4.201 guestuser1 snmpEngineID
Enter Authentication password :guestuser1password
Enter Privacy password      :privacypasswd1
snmpEngineID = END_OF_MIB_VIEW_EXCEPTION
```

This example shows how to verify the SNMPv2c setup for public access from a workstation:

```
workstation% getnext -v2c 10.6.4.201 public snmpEngineID
snmpEngineID.0 =
00 00 00 09 00 10 7b f2 82 00 00 00
```

This example shows how to increase guestgroup's access right to read privileges for snmpEngineMibView:

```
Console> (enable) set snmp view snmpEngineMibView 1.3.6.1.6.3.10.2.1 included
Snmp view name was set to snmpEngineMibView with subtree 1.3.6.1.6.3.10.2.1 included,
nonvolatile
```

```
Console> (enable) set snmp access guestgroup security-model v3 authentication read
snmpEngineMibView
Snmp access group was set to guestgroup version v3 level authentication,
readview snmpEngineMibView, nonvolatile.
```

This example shows how to verify the SNMPv3 access for guestuser1 from a workstation:

```
% getnext -v3 10.6.4.201 guestuser1 snmpEngineID
Enter Authentication password :guestuser1password
Enter Privacy password      :privacypasswd1
snmpEngineID.0 =
00 00 00 09 00 10 7b f2 82 00 00 00
```

This example shows how to remove access for guestgroup:

```
Console> (enable) clear snmp acc guestgroup security-model v3 authentication
Cleared snmp access guestgroup version v3 level authentication.
```

This example shows how to verify that the access for guestuser1 has been removed from a workstation:

```
% getnext -v3 10.6.4.201 guestuser1 ifDescr.1
Enter Authentication password :guestuser1password
Enter Privacy password      :privacypasswd1
Error code set in packet - AUTHORIZATION_ERROR:1.
```

CISCO Confidential - DRAFT

This example shows how to verify the access for guestuser2 from a workstation:

```
% getnext -v3 10.6.4.201 guestuser2 ifDescr.1
Enter Authentication password :guestuser2password
Enter Privacy password      :privacypasswd2
REPORT received, cannot recover:
usmStatsUnsupportedSecLevels.0 = 1
```

Using CiscoWorks2000

CiscoWorks2000 is a family of web-based and management platform-independent products for managing Cisco enterprise networks and devices. CiscoWorks2000 includes Resource Manager Essentials and CWSI Campus, which allow you to deploy, configure, monitor, manage, and troubleshoot a switched internetwork. For more information, refer to the following publications:

- *Getting Started with Resource Manager Essentials*
- *Getting Started with CWSI Campus*

CISCO Confidential - DRAFT

Configuring RMON

This chapter describes how to configure RMON on the Catalyst enterprise LAN switches.

**Note**

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 4500 Series, Catalyst 2948G, and Catalyst 2980G Switches Command Reference*.

This chapter consists of these sections:

- [Understanding How RMON Works, page 25-1](#)
- [Enabling RMON, page 25-2](#)
- [Viewing RMON Data, page 25-2](#)
- [Supported RMON and RMON2 MIB Objects, page 25-2](#)

Understanding How RMON Works

RMON is an Internet Engineering Task Force (IETF) standard monitoring specification that allows various network agents and console systems to exchange network monitoring data. The supervisor engine software provides embedded support for these components of the RMON specification (see the [“Supported RMON and RMON2 MIB Objects” section on page 25-2](#) for details):

- The following RMON groups are defined in RFC 1757:
 - Statistics (RMON group 1) for Ethernet, Fast Ethernet, Fast EtherChannel, and Gigabit Ethernet switch ports (uses 140 bytes of supervisor engine module RAM per port)
 - History (RMON group 2) for Ethernet, Fast Ethernet, Fast EtherChannel, and Gigabit Ethernet switch ports (uses 3 KB of supervisor engine module RAM for the first 50 buckets; each additional bucket uses another 56 bytes)
 - Alarm (RMON group 3; each alarm configured uses 1.3 KB of supervisor engine RAM)
 - Event (RMON group 9; each event configured uses 1.3 KB of supervisor engine RAM)
- The following RMON2 groups are defined in RFC 2021:
 - UsrHistory (RMON2 group 18)
 - ProbeConfig (RMON2 group 19)

The embedded RMON agent allows the switch to monitor network traffic from all ports simultaneously at the data-link layer of the OSI model without requiring a dedicated monitoring probe or network analyzer.

Enabling RMON



Note

RMON is disabled by default.

To enable RMON, perform this procedure in privileged mode:

	Task	Command
Step 1	Enable RMON.	set snmp rmon enable
Step 2	Verify that RMON is enabled.	show snmp

This example shows how to enable RMON and how to verify that RMON is enabled:

```

Console> (enable) set snmp rmon enable
SNMP RMON support enabled.
Console> (enable) show snmp
RMON:                               Enabled
Extended RMON:                      Extended RMON module is not present
Traps Enabled:
Port,Module,Chassis,Bridge,Repeater,Vtp,Auth,ippermit,Vmps,config,entity,stpx
Port Traps Enabled: 1/1-2,4/1-48,5/1
Community-Access      Community-String
-----
read-only              Everyone
read-write             Administrators
read-write-all        Root
Trap-Rec-Address
-----
172.16.10.10           read-write
172.16.10.20           read-write-all
Console> (enable)
  
```

Viewing RMON Data

Access to RMON data is available only on an NMS that supports RFC 1757 and RFC 1513 (see the [“Using CiscoWorks2000” section on page 24-17](#)). You cannot access RMON data through the switch CLI; however, CLI **show** commands provide similar information (refer to the *Catalyst 4500 Series*, *Catalyst 2948G*, and *Catalyst 2980G Switches Command Reference*).

Supported RMON and RMON2 MIB Objects

[Table 25-1](#) lists the RMON and RMON2 MIB objects that are supported by the supervisor engine software.

*CISCO Confidential - DRAFT***Table 25-1 Supervisor Engine RMON and RMON2 Support**

Module	Object Identifier (OID)	Definition	Source
Supervisor engine	...mib-2(1).rmon(16).statistics(1).etherStatsTable(1)	Counters for packets, octets, broadcasts, errors, etc.	RFC 1757
Supervisor engine	...mib-2(1).rmon(16).history(2).historyControlTable(1) ...mib-2(1).rmon(16).history(2).etherHistoryTable(2)	Periodically samples and saves statistics group counters for later retrieval.	RFC 1757 RFC 1757
Supervisor engine	...mib-2(1).rmon(16).alarm(3)	A threshold set on critical RMON variables for network management.	RFC 1757
Supervisor engine	...mib-2(1).rmon(16).event(9)	Generates SNMP traps when an Alarms group threshold is exceeded and logs the events.	RFC 1757
Supervisor engine	...mib-2(1).rmon(16).usrHistory(18)	Extends history beyond RMON1 link-layer statistics to include any RMON, RMON2, MIB-I, or MIB-II statistic.	RFC 2021
Supervisor engine	...mib-2(1).rmon(16).probeConfig(19)	Displays a list of agent capabilities and configurations.	RFC 2021

CISCO Confidential - DRAFT

Configuring SPAN and RSPAN

This chapter describes how to configure the Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) on the Catalyst 4000 family switches.

**Note**

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 4500 Series, Catalyst 2948G, and Catalyst 2980G Switches Command Reference*.

This chapter consists of these sections:

- [Understanding How SPAN and RSPAN Work, page 26-1](#)
- [SPAN and RSPAN Session Limits, page 26-4](#)
- [Configuring SPAN, page 26-4](#)
- [Configuring RSPAN, page 26-8](#)

**Note**

To configure SPAN or RSPAN from a Network Management System (NMS), refer to the NMS documentation (and see the [“Using CiscoWorks2000” section on page 24-17](#)).

Understanding How SPAN and RSPAN Work

The following sections describe the concepts and terminology that are associated with SPAN and RSPAN configuration.

SPAN Session

A SPAN session is an association of a destination port with a set of source ports, configured with parameters that specify the monitored network traffic. You can configure multiple SPAN sessions in a switched network. SPAN sessions do not interfere with the normal operation of the switches. You can enable or disable SPAN sessions with command-line interface (CLI) or SNMP commands. When enabled, a SPAN session might become active or inactive based on various events or actions that would be indicated by a syslog message. The “Status” field in the **show span** and **show rspan** commands displays the operational status of a SPAN or RSPAN session.

After the system is on, a SPAN or RSPAN destination session remains inactive until the destination port is operational. An RSPAN source session remains inactive until any of the source ports are operational or the RSPAN VLAN becomes active.

CISCO Confidential - DRAFT

Destination Port

A destination port (also called a *monitor port*) is a switch port where SPAN sends packets for analysis. After a port becomes an active destination port, it does not forward any traffic except that required for the SPAN session. By default, an active destination port disables incoming traffic (from the network to the switching bus), unless you specifically enable the port. If incoming traffic is enabled for the destination port, it is switched in the native VLAN of the destination port. **The destination port does not participate in spanning tree while the SPAN session is active.** See the caution statement in the “Configuring SPAN” section on page 26-6 for information on how to prevent loops in your network topology.

Only one destination port is allowed per SPAN session, and the same port cannot be a destination port for multiple SPAN sessions. A switch port that is configured as a destination port cannot be configured as a source port or a reflector port. EtherChannel ports cannot be SPAN destination ports.

If the trunking mode of a SPAN destination port is “on” or “nonegotiate” during SPAN session configuration, the SPAN packets forwarded by the destination port have the encapsulation that is specified by the trunk type; however, the destination port stops trunking. The **show trunk** command reflects the trunking status for the port prior to SPAN session configuration.

Source Port

A source port is a switch port that is monitored for network traffic analysis. The traffic through the source ports can be categorized as ingress, egress, or both. You can monitor one or more source ports in a single SPAN session with user-specified traffic types (ingress, egress, or both) that are applicable for all the source ports.

You can configure source ports in any VLAN. You can configure VLANs as source ports (*src_vlans*), which means that all ports in the specified VLANs are source ports for the SPAN session.

Source ports are administrative (*Admin Source*) or operational (*Oper Source*) or both. Administrative source ports are the source ports or source VLANs that are specified during SPAN session configuration. Operational source ports are the source ports that are monitored by the destination port. For example, when source VLANs are used as the administrative source, the operational source is all the ports in all the specified VLANs.

The operational sources are always active ports. If a port is not in the spanning tree, it is not an operational source. All physical ports in an EtherChannel source are included in operational sources if the logical port is included in the spanning tree.

The destination port and reflector port, if they belong to any of the administrative source VLANs, are excluded from the operational source.

You can configure a port as a source port in multiple active SPAN sessions, but you cannot configure an active source port as a destination port or reflector port for any SPAN session.

If a SPAN session is inactive, the “oper source” field does not update until the session becomes active.

You can configure trunk ports as source ports and mix them with nontrunk source ports; however, the trunk settings of the destination port during the SPAN session configuration determine the encapsulation of the packets forwarded by the destination port.

CISCO Confidential - DRAFT

Reflector Port

The reflector port is the mechanism that you use to copy packets onto an RSPAN VLAN. The reflector port forwards only the traffic from the RSPAN source session with which it is affiliated. Any device that is connected to a port set as a reflector port loses connectivity until the RSPAN source session is disabled.

If the bandwidth of the reflector port is not sufficient to handle the traffic from the corresponding source ports, the excess packets are dropped. A 10/100 port reflects at 100 Mbps. A Gigabit port reflects at 1 Gbps. A blocking gigabit port reflects at a slightly lower rate.

The reflector port cannot be an EtherChannel port, does not trunk, and cannot do protocol filtering. A port that is used as a reflector port cannot be a SPAN source or destination port, and it cannot be a reflector port for more than one session at a time. Spanning tree is automatically disabled on a reflector port; the port remains in the forwarding state even though the port is in loopback mode.

The following ports cannot be used as reflector ports:

- Gigabit uplink ports on the WS-4013 Supervisor II
- Gigabit uplink ports on the 2980G-A
- Gigabit ports on the WS-4232-L3 module

The **SPAN** line in the output of the **show port capabilities** command indicates whether a port can be used as a reflector port.

Ingress SPAN

Ingress SPAN copies network traffic that is received by the source ports for analysis at the destination port.

Egress SPAN

Egress SPAN copies network traffic that is transmitted from the source ports for analysis at the destination port.

VSPAN

You can use VLAN-based SPAN (VSPAN) to analyze the network traffic in one or more VLANs. You can configure VSPAN in a bidirectional mode (ingress and egress). All the ports in the source VLANs become operational source ports for the VSPAN session. The destination port or the reflector port, if they belong to any of the administrative source VLANs, are excluded from the operational source. If you add or remove ports from the administrative source VLANs, the operational sources modify accordingly.

Use the following guidelines for VSPAN sessions:

- Trunk ports are included as source ports for VSPAN sessions, but only the VLANs that are in the Admin source list are monitored, provided these VLANs are active for the trunk.
- An inband port is not included as Oper source for VSPAN sessions.
- When a VLAN is cleared, it is removed from the source list for VSPAN sessions.
- A VSPAN session is disabled if the Admin source VLANs list is empty.

CISCO Confidential - DRAFT

- Inactive VLANs are not allowed for VSPAN configuration.
- A VSPAN session is made inactive if any of the source VLANs become RSPAN VLANs.

Trunk VLAN Filtering

In software release 6.3(1) and later releases, you can use the **filter** option to select a set of VLANs in a trunk that is used in a SPAN session. Trunk VLAN filtering is the analysis of network traffic on a selected set of VLANs on trunk source ports. If you specify a set of VLANs with the **filter** option, the traffic that is spanned by the session is limited to the VLANs that are specified. You can combine trunk VLAN filtering with other source ports that belong to any of the selected VLANs, and you can also use trunk VLAN filtering for RSPAN. Based on the traffic type (ingress, egress, or both), SPAN sends a copy of the network traffic in the selected VLANs to the destination port.

Use trunk VLAN filtering only with trunk source ports. If you combine trunk VLAN filtering with other source ports that belong to VLANs that are not included in the selected list of filter VLANs, SPAN includes only the ports that belong to one or more of the selected VLANs in the operational sources.

When a VLAN is cleared, it is removed from the VLAN filter list. A SPAN session is disabled if the VLAN filter list becomes empty.

Trunk VLAN filtering is not applicable to VSPAN sessions.

Trunk VLAN filtering is available for local SPAN sessions and RSPAN sessions.

SPAN Traffic

All network traffic, including multicast and bridge protocol data unit (BPDU) packets, can be monitored using SPAN (RSPAN does not support monitoring of BPDU packets).

SPAN and RSPAN Session Limits

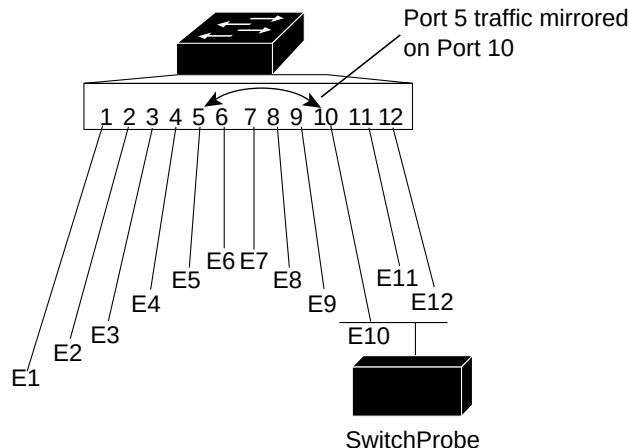
You can configure (and store in NVRAM) up to five SPAN sessions in a Catalyst 4000 family switch. The five sessions can be split any way between SPAN, RSPAN source, and RSPAN destination sessions.

Configuring SPAN

The following sections describe how to configure SPAN.

Understanding How SPAN Works

SPAN selects network traffic for analysis by a SwitchProbe device or other RMON probe. SPAN mirrors traffic from one or more source ports (Ethernet, Fast Ethernet, or Gigabit Ethernet) on one or more VLANs to a destination port for analysis (see [Figure 26-1](#)). In [Figure 26-1](#), all traffic on Ethernet port 5 (the source port) is mirrored to Ethernet port 10. A network analyzer on Ethernet port 10 receives all network traffic from Ethernet port 5 without being physically attached to it.

*CISCO Confidential - DRAFT***Figure 26-1 Example SPAN Configuration**

For SPAN configuration, the source ports and the destination port must be on the same switch.

SPAN does not affect the switching of network traffic on source ports; copies of the packets that are received or transmitted by the source ports are sent to the destination port.

SPAN Configuration Guidelines

This section describes the configuration guidelines for configuring SPAN:

- Incoming traffic on the SPAN destination port is disabled by default. You can enable it using the **inpkts enable** keywords. However, while the port receives traffic for its assigned VLAN, it does not participate in spanning tree for that VLAN. To avoid creating spanning tree loops with incoming traffic enabled, assign the SPAN destination port to an unused VLAN.
- In software release 5.2 and later releases, with the **inpkts** option enabled, you can prevent the switch from learning source MAC addresses from traffic that is received on the SPAN destination port using the **learning disable** keywords. If you want the switch to learn source MAC addresses from traffic that is received on the SPAN destination port, enter the **learning enable** keywords. By default, the switch learns source MAC addresses from incoming traffic (**learning enable**) if the **inpkts** option is enabled. The source MAC address learning options only affect traffic that is received from a device that is attached to the SPAN destination port itself, not from traffic that is mirrored from the SPAN source.
- When monitoring a VLAN on a switch, you must monitor both transmit and receive traffic (**both**). You cannot monitor only transmit (**Tx**) or only receive (**Rx**) traffic.
- If you specify a set of VLANs with the **filter** option, the traffic that is spanned by the session is limited to the VLANs specified.
- You cannot configure SPAN on sc0.
- Any traffic between two network nodes that are attached to a switch port that is configured as a SPAN source port is not mirrored to the SPAN destination port. You can span local traffic that passes through the switch.
- You can have up to five SPAN sessions running at the same time with any combination of ingress and egress sessions.

CISCO Confidential - DRAFT

Configuring SPAN

To configure SPAN, perform this task in privileged mode:

	Task	Command
Step 1	Configure a SPAN source and a SPAN destination port.	set span {src_mod/src_ports src_vlan} dest_mod/dest_port [rx tx both] [filter vlan] [inpkts {enable disable}] [learning {enable disable}] [create]
Step 2	Verify the SPAN configuration.	show span



Caution

If the SPAN destination port is connected to another device and reception of incoming packets is enabled (using the **inpkts enable** keywords), the SPAN destination port receives traffic for the VLAN to which the SPAN destination port belongs. However, the SPAN destination port does *not* participate in spanning tree for that VLAN, so avoid creating network loops with the SPAN destination port.

This example shows how to configure SPAN so that both the transmit and receive traffic from port 2/4 (the SPAN source) is mirrored on port 3/6 (the SPAN destination):

```
Console> (enable) set span 2/4 3/6
Overwrote Port 3/6 to monitor transmit/receive traffic of Port 2/4
Incoming Packets disabled. Learning enabled.
Console> (enable) show span
```

```
Destination      : Port 3/6
Admin Source     : Port 2/4
Oper Source      : None
Direction        : transmit/receive
Incoming Packets : disabled
Learning         : enabled
Filter           : -
Status           : active
```

```
-----
Total local span sessions: 1
Console> (enable)
```

This example shows how to set VLAN 522 as the SPAN source and port 2/1 as the SPAN destination:

```
Console> (enable) set span 522 2/1
Overwrote Port 2/1 to monitor transmit/receive traffic of VLAN 522
Incoming Packets disabled. Learning enabled.
Console> (enable) show span
```

```
Destination      : Port 2/1
Admin Source     : VLAN 522
Oper Source      : Port 2/1-2
Direction        : transmit/receive
Incoming Packets : disabled
Learning         : enabled
Filter           : -
Status           : active
```

```
-----
Total local span sessions: 1
Console> (enable)
```

CISCO Confidential - DRAFT

This example shows how to set VLAN 522 as the SPAN source and port 2/12 as the SPAN destination. Only transmit traffic is monitored. Normal incoming packets on the SPAN destination port are allowed.

```
Console> (enable) set span 522 2/12 tx inpkts enable
Overwrote Port 2/12 to monitor transmit/receive traffic of VLAN 522
Incoming Packets enabled. Learning enabled.
Console> (enable) show span
Destination      : Port 2/12
Admin Source     : VLAN 522
Oper Source      : Port 2/1-2
Direction       : transmit
Incoming Packets : enabled
Filter           : -
Status           : active
```

```
-----
Total local span sessions: 1
Console> (enable)
```

This example shows how to set multiple SPAN sessions using the following configurations:

- Port 3/1 as the SPAN source and port 2/3 as the SPAN destination
- Port 3/2 as the SPAN source and port 2/5 as the SPAN destination

```
Console> (enable) set span 3/1 2/3
Overwrote Port 2/3 to monitor transmit/receive traffic of Port 3/1
Incoming Packets disabled. Learning enabled.
Console> (enable) set span 3/2 2/5 tx create
Created Port 2/5 to monitor transmit traffic of Port 3/2
Incoming Packets disabled. Learning enabled.
Console> (enable) show span
```

```
Destination      : Port 2/3
Admin Source     : Port 3/1
Oper Source      : None
Direction       : transmit/receive
Incoming Packets : disabled
Learning        : enabled
Filter           : -
Status           : inactive
```

```
-----
Destination      : Port 2/5
Admin Source     : Port 3/2
Oper Source      : None
Direction       : transmit
Incoming Packets : disabled
Learning        : enabled
Filter           : -
Status           : inactive
-----
```

```
Total local span sessions: 2
Console> (enable)
```

This example shows how to configure SPAN so that both transmit and receive traffic from the trunking port 3/4 (the SPAN source) are mirrored on port 3/5 (the SPAN destination) and both VLANs 50 and 850 are filtered:

```
Console> (enable) set span 3/4 3/5 both filter 50,850
Overwrote Port 3/5 to monitor transmit/receive traffic of Port 3/4
Incoming Packets disabled. Learning enabled.
Console> (enable) show span
```

```
Destination      : Port 3/5
```

CISCO Confidential - DRAFT

```
Admin Source      : Port 3/4
Oper Source       : None
Direction        : transmit/receive
Incoming Packets  : disabled
Learning         : enabled
Filter           : 50,850
Status           : inactive
```

```
-----
Total local span sessions: 1
Console> (enable)
```

To disable SPAN, perform this task in privileged mode:

Task	Command
Disable SPAN on the switch.	set span disable [<i>dest_mod/dest_port</i> <i>all</i>]

This example shows how to disable SPAN on the switch:

```
Console> (enable) set span disable 2/3
This command may disable your span session(s).
Do you want to continue (y/n) [n]? y
Disabled Port 2/3 to monitor transmit/receive traffic of Port
Incoming Packets disabled. Learning enabled.
Console> (enable)
```

Configuring RSPAN

The following sections describe how to configure RSPAN.

RSPAN Software and Hardware Requirements

You must have software release 6.3(1) or a later release to use the RSPAN functionality on the Catalyst 4000 family switches or to use a Catalyst 4000 family switch as an intermediate switch in an RSPAN session.

RSPAN supervisor engine requirements are as follows:

- For source switches—Any Catalyst 4000 family switch supervisor engine
- For destination or intermediate switches—Any Catalyst 4000 family or Catalyst 6500 series switch supervisor engine

You cannot place any third-party or other Cisco switches in the end-to-end path for RSPAN traffic.

Understanding How RSPAN Works

**Note**

See the “[Understanding How SPAN and RSPAN Work](#)” section on page 26-1 for concepts and terminology that apply to both SPAN and RSPAN configuration.

CISCO Confidential - DRAFT

RSPAN has all the features of SPAN (see the [“Understanding How SPAN Works”](#) section on page 26-4), plus support for source ports and destination ports that are distributed across multiple switches, allowing remote monitoring of multiple switches across your network.

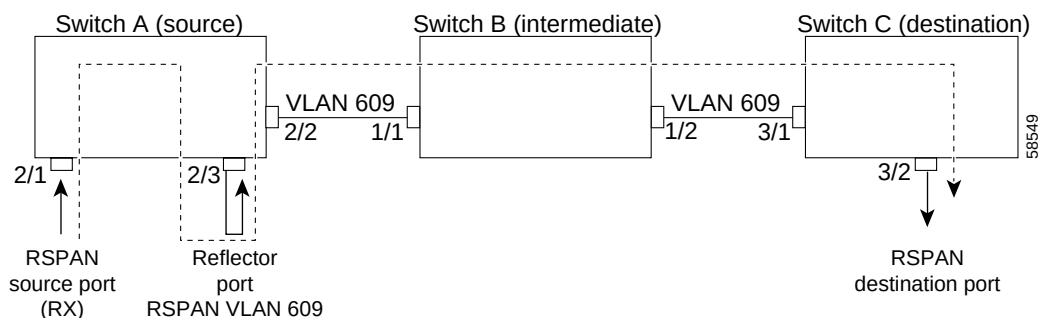
The traffic for each RSPAN session is carried over a user-specified RSPAN VLAN that is dedicated for that RSPAN session in all participating switches. The SPAN traffic from the sources is copied onto the RSPAN VLAN through the reflector port and then forwarded over trunk ports carrying the RSPAN VLAN to RSPAN destination ports monitoring the RSPAN VLAN.

Traffic sent out through the source port is also sent out on the reflector port. Because the reflector port is an access (nontrunking) port in loopback mode, the traffic is switched out with no VLAN tag and is immediately sent back to the switch. In the loopback, the traffic is encoded into the RSPAN VLAN. A switch with an RSPAN destination session receives the traffic (see [Figure 26-2](#)).

The traffic type for sources (ingress, egress, or both) in an RSPAN session can be different for source switches, but must be the same for all source ports on a given switch.

Do not configure any ports in an RSPAN VLAN except those selected to carry RSPAN traffic. Learning is disabled on the RSPAN VLAN.

Figure 26-2 Flow of RSPAN Monitored Traffic



RSPAN Configuration Guidelines

This section describes the guidelines for configuring RSPAN:



Tip

Because RSPAN VLANs have special properties, we recommend that you reserve a few VLANs across your network for use as RSPAN VLANs. Do not assign access ports to these VLANs.

- All the items in the [“SPAN Configuration Guidelines”](#) section on page 26-5 apply to RSPAN.
- RSPAN sessions can coexist with SPAN sessions to a maximum of five sessions. The limit on the number of sessions the Catalyst 4000 family switches can carry as an intermediate switch is the maximum number of VLANs for the switch.
- For RSPAN configuration, you can distribute the source ports and the destination port across multiple switches.
- A port cannot serve as an RSPAN source port or RSPAN destination port while designated as an RSPAN reflector port.

CISCO Confidential - DRAFT

- For RSPAN, trunking is required if you have a source switch with all source ports in one VLAN (VLAN 2, for example) and it is connected to the destination switch through an uplink port that is also in the same VLAN. With RSPAN, the traffic is forwarded to remote switches in the RSPAN VLAN. The RSPAN VLAN is configured only on trunk ports, not on access ports.
- The learning option applies to RSPAN destination ports only.
- RSPAN does not support BPDU packet monitoring.
- RSPAN VLANs are not included as sources for port-based RSPAN sessions when source trunk ports have active RSPAN VLANs. Additionally, RSPAN VLANs cannot be sources in VSPAN sessions.
- You can configure any VLAN as an RSPAN VLAN as long as these conditions are met:
 - The same RSPAN VLAN is used for an RSPAN session in all the switches.
 - All participating switches have appropriate hardware and software.
 - No access port (including the sc0 interface) is configured in the RSPAN VLAN.
- If you enable VLAN Trunking Protocol (VTP) and VTP pruning, RSPAN traffic is pruned in the trunks to prevent the unwanted flooding of RSPAN traffic across the network.
- If you enable GARP VLAN Registration Protocol (GVRP) and GVRP requests conflict with existing RSPAN VLANs, you might observe unwanted traffic in the respective RSPAN sessions.
- You can use RSPAN VLANs in Inter-Switch Link (ISL) to map dot1q. However, ensure that the special properties of RSPAN VLANs are supported in all the switches to avoid unwanted traffic in these VLANs.
- Incoming traffic on the RSPAN destination port is disabled by default. You can enable it using the **inpkts enable** keywords. However, while the port receives traffic for its assigned VLAN, it does not participate in spanning tree for that VLAN. To avoid creating spanning tree loops with incoming traffic enabled, assign the RSPAN destination port to an unused VLAN.
- When the **inpkts** option is enabled, you can prevent the switch from learning source MAC addresses from traffic that is received on the RSPAN destination port using the **learning disable** keywords. If you want the switch to learn source MAC addresses from traffic that is received on the RSPAN destination port, enter the **learning enable** keywords. By default, the switch learns source MAC addresses from incoming traffic (**learning enable**) if the **inpkts** option is enabled. The source MAC address learning options only affect traffic that is received from a device that is attached to the RSPAN destination port itself, not from traffic that is mirrored from the RSPAN source.

Configuring RSPAN

The first step in configuring an RSPAN session is to select an RSPAN VLAN for the RSPAN session that *does not* exist in any of the switches that will participate in RSPAN. With VTP enabled in the network, you can create the RSPAN VLAN in one switch and VTP propagates it to the other switches in the VTP domain.

Use VTP pruning to get efficient flow of RSPAN traffic, or manually delete the RSPAN VLAN from all trunks that do not need to carry the RSPAN traffic.

Once the RSPAN VLAN is created, you configure the source and destination switches using the **set rspan** command.

To configure RSPAN VLANs, perform this task in privileged mode:

CISCO Confidential - DRAFT

	Task	Command
Step 1	Configure RSPAN VLANs.	set vlan <i>vlan_num</i> [rspan]
Step 2	Verify the RSPAN VLAN configuration.	show vlan

This example shows how to set VLAN 500 as an RSPAN VLAN:

```

Console> (enable) set vlan 500 rspan
vlan 500 configuration successful
Console> (enable)
Console> (enable) show vlan
.
display truncated
.
VLAN DynCreated  RSPAN
-----
1      static      disabled
2      static      disabled
3      static      disabled
99     static      disabled
500    static      enabled
Console> (enable)

```

To configure RSPAN source ports, perform this task in privileged mode:

	Task	Command
Step 1	Configure RSPAN source ports. Use this command on each of the source switches participating in RSPAN.	set rspan source {<i>mod/ports...</i> <i>vlans...</i>} {<i>rspan_vlan</i>} reflector <i>mod/port</i> [<i>rx</i> <i>tx</i> <i>both</i>] [<i>filter vlans...</i>] [<i>create</i>]
Step 2	Verify the RSPAN configuration.	show rspan

This example shows how to specify port 2/3 as an ingress source port for RSPAN VLAN 500 with port 2/34 as the reflector port:

```

Console> (enable) set rspan source 2/3 500 reflector 2/34 rx
Rspan Type      : Source
Destination     : -
Reflector       : Port 2/34
Rspan Vlan      : 500
Admin Source    : Port 2/3
Oper Source     : Port 2/3
Direction       : receive
Incoming Packets: -
Learning        : -
Filter          : -
Status          : active

```

```

Console> (enable) 2001 May 02 13:22:17 %SYS-5-SPAN_CFGSTATECHG:remote span source session
active for remote span vlan 500

```

This example shows how to specify port 2/3 as a source port for RSPAN VLAN 500 with port 2/34 as the reflector port and to filter VLANs 50 and 850:

```

Console> (enable) set rspan source 2/3 500 reflector 2/34 filter 50,850
Rspan Type      : Source
Destination     : -
Reflector       : Port 2/34
Rspan Vlan      : 500

```

CISCO Confidential - DRAFT

```

Admin Source      : Port 2/3
Oper Source       : Port 2/3
Direction        : transmit/receive
Incoming Packets: -
Learning         : -
Filter           : 50,850
Status           : active

```

```

Console> (enable) 2001 May 02 13:25:59 %SYS-5-SPAN_CFGSTATECHG:remote span source session
active for remote span vlan 500

```

To configure RSPAN source VLANs, perform this task in privileged mode:

	Task	Command
Step 1	Configure RSPAN source VLANs. All the ports in the source VLAN become operational source ports.	set rspan source { <i>mod/ports...</i> <i>vlangs...</i> } { <i>rspan_vlan</i> } reflector <i>mod/port</i> [rx tx both] [filter <i>vlangs...</i>] [create]
Step 2	Verify the RSPAN configuration.	show rspan

This example shows how to specify VLAN 200 as a source VLAN for RSPAN VLAN 500:

```

Console> (enable) set rspan source 200 500
Rspan Type       : Source
Destination      : -
Rspan Vlan       : 500
Admin Source     : VLAN 200
Oper Source      : None
Direction        : transmit/receive
Incoming Packets: -
Learning         : -
Multicast        : enabled
Filter           : -
Console> (enable)

```

To configure RSPAN destination ports, perform this task in privileged mode:

	Task	Command
Step 1	Configure RSPAN destination ports. Use this command on each of the destination switches participating in RSPAN.	set rspan destination { <i>mod_num/port_num</i> } { <i>rspan_vlan</i> } [inpkts { enable disable }] [learning { enable disable }] [create]
Step 2	Verify the RSPAN configuration.	show rspan

**Caution**

If the RSPAN destination port is connected to another device and reception of incoming packets is enabled (using the **inpkts enable** keywords), the RSPAN destination port receives traffic for the VLAN to which the RSPAN destination port belongs. However, the RSPAN destination port does *not* participate in spanning tree for that VLAN, so avoid creating network loops with the RSPAN destination port.

This example shows how to specify port 3/1 as the RSPAN destination port in VLAN 500:

```

Console> (enable) set rspan destination 3/1 500
Rspan Type       : Destination
Destination      : Port 3/1
Rspan Vlan       : 500
Admin Source     : -

```

CISCO Confidential - DRAFT

```

Oper Source      : -
Direction       : -
Incoming Packets : disabled
Learning        : enabled
Filter          : -
Status          : active
Console> (enable)

```

Disabling RSPAN Sessions

When disabling an RSPAN session, you must disable all source and destination sessions on all participating switches. Leaving RSPAN source sessions enabled consumes bandwidth with RSPAN VLAN traffic.

To disable RSPAN, perform this task in privileged mode:

	Task	Command
Step 1	Disable RSPAN source sessions on the switch.	set rspan disable source [<i>rspan_vlan</i> all]
Step 2	Disable RSPAN destination sessions on the switch.	set rspan disable destination [<i>mod_num/port_num</i> all]

This example shows how to disable all enabled source sessions on the switch:

```

Console> (enable) set rspan disable source all
This command will disable all remote span source session(s).
Do you want to continue (y/n) [n]? y
Disabled monitoring of all source(s) on the switch for remote span.
Console> (enable)

```

This example shows how to disable one source session by *rspan_vlan* number:

```

Console> (enable) set rspan disable source 903
Disabled monitoring of all source(s) on the switch for rspan_vlan 903.
Console> (enable)

```

This example shows how to disable all enabled destination sessions on the switch:

```

Console> (enable) set rspan disable destination all
This command will disable all remote span destination session(s).
Do you want to continue (y/n) [n]? y
Disabled monitoring of remote span traffic for all rspan destination ports.
Console> (enable)

```

This example shows how to disable one destination session by *mod_num/port_num*:

```

Console> (enable) set rspan disable destination 4/1
Disabled monitoring of remote span traffic on port 4/1.
Console> (enable)

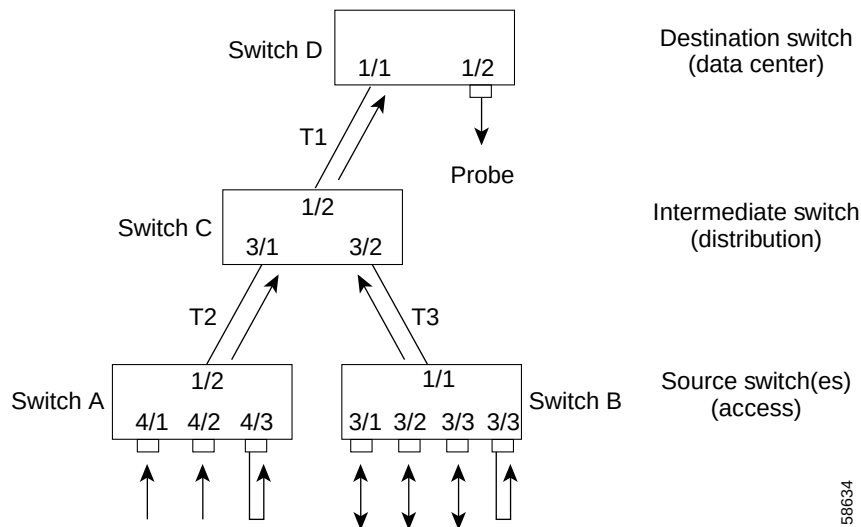
```

RSPAN Configuration Examples

The following sections provide examples that show how to configure RSPAN.

*CISCO Confidential - DRAFT***Configuring a Single RSPAN Session**

This example shows how to configure a single RSPAN session. Figure 26-3 shows an RSPAN configuration; see Table 26-1 for the necessary commands to configure this RSPAN session. Table 26-1 assumes that you have already set up RSPAN VLAN 901 for this session on all the switches using the **set vlan vlan_num rspan** command. With VTP enabled in the network, you can create the RSPAN VLAN in one switch and VTP propagates it to the other switches in the VTP domain. Note that in the configuration example shown in Table 26-1, the RSPAN session may be disabled in Switch A or B or both without modifying the configuration in Switch C or Switch D.

Figure 26-3 Single RSPAN Session**Table 26-1 Configuring a Single RSPAN Session**

Switch	Ports	Reflector Port	RSPAN VLAN	Direction	RSPAN CLI Commands
A (source)	4/1, 4/2	4/3	901	Ingress	set rspan source 4/1-2 901 rx reflector 4/3
B (source)	3/1, 3/2, 3/3	3/4	901	Bidirectional	set rspan source 3/1-3 901 reflector 3/4
C (intermediate)	—	—	901	—	No RSPAN CLI command needed
D (destination)	1/2	—	901	—	set rspan destination 1/2 901

Modifying an Active RSPAN Session

This example shows how to modify an active RSPAN session. Use Figure 26-3 for reference; see Table 26-2 for the necessary commands to disable an RSPAN session and to add or remove source ports from an RSPAN session.

Table 26-2 Making Modifications to an Active RSPAN Session

Switch	Action	RSPAN CLI Commands
A (source)	Disable the RSPAN session.	set rspan disable source 901

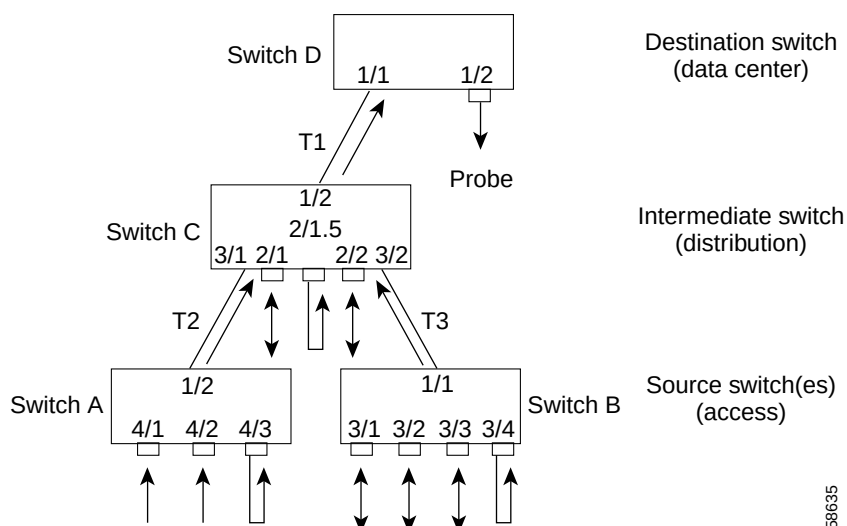
CISCO Confidential - DRAFT

Table 26-2 Making Modifications to an Active RSPAN Session

Switch	Action	RSPAN CLI Commands
B (source)	Remove source port 3/2 from RSPAN session.	set rspan source 3/1, 3/3 901 reflector 3/4
B (source)	Add source port 3/2 to RSPAN session.	set rspan source 3/1-3 901 reflector 3/4

Adding RSPAN Source Ports in Intermediate Switches

This example shows how to add RSPAN source ports in intermediate switches. Figure 26-4 shows an RSPAN configuration; see Table 26-3 for the necessary commands to configure this RSPAN session. Ports 2/1-2 in Switch C can be configured for the same RSPAN session.

Figure 26-4 Adding RSPAN Source Ports in Intermediate Switch**Table 26-3 Adding RSPAN Source Ports in Intermediate Switch**

Switch	Ports	Reflector Port	RSPAN VLAN	Direction	RSPAN CLI Commands
A (source)	4/1, 4/2	4/3	901	Ingress	set rspan source 4/1-2 901 rx reflector 4/3
B (source)	3/1, 3/2, 3/3	3/4	901	Bidirectional	set rspan source 3/1-3 901 reflector 3/4
C (intermediate)	—	—	901	—	No RSPAN CLI command needed
C (source)	2/1, 2/2	2/3	901	Bidirectional	set rspan source 2/1-2 901 reflector 2/3
D (destination)	1/2	—	901	—	set rspan destination 1/2 901

Configuring Multiple RSPAN Sessions

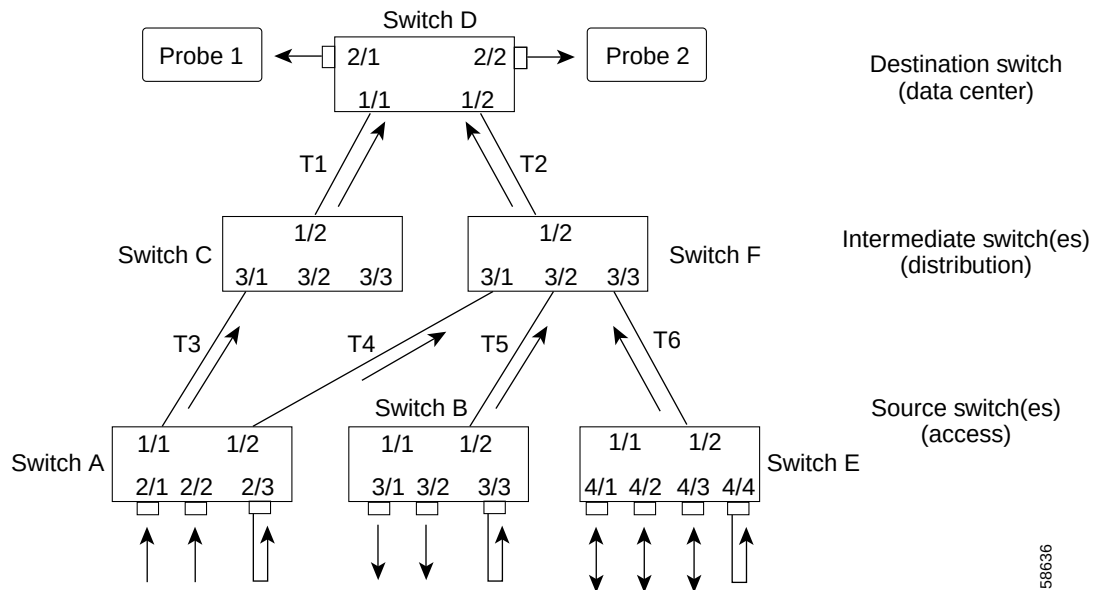
This example shows how to configure multiple RSPAN sessions. Figure 26-5 shows an RSPAN configuration; see Table 26-4 for the necessary configuration commands to configure this RSPAN session. This is a typical scenario where the monitoring probes would be placed in the data center and

CISCO Confidential - DRAFT

source ports in the access switches (other ports in any of the switches can also be configured for RSPAN). If there is no change in the route for SPAN traffic, the destination switch and the intermediate switches need to be configured only once.

In [Figure 26-5](#), two RSPAN sessions are used with RSPAN VLANs 901 (for probe 1) and 902 (for probe 2). The direction of traffic over trunks T1 through T6 is shown only for understanding; the direction of the trunks depends on the STP states of the respective trunks for the RSPAN VLAN(s). You need to configure the RSPAN VLANs in each of the switches for the respective RSPAN sessions. With VTP enabled in the network, you can create the RSPAN VLAN in one switch and VTP propagates it to the other switches in that VTP domain. With VTP disabled, create the RSPAN VLANs in each switch.

Figure 26-5 Configuring Multiple RSPAN Sessions



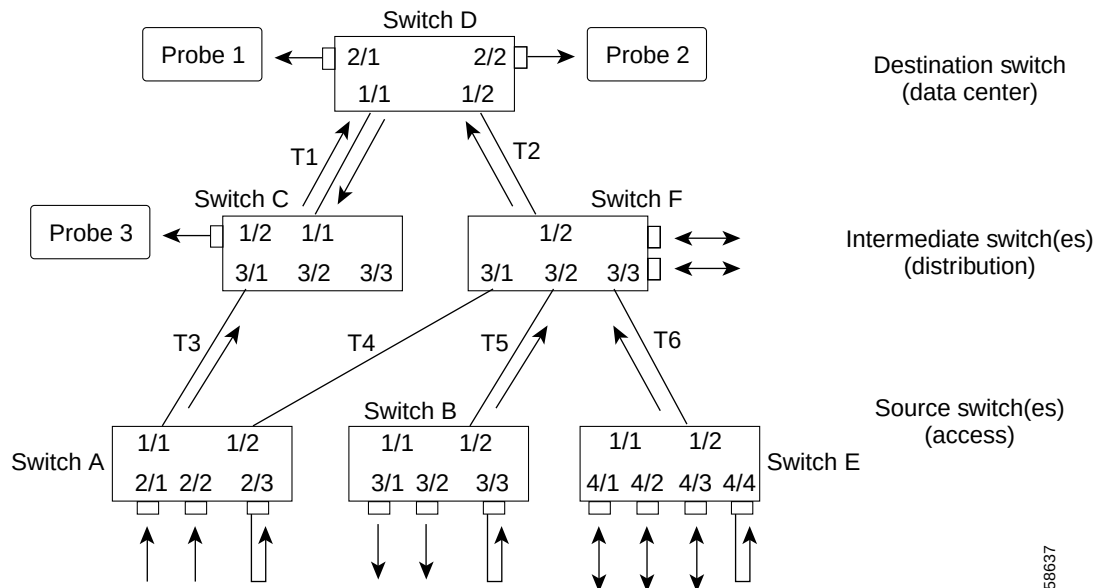
58636

Table 26-4 Configuring Multiple RSPAN Sessions

Switch	Port	Reflector Port	RSPAN VLAN(s)	Direction	RSPAN CLI Commands
A (source)	2/1-2	2/3	901	Ingress	set rspan source 2/1-2 901 rx reflector 2/3
B (source)	3/1-2	3/3	901	Egress	set rspan source 3/1-2 901 tx reflector 3/3
C (intermediate)	—	—	901, 902	—	No RSPAN CLI command needed
D (destination)	2/1	—	901	—	set rspan destination 2/1 901
D (destination)	2/2	—	902	—	set rspan destination 2/2 902
E (source)	4/1-3	4/4	901	Both	set rspan source 4/1-3 902 reflector 4/4
F (intermediate)	—	—	901, 902	—	No RSPAN CLI command needed

Adding Multiple Network Analyzers to an RSPAN Session

You can attach multiple network analyzers (probes) to the same RSPAN session. For example, in [Figure 26-6](#), you can add probe 3 in Switch B to monitor RSPAN VLAN 901 using the **set rspan destination 1/2 901** command. Similarly, you could add source ports to Switch C.

*CISCO Confidential - DRAFT***Figure 26-6 Adding Multiple Probes to an RSPAN Session**

58637

Disabling the RSPAN Session

To completely disable the previous RSPAN session, you need to disable every RSPAN source and RSPAN destination on each source and destination switch. [Table 26-5](#) lists the commands necessary to completely disable the RSPAN session.

Table 26-5 Disabling the RSPAN Sessions

Switch	Port	Reflector Port	RSPAN VLAN(s)	Direction	RSPAN CLI Commands
A (source)	2/1-2	2/3	901	Ingress	set rspan disable source 901
B (source)	3/1-2	3/3	901	Egress	set rspan disable source 901
B (destination)	1/2	—	901	—	set rspan disable destination all
C (intermediate)	—	—	901, 902	—	No RSPAN CLI command needed
D (destination)	2/1	—	901	—	set rspan disable destination all
D (destination)	2/2	—	902	—	set rspan disable destination all
E (source)	4/1-3	4/4	901	Both	set rspan disable source all
F (intermediate)	—	—	901, 902	—	No RSPAN CLI command needed

CISCO Confidential - DRAFT

Administering the Switch

This chapter describes how to perform administrative tasks on the Catalyst enterprise LAN switches.

**Note**

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 4500 Series, Catalyst 2948G, and Catalyst 2980G Switches Command Reference*.

This chapter consists of these major sections:

- [Setting the System Name and System Prompt, page 27-1](#)
- [Setting the System Contact and Location, page 27-3](#)
- [Setting the System Clock, page 27-4](#)
- [Creating a Login Banner, page 27-4](#)
- [Enabling or Disabling the “Cisco Systems Console” Telnet Login Banner, page 27-5](#)
- [Defining and Using Command Aliases, page 27-6](#)
- [Defining and Using IP Aliases, page 27-7](#)
- [Configuring Permanent and Static ARP Entries, page 27-8](#)
- [Configuring Static Routes, page 27-9](#)
- [Scheduling a System Reset, page 27-10](#)
- [Generating System Status Reports for Tech Support, page 27-12](#)

Setting the System Name and System Prompt

The system name on the switch is a user-configurable string that identifies the device. The default configuration has no system name configured.

If you do not manually configure a system name, the switch obtains the system name through a Domain Name System (DNS) lookup. To configure the switch manually, complete the following:

- Assign the sc0 interface an IP address that is mapped to the switch name on the DNS server
- Enable DNS on the switch
- Specify at least one valid DNS server on the switch

If the DNS lookup is successful, the DNS host name of the switch is configured as the system name of the switch and is saved in NVRAM (the domain name is removed).

CISCO Confidential - DRAFT

If you have not configured a system prompt, the first 20 characters of the system name are used as the system prompt (a greater-than symbol [`>`] is appended). The prompt is updated whenever the system name changes, unless you have manually configured the prompt using the **set prompt** command.

The switch performs a DNS lookup for the system name whenever one of the following occurs:

- When the switch is initialized (power on or reset)
- When you configure the IP address on the sc0 interface using the CLI or Simple Network Management Protocol (SNMP)
- When you configure a route using the **set ip route** command
- When you clear the system name using the **set system name** command
- When you enable DNS or specify DNS servers

If you configured the system name, no DNS lookup is performed.

Configuring a System Name and Prompt

The following sections describe how to configure the system name and prompt.

Setting a System Name

To set the system name, perform this task in privileged mode:

Task	Command
Set the system name.	set system name <i>name_string</i>



Note

When you set the system name, the system name is used as the system prompt; you can override this with the **set prompt** command.

This example shows how to set the system name on the switch:

```

Console> (enable) set system name Catalyst 4003
System name set.
Catalyst 4003> (enable)
  
```

Setting a System Prompt

To set the system prompt, perform this task in privileged mode:

Task	Command
Set the system prompt.	set prompt <i>prompt_string</i>

CISCO Confidential - DRAFT

This example shows how to set the system prompt for the switch:

```
Console> (enable) set prompt Catalyst4012>
Catalyst4012> (enable)
```

Clearing the System Name

To clear the system name, perform this task in privileged mode:

Task	Command
Clear the system name.	set system name

This example shows how to clear the system name:

```
Console> (enable) set system name
System name cleared.
Console> (enable)
```

Setting the System Contact and Location

You can set the contact name and location to help you with resource management tasks. To set the system contact and location, perform this task in privileged mode:

	Task	Command
Step 1	Set the system contact.	set system contact <i>[contact_string]</i>
Step 2	Set the system location.	set system location <i>[location_string]</i>
Step 3	Verify the global system information.	show system

This example shows how to set the system contact to sysadmin@corp.com and location to Sunnyvale, CA:

```
Console> (enable) set system contact sysadmin@corp.com
System contact set.
Console> (enable) set system location Sunnyvale CA
System location set.
```

This example shows how to verify the configuration:

```
Console> (enable) show system
PS1-Status PS2-Status PS3-Status PEM Installed PEM Powered
-----
ok          ok          ok          yes         no

Fan-Status Temp-Alarm Sys-Status Uptime d,h:m:s Logout
-----
ok          off         ok          0,18:24:41 none

PS1-Type          PS2-Type          PS3-Type
-----
WS-X4008-DC-650W WS-X4008          WS-X4008

Modem   Baud   Traffic Peak Peak-Time
-----
```

CISCO Confidential - DRAFT

```
disable 9600 0% 0% Wed Apr 24 2002, 15:46:01

Power Capacity of the Chassis:2 supplies

WARNING:Power supplies of different values have been inserted

System Name          System Location          System Contact          CC
-----
Console> (enable)   Sunnyvale CA          sysadmin@corp.com      4006
```

Setting the System Clock



Note

You can configure the switch to obtain the time and date using the Network Time Protocol (NTP). For information on configuring NTP, see [Chapter 39, “Configuring NTP.”](#)

To set the system clock, perform this task in privileged mode:

	Task	Command
Step 1	Set the system clock.	set time [day_of_week] [mm/dd/yy] [hh:mm:ss]
Step 2	Display the current date and time.	show time

This example shows how to set the system clock and display the current date and time:

```
Console> (enable) set time Fri 06/15/01 12:30:00
Fri Jun 15 2001, 12:30:00
Console> (enable) show time
Fri Jun 15 2001, 12:30:02
Console> (enable)
```

Creating a Login Banner

You can create a single or multiline message-of-the-day (MOTD) banner that appears on the screen when someone logs in to the switch. The first character following the **motd** keyword is used to delimit the beginning and end of the banner text. Characters following the ending delimiter are discarded. After entering the ending delimiter, press **Return**. The banner must be fewer than 3070 characters.

Configuring a Login Banner

To configure a login banner, perform this task in privileged mode:

	Task	Command
Step 1	Set the message of the day.	set banner motd c message_of_the_day c
Step 2	Display the login banner by logging out and logging back in to the switch.	—

CISCO Confidential - DRAFT

This example shows how to set the login banner for the switch. The # symbol indicates the beginning and ending delimiter, but you can use any character for the delimiter.

```
Console> (enable) set banner motd #
Welcome to the Catalyst 4012 Switch!
Unauthorized access prohibited.
Contact sysadmin@corp.com for access.
#
MOTD banner set
Console> (enable)
```

Clearing the Login Banner

To clear the login banner, perform this task in privileged mode:

Task	Command
Clear the message of the day.	set banner motd cc

This example shows how to clear the login banner:

```
Console> (enable) set banner motd ##
MOTD banner cleared
Console> (enable)
```

Enabling or Disabling the “Cisco Systems Console” Telnet Login Banner

By default, the Cisco Systems Console Telnet login banner is enabled.

To enable or disable the “Cisco Systems Console” Telnet login banner, perform this task in privileged mode:

	Task	Command
Step 1	Display or suppress the Cisco Systems Console Telnet login banner.	set banner telnet {enable disable}
Step 2	Display the Cisco Systems Console Telnet login banner setting.	show banner

This example shows how to enable the Cisco Systems Console Telnet login banner:

```
Console> (enable) set banner telnet enable
Cisco Systems Console banner will be printed at telnet.
Console> (enable)
```

This example shows how to disable the Cisco Systems Console Telnet login banner:

```
Console> (enable) set banner telnet disable
Cisco Systems Console banner will not be printed at telnet.
Console> (enable)
```

This example shows how to display the Cisco Systems Console Telnet login banner content:

CISCO Confidential - DRAFT

```

Console> (enable) show banner
MOTD banner:
Welcome to the Catalyst 4012 Switch!
Unauthorized access prohibited.
Contact sysadmin@corp.com for access.

```

```

LCD config:

```

```

Telnet Banner:
disabled
Console> (enable)

```

Defining and Using Command Aliases

You can use the **set alias** command to define up to 100 command aliases (short versions of command names) for frequently used or long and complex commands. Using command aliases can save you time and help prevent typing errors when you are configuring or monitoring the switch.

For the *name* argument, specify a name for the command alias. The *parameter* argument is the text the user types at the command line to activate the command.

To define a command alias on the switch, perform this task in privileged mode:

	Task	Command
Step 1	Define a command alias on the switch.	set alias <i>name</i> <i>command</i> [<i>parameter</i>] [<i>parameter</i>]
Step 2	Verify the currently defined command aliases.	show alias [<i>name</i>]

This example shows how to define two command aliases:

- **sm3**, which executes the **show module 3/1** command
- **sp3**, which executes the **show port 3** command.

```

Console> (enable) set alias sm3 show module 3
Command alias added.
Console> (enable) set alias sp3 show port 3/1
Command alias added.
Console> (enable)

```

This example shows how to verify the currently defined command aliases:

```

Console> (enable) show alias
sm8          show module 3
sp8          show port 3

```

These examples show what happens when you enter the command aliases at the command line:

```

Console> (enable) sm3
Mod Slot Ports Module-Type          Model          Sub Status
---
3   3    6    1000BaseX Ethernet      WS-X4306      no  ok

Mod Module-Name          Serial-Num
---
3                        JAB024000YY

Mod MAC-Address(es)      Hw    Fw    Sw
---
3   00-10-7b-f6-b2-1a to 00-10-7b-f6-b2-1f 0.2

```


CISCO Confidential - DRAFT

```

Console> (enable) sp3
Port  Name              Status      Vlan      Level Duplex Speed Type
-----
  3/1                    notconnect  1          normal   full  1000 1000BaseSX

Port  Security Violation Shutdown-Time Age-Time Max-Addr Trap      IfIndex
-----
  3/1  disabled  shutdown          0          0          1 disabled      9

Port  Num-Addr Secure-Src-Addr Age-Left Last-Src-Addr Shutdown/Time-Left
-----
  3/1          0          -          -          -          -          -

Port  Send FlowControl Receive FlowControl RxPause TxPause Unsupported
      admin   oper      admin   oper              opcodes
-----
  3/1  desired  off      off      off              0          0          0

Port  Status      Channel Admin Ch
      Mode              Group Id
-----
  3/1  notconnect auto silent      29      0

Port  Align-Err FCS-Err Xmit-Err Rcv-Err UnderSize
-----
  3/1          -          0          0          0          0

Port  Single-Col Multi-Coll Late-Coll Excess-Col Carri-Sen Runts      Giants
-----
  3/1          0          0          0          0          0          0          0

Last-Time-Cleared
-----
Mon Jun 26 2000, 08:53:49
Console> (enable)

```

Defining and Using IP Aliases

You can use the **set ip alias** command to define aliases for IP addresses. IP aliases can make it easier to refer to other network devices when you use **ping**, **telnet**, and other commands, even when DNS is not enabled.

For the *name* argument, specify a name for your IP alias. For the *ip_addr* argument, specify the IP address to which the name refers.

To define an IP alias on the switch, perform this task in privileged mode:

	Task	Command
Step 1	Define an IP alias on the switch.	set ip alias <i>name ip_addr</i>
Step 2	Verify the currently defined IP aliases.	show ip alias [<i>name</i>]

This example shows how to define two IP aliases, **sparc**, which refers to IP address 172.20.52.3, and **cat4003**, which refers to IP address 172.20.52.71. This example also shows how to verify the currently defined IP aliases:

```

Console> (enable) set ip alias sparc 172.20.52.3
IP alias added.

```

CISCO Confidential - DRAFT

```
Console> (enable) set ip alias cat4003 172.20.52.71
IP alias added.
```

This example shows what happens when you use the IP aliases with the **ping** command:

```
Console> (enable) show ip alias
default      0.0.0.0
sparc        172.20.52.3
cat5509      172.20.52.71
Console> (enable) ping sparc
sparc is alive
Console> (enable) ping cat4003
cat4003 is alive
Console> (enable)
```

Configuring Permanent and Static ARP Entries

To enable your Catalyst LAN switch to communicate with devices that do not respond to Address Resolution Protocol (ARP) requests, you can configure a static or permanent ARP entry that maps the IP addresses of those devices to their MAC addresses. You can configure an ARP entry so that it does not age out, by configuring it as either static or permanent. When you configure a static ARP entry using the **set arp static** command, the entry is removed from the ARP cache after a system reset. When you configure a permanent ARP by using the **set arp permanent** command, the ARP entry is retained even after a system reset.

Because most hosts support dynamic resolution, you usually do not need to specify static or permanent ARP cache entries. When a device does not respond to ARP requests, you can configure an ARP entry to be statically or permanently entered into the ARP cache so that those devices can still be reached.

To configure a static or permanent ARP entry, perform this task in privileged mode:

	Task	Command
Step 1	Configure a static or permanent ARP entry.	set arp [dynamic permanent static] {ip_addr hw_addr}
Step 2	(Optional) Specify the ARP aging time.	set arp agingtime seconds
Step 3	Verify the ARP configuration.	show arp

This example shows how to define a static ARP entry:

```
Console> (enable) set arp static 20.1.1.1 00-80-1c-93-80-40
Static ARP entry added as 20.1.1.1 at 00-80-1c-93-80-40 on vlan 1
Console> (enable)
```

This example shows how to define a permanent ARP entry:

```
Console> (enable) set arp permanent 10.1.1.1 00-80-1c-93-80-60
Permanent ARP entry added as
10.1.1.1 at 00-80-1c-93-80-60 on vlan 1
Console> (enable)
```

This example sets the ARP aging time:

```
Console> (enable) set arp agingtime 300
ARP aging time set to 300 seconds.
Console> (enable)
```

This example shows how to display the ARP cache:

CISCO Confidential - DRAFT

```

Console> (enable) show arp
ARP Aging time = 300 sec
+ - Permanent Arp Entries
* - Static Arp Entries
* 20.1.1.1 at 00-80-1c-93-80-40 on vlan 1
172.20.52.35 at 00-80-1c-93-80-40 on vlan 1
172.20.52.35 at 00-80-1c-93-80-40 on vlan 1
Console> (enable)

```

To clear ARP entries, perform this task in privileged mode:

	Task	Command
Step 1	Clear a dynamic, static, or permanent ARP entry.	clear arp [dynamic permanent static] { <i>ip_addr hw_addr</i> }
Step 2	Verify the ARP configuration.	show arp

This example shows how to clear all permanent ARP entries and verify the configuration:

```

Console> (enable) clear arp permanent
Permanent ARP entries cleared.

Console> (enable) show arp
ARP Aging time = 300 sec
+ - Permanent Arp Entries
* - Static Arp Entries
+ 10.1.1.1 at 00-80-1c-93-80-60 on vlan 1
* 20.1.1.1 at 00-80-1c-93-80-40 on vlan 1
Console> (enable)

```

Configuring Static Routes



Note

For information on configuring a default gateway (default route), see the [“Configuring Default Gateways” section on page 3-6](#).

In some situations, you might need to add a static routing table entry for one or more destination networks. Static route entries consist of the destination IP network address, the IP address of the next-hop router, and the metric (hop count) for the route.

In software release 5.1 and later releases, you can configure Classless InterDomain Routing (CIDR) routes, such as IP supernets, in the switch IP routing table. You can specify the subnet mask for a destination network using the number of subnet bits or using the subnet mask in dotted decimal format. If no subnet mask is specified, the default (classful) mask is used.

The switch uses the longest-match network address in the IP routing table to determine which gateway to use to forward IP traffic. In releases prior to software release 5.1, the switch always uses the classful subnet mask for IP routing table entries.

The switch forwards IP traffic that is generated by the switch using the longest address match in the IP routing table. The switch does not use the IP routing table to forward traffic from connected devices. The IP routing table is used by the switch only to forward IP traffic that is generated by the switch itself (for example, Telnet, TFTP, and ping).

In software releases prior to software release 5.1, the classful subnet mask is always used (you cannot specify the subnet mask for the destination network).

CISCO Confidential - DRAFT

To configure a static route, perform this task in privileged mode:

	Task	Command
Step 1	Configure a static route to the remote network.	set ip route <i>destination</i> [/ <i>netmask</i>] <i>gateway</i> [<i>metric</i>]
Step 2	Verify that the static route appears correctly in the IP routing table.	show ip route

This example shows how to configure a static route on the switch and how to verify that the route is configured properly in the routing table:

```
Console> (enable) set ip route 172.16.16.0/20 172.20.52.127
```

```
Route added.
```

```
Console> (enable) show ip route
```

```
Fragmentation    Redirect    Unreachable
```

```
-----
```

```
enabled          enabled     enabled
```

```
The primary gateway: 172.20.52.121
```

Destination	Gateway	RouteMask	Flags	Use	Interface
172.16.16.0	172.20.52.127	0xfffff000	UG	0	sc0
default	172.20.52.121	0x0	UG	0	sc0
172.20.52.120	172.20.52.124	0xffffffff8	U	1	sc0
default	default	0xff000000	UH	0	sl0

```
Console> (enable)
```

Scheduling a System Reset

You can use the **reset at** command to schedule a system to reset at a future time. This feature allows you to upgrade software during business hours and schedule the system upgrade after business hours to avoid a major impact on users.

You can also use the schedule reset feature when trying out new features on a switch. To avoid misconfiguration or the possibility of losing network connectivity to the device, you can set up the startup configuration feature and schedule a reset to occur in 30 minutes. You can then change the configuration, and if connectivity is lost, the system will reset in 30 minutes and return to the previous configuration.

Scheduling a Reset at a Specific Time

You can specify an absolute time and date at which the reset will take place, using the **reset at** command. The month and day argument is optional. If you do not specify a month and day, the reset will take place on the current day if the time that is specified is later than the current time. If the time that is scheduled for reset is earlier than the current time, the reset will take place on the following day.



Note

The maximum scheduled reset time is 24 days.

To schedule a reset at a specific time, perform this task in privileged mode:

CISCO Confidential - DRAFT

	Task	Command
Step 1	Schedule the reset time at a specific time.	reset [mindown] at {hh:mm} [mm/dd] [reason]
Step 2	Verify the scheduled reset.	show reset

This example shows how to schedule a reset at a specific time:

```
Console> (enable) reset at 20:00
Reset scheduled at 20:00:00, Sat Aug 18 2001.
Proceed with scheduled reset? (y/n) [n]? y
Reset scheduled for 20:00:00, Sat Aug 18 2001 (in 0 day 5 hours 40 minutes).
Console> (enable)
```

This example shows how to schedule a reset at a specific time and include a reason for the reset:

```
Console> (enable) reset at 23:00 08/18 Software upgrade to 5.3(1)
Reset scheduled at 23:00:00, Sat Aug 18 2001.
Reset reason: Software upgrade to 6.3(1).
Proceed with scheduled reset? (y/n) [n]? y
Reset scheduled for 23:00:00, Sat Aug 18 2001 (in 0 day 8 hours 39 minutes).
Console> (enable)
```

This example shows how to schedule a reset with a minimum of downtime:

```
Console> (enable) reset mindown at 23:00 08/18 Software upgrade to 6.3(1)
Reset scheduled at 23:00:00, Sat Aug 18 2001.
Reset reason: Software upgrade to 6.3(1).
Proceed with scheduled reset? (y/n) [n]? y
Reset mindown scheduled for 23:00:00, Sat Aug 18 2001 (in 0 day 8 hours 39 minutes).
Console> (enable)
```

Scheduling a Reset Within a Specified Amount of Time

You can schedule a reset within a specified time with the **reset in** command. For instance, if the current system time is 9:00 a.m. and the reset is scheduled to take place in one hour, the scheduled reset will take place at 10:00 a.m. If you or NTP advances the system clock to 10:00 a.m., the reset will take place at 11:00 a.m. If the clock is advanced ahead of the scheduled reset time, the reset will take place 5 minutes after the command is issued.

To schedule a reset within a specified time, perform this task in privileged mode:

	Task	Command
Step 1	Schedule the reset time within a specific amount of time.	reset [mindown] in [hh] {mm} [reason]
Step 2	Verify that the scheduled reset time is correct.	show reset



Note

The minimum downtime argument is valid only if the system has a redundant supervisor engine.

This example shows how to schedule a reset in a specified time:

```
Console> (enable) reset in 5:20 Configuration update
Reset scheduled in 5 hours 20 minutes.
Reset reason: Configuration update
Proceed with scheduled reset? (y/n) [n]? y
```

CISCO Confidential - DRAFT

```
Reset scheduled for 19:56:01, Wed Aug 18 1999 (in 5 hours 20 minutes).
Reset reason: Configuration update
Console> (enable)
```

Generating System Status Reports for Tech Support

Using a single command, you can generate a report that contains status information about your switch. This command is a combination of several **show system status** commands. (Refer to the *Catalyst 4500 Series, Catalyst 2948G, and Catalyst 2980G Switches Command Reference* for these commands.) You can upload the report to a TFTP server and send it to the Cisco Technical Assistance Center (TAC).

You can use keywords to limit the report, such as for specific modules, VLANs, and ports. If you do not specify any keywords, a report for the entire system is generated.

To write and send a report for TAC, perform this task in privileged mode:

Task	Command
Generate a system status report for TAC.	write tech-support {host} {file} [module mod_num] [port mod_num/port_num] [vlan vlan_num] [memory] [config]

This example shows a report sent to host 172.20.32.10 and to a filename **techsupport.txt**. No keywords are specified, so the complete status of the switch is included in the report.

```
Console> (enable) write tech-support 172.20.32.10 techsupport.txt
Upload tech-report to techsupport.txt on 172.20.32.10 (y/n) [n]? y
/
Finished network upload. (67784 bytes)
Console> (enable)
```

Power Management

This chapter describes the power management feature in the Catalyst 4500 series and Catalyst 4000 series switches.

**Note**

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 4500 Series, Catalyst 2948G, and Catalyst 2980G Switches Command Reference*.

This chapter consists of these sections:

- [Understanding How Power Management Works on the Catalyst 4500 Series Switches, page 28-1](#)
- [Understanding How Power Management Works on the Catalyst 4006 Switch, page 28-6](#)
- [Power Consumption for Modules, page 28-9](#)
- [Migrating a Supervisor Engine II from a Catalyst 4006 Switch to a Catalyst 4500 Series Switch, page 28-10](#)
- [Understanding How Inline Power Works, page 28-11](#)
- [Configuring Power Management, page 28-14](#)
- [Configuring Inline Power, page 28-18](#)

Understanding How Power Management Works on the Catalyst 4500 Series Switches

These sections describe how to manage power for the Catalyst 4500 series switches.

**Note**

For more information on power management for the Catalyst 4006 switch, see the [“Understanding How Power Management Works on the Catalyst 4006 Switch”](#) section on page 28-6.

Power Management Overview

Catalyst 4500 series switches support the following power supplies:

- Fixed wattage—These power supplies always deliver a fixed amount of inline and system power:
 - 1000 W AC

CISCO Confidential - DRAFT

- 2800 W AC
- Variable wattage—These power supplies automatically adjust the wattage to accommodate inline and system power requirements:
 - 1300 W AC
 - 1400 W DC

For more information on available wattage for the power supplies, see [Table 28-1 on page 28-4](#).

**Caution**

Do not use the 1400 W DC power supply with any other power supply, even for a hot swap or other short-term emergency, because you can seriously damage your switch.

**Note**

If you use power supplies with different types or wattages in your switch, the switch uses the power supply in power supply bay 1 (PS1) and ignores the power supply in power supply bay (PS2). Your switch will not have power redundancy.

Understanding Power Management Modes

Catalyst 4500 series switches support these two power management modes:

- Redundant mode—Uses one power supply as a primary power supply and the second power supply as a backup. If the primary power supply fails, the second power supply supports the switch without disrupting the network. Both power supplies must have the same wattage. A single power supply must have enough power to support the switch configuration. By default, the power supplies in the Catalyst 4500 series switch are set to redundant mode.
- Combined mode—Uses the power from all installed power supplies to support the power requirements of the switch configuration. Combined mode has no power redundancy; if a power supply fails, one or more modules might shut down. Combined mode requires that your switch has two power supplies. The 1400 W DC power supply does not support combined mode.

Your switch hardware configuration dictates which power supply or supplies you should use. For example, if your switch configuration requires more power than a single power supply provides, use the combined mode. In combined mode, however, the switch has no power redundancy.

**Note**

See [Table 28-1 on page 28-4](#) for a list of the maximum available power that is provided by the power supplies in either combined or redundant mode for the Catalyst 4500 series switches. See [Table 28-2 on page 28-9](#) for the power requirements of the Catalyst 4500 series switching modules.

Redundant Mode Guidelines

This section describes the guidelines for using redundant mode in the Catalyst 4500 series switches:

- By default, the power supplies in a Catalyst 4500 series switch are set to redundant mode.
- The two power supplies must be the same type.

**Caution**

Do not use the 1400 W DC power supply with any other power supply, even for a hot swap or other short-term emergency, because you can seriously damage your switch.

CISCO Confidential - DRAFT

- If you set your switch to redundant mode and only one power supply is installed, your switch accepts the configuration but operates without redundancy.

**Note**

If you use power supplies with different types or wattages in your switch, the switch uses the power supply in power supply bay 1 (PS1) and ignores the power supply in power supply bay (PS2). Your switch will not have power redundancy.

- When using fixed power supplies, choose a power supply that can support the switch configuration.
- When using variable power supplies, choose a power supply that supplies enough power so that the chassis and inline power requirements are less than the maximum available power for the chassis and inline power for the power supply. Variable power supplies automatically adjust the power resources to accommodate the chassis and inline power requirements when a system boots. Modules are brought up first, followed by powered devices.
- See [Table 28-1 on page 28-4](#) for a list of the maximum available power for chassis and inline power for each power supply.

Combined Mode Guidelines

This section describes the guidelines for using combined mode in the Catalyst 4500 series switches:

- The two power supplies must be the same type.
- If you use power supplies with different types or wattages, the switch uses only one power supply. Your switch will have no power redundancy.
- The 1400 W DC power supply does not support combined mode. If you set the power budget to 2, the switch disregards this setting. For more information about the 1400 W DC power supply, see the [“1400 W DC Power Supply Guidelines and Restrictions” section on page 28-5](#).
- When you set your switch to combined mode and only one power supply is installed, your switch continues to operate in combined mode.
- When using variable power supplies, choose a power supply that supplies enough power so that the chassis and inline power requirements are less than the maximum available power for the chassis and inline power for the power supply. Variable power supplies automatically adjust the power resources to accommodate the chassis and inline power requirements.
- When your switch is set to combined mode, the total available power is not the mathematical sum of the individual power supplies. The power supplies have a predetermined current sharing ratio. The total power available is $P + (P * \text{ratio})$.
- See [Table 28-1 on page 28-4](#) for a list of the maximum available power for chassis and inline power for each power supply.

Available Power for Power Supplies

[Table 28-1](#) lists the power that is provided by the power supplies for the Catalyst 4500 series switches.

*CISCO Confidential - DRAFT***Table 28-1 Available Power**

Power Supply	Redundant Mode (W)	Combined Mode (W)
1000 W AC	Chassis ¹ = 1000 Inline = 0	Chassis = 1667 Inline = 0
1300 W AC ²	Chassis (max) = 1000 Inline (max) = 800 Chassis + inline + backplane ≤ 1300	Chassis (min) = 767 Chassis (max) = 1667 Inline (min) = 433 Inline (max) = 1333 Chassis + inline + backplane ≤ 2166
1400 W DC ³	Chassis (min) = 200 Chassis (max) = 1360 Inline (max) ⁴ = (DC input ⁵ – [Chassis (min) + backplane] / 0.75) * 0.96	N/A
2800 W AC	Chassis = 1360 In-line = 1400	Chassis = 2473 Inline = 2545

1. The chassis power includes power for the supervisor engine(s), all line cards, and the fan tray.
2. The backplane consumes 10 W in both redundant and combined mode.
3. The backplane consumes 10 W in redundant mode.
4. 0.75 is the efficiency for the 1400 W DC power supply. 0.96 applied to inline power.
5. The DC input can vary for the 1400 W DC power supply and is configurable. For more information, see the [“Power Management Limitations” section on page 28-4](#).

Power Management Limitations

This section describes the power-management limitations for the Catalyst 4500 series switches.



Note

To compute the power requirements for your system and verify that your system has enough power, add the power that is consumed by the supervisor engine module(s), the fan trays, and the installed modules (including inline power). For more information, see the [“Power Consumption for Modules” section on page 28-9](#).

- You can set the power requirements for the installed modules to exceed the power that is provided by the power supplies.
- If you insert a single power supply into the switch and then set combined mode, the switch displays this message:

Insufficient power supplies present for specified configuration.
- Combined mode requires that you install two power supplies in your switch. If you have only one power supply, and you set the switch to combined mode, the switch places each module in reset mode.
- If the power requirements for the installed modules exceed the power that is provided by the power supplies, the switch displays this message:

CISCO Confidential - DRAFT

Insufficient power available for the current chassis configuration.

- If you try to insert additional modules that exceed the power of the power supplies into the switch, the switch places the newly inserted module into reset mode and displays this message:
`Module has been inserted and Insufficient power supplies operating.`
- If you power down a switch, and you insert an additional module or change the module configuration so that the power requirements exceed the available power, when you power on the switch again, one or more modules are placed in reset mode.
- If too many powered devices are drawing power from the system, the power to the devices is cut and some devices may power down.

**Note**

A module in the reset mode continues to draw power as long as it is installed in the chassis.

1400 W DC Power Supply Guidelines and Restrictions

This section describes the guidelines and restrictions for using a 1400 W DC power supply in the Catalyst 4500 series switches:

**Caution**

Do not use the 1400 W DC power supply with any other power supply, even for a hot swap or other short-term emergency, because you can seriously damage your switch.

- The 1400 W DC power supply works with a variety of DC sources. The DC input can vary from 300 W to 7500 W. Refer to the power supply documentation that shipped with your power supply for additional information.
- Supervisor Engine II cannot detect the DC source that is plugged into the 1400 W DC power supply. If you use the 1400 W DC power supply with Supervisor Engine II, use the **set power dcinput** command to set the DC input power. For more information, refer to the *Catalyst 4500 Series, Catalyst 2948G, and Catalyst 2980G Switches Command Reference*.
- Software automatically adjusts between system power (for modules, backplane, and fans) and inline power. The inline power is 96 percent efficient, and system power has only 75 percent efficiency. For example, each 120 W of system power requires 160 W from the DC input.
- The 1400 W DC power supply does not support combined mode. If you set the power budget to 2 (combined mode), the switch disregards the setting and remains in redundant mode.
- The 1400 W DC power supply has a separate power on/off switch for inline power. The power supply fan status is tied to the power supply status so that the status of the inline power switch can be reported to software. If the power supply fan fails, the display shows the power as faulty, even if the main power is working properly.

CISCO Confidential - DRAFT

Understanding How Power Management Works on the Catalyst 4006 Switch

These sections describe how to manage power for the Catalyst 4006 switch.

**Note**

For more information on power management for the Catalyst 4500 series switches, see the [“Understanding How Power Management Works on the Catalyst 4500 Series Switches”](#) section on page 28-1.

The power management feature for the Catalyst 4000 series switches support a limited module configuration on a reduced number of power supplies.

The Catalyst 4000 series switch chassis supports only the 400 W AC, 400 W DC, and 650 W DC power supplies and allows you to use AC-input and DC-input power supplies in the same chassis. In systems with redundant power supplies, both power supplies should have the same wattage. If you use a 400 W power supply and a 650 W power supply, the switch acts as if there were two 400 W power supplies. For more information, refer to the *Catalyst 4000 Series Switch Installation Guide*.

Understanding Power Redundancy

The Catalyst 4006 switch contains holding bays for up to three power supplies. You need two primary power supplies to operate a fully loaded Catalyst 4006 chassis. You can set the power redundancy to two primary plus one redundant power supply (2+1 redundancy mode) or to one primary plus one redundant power supply (1+1 redundancy mode). The 1+1 redundancy mode might not support a fully loaded chassis.

If your switch has only two power supplies and is in 2+1 redundancy mode (the default mode), there is no redundancy. You can create redundancy with only two power supplies by setting the power redundancy to operate in 1+1 redundancy mode (one primary plus one redundant power supply). However, 1+1 redundancy will not support all configurations.

The modules for the Catalyst 4006 switch have different power requirements; some switch configurations require more power than 1+1 redundancy mode (a single power supply) can provide. In those configurations, redundancy requires three power supplies.

The 1+1 redundancy mode is designed and optimized for these hardware configurations:

- One Catalyst 4006 chassis with a WS-X4013 supervisor engine with two 400 W power supplies (in 1+1 redundancy mode) and four WS-X4148-RJ or WS-X4148-RJ21 modules
- One Catalyst 4006 chassis with a WS-X4013 supervisor engine with two 650 W power supplies (in 1+1 redundancy mode) and five WS-X4148-RJ or WS-X4148-RJ21 modules

Although other configurations are possible, we do not recommend that you use them without carefully considering the power usage of the system. For example, other similar and possible configurations may consist of four modules that consume less power, and the total module power usage does not exceed the absolute maximum power usage for the system.

The supervisor engine uses 110 W and the fan tray uses 25 W. The total load for the modules, the supervisor engine, and the fan cannot total more than the power that is supplied by the power supply. The 1+1 redundancy mode might not support a fully loaded chassis. You may need to leave one slot of the chassis empty. An attempt to use five modules risks an oversubscription of available power.

CISCO Confidential - DRAFT

If you choose to use the 1+1 redundancy mode, the type and number of modules that are supported are limited by the power that is available from a single power supply. To determine the power consumption for each module in your chassis, see the [“Power Consumption for Modules” section on page 28-9](#).

To choose a 1+1 redundancy configuration, you must change the system configuration from the default 2+1 redundancy mode to 1+1 redundancy mode by using the **set power budget** command. Use the **set power budget 1** command to set the power budget to accommodate a 1+1 redundancy mode. In the 1+1 redundancy mode, the nonredundant power available to the system is the power of a single power supply. The second power supply provides full redundancy.

1+1 Redundancy Mode Guidelines and Restrictions

This section describes the guidelines and restrictions for the 1+1 redundancy mode in the Catalyst 4006 switch:

- To compute the power requirements for your system and verify that your system has enough power, add up the power that is consumed by the supervisor engine module, the fan tray, and the installed modules. See the [“Power Consumption for Modules” section on page 28-9](#) for more information on the power consumption for the various components of your switch.
- A module in reset mode continues to draw power as long as it is installed in the chassis; however, the module is not shown in the **show module** command output, because the system considers it removed.
- A single power supply provides 400 W or 650 W. Two 400 W power supplies provide 750 W. Two 650 W power supplies supply only 750 W; this power supply cooling capacity restriction applies to the Catalyst 4006 switch.
- When considering the 1+1 redundancy mode, you must carefully plan the configuration of the module power usage of your chassis. An incorrect configuration will disrupt your system during the evaluation cycle. To avoid a disruption, ensure that your configuration is within the power limits, or return to the default 2+1 redundancy configuration by installing a third power supply in your switch and set the power budget to 2+1 redundancy mode.
- Use the **set power budget 2** command to set the power budget to the 2+1 redundancy mode.

1+1 Redundancy Mode Limitations

This section describes the 1+1 redundancy mode limitations for the Catalyst 4006 switch.

If you try to configure the switch to operate in 1+1 redundancy mode, and you have more modules that are installed in the chassis than a single power supply can handle, the switch displays this message:

```
Insufficient power supplies for the specified configuration.
```

If you are already operating in 1+1 redundancy mode with a valid module configuration and you try to insert additional modules that require more power than the single power supply provides, the switch places the newly inserted module into reset mode and displays this message:

```
Module has been inserted and Insufficient power supplies operating.
```

If you power down a chassis that has been operating in 1+1 redundancy mode with a valid module configuration, and you insert a module or change the module configuration inappropriately and power on the switch again, the module(s) in the chassis (at boot up) that require more power than is available, are placed into reset mode.

CISCO Confidential - DRAFT

These scenarios initiate the five-minute evaluation countdown timer. When this timer runs out, the switch tries to resolve this power limitation by evaluating the type and number of modules that are installed. The evaluation process may require several cycles to stabilize the chassis' power usage.

During the evaluation cycle, the modules are removed and reinserted, thus disrupting network connectivity. The switch reactivates only the modules that it is able to support with the limited power available and leaves the remaining modules in reset mode. The supervisor engine always remains enabled. Modules that are placed in reset mode still consume some power. If the chassis module combination and the modules in reset mode still require more power than is available, the timer starts again, and additional modules are placed into reset mode until the power usage is stable.

If the power requirement of the active modules and the modules in reset do not exceed the available power, the switch is stable and no more evaluation cycles are run, until something again causes insufficient power usage. One or two cycles are required to stabilize the switch. If you configure the chassis correctly, the switch does not enter the evaluation cycle.

**Note**

If all three power supplies are installed in your Catalyst 4006 switch and you set 1+1 redundancy mode but later add additional modules that exceed the power available, the timer starts again. The switch may require several evaluation cycles to stabilize the system. You can either remove the extra modules or change the power budget to 2+1 redundancy mode. If you change to 2+1 redundancy mode, each module in reset mode is brought up one at a time to an operational state.

If you use a 400 W power supply and a 650 W power supply in your switch, the switch acts as if there were two 400 W power supplies.

If you have one 400 W power supply and one 650 W power supply in 1+1 redundancy mode, and a second 650 W power supply is set as the backup, the switch acts as if there were a total of 400 W. If the 400 W power supply fails, the backup 650 W power supply comes into service; however, the switch still has only 400 W available. You must remove the failed 400 W power supply so that the switch can use the available 650 W.

The following configuration requires a minimum of 395 W:

- WS-X4013 supervisor engine—110 W
- Four WS-X4148-RJ modules—65W each (260 W total—the optimized module configuration)
- Fan tray—25 W

The following configuration requires more power than a single 400 W power supply can provide. It requires 445 W and cannot be used in 1+1 redundancy mode for a 400 W power supply. A single 650 W power supply provides enough power for 1+1 redundancy mode for this configuration.

- WS-X4013 supervisor engine—110 W
- Two WS-X4148-RJ modules in slots 2 and 3—65 W each (130 W total)
- Two WS-X4448-GB-LX modules in slots 4 and 5—90 W each (180 W total)
- Fan tray—25 W

The following configuration requires more power than either a single 400 W or 650 W power supply can provide. It requires 735 W and cannot be used in 1+1 redundancy mode for either a 400 W or 650 W power supply.

- WS-X4013 supervisor engine—110 W
- Five 48-port 100BASE-FX modules in slots 2 through 6—120 W each (600 W total)
- Fan tray—25 W

CISCO Confidential - DRAFT

Power Consumption for Modules

Table 28-2 lists how much power is consumed by the components on the Catalyst 4500 series and the Catalyst 4006 switch. See Table 28-2.

Table 28-2 Power Consumption for Catalyst 4500 Series and 4000 Series Components

Module	Power Consumed During Operation (W)	Power Consumed in Reset Mode (W)
Supervisor Engine II	110	110
Catalyst 4003 and 4006 fan tray	25	25
Catalyst 4503 fan tray	30	30
Catalyst 4506 fan tray	50	50
Catalyst 4003 and 4006 switch backplane	0	0
Catalyst 4503 switch backplane	10	10
Catalyst 4506 switch backplane	10	10
6-port 1000BASE-X (GBIC) Gigabit Ethernet WS-X4306-GB	35	30
32-port 10/100 Fast Ethernet RJ-45 WS-X4232-RJ-XX	50	35
Catalyst 4000 Access Gateway Module with IP/FW IOS WS-X4604-GWY	120	60
24-port 100BASE-FX Fast Ethernet switching module WS-X4124-FX-MT	90	75
32-port 10/100 Fast Ethernet RJ-45, plus 2-port 1000BASE-X (GBIC) Gigabit Ethernet WS-4232-GB-RJ	55	35
48-port 100BASE-FX Fast Ethernet switching module WS-4148-FX-MT	120	10
18-port server switching 1000BASE-X (GBIC) Gigabit Ethernet WS-4418-GB	80	50
Catalyst 4006 Backplane Channel Module WS-X4019	10	10
48-port 10/100 Fast Ethernet RJ-45 WS-X4148-RJ	65	40
Catalyst 4003 and 4006 Layer 3 Services Module WS-X4232-L3	120	70
12-port 1000BASE-T Gigabit Ethernet, plus 2-port 1000BASE-X (GBIC) Gigabit Ethernet WS-X4416	110	70
24-port 1000BASE-X Gigabit Ethernet WS-X4424-GB-RJ45	90	50
48-port 1000BASE-X Gigabit Ethernet WS-X4448-GB-RJ45	120	72

*CISCO Confidential - DRAFT***Table 28-2 Power Consumption for Catalyst 4500 Series and 4000 Series Components (continued)**

Module	Power Consumed During Operation (W)	Power Consumed in Reset Mode (W)
48-port 1000BASE-X Gigabit Ethernet WS-X4448-GB-LX	90	50
48-port Telco 10/100BASE-TX switching module WS-X4148-RJ21	65	40
48-port inline power 10/100BASE-TX switching module WS-X4148-RJ45V	60	50
4-port MT-RJ uplink module WS-U4504-FX-MT	10	10
48-port MT-RJ 100BASE-LX switching module WS-X4148-FE-LX-MT	88	10
48-port 10/100/1000BASE-T switching module WS-X4548-GB-RJ45	58	15
2-port 1000BASE-X (GBIC) Gigabit Ethernet WS-X4302-GB	35	30

Migrating a Supervisor Engine II from a Catalyst 4006 Switch to a Catalyst 4500 Series Switch

If you migrate a Supervisor Engine II from a Catalyst 4006 switch to a Catalyst 4503 or 4506 switch, save your configuration and reload the configuration file after you insert the supervisor engine into the Catalyst 4500 series chassis.

The Catalyst 4006 switch has 1024 MAC addresses that you can use as bridge identifiers; the Catalyst 4500 series switches have 64 MAC addresses. MAC address reduction is always enabled on the Catalyst 4500 series switches; however, MAC address reduction may or may not be enabled on a Catalyst 4006 switch. This might affect the selection of the root bridge after you migrate your supervisor engine. Here are two scenarios to consider:

- The Catalyst 4006 switch is not a root switch

In this case, the spanning tree topology does not change. If you add a Catalyst 4500 series switch with MAC reduction enabled and a default spanning tree bridge ID priority set to 32,768 to the network, the bridge ID priority of the new switch becomes the bridge ID priority that is added to a system ID extension. The system ID extension, which is the VLAN number, can vary from 1 to 4094. If the switch is in VLAN 1, the new bridge ID priority will be 32,789. Because 32,769 is greater than 32,768, this switch cannot become the root switch.

- The Catalyst 4006 switch is a root switch

In this case, the spanning tree topology may change. If the other switches in the network are not running MAC address reduction, the topology will change after you replace the chassis with a Catalyst 4500 series switch. The bridge ID priority of the new Catalyst 4500 series switch increments in the same manner as in the previous scenario (bridge ID priority + VLAN number). If the switch is in VLAN 1, the new bridge ID will be 32,789. Because 32,769 is greater than 32,768, this switch cannot become the root switch. The network designates a new root switch; the spanning tree topology also changes to reflect the new root switch.

CISCO Confidential - DRAFT

If the bridge priority of the Catalyst 4006 switch has been lowered administratively and you use the same configuration in the new Catalyst 4500 series switch, then the switch remains the root switch and the spanning tree topology does not change.

Understanding How Inline Power Works

The Catalyst 4006 switch and the Catalyst 4500 series switches can sense if a powered device is connected to an inline power module. The Catalyst 4006 switch and the Catalyst 4500 series switches can supply inline power to the powered device if there is no power on the circuit. The powered device can also be connected to an AC power source and supply its own power to the voice circuit. If there is power on the circuit, the switch does not supply it.


Note

A powered device is any device that is connected to the switch that requires external power or can utilize inline power. An access point or IP phone is an example of this device type.

Table 28-3 lists the switch components that support inline power.

Table 28-3 Switch Components Supporting Inline Power

Switch Chassis	Modules	Power Supplies
Catalyst 4006	WS-X4148-RJ45V	Catalyst 4000 Series Power Entry Module (PEM)
Catalyst 4503 Catalyst 4506	WS-X4148-RJ45V	1300 W AC 2800 W AC 1400 W DC

You can configure the switch not to supply power to the powered device and to disable the detection mechanism. If your switch has a module that can provide inline power to end stations, you can set each port on the module to detect and apply inline power automatically if the end station requires power.


Note

For information on powering powered devices that are connected to other Catalyst switching modules, refer to the *Catalyst Family Inline-Power Patch Panel Installation Note*.

You can power only one device for each port; you must connect the phone directly to the switch port. If you daisy chain a second phone off the phone that is connected to the switch port, the switch cannot power the second phone.

The WS-X4148-RJ45V switching modules can supply a maximum of 6.3 W per port and is 100% efficient.

To determine the power requirements for your configuration, you need to estimate the following:

- Power requirements for all powered devices for the entire switch and for each module.
- Maximum power that is available per port for each module.
- Total available inline power available for the switch (see [Table 28-1 on page 28-4](#) and the PEM documentation).
- When using variable power supplies, consider the required system power (see [Table 28-2 on page 28-9](#)).

CISCO Confidential - DRAFT

Inline Power Management Modes

Each port is configured through the CLI, SNMP, or a configuration file in one of the following modes (configured through the **set port inlinepower** CLI command):

- **Auto**—The supervisor engine directs the switching module to power up the port *only* if the switching module discovers that the phone and the switch have enough power. You can specify the maximum wattage that is allowed on the port. If you do not specify a wattage, then the switch delivers no more than the hardware-supported maximum value.
- **Static**—The supervisor engine directs the switching module to power up the port to the wattage you specify *only* if the switching module discovers the phone. You can specify the maximum wattage that is allowed on the port. If you do not specify a wattage, then the switch allows the hardware-supported maximum value. The maximum wattage, whether determined by the switch or specified by you, is preallocated to the port. If the switch does not have enough power for the allocation, the command will fail.
- **Off**—The supervisor engine does not direct the switching module to power up the port even if an unpowered phone is connected.

Each port has a status that is defined as one of the following:

- **on**—Power is supplied by the port.
- **off**—The power is not supplied by the port.
- **Power-deny**—The supervisor engine does not have enough power to allocate to the port, or the power that is configured for the port is less than the power that is required by the port. The power is not being supplied by the port.
- **err-disable**—The port cannot provide power to the connected device that is configured in Static mode.
- **faulty**—The port failed diagnostic tests.

Power Requirements

This section provides information about the power requirements for the powered devices.

Each powered device has different power requirements. [Table 28-4](#) lists the power requirements for the different classes of IP phones and several other powered devices. The supervisor engine initially calculates the power allocation for each port based on the per-port configuration, and default power allocation. If the correct amount of power is determined from the CDP messaging with the Cisco-powered device, the supervisor engine reduces or increases the allocated power for any ports that are set to Auto mode. Allocated power is not adjusted for ports that are set to Static mode.

For example, the default allocated power is 7 W for a Cisco IP Phone requiring 6.3 W. 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 if the port is set to Auto mode.

Table 28-4 Power Requirements for Some Powered Devices

Device	Required Power (W)
Cisco legacy IP phone	6.3
Cisco + IEEE IP phone	7

*CISCO Confidential - DRAFT***Table 28-4 Power Requirements for Some Powered Devices (continued)**

Device	Required Power (W)
Cisco high power powered device	15.4
Cisco Aironet 1200 Access Point with 802.11a and 802.11b radio installed	11

Wall-Powered Phones

When a wall-powered phone is present on a switching module port, the switching module cannot detect its presence. The supervisor engine discovers the phone through CDP messaging with the port. If the phone supports inline power (the supervisor engine determines this through CDP), and the mode is set to Auto, Static, or Off, the supervisor engine does not attempt to power on the port. If a power outage occurs, and the mode is set to Auto, the phone loses power, but the switching module discovers the phone and informs the supervisor engine, which then applies inline power to the phone. If a power outage occurs, and the mode is set to Static, the phone loses power, but the switching module discovers the phone and applies the preallocated inline power to the phone.

Powering Off the Phone

The supervisor engine can turn off power to a specific port by sending a message to the switching module. The power for a port in Auto mode is then added back to the available system power. Power for ports in Static mode is not added back to the available system power. This situation occurs only when you power off the phone through the CLI or SNMP.

Phone Removal

The switching module informs the supervisor engine if a *powered* phone is removed using a link-down message. The supervisor engine then adds the allocated power for that port back to the available inline power if the port is in Auto mode.

In addition, the switching module informs the supervisor engine if an *unpowered* phone is removed.

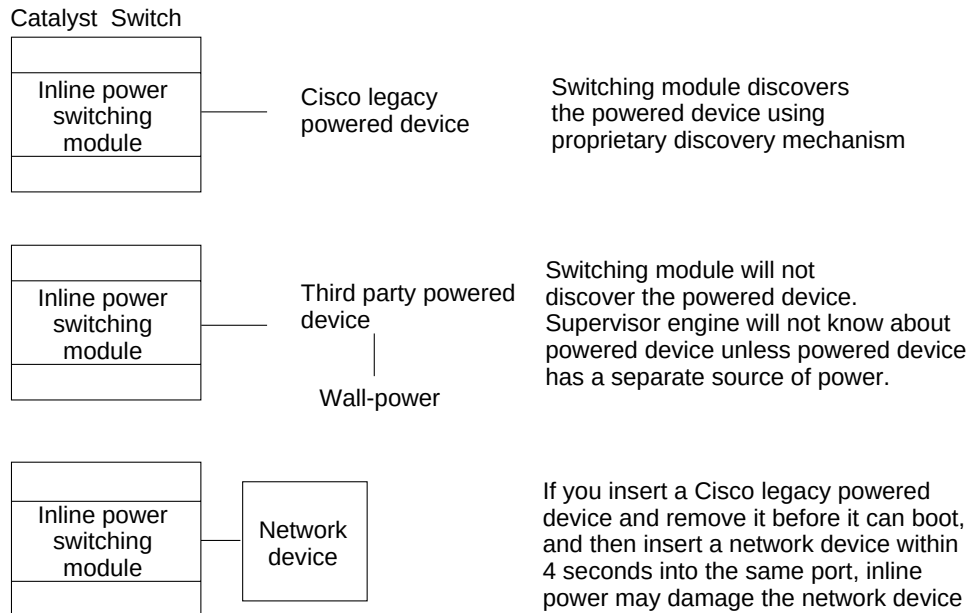
**Caution**

When you plug a Cisco IP phone into a port and turn the power on, the supervisor engine waits 4 seconds for the link to go up on the line. During this time, if you unplug the phone cable and plug in a network device, you could damage the device. We recommend that you wait at least 10 seconds between unplugging a device and plugging in a new device. .

Phone Detection Summary

Figure 28-1 shows how the system detects a phone that is connected to a Catalyst 4006 switch or a Catalyst 4500 series switch port.

Figure 28-1 Power Detection Summary



94285

Configuring Power Management

These sections describe how to configure power management on the Catalyst 4500 series switches and the Catalyst 4006 switch.



Note

The tasks in these sections apply to only the Catalyst 4500 series and Catalyst 4006 switches unless otherwise noted.

Setting Redundant Mode for the Catalyst 4500 Series Switches

To set redundant mode on the Catalyst 4500 series switch, perform this task in privileged mode:

	Task	Command
Step 1	Set the system power management mode to redundant mode.	set power budget 1
Step 2	Verify the system power management mode and the current power usage for the switch.	show environment power

CISCO Confidential - DRAFT

This example shows how to configure the power management mode to redundant:

```

Console>(enable) set power budget 1
Console> (enable) show environment power
Total Inline Power Available: 774.00 Watts (15.48 Amps @50V)
Total Inline Power Drawn From the System: 62.00 Watts ( 1.24 Amps @50V)
Remaining Inline Power in the System: 696.50 Watts (13.93 Amps @50V)
Configured Default Inline Power allocation per port: 15.400 Watts (0.30 Amps @50V)
Module Total Allocated Max H/W Supported Max H/W Supported
To Module (Watts) Per Module (Watts) Per Port (Watts)
-----
2 31.00 836.00 15.400
3 31.00 836.00 15.400
DC Power supplies are configured for 2500Watts DC input
Power Budget is : 1 supply
Power Available to the System (excluding voice power): 1000 Watts (83.33 Amps @12V)
Power Drawn from the System (excluding voice power): 516 Watts (43.00 Amps @12V)
Remaining Power (excluding voice power): 484 Watts (40.33 Amps @12V)
Console>(enable)

```

Setting Combined Mode on the Catalyst 4500 Series Switches

To set combined mode on the Catalyst 4500 series switch, perform this task in privileged mode:

	Task	Command
Step 1	Set the system power management mode to combined mode.	set power budget 2
Step 2	Verify the system power management mode and the current power usage for the switch.	show environment power

This example shows how to configure the power management mode to combined mode:

```

Console>(enable) set power bidget 2
Console> (enable) show environment power
Total Inline Power Available: 1333.00 Watts (26.66 Amps @50V)
Total Inline Power Drawn From the System: 62.00 Watts ( 1.24 Amps @50V)
Remaining Inline Power in the System: 1255.50 Watts (25.11 Amps @50V)
Configured Default Inline Power allocation per port: 15.400 Watts (0.30 Amps @50V)
Module Total Allocated Max H/W Supported Max H/W Supported
To Module (Watts) Per Module (Watts) Per Port (Watts)
-----
2 31.00 836.00 15.400
3 31.00 836.00 15.400
DC Power supplies are configured for 2500Watts DC input
Power Budget is : 2 supplies
Power Available to the System (excluding voice power): 1666 Watts (138.83 Amps @12V)
Power Drawn from the System (excluding voice power): 516 Watts (43.00 Amps @12V)
Remaining Power (excluding voice power): 1150 Watts (95.83 Amps @12V)
Console>(enable)

```

Setting the DC Power Input

To set the DC power input for the 1400 W DC power supply, perform this task in privileged mode:

CISCO Confidential - DRAFT

	Task	Command
Step 1	Set the input wattage for the 1400 W DC power supply.	set power dcinput
Step 2	Verify the configuration.	show environment power

This example shows how to set the DC power input to 5000 W and confirm the setting:

```

Console> (enable) set power dcinput 5000
Console> (enable) show enviroment power
Total Inline Power Available: 4166.00 Watts (83.32 Amps @50V)
Total Inline Power Drawn From the System: 0 Watt
Remaining Inline Power in the System: 4166.00 Watts (83.32 Amps @50V)
Configured Default Inline Power allocation per port: 6.00 Watts (0.12 Amps @50V)
Module Total Allocated Max H/W Supported Max H/W Supported
To Module (Watts) Per Module (Watts) Per Port (Watts)
-----
2 0.00 830.562 15.400
3 0.00 830.562 15.400
4 0.00 830.562 15.400
5 0.00 830.562 15.400
6 0.00 830.562 15.400
DC Power supplies are configured for 5000Watts DC input
Power Budget is : 1 supply
Power Available to the System (excluding voice power): 1360 Watts (113.33 Amps @
12V)
Power Drawn from the System (excluding voice power): 485 Watts (40.42 Amps @12V)
Remaining Power (excluding voice power): 875 Watts (72.92 Amps @12V)
Console> (enable)

```

Setting the Power Budget for the Catalyst 4006 Switch

To set the power budget for the Catalyst 4006 switch, perform this task in privileged mode:

	Task	Command
Step 1	Set the power budget for the Catalyst 4006 switch.	set power budget {1 2}
Step 2	Verify the power budget and the current power usage for the switch.	show environment power

This example shows how to set the power budget to 1 (1+1 redundancy mode), and display the power budget and current power usage for the switch:

```

Console> (enable) set power budget 1
Warning:
Your power supply budget will be constrained to
the power available from only one power supply.
Do you want to continue? [confirm (y/n)]:y
Console> (enable) show environment power
Total Inline Power Available:0 Watt
Total Inline Power Drawn From the System:0 Watt
Remaining Inline Power in the System:0 Watt
Default Inline Power allocation per port:6.00 Watts (0.11 Amps @51V)

Module          Inline Power Allocated(mA)
-----
1                0
2                0

```

CISCO Confidential - DRAFT

3 0

```

➔ Power Budget is :2 supplies
Power Available to the System (excluding voice power):750 Watts (62.06 Amps
@12V)
Power Drawn from the System (excluding voice power):265 Watts (22.01 Amps
@12V)
Remaining Power (excluding voice power):485 Watts (40.05 Amps @12V)
Console> (enable)

```

Displaying System Information

To display information on the power supplies installed in the chassis and other chassis information, perform this task:

Task	Command
Display system information.	show system

This example shows how to display the output for the **show system** command with mixed power supplies:

```

Switch# show system
PS1-Status PS2-Status
-----
➔ ok          err-disable

Fan-Status Temp-Alarm Sys-Status Uptime d,h:m:s Logout
-----
ok          off          ok          74,23:42:50    20 min

PS1-Type          PS2-Type
-----
➔ PWR-C45-2800AC  PWR-C45-1000AC

Modem  Baud  Traffic Peak Peak-Time
-----
disable 9600 0%      0% Fri May 31 2002, 10:24:04

Power Capacity of the Chassis: 1 supply

System Name          System Location          System Contact          CC
-----
Switch#

```

CISCO Confidential - DRAFT

Migrating a Supervisor Engine II from a Catalyst 4006 Switch to a Catalyst 4500 Series Switch

To migrate your supervisor engine from a Catalyst 4006 switch to a Catalyst 4503 or 4506 switch, perform this task:

	Task	Command
Step 1	Change the nondefault configuration mode to text and specify the configuration file to use at boot up.	set config mode text bootflash:switch.cfg
Step 2	Save the current nondefault configuration to NVRAM.	write memory
Step 3	Save the configuration on the Catalyst 4006 switch.	copy config flash
Step 4	Remove the supervisor engine from the Catalyst 4006 switch and insert it into the Catalyst 4500 series switch.	
Step 5	Clear the current configuration.	clear config all
Step 6	Load the saved configuration.	configure bootflash:switch.cfg
Step 7	If you have only one power supply in your Catalyst 4506 switch, set the power budget to 1. If you have two power supplies, set the power budget to 2.	set power budget 1

Configuring Inline Power

These sections show how to configure inline power for the Catalyst 4500 series switches and the Catalyst 4006 switch.

Setting the Power Mode of a Port or Group of Ports

To set the power mode of a port or group of ports, perform this task in privileged mode:

Task	Command
Set the power mode of a port or group of ports.	set port inlinepower mod/port {[auto static] [max-wattage] off}

This example shows how to set the power mode of a port or group of ports:

```
Console> (enable) set port inlinepower 2/5 off
Inline power for port 2/5 set to off.
```

This example shows how to set the maximum wattage allowed for ports 2/3-9 to not exceed 800 mW:

```
Console> (enable) set port inlinepower 2/3-9 800
Inline power for ports 2/3-9 set to auto and max-wattage to 800 mWatt.
Console> (enable)
```


CISCO Confidential - DRAFT

Setting the Default Power Allocation for a Port

To set the default power allocation for each port, perform this task in privileged mode:

Task	Command
Set the default power allocation for each port.	set inlinepower defaultallocation <i>value</i>

This example shows how to set the default power allocation for a port:

```
Console> (enable) set inlinepower defaultallocation 9500
Default inline power allocation set to 9500 mWatt per applicable port.
Console> (enable)
```

Displaying the Power Status for Modules and Individual Ports

To display the power status for modules and individual ports, perform this task in normal mode:

Task	Command
Display the power status for individual ports.	show port inlinepower [<i>mod[/port]</i>]

This example shows how to display the power status for modules and individual ports:

```
Console> show port inlinepower 6/1
Configured Default Inline Power allocation per port:15.400 Watts (0.36 Amps @42V)
Total inline power drawn by module 6: 26.46 Watts ( 0.63 Amps @42V)

Port      InlinePowered      PowerAllocated Device      IEEE class DiscoverMode
Admin Oper   Detected mWatt mA @42V
-----
6/1  static on       yes      5040 120      Cisco      None      cisco

Port Maximum Power      Actual Consumption absentCounter OverCurrent
      mWatt   mA @42V      mWatt   mA @42V
-----
6/1  5200    123      5000    119      0          0
Console> (enable)
```

CISCO Confidential - DRAFT



Configuring VoIP

This chapter describes how to configure voice-over-IP (VOIP) for the Catalyst 4500 series switches. This chapter consists of these major sections:

- [Hardware and Software Requirements, page 29-1](#)
- [Overview of IP Phones, page 29-2](#)
- [Configuring VoIP on a Switch, page 29-3](#)

Hardware and Software Requirements

The hardware and software requirements for the Catalyst 4500 series switches and Cisco CallManager are as follows:

- Catalyst 4006, Catalyst 4500 series, Catalyst 5000 family, and Catalyst 6500 series switches running supervisor engine software release 6.1(1) or later releases
- Catalyst 4006, Catalyst 4500 series, and Catalyst 6500 series switches running supervisor engine software release 7.7(1) or later releases for IEEE 802.3af compliance
- Cisco CallManager release 3.0 or later releases
- If you want to utilize inline power, [Table 29-1](#) lists the Catalyst 4000 family components that support inline power.

Table 29-1 Catalyst 4000 Family Components Supporting Inline Power

Switch Chassis	Modules	Power Supplies
Catalyst 4006	WS-X4148-RJ45V ¹	Catalyst 4000 Family Power Entry Module (PEM)
Catalyst 4503 Catalyst 4506	WS-X4148-RJ45V	1300 W AC 2800 W AC 1400 W DC

1. The Catalyst 4006 switch can only provide a maximum 400 W of inline power per module.

- If you do not want to utilize inline power, then you can plug a powered device, with an external power source, into any 10/100 or 10/100/1000 switching module.

Overview of IP Phones

Catalyst 4000, 4500, 2948G, or 2980G series switches can connect to an IP phone and carry IP voice traffic. If necessary, the switch can supply electrical power to the circuit connecting it to an IP phone.

Cisco classifies three types of IP phones based on the discovery methods used to discover the phone:

- Legacy Cisco IP Phone—uses Cisco proprietary discovery method to detect an IP phone, and uses "link disconnect" to verify an IP phone has been removed from the network
- Cisco/IEEE 802.3af compliant—uses enhanced CDP and /or IEEE 802.3af to discover and remove an IP phone
- Third party IEEE 802.3af compliant—uses IEEE 802.3af specified "detection of phone" to detect an IP phone and "detection of phone removed" to verify an IP phone has been removed from the network.

An IP phone contains an integrated three-port 10/100 switch. The ports are dedicated connections as described below:

- Port 1 connects to the switch or other device that supports voice-over-IP.
- Port 2 is an internal 10/100 interface that carries the phone traffic.
- Port 3 connects to a PC or other device.

Figure 29-1 shows one way to configure a IP phone.

Figure 29-1 IP phone Connected to a Catalyst 4000 Family Switch



When the IP phone connects to a 10/100 port on the Catalyst 4500 series switch, the *access port* (PC-to-phone jack) of the IP phone can be used to connect a PC.

Packets to and from the PC and to and from the phone share the same physical link to the switch and the same port of the switch.

Introducing IP-based phones into existing switch-based networks raises the following issues:

- The current VLANs might be configured on an IP subnet basis and additional IP addresses might not be available to assign the phone to a port so that it belongs to the same subnet as other devices (PC) that are connected to the same port.
- Data traffic present on the VLAN supporting phones might reduce the quality of VoIP traffic.

You can resolve these issues by isolating the voice traffic onto a separate VLAN on each of the ports that are connected to a phone. The switch port that is configured for connecting a phone would have separate VLANs that are configured for carrying the following:

- Voice traffic to and from the IP phone (auxiliary VLAN)
- Data traffic to and from the PC that is connected to the switch through the access port of the IP phone (native VLAN)

Isolating the phones on a separate, auxiliary VLAN increases the quality of the voice traffic and allows a large number of phones to be added to an existing network where there are not enough IP addresses. A new VLAN means a new subnet and a new set of IP addresses.

Configuring VoIP on a Switch

In order for an IP phone to work in your voice network, you must do the following:

- Configure the auxiliary VLANs for the port.

For more information on setting the auxiliary VLANs, see [“Configuring Auxiliary VLANs” section on page 10-12](#).

- Configure inline power if necessary.

The Catalyst 4500 series switch senses if it is connected to a Cisco IP phone. A Catalyst 4006 or Catalyst 4500 series switch can supply inline power to an IP phone if there is no power on the circuit. An IP phone can also be connected to an AC power source and supply its own power to the voice circuit. If there is power on the circuit, the switch does not supply it.

You can configure the switch not to supply power to an IP phone and to disable the detection mechanism. See the [“Configuring Inline Power” section on page 30-15](#) for the CLI commands that you can use to supply inline power to an IP phone.

Configuring Switch Access Using AAA

This chapter describes how to configure authentication, authorization, and accounting (AAA) to monitor and control access to the command-line interface (CLI) on the Catalyst enterprise LAN switches.

**Note**

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 4500 Series, Catalyst 2948G, and Catalyst 2980G Switches Command Reference*.

**Note**

For information on configuring 802.1x authentication to restrict unauthorized devices from connecting to a LAN through publicly accessible ports, see [Chapter 31, “Configuring 802.1x Authentication.”](#)

**Note**

For information on configuring ports to allow or restrict traffic based on host MAC addresses, see [Chapter 16, “Configuring Port Security.”](#)

This chapter consists of these sections:

- [Understanding How Authentication Works, page 30-1](#)
- [Configuring Authentication, page 30-8](#)
- [Authentication Example, page 30-39](#)
- [Understanding How Authorization Works, page 30-40](#)
- [Configuring Authorization, page 30-41](#)
- [Authorization Example, page 30-45](#)
- [Understanding How Accounting Works, page 30-46](#)
- [Configuring Accounting, page 30-49](#)
- [Accounting Example, page 30-52](#)

Understanding How Authentication Works

You can configure any combination of these authentication methods to control access to the switch:

- Login authentication
- Local authentication

CISCO Confidential - DRAFT

- Local user authentication
- TACACS+ authentication
- RADIUS authentication
- Kerberos authentication

**Note**

Kerberos authentication does not work if TACACS+ is used as the authentication method.

When local authentication is enabled together with one or more other authentication methods, local authentication is always attempted *last*. However, you can specify different authentication methods for console and Telnet connections. For example, you might use local authentication for console connections and RADIUS authentication for Telnet connections.

The following sections describe how the different authentication methods work.

Understanding How Login Authentication Works

Login authentication increases the security of the system by preventing unauthorized users from guessing the password. The user is allowed only a specific number of attempts to successfully log in to the switch. If the user fails to authorize the password, the system delays any subsequent accesses and captures the user ID and the IP address of the station in the syslog and in the SNMP trap.

You can configure the maximum number of login attempts from the CLI and SNMP with the **set authentication login attempt** command. (You would use the **set authentication enable attempt** command to set login limits for accessing enable mode.) The configurable range is three (default) to ten tries. Setting the limit to zero (0) disables login authentication.

All authentication methods (RADIUS, TACACS+, Kerberos, or local) are supported.

The lockout (delay) time is also configurable from the CLI and SNMP with the **set authentication login lockout** command. (You would use the **set authentication enable lockout <time>** command to set a delay time for accessing enable mode.) The configurable range is 30 to 43,200 seconds; setting the lockout time to zero (0) disables this function.

If you are locked out at the console, the console does not allow you to log in during that lockout time. If you are locked out from a Telnet session, the connection closes when the limit is reached. The switch closes any subsequent access from that station during the lockout time and provides an appropriate notice.

Understanding How Local Authentication Works

Local authentication uses locally configured login and enable passwords to authenticate login attempts. The login and enable passwords are local to each switch and are not mapped to individual usernames.

Local authentication is enabled by default, but can be disabled if one of the other authentication methods is enabled. If local authentication is disabled and you then disable all other authentication methods, local authentication is reenabled automatically.

You can enable local authentication and one or more of the other authentication methods at the same time. Local authentication is only attempted if the other authentication methods fail.

CISCO Confidential - DRAFT

Understanding How Local User Authentication Works

Local user authentication uses local user accounts and passwords that you create to validate the login attempts of local users. Each switch can have a maximum of 25 local user accounts. Before you can enable local user authentication, you must define at least one local user account.

You set up local user accounts by creating a unique username and password combination for each local user. Each username must be fewer than 65 characters and can be any alphanumeric character, at least one of which must be alphabetic.

You configure each local user account with a privilege level; valid privilege levels are 0 or 15. A local user with a privilege level of 0 can access commands in normal mode, while a local user with a privilege level of 15 can access commands in both normal or privileged mode.

Once a local user is logged in, the user can use only commands that are available for that privilege level. A local user can enter privileged mode only if that user enters the correct enable password.

**Note**

If you are running a CiscoView image or are logging in using HTTP login, the system completes its initial authentication using the username and password combination. You can enter privileged mode by either providing the privilege password or using the username and password combination, provided the local user has a privilege level of 15.

Understanding How TACACS+ Authentication Works

TACACS+ is an enhanced version of TACACS, which is a User Datagram Protocol (UDP)-based access-control protocol that is specified by RFC 1492. TACACS+ controls access to network devices by exchanging Network Access Server (NAS) information between a network device and a centralized database to determine the identity of a user or device. TACACS+ uses TCP to ensure reliable delivery and encrypt all traffic between the TACACS+ server and the TACACS+ daemon on a network device.

TACACS+ works with many authentication types, including fixed password, one-time password, and challenge-response authentication. TACACS+ authentication usually occurs in these instances:

- When you first log onto a machine
- When you send a service request that requires privileged access

When you request privileged or restricted services, TACACS+ encrypts your user password information using the MD5 encryption algorithm and adds a TACACS+ packet header. This header information identifies the packet type being sent (for example, an authentication packet), the packet sequence number, the encryption type used, and the total packet length. The TACACS+ protocol then forwards the packet to the TACACS+ server.

A TACACS+ server can provide authentication, authorization, and accounting functions. These services, while all part of TACACS+, are independent of one another, so that a given TACACS+ configuration can use any or all of the three services.

When the TACACS+ server receives the packet, it does the following:

- Authenticates user information and notifies the client that authentication has either passed or failed.
- Notifies the client that authentication will continue and that the client must provide additional information. This challenge-response process can continue through multiple iterations until authentication either passes or fails.

CISCO Confidential - DRAFT

You can configure a TACACS+ key on the client and server. If you configure a key on the switch, it must be the same as the one that is configured on the TACACS+ servers. The TACACS+ clients and servers use the key to encrypt all TACACS+ transmitted packets. If you do not configure a TACACS+ key, packets are not encrypted. The TACACS+ key must be fewer than 100 characters.

With TACACS+, you can do the following:

- Enable or disable TACACS+ authentication to determine whether a user has permission to access the switch
- Enable or disable TACACS+ authentication to determine whether a user has permission to enter privileged mode
- Specify a key that is used to encrypt the protocol packets
- Specify the server on which the TACACS+ server daemon resides
- Set the number of login attempts that are allowed
- Set the timeout interval for server daemon response
- Enable or disable the directed-request option

TACACS+ authentication is disabled by default. You can enable TACACS+ authentication and local authentication at the same time.

If local authentication is disabled and you then disable all other authentication methods, local authentication is reenabled automatically.

Understanding How RADIUS Authentication Works

RADIUS is a client-server authentication and authorization access protocol that is used by the NAS to authenticate users attempting to connect to a network device. The NAS functions as a client, passing user information to one or more RADIUS servers. The NAS permits or denies network access to a user based on the response it receives from one or more RADIUS servers. RADIUS uses UDP for transport between the RADIUS client and server.

You can configure a RADIUS key on the client and server. If you configure a key on the client, it must be the same as the one that is configured on the RADIUS servers. The RADIUS clients and servers use the key to encrypt all RADIUS transmitted packets. If you do not configure a RADIUS key, packets are not encrypted. The key itself is never transmitted over the network.

**Note**

For more information about the RADIUS protocol, refer to RFC 2138, “Remote Authentication Dial In User Service (RADIUS).”

With RADIUS, you can do the following:

- Enable or disable RADIUS authentication to control login access
- Enable or disable RADIUS authentication to control enable access
- Specify the IP addresses and UDP ports of the RADIUS servers
- Specify the RADIUS key that is used to encrypt RADIUS packets
- Specify the RADIUS server timeout interval
- Specify the RADIUS retransmit count
- Specify the RADIUS server deadtime interval

CISCO Confidential - DRAFT

RADIUS authentication is disabled by default. You can enable RADIUS authentication and other authentication methods at the same time. You can specify which method to use first using the **primary** keyword.

If local authentication is disabled and you then disable all other authentication methods, local authentication is reenabled automatically.

Understanding How Kerberos Authentication Works

Kerberos is a client-server-based secret-key network authentication method that uses a trusted Kerberos server to verify secure access to both services and users. In Kerberos, this trusted server is called the key distribution center (KDC). The KDC issues tickets to validate users and services. A ticket is a temporary set of electronic credentials that verify the identity of a client for a particular service.

These tickets have a limited life span and can be used in place of the standard user password authentication mechanism if a service trusts the Kerberos server from which the ticket was issued. If the standard user password method is used, Kerberos encrypts user passwords into the tickets, ensuring that passwords are not sent on the network in clear text. When you use Kerberos, passwords are not stored on any machine (except for the Kerberos server) for more than a few seconds. Kerberos also guards against intruders who might pick up the encrypted tickets from the network.

Table 30-1 defines terms used in Kerberos.

Table 30-1 Kerberos Terminology

Term	Definition
Kerberized	Applications and services that have been modified to support the Kerberos credential infrastructure.
Kerberos credential	General term referring to authentication tickets, such as ticket granting tickets and service credentials. Kerberos Credentials verify the ticket of a user or service. If a network service decides to trust the Kerberos server that issued the ticket, it can be used in place of retyping in a username and password. Credentials have a default life span of 8 hours.
Kerberos identity	(See Kerberos principal.)
Kerberos principal	Who you are or what a service is according to the Kerberos server. Also known as a Kerberos identity.
Kerberos realm	A domain consisting of users, hosts, and network services that are registered to a Kerberos server. (The Kerberos server is trusted to verify the identity of a user or network service to another user or network service.) Kerberos realms must always be in uppercase characters.
Kerberos server	A daemon running on a network host. Users and network services register their identity with the Kerberos server. Network services query the Kerberos server to authenticate other network services.
Key distribution center (KDC)	A Kerberos server and database program running on a network host that allocates the Kerberos credentials to different users or network services.
Service credential	A credential for a network service. When issued from the KDC, this credential is encrypted with the password that is shared by the network service and the KDC and with the user's TGT.

*CISCO Confidential - DRAFT***Table 30-1 Kerberos Terminology (continued)**

Term	Definition
SRVTAB	A password that a network service shares with the KDC. The network service authenticates an encrypted service credential by using the SRVTAB (also known as a KEYTAB) to decrypt it.
Ticket granting ticket (TGT)	A credential that the KDC issues to authenticated users. When users receive a TGT, they can authenticate network services within the Kerberos realm represented by the KDC.

Telnet clients and servers through both the console and in-band management port can be Kerberized.

**Note**

Kerberos authentication does not work if TACACS+ is used as the authentication mechanism.

**Note**

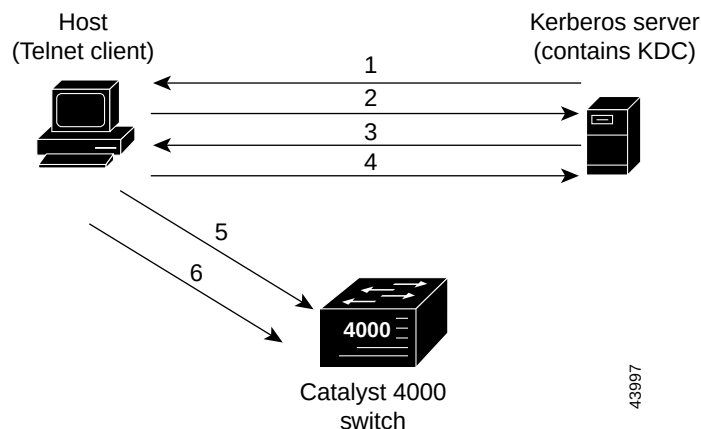
If you are logged in to the console through a modem or a terminal server, you cannot use a Kerberized login procedure.

Using a Kerberized Login Procedure

You can use a Kerberized Telnet session if you are logging in through the in-band management port. After the Telnet client and services have been Kerberized, the following process takes place when a user attempts to Telnet to the switch:

1. The Telnet client asks the user for the username and issues a request for a TGT to the KDC on the Kerberos server.
2. The KDC creates the TGT, which contains the user's identity, the KDC's identity, and the TGT's expiration time. The KDC then encrypts the TGT with the user's password and sends the TGT to the client.
3. When the Telnet client receives the encrypted TGT, it prompts the user for the password. If the Telnet client can decrypt the TGT with the entered password, the user is successfully authenticated to the KDC. The client then builds a service credential request and sends this request to the KDC. This request contains the user's identity and a message saying that it wants to Telnet to the switch. This request is encrypted using the TGT.
4. When the KDC successfully decrypts the service credential request with the TGT that it issued to the client, it builds a service to the switch. The service credential has the client's identity and the identity of the desired Telnet server. The KDC then encrypts the credential with the password that it shares with the switch's Telnet server and encrypts the resulting packet with the Telnet client's TGT and sends this packet to the client.
5. The Telnet client decrypts the packet first with its TGT. If encryption is successful, the client then sends the resulting packet to the switch's Telnet server. At this point, the packet is still encrypted with the password that the switch's Telnet server and the KDC share.
6. If the Telnet client has been instructed to do so, it forwards the TGT to the switch. This ensures that the user does not need to get another TGT in order to use another network service from the switch.

Figure 30-1 illustrates the Kerberos Telnet connection process.

*CISCO Confidential - DRAFT***Figure 30-1 Kerberized Telnet Connection****Using a Non-Kerberized Login Procedure**

If you log into a switch using a non-Kerberized login procedure, the switch takes care of authentication to the KDC on behalf of the login client. However, the user password transfers, in clear text, from the login client to the switch.

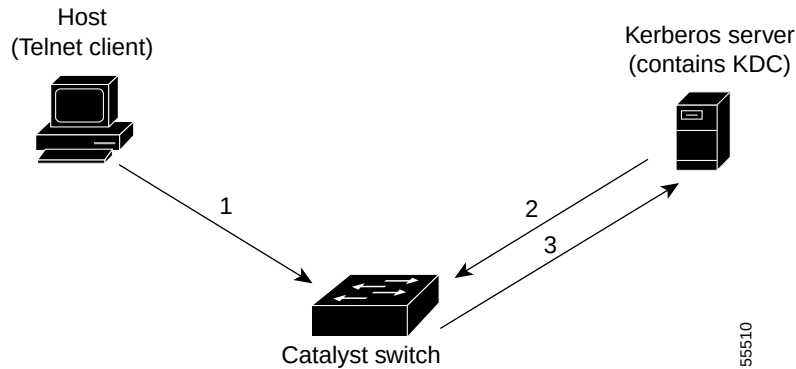
**Note**

You can launch a non-Kerberized login through a modem or terminal server through the inband management port. Telnet does not support non-Kerberized login.

When you launch a non-Kerberized login, the following process takes place:

1. The switch prompts you for a username and password.
2. The switch requests a TGT from the KDC so that you can be authenticated to the switch.
3. The KDC sends an encrypted TGT to the switch, which contains your identity, KDC's identity, and TGT's expiration time.
4. The switch tries to decrypt the TGT with the password that you entered. If the decryption is successful, you are authenticated to the switch.
5. If you want to access other network services, you must contact the KDC directly for authentication. To obtain the TGT, run the program **kinit**, which is the client software that is provided with the Kerberos package.

Figure 30-2 illustrates the non-Kerberized login process.

*CISCO Confidential - DRAFT***Figure 30-2 Non-Kerberized Telnet Connection**

Configuring Authentication

The following sections describe how to configure the different authentication methods.

Authentication Default Configuration

Table 30-2 shows the default configuration for authentication.

Table 30-2 Default Authentication Configuration

Feature	Default
Login authentication (console and Telnet)	Enabled
Local authentication (console and Telnet)	Enabled
Local user authentication	Disabled
TACACS+ login authentication (console and Telnet)	Disabled
TACACS+ enable authentication (console and Telnet)	Disabled
TACACS+ key	None specified
TACACS+ login attempts	3 times
TACACS+ server timeout	5 sec
TACACS+ directed request	Disabled
RADIUS login authentication (console and Telnet)	Disabled
RADIUS enable authentication (console and Telnet)	Disabled
RADIUS server IP address	None specified
RADIUS server UDP auth-port	Port 1812
RADIUS key	None specified
RADIUS server timeout	5 sec
RADIUS server deadtime	0 (servers not marked dead)
RADIUS retransmit attempts	2 times
Kerberos login authentication (console and Telnet)	Disabled

*CISCO Confidential - DRAFT***Table 30-2 Default Authentication Configuration (continued)**

Feature	Default
Kerberos enable authentication (console and Telnet)	Disabled
Kerberos server IP address	None specified
Kerberos DES key	None specified
Kerberos server auth-port	Port 750
Kerberos local-realm name	NULL string
Kerberos credentials forwarding	Disabled
Kerberos clients mandatory	Not mandatory
Kerberos preauthentication	Disabled

Authentication Configuration Guidelines

This section lists the guidelines for configuring authentication on the switch:

- Authentication configuration applies both to console and Telnet connection attempts unless you use the **console** and **telnet** keywords to specify the authentication methods to use for each connection type individually.
- If you configure a RADIUS or TACACS+ key on the switch, make sure that you configure an identical key on the RADIUS or TACACS+ server.
- The TACACS+ key must be less than 100 characters long.
- You must specify a RADIUS or TACACS+ server before enabling RADIUS or TACACS+ on the switch.
- If you configure multiple RADIUS or TACACS+ servers, the first server that you configure is the primary server, and authentication requests are sent to this server first. You can specify a particular server as primary by using the **primary** keyword.
- RADIUS and TACACS+ support one privileged mode only (level 1).
- Kerberos authentication does not work if TACACS+ is also used as an authentication mechanism.
- Before you can enable local user authentication, you must define at least one username.
- Local user accounts and passwords must be fewer than 65 characters and can consist of any alphanumeric characters. Local user accounts must contain at least one alphabetic character.

Configuring Login Authentication

The next two sections describe how to configure login authentication on the switch.

Setting Authentication Login Attempts on the Switch

To set authentication login attempts on the switch, perform this task in privileged mode:

CISCO Confidential - DRAFT

	Task	Command
Step 1	Set authentication login attempts on the switch. Use the console or telnet keywords if you want to enable local authentication only for the console port or for Telnet connection attempts.	set authentication login attempt {count} [console telnet]
Step 2	Enable login lockout time on the switch. Use the console or telnet keywords if you want to enable local authentication only for the console port or for Telnet connection attempts.	set authentication login lockout {time} [console telnet]
Step 3	Verify the local authentication configuration.	show authentication

This example shows how to set the authentication login attempts to 5, set the lockout time for both console and Telnet connections to 50 seconds, and verify the configuration:

```

Console> (enable) set authentication login attempt 5
Login authentication attempts for console and telnet logins set to 5.
Console> (enable) set authentication login lockout 50
Login lockout time for console and telnet logins set to 50.
Console> (enable) show authentication

```

```

Login Authentication: Console Session Telnet Session Http Session
-----
tacacs                disabled          disabled          disabled
radius               disabled          disabled          disabled
kerberos             disabled          disabled          disabled
local                enabled(primary) enabled(primary) enabled(primary)
attempt limit         5                5                -
lockout timeout (sec) 50               50               -

```

```

Enable Authentication: Console Session Telnet Session Http Session
-----
tacacs                disabled          disabled          disabled
radius               disabled          disabled          disabled
kerberos             disabled          disabled          disabled
local                enabled(primary) enabled(primary) enabled(primary)
attempt limit         3                3                -
lockout timeout (sec) disabled          disabled          -
Console> (enable)

```

Setting Authentication Login Attempts for Privileged Mode

To set authentication login attempts for privileged mode, perform this task in privileged mode:

	Task	Command
Step 1	Set authentication login attempts for privileged mode. Enter the console or telnet keywords if you want to enable local authentication only for the console port or for Telnet connection attempts.	set authentication enable attempt {count} [console telnet]

CISCO Confidential - DRAFT

	Task	Command
Step 2	Enable the login lockout time for privileged mode. Enter the console or telnet keywords if you want to enable local authentication only for the console port or for Telnet connection attempts.	set authentication enable lockout {time} [console telnet]
Step 3	Verify the local authentication configuration.	show authentication

This example shows how to set enable mode authentication login attempts to 5, set the enable mode lockout time for both console and Telnet connections to 50 seconds, and verify the configuration:

```
Console> (enable) set authentication enable attempt 5
Enable mode authentication attempts for console and telnet logins set to 5.
Console> (enable) set authentication enable lockout 50
Enable mode lockout time for console and telnet logins set to 50.
Console> (enable) show authentication
```

Login Authentication:	Console Session	Telnet Session	Http Session
-----	-----	-----	-----
tacacs	disabled	disabled	disabled
radius	disabled	disabled	disabled
kerberos	disabled	disabled	disabled
local	enabled(primary)	enabled(primary)	enabled(primary)
attempt limit	5	5	-
lockout timeout (sec)	50	50	-

Enable Authentication:	Console Session	Telnet Session	Http Session
-----	-----	-----	-----
tacacs	disabled	disabled	disabled
radius	disabled	disabled	disabled
kerberos	disabled	disabled	disabled
local	enabled(primary)	enabled(primary)	enabled(primary)
attempt limit	5	5	-
lockout timeout (sec)	50	50	-

```
Console> (enable)
```

Configuring Local Authentication

The following sections describe how to configure local authentication on the switch.

Enabling Local Authentication



Note

Local login and enable authentication are enabled for both console and Telnet connections by default. You do not need to perform these tasks unless you want to modify the default configuration or you have disabled local authentication.

To enable local authentication on the switch, perform this task in privileged mode:

CISCO Confidential - DRAFT

	Task	Command
Step 1	Enable local login authentication on the switch. Enter the console or telnet keywords to enable local authentication only for console or Telnet connection attempts.	set authentication login local enable [all console http telnet]
Step 2	Enable local enable authentication on the switch. Enter the console or telnet keywords to enable local authentication only for console or Telnet connection attempts.	set authentication enable local enable [all console http telnet]
Step 3	Verify the local authentication configuration.	show authentication

This example shows how to enable local login and enable authentication for both console and Telnet connections and how to verify the configuration:

```

Console> (enable) set authentication login local enable
local login authentication set to enable for console and telnet session.
Console> (enable) set authentication enable local enable
local enable authentication set to enable for console and telnet session.
Console> (enable) show authentication

```

```

Login Authentication:  Console Session  Telnet Session
-----
tacacs                disabled      disabled
radius               disabled      disabled
kerberos              disabled      disabled
local                 enabled(primary)  enabled(primary)

```

```

Enable Authentication: Console Session  Telnet Session
-----
tacacs                disabled      disabled
radius               disabled      disabled
kerberos              disabled      disabled
local                 enabled(primary)  enabled(primary)
Console> (enable)

```

Setting the Login Password

The login password controls access to the user mode CLI. Passwords are case sensitive, contain up to 30 characters, and use any printable ASCII characters, including a space.



Note

Passwords that are set in software release 5.3 and earlier releases remain non-case sensitive. You must reset the password after installing software release 5.4 or a later release to activate case sensitivity.

To set the login password for local authentication, perform this task in privileged mode:

Task	Command
Set the login password for access. Enter your old password (press Return on a switch with no password configured), enter your new password, and reenter your new password.	set password

This example shows how to set the login password on the switch:

CISCO Confidential - DRAFT

```

Console> (enable) set password
Enter old password:old_password
Enter new password:new_password
Retype new password:new_password
Password changed.
Console> (enable)

```

Setting the Enable Password

The enable password controls access to the privileged mode CLI. Passwords are case sensitive, contain up to 30 characters, and use any printable ASCII characters, including a space.



Note

Passwords that are set in software release 5.3 and earlier releases remain non-case sensitive. You must reset the password after installing software release 5.4 or a later release to activate case sensitivity.

To set the enable password for local authentication, perform this task in privileged mode:

Task	Command
Set the password for privileged mode. Enter your old password (press Return on a switch with no password configured), enter your new password, and reenter your new password.	set enablepass

This example shows how to set the enable password on the switch:

```

Console> (enable) set enablepass
Enter old password:<old_password>
Enter new password:<new_password>
Retype new password:<new_password>
Password changed.
Console> (enable)

```

Disabling Local Authentication



Caution

Make sure that RADIUS or TACACS+ authentication is configured and operating correctly before disabling local login or enabling authentication. If you disable local authentication when RADIUS or TACACS+ is not correctly configured, or if the RADIUS or TACACS+ server is not online, you may be unable to log in to the switch.

To disable local authentication on the switch, perform this task in privileged mode:

CISCO Confidential - DRAFT

	Task	Command
Step 1	Disable local login authentication on the switch. Enter the console or telnet keywords to disable local authentication only for console or Telnet connection attempts.	set authentication login local disable [all console http telnet]
Step 2	Disable local enable authentication on the switch. Enter the console or telnet keywords to disable local authentication only for console or Telnet connection attempts.	set authentication enable local disable [all console http telnet]
Step 3	Verify the local authentication configuration.	show authentication

This example shows how to disable local login and enable authentication for both console and Telnet connections, and how to verify the configuration (you must have RADIUS or TACACS+ authentication enabled before you disable local authentication):

```
Console> (enable) set authentication login local disable
local login authentication set to disable for console and telnet session.
Console> (enable) set authentication enable local disable
local enable authentication set to disable for console and telnet session.
Console> (enable) show authentication
```

```
Login Authentication: Console Session Telnet Session
-----
tacacs                disabled          disabled
radius                enabled(primary) enabled(primary)
kerberos              disabled          disabled
local                 disabled          disabled
```

```
Enable Authentication: Console Session Telnet Session
-----
tacacs                disabled          disabled
radius                enabled(primary) enabled(primary)
kerberos              disabled          disabled
local                 disabled          disabled
Console> (enable)
```

Recovering a Lost Password

To recover a lost local authentication password, follow these steps. You must complete Steps 3 through Step 7 within 30 seconds of a power cycle or the recovery will fail. If you have lost both the login and enable passwords, repeat the process for each password.

Step 1	Connect to the switch through the supervisor engine console port. You cannot recover the password if you are connected through a Telnet connection.
Step 2	Enter the reset system command to reboot the switch.
Step 3	At the “Enter Password” prompt, press Return . The login password is null for 30 seconds when you are connected to the console port.
Step 4	Enter privileged mode using the enable command.
Step 5	At the “Enter Password” prompt, press Return . The enable password is null for 30 seconds when you are connected to the console port.
Step 6	Enter the set password or set enablepass command, as appropriate.

CISCO Confidential - DRAFT

- Step 7** When prompted for your old password, press **Return**.
- Step 8** Enter and confirm your new password.

Configuring Local User Authentication

The following sections describe how to configure local user authentication authentication on the switch.

Creating a Local User Account

Local user accounts and passwords must be fewer than 65 characters in length and can consist of any alphanumeric characters. Local user accounts must contain at least one alphabetic character.

To create a local user account on the switch, perform this task in privileged mode:

	Task	Command
Step 1	Create a new local user account.	set localuser user <i>username</i> password <i>pwd</i> privilege <i>privilege_level</i>
Step 2	Verify the local user account.	show localusers

This example shows how to create a local user account and password, set the privilege level, and verify the configuration:

```

Console> (enable) set localuser user picard password captain privilege 15
Added local user picard.
Console> (enable) show localusers
Local User Authentication: disabled
Username                               Privilege Level
-----
picard                                15
Console> (enable)

```

Enabling Local User Authentication

To enable local user authentication on the switch, perform this task in privileged mode:

	Task	Command
Step 1	Enable local user authentication.	set localuser authentication enable
Step 2	Verify the local user authentication configuration.	show authentication

This example shows how to create a local user account, enable local user authentication, and verify the configuration:

```

Console> (enable) set localuser authentication enable
Local User Authentication enabled.
Console> (enable) show authentication
Login Authentication:  Console Session  Telnet Session  Http Session
-----
tacacs                disabled        disabled        disabled
radius               disabled        disabled        disabled

```

CISCO Confidential - DRAFT

```

kerberos          disabled          disabled          disabled
local *           enabled(primary)  enabled(primary) enabled(primary)
attempt limit     3                  3                  -
lockout timeout (sec) disabled      disabled          -

Enable Authentication: Console Session  Telnet Session  Http Session
-----
tacacs            disabled            disabled        disabled
radius            disabled            disabled        disabled
kerberos          disabled            disabled        disabled
local *           enabled(primary)    enabled(primary) enabled(primary)
attempt limit     3                  3              -
lockout timeout (sec) disabled        disabled        -
* Local User Authentication enabled.
Console> (enable)

```

Disabling Local User Authentication

To disable local user authentication on the switch, perform this task in privileged mode:

	Task	Command
Step 1	Disable local user authentication.	set localuser authentication disable
Step 2	Verify the local authentication configuration.	show authentication

This example shows how to disable local user authentication for the switch and how to verify the configuration:

```

Console> (enable) set localuser authentication disable
local user authentication set to disable.
Console> (enable) show authentication
Login Authentication: Console Session  Telnet Session  Http Session
-----
tacacs            disabled            disabled        disabled
radius            disabled            disabled        disabled
kerberos          disabled            disabled        disabled
local *           enabled(primary)    enabled(primary) enabled(primary)
attempt limit     3                  3              -
lockout timeout (sec) disabled        disabled        -

Enable Authentication: Console Session  Telnet Session  Http Session
-----
tacacs            disabled            disabled        disabled
radius            disabled            disabled        disabled
kerberos          disabled            disabled        disabled
local *           enabled(primary)    enabled(primary) enabled(primary)
attempt limit     3                  3              -
lockout timeout (sec) disabled        disabled        -
* Local User Authentication disabled.
Console> (enable)

```

Deleting a Local User Account

To delete a local user account on the switch, perform this task in privileged mode:

CISCO Confidential - DRAFT

	Task	Command
Step 1	Delete a local user account.	clear localuser picard
Step 2	Verify that the local user account has been deleted.	show localusers

This example shows how to disable local user authentication for the switch and how to verify the configuration:

```
Console> (enable) clear localuser number1
```

```
Console> (enable) show localusers
Username                               Privilege Level
-----                               -
picard                                15
Console> (enable)
```

Configuring TACACS+ Authentication

The following sections describe how to configure TACACS+ authentication on the switch.

Specifying TACACS+ Servers

Specify one or more TACACS+ servers before you enable TACACS+ authentication on the switch. The first server that you specify is the primary server, unless you explicitly make one server the primary server by using the **primary** keyword.

To specify one or more TACACS+ servers, perform this task in privileged mode:

	Task	Command
Step 1	Specify the IP address of one or more TACACS+ servers.	set tacacs server ip_addr [primary]
Step 2	Verify the TACACS+ configuration.	show tacacs

This example shows how to specify TACACS+ servers and verify the configuration:

```
Console> (enable) set tacacs server 172.20.52.3
172.20.52.3 added to TACACS server table as primary server.
Console> (enable) set tacacs server 172.20.52.2 primary
172.20.52.2 added to TACACS server table as primary server.
Console> (enable) set tacacs server 172.20.52.10
172.20.52.10 added to TACACS server table as backup server.
Console> (enable) show tacacs
```

```
Login Authentication:  Console Session  Telnet Session
-----
tacacs                disabled      disabled
radius               disabled      disabled
local                enabled(primary)  enabled(primary)

Enable Authentication: Console Session  Telnet Session
-----
tacacs                disabled      disabled
radius               disabled      disabled
local                enabled(primary)  enabled(primary)
```

```
Tacacs key:
Tacacs login attempts: 3
Tacacs timeout: 5 seconds
Tacacs direct request: disabled

Tacacs-Server                               Status
-----
172.20.52.3
172.20.52.2                                primary
172.20.52.10
Console> (enable)
```

Enabling TACACS+ Authentication



Note Specify at least one TACACS+ server before enabling TACACS+ authentication on the switch. For more information on specifying TACACS+ servers, see the [“Specifying TACACS+ Servers” section on page 30-17](#).

You can enable TACACS+ authentication for login and enable access to the switch. If desired, you can enter the **console** and **telnet** keywords to specify that TACACS+ authentication be used only on console or Telnet connections. If you are using both RADIUS and TACACS+, you can enter the **primary** keyword to force the switch to try TACACS+ authentication first.

To enable TACACS+ authentication, perform this task in privileged mode:

	Task	Command
Step 1	Enable TACACS+ authentication for normal login mode. Enter the console or telnet keywords if you want to enable TACACS+ only for console port or Telnet connection attempts.	set authentication login tacacs enable [all console http telnet] [primary]
Step 2	Enable TACACS+ authentication for enable mode. Enter the console or telnet keywords if you want to enable TACACS+ only for console port or Telnet connection attempts.	set authentication enable tacacs enable [all console http telnet] [primary]
Step 3	Verify the TACACS+ configuration.	show authentication

This example shows how to enable TACACS+ authentication for console and Telnet connections and how to verify the configuration:

```
Console> (enable) set authentication login tacacs enable
tacacs login authentication set to enable for console and telnet session.
Console> (enable) set authentication enable tacacs enable
tacacs enable authentication set to enable for console and telnet session.
Console> (enable) show authentication
```

```
Login Authentication: Console Session Telnet Session
-----
tacacs                enabled(primary) enabled(primary)
radius               disabled      disabled
local                enabled      enabled
Enable Authentication: Console Session Telnet Session
-----
tacacs                enabled(primary) enabled(primary)
radius               disabled      disabled
```


CISCO Confidential - DRAFT

```

local          enabled          enabled
Console> (enable)

```

Specifying the TACACS+ Key


Note

If you configure a TACACS+ key on the client, make sure that you configure an identical key on the TACACS+ server.

To specify the TACACS+ key, perform this task in privileged mode:

	Task	Command
Step 1	Specify the TACACS+ key that is used to encrypt packets.	set tacacs key <i>key</i>
Step 2	Verify the TACACS+ configuration.	show tacacs

This example shows how to specify the TACACS+ key and verify the configuration:

```

Console> (enable) set tacacs key Secret_TACACS_key
The tacacs key has been set to Secret_TACACS_key.
Console> (enable) show tacacs
Tacacs key: Secret_TACACS_key
Tacacs login attempts: 3
Tacacs timeout: 5 seconds
Tacacs direct request: disabled

```

```

Tacacs-Server          Status
-----
172.20.52.3
172.20.52.2            primary
172.20.52.10
Console> (enable)

```

Setting the TACACS+ Timeout Interval

You can set the timeout interval between retransmissions to the TACACS+ server. The default timeout is 5 seconds.

To set the TACACS+ timeout interval, perform this task in privileged mode:

	Task	Command
Step 1	Set the TACACS+ timeout interval.	set tacacs timeout <i>seconds</i>
Step 2	Verify the TACACS+ configuration.	show tacacs

This example shows how to set the server timeout interval and verify the configuration:

```

Console> (enable) set tacacs timeout 30
Tacacs timeout set to 30 seconds.
Console> (enable) show tacacs
Tacacs key: Secret_TACACS_key
Tacacs login attempts: 3
Tacacs timeout: 30 seconds
Tacacs direct request: disabled

```

CISCO Confidential - DRAFT

```
Tacacs-Server                      Status
-----
172.20.52.3
172.20.52.2                      primary
172.20.52.10
Console> (enable)
```

Setting the TACACS+ Login Attempts

You can set the number of failed login attempts that are allowed.

To set the number of login attempts that are allowed, perform this task in privileged mode:

	Task	Command
Step 1	Set the number of allowed login attempts.	set tacacs attempts <i>number</i>
Step 2	Verify the TACACS+ configuration.	show tacacs

This example shows how to set the number of login attempts and verify the configuration:

```
Console> (enable) set tacacs attempts 5
Tacacs number of attempts set to 5.
Console> (enable) show tacacs
Tacacs key: Secret_TACACS_key
Tacacs login attempts: 5
Tacacs timeout: 30 seconds
Tacacs direct request: disabled
```

```
Tacacs-Server                      Status
-----
172.20.52.3
172.20.52.2                      primary
172.20.52.10
Console> (enable)
```

Enabling TACACS+ Directed Request

When TACACS+ directed request is enabled, you must specify the host name of a configured TACACS+ server (in the form *username@server_hostname*) or the authentication request will fail.

To enable TACACS+ directed request, perform this task in privileged mode:

	Task	Command
Step 1	Enable TACACS+ directed request on the switch.	set tacacs directedrequest enable
Step 2	Verify the TACACS+ configuration.	show tacacs

This example shows how to enable TACACS+ directed request and verify the configuration:

```
Console> (enable) set tacacs directedrequest enable
Tacacs direct request has been enabled.
Console> (enable) show tacacs
Tacacs key: Secret_TACACS_key
Tacacs login attempts: 5
Tacacs timeout: 30 seconds
Tacacs direct request: enabled
```

CISCO Confidential - DRAFT

```
Tacacs-Server
-----
172.20.52.3
172.20.52.2
172.20.52.10
Console> (enable)
Status
-----
primary
```

Disabling TACACS+ Directed Request

To disable TACACS+ directed request, perform this task in privileged mode:

	Task	Command
Step 1	Disable TACACS+ directed request on the switch.	set tacacs directedrequest disable
Step 2	Verify the TACACS+ configuration.	show tacacs

This example shows how to disable TACACS+ directed request:

```
Console> (enable) set tacacs directedrequest disable
Tacacs direct request has been disabled.
Console> (enable)
```

Clearing TACACS+ Servers

To clear one or more TACACS+ servers, perform this task in privileged mode:

	Task	Command
Step 1	Specify the IP address of the TACACS+ server to clear from the configuration. Use the all keyword to clear all of the servers from the configuration.	clear tacacs server [ip_addr all]
Step 2	Verify the TACACS+ server configuration.	show tacacs

This example shows how to clear a specific TACACS+ server from the configuration:

```
Console> (enable) clear tacacs server 172.20.52.3
172.20.52.3 cleared from TACACS table
Console> (enable)
```

This example shows how to clear all TACACS+ servers from the configuration:

```
Console> (enable) clear tacacs server all
All TACACS servers cleared
Console> (enable)
```

Clearing the TACACS+ Key

To clear the TACACS+ key, perform this task in privileged mode:

CISCO Confidential - DRAFT

	Task	Command
Step 1	Clear the TACACS+ key.	clear tacacs key
Step 2	Verify the TACACS+ configuration.	show tacacs

This example shows how to clear the TACACS+ key:

```
Console> (enable) clear tacacs key
TACACS server key cleared.
Console> (enable)
```

Disabling TACACS+ Authentication

If you disable TACACS+ authentication with both RADIUS and local authentication disabled, local authentication is reenabled automatically.

To disable TACACS+ authentication, perform this task in privileged mode:

	Task	Command
Step 1	Disable TACACS+ authentication for normal login mode. Use the console or telnet keywords if you want to disable TACACS+ only for console port or Telnet connection attempts.	set authentication login tacacs disable [all console http telnet]
Step 2	Disable TACACS+ authentication for enable mode. Use the console or telnet keywords if you want to disable TACACS+ only for console port or Telnet connection attempts.	set authentication enable tacacs disable [all console http telnet]
Step 3	Verify the TACACS+ configuration.	show authentication

This example shows how to disable TACACS+ authentication for console and Telnet connections and how to verify the configuration:

```
Console> (enable) set authentication login tacacs disable
tacacs login authentication set to disable for console and telnet session.
Console> (enable) set authentication enable tacacs disable
tacacs enable authentication set to disable for console and telnet session.
Console> (enable) show authentication
```

```
Login Authentication:  Console Session  Telnet Session
-----
tacacs                disabled      disabled
radius                disabled      disabled
local                 enabled(primary)  enabled(primary)
```

```
Enable Authentication: Console Session  Telnet Session
-----
tacacs                disabled      disabled
radius                disabled      disabled
local                 enabled(primary)  enabled(primary)
Console> (enable)
```

Configuring RADIUS Authentication

The following sections describe how to configure RADIUS authentication on the switch.

Specifying RADIUS Servers

To specify one or more RADIUS servers, perform this task in privileged mode:

	Task	Command
Step 1	Specify the IP address of up to three RADIUS servers. Specify the primary server using the primary keyword. Optionally, specify the destination UDP port to use on the server.	set radius server <i>ip_addr</i> [auth-port <i>port_number</i>] [primary]
Step 2	Verify the RADIUS server configuration.	show radius

This example shows how to specify a RADIUS server and verify the configuration:

```
Console> (enable) set radius server 172.20.52.3
172.20.52.3 with auth-port 1812 added to radius server table as primary server.
Console> (enable) show radius
```

```

Login Authentication: Console Session Telnet Session
-----
tacacs                disabled        disabled
radius                disabled        disabled
local                 enabled(primary) enabled(primary)

Enable Authentication: Console Session Telnet Session
-----
tacacs                disabled        disabled
radius                disabled        disabled
local                 enabled(primary) enabled(primary)

Radius Deadtime:           0 minutes
Radius Key:
Radius Retransmit:        2
Radius Timeout:           5 seconds

Radius-Server              Status Auth-port
-----
172.20.52.3                primary 1812
Console> (enable)

```

Enabling RADIUS Authentication



Note

Specify at least one RADIUS server before enabling RADIUS authentication on the switch. For information on specifying a RADIUS server, see the [“Specifying RADIUS Servers” section on page 30-23](#).

You can enable RADIUS authentication for login and enable access to the switch. If desired, you can use the **console** and **telnet** keywords to specify that RADIUS authentication be used only on console or Telnet connections. If you are using both RADIUS and TACACS+, you can use the **primary** keyword to force the switch to try RADIUS authentication first.

CISCO Confidential - DRAFT

To configure RADIUS authentication, perform this task in privileged mode:

	Task	Command
Step 1	Enable RADIUS authentication for normal login mode.	set authentication login radius enable [all console http telnet] [primary]
Step 2	Enable RADIUS authentication for enable mode.	set authentication enable radius enable [all console http telnet] [primary]
Step 3	Create a user \$enab15\$ on the RADIUS server, and assign a password to that user.	See the Note on Table 30-2 on page 30-24 for additional information.
Step 4	Verify the RADIUS configuration.	show authentication

**Note**

To use RADIUS authentication for enable mode, you need to create a user with the name \$enab15\$ on the RADIUS server, and assign a password to that user. This user needs to be created in addition to your assigned username and password on the RADIUS server (example: username **john**, password **hello**.) After you log in to the Catalyst 4000 family switch with your assigned username and password (john/hello), you can enter enable mode using the password that is assigned to the \$enab15\$ user.

If your RADIUS server does not support the \$enab15\$ username, you can set the service-type attribute (attribute 6) to Administrative (value 6) for a RADIUS user to directly launch the user into enable mode without asking for a separate enable password.

This example shows how to enable RADIUS authentication and verify the configuration:

```

Console> (enable) set authentication login radius enable
radius login authentication set to enable for console and telnet session.
Console> (enable) set authentication enable radius enable
radius enable authentication set to enable for console and telnet session.
Console> (enable) show authentication

```

```

Login Authentication:  Console Session  Telnet Session
-----
tacacs                disabled      disabled
radius                enabled(primary)  enabled(primary)
local                 enabled      enabled

Enable Authentication: Console Session  Telnet Session
-----
tacacs                disabled      disabled
radius                enabled(primary)  enabled(primary)
local                 enabled      enabled
Console> (enable)

```

Specifying the RADIUS Key

The RADIUS key is used to encrypt and authenticate all communication between the RADIUS client and server. You must configure the same key on the client and the RADIUS server.

The length of the key is limited to 65 characters. It can include any printable ASCII characters except tabs.

To specify the RADIUS key, perform this task in privileged mode:

CISCO Confidential - DRAFT

	Task	Command
Step 1	Specify the RADIUS key that is used to encrypt packets sent to the RADIUS server.	set radius key <i>key</i>
Step 2	Verify the RADIUS configuration.	show radius

This example shows how to specify the RADIUS key and verify the configuration (in normal mode, the RADIUS key value is hidden):

```
Console> (enable) set radius key Secret_RADIUS_key
Radius key set to Secret_RADIUS_key
```

```
Console> (enable) show radius
```

```
Login Authentication:  Console Session  Telnet Session
-----
tacacs                disabled      disabled
radius               enabled(primary)  enabled(primary)
local                enabled       enabled
```

```
Enable Authentication: Console Session  Telnet Session
-----
tacacs                disabled      disabled
radius               enabled(primary)  enabled(primary)
local                enabled       enabled
```

```
Radius Deadtime:      0 minutes
Radius Key:           Secret_RADIUS_key
Radius Retransmit:    2
Radius Timeout:       5 seconds
```

```
Radius-Server         Status  Auth-port
-----
172.20.52.3           primary 1812
Console> (enable)
```

Setting the RADIUS Timeout Interval

You can set the timeout interval between retransmissions to the RADIUS server. The default timeout is 5 seconds.

To set the RADIUS timeout interval, perform this task in privileged mode:

	Task	Command
Step 1	Set the RADIUS timeout interval.	set radius timeout <i>seconds</i>
Step 2	Verify the RADIUS configuration.	show radius

This example shows how to set the RADIUS timeout interval and verify the configuration:

```
Console> (enable) set radius timeout 10
Radius timeout set to 10 seconds.
Console> (enable) show radius
```

```
Login Authentication:  Console Session  Telnet Session
-----
tacacs                disabled      disabled
```

CISCO Confidential - DRAFT

```

radius          enabled(primary)  enabled(primary)
local           enabled           enabled

Enable Authentication: Console Session  Telnet Session
-----
tacacs          disabled           disabled
radius          enabled(primary)  enabled(primary)
local           enabled           enabled

Radius Deadtime:          0 minutes
Radius Key:              Secret_RADIUS_key
Radius Retransmit:       2
Radius Timeout:          10 seconds

Radius-Server           Status   Auth-port
-----
172.20.52.3             primary 1812
Console> (enable)

```

Setting the RADIUS Retransmit Count

You can set the number of times the switch will attempt to contact a RADIUS server before the next configured server is tried. By default, each RADIUS server will be tried two times.

To set the RADIUS retransmit count, perform this task in privileged mode:

	Task	Command
Step 1	Set the RADIUS server retransmit count.	set radius retransmit <i>count</i>
Step 2	Verify the RADIUS configuration.	show radius

This example shows how to set the RADIUS retransmit count as 4 and how to verify the configuration:

```

Console> (enable) set radius retransmit 4
Radius retransmit count set to 4.
Console> (enable) show radius

```

```

Login Authentication: Console Session  Telnet Session
-----
tacacs          disabled           disabled
radius          enabled(primary)  enabled(primary)
local           enabled           enabled

Enable Authentication: Console Session  Telnet Session
-----
tacacs          disabled           disabled
radius          enabled(primary)  enabled(primary)
local           enabled           enabled

Radius Deadtime:          0 minutes
Radius Key:              Secret_RADIUS_key
Radius Retransmit:       4
Radius Timeout:          10 seconds

Radius-Server           Status   Auth-port
-----
172.20.52.3             primary 1812
Console> (enable)

```


CISCO Confidential - DRAFT

Setting the RADIUS Dead Time

You can configure the switch so that when a RADIUS server does not respond to an authentication request, the switch marks that server as dead for the length of time that is specified in the **set radius deadtime** command. Any authentication requests that are received during the dead time interval (such as other users attempting to log in to the switch) are not sent to a RADIUS server that is marked dead. Configuring a dead time speeds up the authentication process, by eliminating timeouts and retransmissions to the dead RADIUS server.

If you configure only one RADIUS server, or if all of the configured servers are marked dead, the dead time is ignored because there are no alternate servers available.

To set the RADIUS dead time, perform this task in privileged mode:

	Task	Command
Step 1	Set the RADIUS server dead time interval.	set radius deadtime <i>minutes</i>
Step 2	Verify the RADIUS configuration.	show radius

This example shows how to set the RADIUS dead time interval and verify the configuration:

```
Console> (enable) set radius deadtime 5
```

```
Radius deadtime set to 5 minute(s).
```

```
Console> (enable) show radius
```

```

Login Authentication:  Console Session  Telnet Session
-----
tacacs                disabled      disabled
radius               enabled(primary)  enabled(primary)
local                enabled      enabled

Enable Authentication: Console Session  Telnet Session
-----
tacacs                disabled      disabled
radius               enabled(primary)  enabled(primary)
local                enabled      enabled

Radius Deadtime:      5 minutes
Radius Key:           Secret_RADIUS_key
Radius Retransmit:    4
Radius Timeout:       10 seconds

Radius-Server          Status  Auth-port
-----
172.20.52.3            primary 1812
172.20.52.2            primary 1812
Console> (enable)

```

Specifying Optional Attributes for RADIUS Servers

You can specify optional attributes in the RADIUS ACCESS_REQUEST packet. The **set radius attribute** command allows you to specify the transmission of certain optional attributes such as Framed-IP address, NAS-Port, Called-Station-Id, Calling-Station-Id and so on. You can set the attribute transmission by either the attribute number or the attribute name. Transmission of the attributes is disabled by default.

CISCO Confidential - DRAFT**Note**

Software release 7.5(1) supports only the framed-IP address (Attribute 8).

To specify optional attributes for the RADIUS server, perform this task in privileged mode:

	Task	Command
Step 1	Specify optional attributes for the RADIUS server.	set radius attribute <i>[number name]</i> include-in-access-req <i>[enable disable]</i>
Step 2	Verify the RADIUS configuration.	show radius

This example shows how to specify and enable the framed-IP address attribute by number:

```
Console> (enable) set radius attribute 8 include-in-access-req enable
Transmission of Framed-ip address in access-request packet is enabled.
Console> (enable) show radius
RADIUS Deadtime:          0 minutes
RADIUS Key:               123456
RADIUS Retransmit:        2
RADIUS Timeout:           5 seconds
Framed-IP Address Transmit: Enabled
```

```
RADIUS-Server      Status   Auth-port   Acct-port
-----
10.6.140.230       primary  1812        1813
Console> (enable)
```

This example shows how to specify and disable the framed-IP address attribute by name:

```
Console> (enable) set radius attribute framed-ip-address include-in-access-req disable
Transmission of Framed-ip address in access-request packet is disabled.
Console> (enable)
```

Clearing RADIUS Servers

To clear one or more RADIUS servers, perform this task in privileged mode:

	Task	Command
Step 1	Specify the IP address of the RADIUS server to clear from the configuration. Enter the all keyword to clear all of the servers from the configuration.	clear radius server <i>[ip_addr all]</i>
Step 2	Verify the RADIUS server configuration.	show radius

This example shows how to clear a single RADIUS server from the configuration:

```
Console> (enable) clear radius server 172.20.52.3
172.20.52.3 cleared from radius server table.
Console> (enable)
```

This example shows how to clear all RADIUS servers from the configuration:

```
Console> (enable) clear radius server all
All radius servers cleared from radius server table.
Console> (enable)
```

CISCO Confidential - DRAFT

Clearing the RADIUS Key

To clear the RADIUS key, perform this task in privileged mode:

	Task	Command
Step 1	Clear the RADIUS key.	clear radius key
Step 2	Verify the RADIUS configuration.	show radius

This example shows how to clear the RADIUS key and verify the configuration:

```
Console> (enable) clear radius key
Radius key cleared.
Console> (enable) show radius
```

```
Login Authentication:  Console Session  Telnet Session
-----
tacacs                disabled      disabled
radius               disabled      disabled
local                enabled(primary)  enabled(primary)

Enable Authentication: Console Session  Telnet Session
-----
tacacs                disabled      disabled
radius               disabled      disabled
local                enabled(primary)  enabled(primary)

Radius Deadtime:           0 minutes
Radius Key:
Radius Retransmit:         2
Radius Timeout:            5 seconds

Radius-Server              Status   Auth-port
-----
172.20.52.3                primary  1812
Console> (enable)
```

Disabling RADIUS Authentication

If you disable RADIUS authentication with both TACACS+ and local authentication disabled, local authentication is reenabled automatically.

To disable RADIUS authentication, perform this task in privileged mode:

	Task	Command
Step 1	Disable RADIUS authentication for login mode.	set authentication login radius disable [all console http telnet]
Step 2	Disable RADIUS authentication for enable mode.	set authentication enable radius disable [all console http telnet]
Step 3	Verify the RADIUS configuration.	show radius show authentication

This example shows how to disable RADIUS authentication:

```
Console> (enable) set authentication login radius disable
```

CISCO Confidential - DRAFT

```
radius login authentication set to disable for console and telnet session.
Console> (enable) set authentication enable radius disable
radius enable authentication set to disable for console and telnet session.
Console> (enable) show authentication
```

Login Authentication:	Console Session	Telnet Session
-----	-----	-----
tacacs	disabled	disabled
radius	disabled	disabled
local	enabled(primary)	enabled(primary)

Enable Authentication:	Console Session	Telnet Session
-----	-----	-----
tacacs	disabled	disabled
radius	disabled	disabled
local	enabled(primary)	enabled(primary)

```
Console> (enable)
```

Configuring Kerberos Authentication

Before you can use Kerberos as an authentication method on the switch, you need to configure the Kerberos server. You will need to create a database for the KDC and add the switch to the database.

To configure the Kerberos server, follow these steps:

-
- Step 1** Before you can enter the switch in the Kerberos server's key table, you must create the database that the KDC will use. In the following example, a database called CISCO.EDU is created:
- ```
/usr/local/sbin/kdb5_util create -r CISCO.EDU -s
```
- Step 2** Add the switch to the database. The following example adds a switch called Cat4012 to the CISCO.EDU database:
- ```
ank host/Cat4012.cisco.edu@CISCO.EDU
```
- Step 3** Add the username as follows:
- ```
ank user1@CISCO.EDU
```
- Step 4** Add the Administrative Principals as follows:
- ```
ank user1/admin@CISCO.EDU
```
- Step 5** Create the entry for the switch in the database using the **admin.local ktadd** command as follows:
- ```
ktadd host/Cat4012.cisco.edu@CISCO.EDU
```
- Step 6** Move the **keyadmin** file to a place where the switch can reach it.
- Step 7** Start the KDC server as follows:
- ```
/usr/local/sbin/krb4kdc
/usr/local/sbin/kadmind
```
-

CISCO Confidential - DRAFT

Enabling Kerberos

To enable Kerberos authentication, perform this task in privileged mode:

	Task	Command
Step 1	Enable Kerberos authentication.	set authentication login kerberos enable [all console http telnet] [primary]
Step 2	Verify the configuration.	show authentication

This example shows how to enable Kerberos as the login authentication method for Telnet and verify the configuration:

```
Console> (enable) set authentication login kerberos enable telnet
kerberos login authentication set to enable for telnet session.
Console> (enable) show authentication
```

```
Login Authentication: Console Session   Telnet Session
-----
tacacs          disabled                disabled
radius          disabled                disabled
kerberos        disabled                enabled(primary)
local           enabled(primary)             enabled
```

```
Enable Authentication: Console Session   Telnet Session
-----
tacacs          disabled                disabled
radius          disabled                disabled
kerberos        disabled                enabled(primary)
local           enabled(primary)             enabled
Console> (enable)
```

This example shows how to enable Kerberos as the login authentication method for the console and verify the configuration:

```
Console> (enable) set authentication login kerberos enable console
kerberos login authentication set to enable for console session.
Console> (enable) show authentication
```

```
Login Authentication: Console Session   Telnet Session
-----
tacacs          disabled                disabled
radius          disabled                disabled
kerberos        enabled(primary)           enabled(primary)
local           enabled                  enabled
```

```
Enable Authentication: Console Session   Telnet Session
-----
tacacs          disabled                disabled
radius          disabled                disabled
kerberos        enabled(primary)           enabled(primary)
local           enabled                  enabled
Console> (enable)
```

Defining the Kerberos Local-Realm

The Kerberos realm is a domain consisting of users, hosts, and network services that are registered to a Kerberos server. To authenticate a user defined in the Kerberos database, the switch must know the host name or IP address of the host running the KDC and the name of the Kerberos realm.

CISCO Confidential - DRAFT

To configure the switch to authenticate to the KDC in a specified Kerberos realm, perform this task in privileged mode:

Task	Command
Define the default realm for the switch.	set kerberos local-realm <i>kerberos-realm</i>

**Note**

Make sure that you enter the realm in uppercase letters. Kerberos will not authenticate users if the realm is in lowercase letters.

This example shows how to define a local realm and how to verify the configuration:

```

Console> (enable) set kerberos local-realm CISCO.COM
Kerberos local realm for this switch set to CISCO.COM.
Console> (enable) show kerberos
Kerberos Local Realm:CISCO.COM
Kerberos server entries:
Realm:CISCO.COM, Server:187.0.2.1, Port:750

Kerberos Domain<->Realm entries:
Domain:cisco.com, Realm:CISCO.COM

Kerberos Clients NOT Mandatory
Kerberos Credentials Forwarding Enabled
Kerberos Pre Authentication Method set to None
Kerberos config key:
Kerberos SRVTAB Entries
Srvtab Entry 1:host/niners.cisco.com@CISCO.COM 0 932423923 1 1 8 01;;8>00>50;0=0=0
Console> (enable)

```

Specifying a Kerberos Server

You can specify to the switch which KDC to use in a specific Kerberos realm. Optionally, you can also specify the port number of the port the KDC is monitoring. The Kerberos server maintains information that you enter in a table with one entry for each Kerberos realm. The maximum number of entries in the table is 100.

To specify the Kerberos server, perform this task in privileged mode:

	Task	Command
Step 1	Specify which KDC to use in a given Kerberos realm. Optionally, enter the port number that the KDC is monitoring. (The default port number is 750.)	set kerberos server <i>kerberos-realm</i> { <i>hostname</i> <i>ip-address</i> } [<i>port-number</i>]
Step 2	Clear the Kerberos server entry.	clear kerberos server <i>kerberos-realm</i> { <i>hostname</i> <i>ip-address</i> } [<i>port-number</i>]

This example shows how to define which Kerberos server will serve as the KDC for the specified Kerberos realm and how to clear the entry:

```

Console> (enable) set kerberos server CISCO.COM 187.0.2.1 750
Kerberos Realm-Server-Port entry set to:CISCO.COM - 187.0.2.1 - 750
Console> (enable)

```

CISCO Confidential - DRAFT

```

Console> (enable) clear kerberos server CISCO.COM 187.0.2.1 750
Kerberos Realm-Server-Port entry CISCO.COM-187.0.2.1-750 deleted
Console> (enable)

```

Mapping a Kerberos Realm to a Host Name or DNS Domain

Optionally, you can map a host name or Domain Name Server (DNS) domain to a Kerberos realm.

To map a Kerberos realm to either a host name or DNS domain, perform this task in privileged mode:

	Task	Command
Step 1	(Optional) Map a host name or DNS domain to a Kerberos realm.	set kerberos realm {dns-domain host} <i>kerberos-realm</i>
Step 2	Clear the Kerberos realm domain or host mapping entry.	clear kerberos realm {dns-domain host} <i>kerberos-realm</i>

This example shows how to map a Kerberos realm, called CISCO.COM, to a DNS domain and how to clear the entry:

```

Console> (enable) set kerberos realm CISCO CISCO.COM
Kerberos DnsDomain-Realm entry set to CISCO - CISCO.COM
Console> (enable)

```

```

Console> (enable) clear kerberos realm CISCO CISCO.COM
Kerberos DnsDomain-Realm entry CISCO - CISCO.COM deleted
Console> (enable)

```

Copying SRVTAB Files

To allow remote users to authenticate to the switch using Kerberos credentials, the switch must share a key with the KDC. You must give the switch a copy of the file that is stored in the KDC that contains the key. These files are called SRVTAB files on the switch and KEYTAB files on the servers.

The most secure method of copying SRVTAB files to the hosts in your Kerberos realm is to copy them onto physical media and then manually copy the files onto the system. To copy SRVTAB files to a switch that does not have a physical media drive, you must transfer them through the network by using the Trivial File Transfer Protocol (TFTP).

When you copy the SRVTAB file from the switch to the KDC, the switch parses the information in this file and stores it in the running configuration in the Kerberos SRVTAB entry format. If you enter the SRVTAB directly into the switch, create an entry for each Kerberos principal (service) on the switch. The entries are maintained in the SRVTAB table. The maximum size of the table is 20 entries.

To retrieve SRVTAB files to the switch from the KDC, perform this task in privileged mode:

	Task	Command
Step 1	Retrieve a specified SRVTAB file from the KDC.	set kerberos srvtab remote {hostname ip-address} <i>filename</i>
Step 2	(Optional) You can enter the SRVTAB directly into the switch.	set kerberos srvtab entry <i>kerberos-principal principal-type timestamp key-version number key-type key-length encrypted-keytab</i>

CISCO Confidential - DRAFT

This example shows how to retrieve an SRVTAB file from the KDC, enter an SRVTAB directly into the switch, and verify the configuration:

```

Console> (enable) set kerberos srvtab remote 187.20.32.10 /users/jdoe/krb5/ninerskeytab
Console> (enable)

Console> (enable) set kerberos srvtab entry host/niners.cisco.com@CISCO.COM 0 932423923 1
1 8 03;;5>00>50;0=0=0
Kerberos SRVTAB entry set to
Principal:host/niners.cisco.com@CISCO.COM
Principal Type:0
Timestamp:932423923
Key version number:1
Key type:1
Key length:8
Encrypted key tab:03;;5>00>50;0=0=0

Console> (enable) show kerberos
Kerberos Local Realm:CISCO.COM
Kerberos server entries:
Realm:CISCO.COM, Server:187.0.2.1, Port:750
Realm:CISCO.COM, Server:187.20.2.1, Port:750

Kerberos Domain<->Realm entries:
Domain:cisco.com, Realm:CISCO.COM

Kerberos Clients NOT Mandatory
Kerberos Credentials Forwarding Enabled
Kerberos Pre Authentication Method set to None
Kerberos config key:
Kerberos SRVTAB Entries
Srvtab Entry 1:host/niners.cisco.com@CISCO.COM 0 932423923 1 1 8 03;;5>00>50;0=0=0
Srvtab Entry 2:host/niners.cisco.edu@CISCO.EDU 0 933974942 1 1 8 00?58:127:223=::;9
Console> (enable)

```

Deleting an SRVTAB Entry

To delete an SRVTAB entry, perform this task in privileged mode:

Task	Command
Delete the SRVTAB entry for a particular Kerberos principal.	clear kerberos srvtab entry <i>kerberos-principal principal-type</i>

This example shows how to delete an SRVTAB entry:

```

Console> (enable) clear kerberos srvtab entry host/niners.cisco.com@CISCO.COM 0
Console> (enable)

```

Enabling Credentials Forwarding

A user authenticated to a Kerberized switch has a TGT and can use it to authenticate to a host on the network. However, if forwarding is not enabled and a user tries to list credentials after authenticating to a host, the output will show that no Kerberos credentials are present.

To enable credentials forwarding, configure the switch to forward user TGTs when they authenticate from the switch to Kerberized remote hosts on the network using Kerberized Telnet.

CISCO Confidential - DRAFT

As an additional layer of security, you can configure the switch so that after users authenticate to it, these users can authenticate only to other services on the network with Kerberized clients. If you do not make Kerberos authentication mandatory and Kerberos authentication fails, the application attempts to authenticate users using the default method of authentication for that network service. For example, Telnet prompts for a password.

To configure clients to forward user credentials as they connect to other hosts in the Kerberos realm, perform this task in privileged mode:

	Task	Command
Step 1	Enable all clients to forward user credentials upon successful Kerberos authentication.	set kerberos credentials forward
Step 2	(Optional) Configure Telnet to fail if clients cannot authenticate to the remote server.	set kerberos clients mandatory

This example shows how to configure clients to forward user credentials and verify the configuration:

```

Console> (enable) set kerberos credentials forward
Kerberos credentials forwarding enabled
Console> (enable) show kerberos
Kerberos Local Realm:CISCO.COM
Kerberos server entries:
Realm:CISCO.COM, Server:187.0.2.1, Port:750
Realm:CISCO.COM, Server:187.20.2.1, Port:750

Kerberos Domain<->Realm entries:
Domain:cisco.com, Realm:CISCO.COM

Kerberos Clients NOT Mandatory
Kerberos Credentials Forwarding Enabled
Kerberos Pre Authentication Method set to None
Kerberos config key:
Kerberos SRVTAB Entries
Srvtab Entry 1:host/aspens-niners.cisco.edu@CISCO.EDU 0 933974942 1 1 8 00?91:107:423=::9
Console> (enable)

```

This example shows how to configure the switch so that Kerberos clients are mandatory for users to authenticate to other network services:

```

Console> (enable) set kerberos clients mandatory
Kerberos clients set to mandatory
Console> (enable)

```

Disabling Credentials Forwarding

To disable the credentials forwarding configuration, perform this task in privileged mode:

Task	Command
Disable the credentials forwarding configuration.	clear kerberos credentials forward

This example shows how to disable the credentials forwarding configuration and verify the change:

```

Console> (enable) clear kerberos credentials forward
Kerberos credentials forwarding disabled

```

CISCO Confidential - DRAFT

```
Console> (enable) show kerberos
Kerberos Local Realm not configured
Kerberos server entries:

Kerberos Domain<->Realm entries:

Kerberos Clients NOT Mandatory
Kerberos Credentials Forwarding Disabled
Kerberos Pre Authentication Method set to None
Kerberos config key:
Kerberos SRVTAB Entries
Console> (enable)
```

To clear the Kerberos clients' mandatory configuration, perform this task in privileged mode:

Task	Command
Clear the Kerberos clients' mandatory configuration.	clear kerberos clients mandatory

This example shows how to clear the clients' mandatory configuration and verify the change:

```
Console> (enable) clear kerberos clients mandatory
Kerberos clients mandatory cleared
Console> (enable) show kerberos
Kerberos Local Realm not configured
Kerberos server entries:

Kerberos Domain<->Realm entries:

Kerberos Clients NOT Mandatory
Kerberos Credentials Forwarding Disabled
Kerberos Pre Authentication Method set to None
Kerberos config key:
Kerberos SRVTAB Entries
Console> (enable)
Kerberos server entries:

Kerberos Domain<->Realm entries:

Kerberos Clients Mandatory
Kerberos Credentials Forwarding Disabled
Kerberos Pre Authentication Method set to Encrypted Unix Time Stamp
Kerberos config key:
Kerberos SRVTAB Entries
Console> (enable)
```

Defining and Clearing a Private DES Key

You can define a private DES key for the switch. You can use the private DES key to encrypt the secret key that the switch shares with the KDC so that when the **show kerberos** command is executed, the secret key is not displayed in clear text. The key length should be eight characters or less.

To define a DES key, perform this task in privileged mode:

Task	Command
Define a DES key for the switch.	set key config-key string

CISCO Confidential - DRAFT

This example shows how to define a DES key and verify the configuration:

```

Console> (enable) set key config-key abcd
Kerberos config key set to abcd
Console> (enable) show kerberos
Kerberos Local Realm:CISCO.COM
Kerberos server entries:
Realm:CISCO.COM, Server:170.20.2.1, Port:750
Realm:CISCO.COM, Server:172.20.2.1, Port:750

Kerberos Domain<->Realm entries:
Domain:cisco.com, Realm:CISCO.COM

Kerberos Clients Mandatory
Kerberos Credentials Forwarding Disabled
Kerberos Pre Authentication Method set to Encrypted Unix Time Stamp
Kerberos config key:abcd
Kerberos SRVTAB Entries
Srvtab Entry 1:host/aspen-niners.cisco.edu@CISCO.EDU 0 933974942 1 1 8 12151><88?=>>3>11
Console> (enable)

```

To clear the DES key, perform this task in privileged mode:

Task	Command
Clear a DES key from the switch.	clear key config-key string

This example shows how to clear the DES key:

```

Console> (enable) clear key config-key
Kerberos config key cleared
Console> (enable)

```

Encrypting a Telnet Session

After a user authenticates to the switch using Kerberos and wants to Telnet to a different switch or host, the authentication method that the Telnet server uses determines if the new session is a Kerberized Telnet session. If the Telnet server uses Kerberos for authentication, you can have all the application data packets encrypted for the duration of the Telnet session. To encrypt the Telnet session, select the **encrypt kerberos** option in the **telnet** command.

To encrypt a Telnet session, perform this task in privileged mode:

Task	Command
Encrypt a Telnet session.	telnet [encrypt kerberos] host

This example shows how to configure a Telnet session for Kerberos authentication and encryption:

```

Console> (enable) telnet encrypt kerberos 172.20.52.5

```

Monitoring and Maintaining Kerberos

Use these commands to display and clear Kerberos configurations on the switch:

- **show kerberos**
- **show kerberos creds**

CISCO Confidential - DRAFT

- **clear kerberos creds**

To display the Kerberos configuration, perform this task in privileged mode:

Task	Command
Display the Kerberos configuration.	show kerberos

This example shows how to display the Kerberos configuration:

```

Console> (enable) show kerberos
Kerberos Local Realm:CISCO.COM
Kerberos server entries:
Realm:CISCO.COM, Server:187.0.2.1, Port:750
Realm:CISCO.COM, Server:187.20.2.1, Port:750

Kerberos Domain<->Realm entries:
Domain:cisco.com, Realm:CISCO.COM

Kerberos Clients NOT Mandatory
Kerberos Credentials Forwarding Enabled
Kerberos Pre Authentication Method set to None
Kerberos config key:
Kerberos SRVTAB Entries
Srvtab Entry 1:host/niners.cisco.com@CISCO.COM 0 932423923 1 1 8 03;;5>00>50;0=0=0
Srvtab Entry 2:host/niners.cisco.edu@CISCO.EDU 0 933974942 1 1 8 00?58:127:223=:;9
Console> (enable)

```

To display the Kerberos credentials, perform this task in privileged mode:

Task	Command
Display the Kerberos credentials.	show kerberos creds

This example shows how to display the Kerberos credentials:

```

Console> (enable) show kerberos creds
No Kerberos credentials.
Console> (enable)

```

To clear all Kerberos credentials, perform this task in privileged mode:

Task	Command
Clear all credentials.	clear kerberos creds

This example shows how to clear all credentials from the switch:

```

Console> (enable) clear kerberos creds
Console> (enable)

```

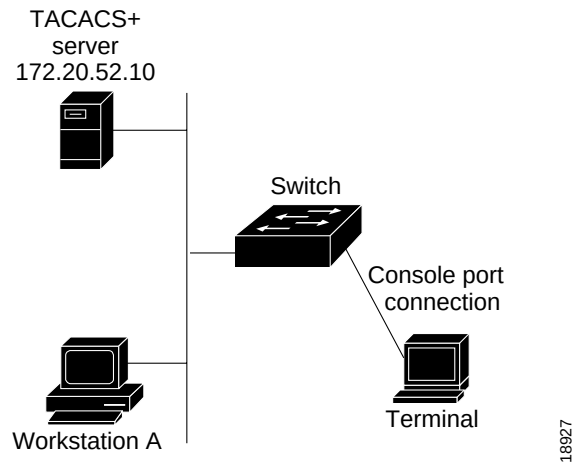
CISCO Confidential - DRAFT

Authentication Example

Figure 30-3 shows a simple network topology using TACACS+. In this example, TACACS+ authentication is enabled and local authentication is disabled for both login and enable access to the switch for all Telnet connections. When Workstation A attempts to connect to the switch, the user is challenged for a TACACS+ username and password.

Only local authentication is enabled for both login and enable access on the console port. Any user with access to the directly connected terminal can access the switch using the login and enable passwords.

Figure 30-3 Example of a TACACS+ Network Topology



This example shows how to configure the switch so that TACACS+ authentication is enabled for Telnet connections and local authentication is enabled for console connections. In addition, a TACACS+ encryption key is specified.

```

Console> (enable) show tacacs
Tacacs key:
Tacacs login attempts: 3
Tacacs timeout: 5 seconds
Tacacs direct request: disabled
  
```

```

Tacacs-Server                                     Status
-----
Console> (enable) set tacacs server 172.20.52.10
172.20.52.10 added to TACACS server table as primary server.
Console> (enable) set tacacs key tintin_et_milou
The tacacs key has been set to tintin_et_milou.
Console> (enable) set authentication login tacacs enable telnet
tacacs login authentication set to enable for telnet session.
Console> (enable) set authentication enable tacacs enable telnet
tacacs enable authentication set to enable for telnet session.
Console> (enable) set authentication login local disable telnet
local login authentication set to disable for telnet session.
Console> (enable) set authentication enable local disable telnet
local enable authentication set to disable for telnet session.
Console> (enable) show tacacs
Tacacs key: tintin_et_milou
Tacacs login attempts: 3
Tacacs timeout: 5 seconds
  
```

CISCO Confidential - DRAFT

Tacacs direct request: disabled

Tacacs-Server	Status
-----	-----
172.20.52.10	primary
Console> (enable)	

Understanding How Authorization Works

The Catalyst 4000 family switch supports TACACS+ and RADIUS authorization to control access to the switch. Authorization limits access to specified users using a dynamically applied access list (or user profile) based on the username and password pair. The access list resides on the host running the TACACS+ or RADIUS server. The server responds to the user password information and applies the access list.

Authorization Events

You can enable TACACS+ authorization for the following:

- **Commands**—When the authorization feature is enabled for commands, the user must supply a valid username and password pair to execute certain commands. You can require authorization for all commands or for configuration (enable mode) commands only. When a user enters a command, the authorization server receives the command and user information and compares it against an access list. If the user is authorized to enter that command, the command is executed; otherwise, the command is not executed.
- **EXEC mode (normal login)**—When the authorization feature is enabled for EXEC mode, the user must supply a valid username and password pair to access the EXEC mode. Authorization is required only if you have enabled the authorization feature.
- **Enable mode (privileged login)**—When the authorization feature is enabled for enable mode, the user must supply a valid username and password pair to access enable mode. Authorization is required only if you have enabled the authorization feature for enable mode.

TACACS+ Primary and Fallback Options

You can specify the primary and fallback options that are used in the authorization process. The following primary options and fallback options are available:

- **tacacs+**—If you have been authenticated and there is no response from the TACACS+ server, authorization succeeds immediately.
- **if-authenticated**—If you have been authenticated and there is no response from the TACACS+ server, authorization succeeds immediately.
- **none**—Authorization succeeds if the TACACS+ server does not respond.
- **deny**—Authorization fails if the TACACS+ server fails to respond. The **Deny** option is a fallback option only. This is the default behavior.

CISCO Confidential - DRAFT

TACACS+ Command Authorization

You can require authorization for all commands or for configuration (enable mode) commands only. Configuration commands include the following:

- **copy**
- **clear**
- **commit**
- **configure**
- **delete**
- **download**
- **format**
- **reload**
- **rollback**
- **session**
- **set**
- **squeeze**
- **switch**
- **undelete**

The following TACACS+ authorization process occurs for every command that you enter:

- If you have disabled the command authorization feature, the TACACS+ server allows you to execute any command on the switch.
- If you have enabled authorization for configuration commands only, the switch verifies that the argument string matches one of the commands listed above. If there is no match, the switch completes the command. If there is a match, the switch forwards the command to the NAS for authorization.
- If you have enabled authorization for all commands, the switch forwards the command to the NAS for authorization.

RADIUS Authorization

RADIUS has limited authorization. The Service-Type attribute in the authentication protocol provides authorization information. This attribute is part of the user-profile.

When you log in using RADIUS authentication and you do not have Administrative/Shell (6) Service-Type access, the NAS authenticates you and logs you in to EXEC mode if authentication succeeds. If you have Administrative/Shell (6) Service-Type access, the NAS authenticates you and logs you in to privileged mode if authentication succeeds.

Configuring Authorization

The following sections describe how to configure authorization.

Authorization Default Configuration

Table 30-3 shows the default authorization configuration.

Table 30-3 Default Authorization Configuration

Feature	Default
TACACS+ login authorization (console and Telnet)	Disabled
TACACS+ EXEC authorization (console and Telnet)	Disabled
TACACS+ enable authorization (console and Telnet)	Disabled
TACACS+ commands authorization (console and Telnet)	Disabled

TACACS+ Authorization Configuration Guidelines

This section describes the guidelines for configuring authorization on the switch:

- TACACS+ authorization is disabled by default.
- Authorization configuration applies to console connections, Telnet connections, or both types of connections.
- You must specify the mode, primary option, fallback option, and connection type when enabling authorization.
- Configure RADIUS and TACACS+ servers before enabling authorization. See the [“Specifying TACACS+ Servers” section on page 30-17](#) or the [“Specifying RADIUS Servers” section on page 30-23](#) for more information on server setup.
- Configure RADIUS and TACACS+ keys to encrypt protocol packets before enabling authorization. See the [“Specifying the TACACS+ Key” section on page 30-19](#) or the [“Specifying the RADIUS Key” section on page 30-24](#) for more information on the key setup.

Configuring TACACS+ Authorization

The next two sections describe how to configure TACACS+ authorization on the switch.

Enabling TACACS+ Authorization

To enable TACACS+ authorization on the switch, perform this task in privileged mode:

CISCO Confidential - DRAFT

	Task	Command
Step 1	Enable authorization for normal login mode. Enter the console or telnet keywords if you want to enable authorization only for console port or Telnet connection attempts. Enter the both keyword to enable authorization for both console port and Telnet connection attempts.	set authorization exec enable {option} {fallbackoption} [console telnet both]
Step 2	Enable authorization for enable mode. Enter the console or telnet keywords if you want to enable authorization only for console port or Telnet connection attempts. Enter the both keyword to enable authorization for both console port and Telnet connection attempts.	set authorization enable enable {option} {fallbackoption} [console telnet both]
Step 3	Enable authorization of configuration commands. Enter the console or telnet keywords if you want to enable authorization only for console port or Telnet connection attempts. Enter the both keyword to enable authorization for both console port and Telnet connection attempts.	set authorization commands enable {config all} {option} {fallbackoption} [console telnet both]
Step 4	Verify the TACACS+ authorization configuration.	show authorization

This example shows how to enable TACACS+ EXEC mode authorization for both console and Telnet connections. Authorization is configured with the **tacacs+** option. The fallback option is **deny**.

```
Console> (enable) set authorization exec enable tacacs+ deny both
Successfully enabled enable authorization.
Console>
```

This example shows how to enable TACACS+ enable mode authorization for console and Telnet connections. Authorization is configured with the **tacacs+** option. The fallback option is **deny**.

```
Console> (enable) set authorization enable enable tacacs+ deny both
Successfully enabled enable authorization.
Console>
```

This example shows how to enable TACACS+ command authorization for both console and Telnet connections. Authorization is configured with the **tacacs+** option. The fallback option is **deny**.

```
Console> (enable) set authorization commands enable config tacacs+ deny both
Successfully enabled commands authorization.
Console> (enable)
```

This example shows how to verify the configuration:

```
Console> (enable) show authorization
Telnet:
-----
           Primary      Fallback
           -----      -
exec:      tacacs+      deny
enable:    tacacs+      deny
commands:
  config:  tacacs+      deny
  all:     -            -
Console:
```

CISCO Confidential - DRAFT

```
-----
           Primary   Fallback
           -----   -----
exec:      tacacs+   deny
enable:    tacacs+   deny
commands:
  config:   tacacs+   deny
  all:      -         -
Console> (enable)
```

Disabling TACACS+ Authorization

To disable TACACS+ authorization on the switch, perform this task in privileged mode:

	Task	Command
Step 1	Disable authorization for normal mode. Enter the console or telnet keywords if you want to disable authorization only for console port or Telnet connection attempts. Enter the both keyword to enable authorization for both console port and Telnet connection attempts.	set authorization exec disable [console telnet both]
Step 2	Disable authorization for enable mode. Enter the console or telnet keywords if you want to disable authorization only for console port or Telnet connection attempts. Enter the both keyword to enable authorization for both console port and Telnet connection attempts.	set authorization enable disable [console telnet both]
Step 3	Disable authorization of configuration commands. Enter the console or telnet keywords if you want to disable authorization only for console port or Telnet connection attempts. Enter the both keyword to enable authorization for both console port and Telnet connection attempts.	set authorization commands disable [console telnet both]
Step 4	Verify the TACACS+ authorization configuration.	show authorization

This example shows how to disable TACACS+ EXEC mode authorization for both console and Telnet connections and how to verify the configuration:

```
Console> (enable) set authorization exec disable both
Successfully disabled enable authorization.
Console> (enable)
```

This example shows how to disable TACACS+ enable mode authorization for both console and Telnet connections and how to verify the configuration:

```
Console> (enable) set authorization enable disable both
Successfully disabled enable authorization.
Console> (enable)
```

This example shows how to disable TACACS+ command authorization for both console and Telnet connections and how to verify the configuration:

```
Console> (enable) set authorization commands disable both
Successfully disabled commands authorization.
Console> (enable)
```

CISCO Confidential - DRAFT

This example shows how to verify the configuration:

```
Console> (enable) show authorization
```

```
Telnet:
```

```
-----
           Primary  Fallback
           -----  -----
exec:      tacacs+   deny
enable:    tacacs+   deny
commands:
  config:  tacacs+   deny
  all:     tacacs+   deny
```

```
Console:
```

```
-----
           Primary  Fallback
           -----  -----
exec:      tacacs+   deny
enable:    tacacs+   deny
commands:
  config:  tacacs+   deny
  all:     tacacs+   deny
```

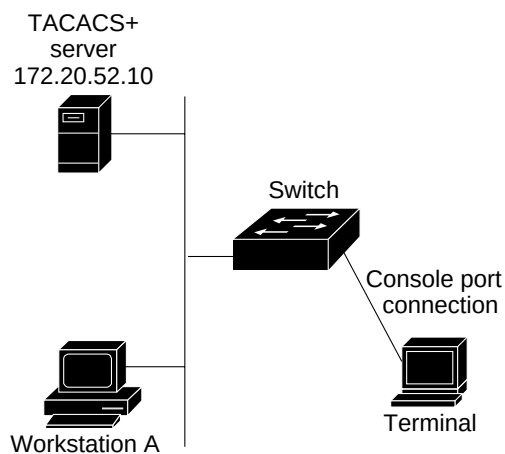
```
Console> (enable)
```

Authorization Example

Figure 30-4 shows a simple example of network topology that uses TACACS+.

In this example, TACACS+ authorization is enabled for enable mode access to the switch for both Telnet and console connections, authorizing configuration commands. When Workstation A initiates a command on the switch, the switch registers a request with the TACACS+ daemon. The TACACS+ daemon determines if the user is authorized to use the feature and sends a response either executing the command or denying access.

Figure 30-4 Example of a TACACS+ Network Topology



This example show that TACACS+ authorization is enabled for enable mode access to the switch for both Telnet and console connections, authorizing configuration commands:

CISCO Confidential - DRAFT

```

Console> (enable) set authorization enable enable tacacs+ deny both
Successfully enabled enable authorization.
Console> (enable) set authorization commands enable config tacacs+ deny both
Successfully enabled commands authorization.
Console> (enable) show authorization
Telnet:
-----
           Primary   Fallback
           -----   -
exec:      tacacs+   deny
enable:    tacacs+   deny
commands:
  config:   tacacs+   deny
  all:      -         -

Console:
-----
           Primary   Fallback
           -----   -
exec:      tacacs+   deny
enable:    tacacs+   deny
commands:
  config:   tacacs+   deny
  all:      -         -
Console> (enable)

```

Understanding How Accounting Works

The following sections describe how accounting works.

Accounting Overview

You can configure these accounting methods to monitor access to the switch:

- TACACS+ accounting
- RADIUS accounting

Accounting allows you to track user activity to a specified host, suspicious connection attempts in the network, and unauthorized changes to the NAS configuration. The accounting information is sent to the accounting server where it is saved as a record. Accounting information typically consists of the user's action and the duration for which the action lasted. You can use the accounting feature for security, billing, and resource allocation purposes.

The accounting protocol operates in a client-server model, using TCP for transport. The NAS acts as the client, and the accounting server acts as the daemon. The NAS sends accounting information to the server. After successfully processing the information, the server sends a response to the NAS, acknowledging the request. All transactions between the NAS and server are authenticated using a key.

After accounting has been enabled and an accountable event occurs on the system, the accounting information is gathered dynamically in memory. When the event ends, an accounting record is created and sent to the NAS; the system then deletes the record from memory. The amount of memory that is used by the NAS for accounting varies depending on the number of concurrent accountable events.

CISCO Confidential - DRAFT

Accounting Events

You can configure accounting for the following types of events:

- EXEC mode accounting—Provides information about user EXEC sessions (normal login sessions) on the NAS. This information includes the duration of the EXEC session but does not include traffic statistics.
- Connect accounting—Provides information about all outbound connections from the NAS (such as Telnet, rlogin).



Note If you get a connection immediately upon login and then your connection is terminated, the EXEC and connect events will overlap and will have almost identical start and stop times.

- System accounting—Provides information on system events not related to users. This information includes system reset, system boot, and user configuration of accounting.
- Command accounting—Sends a record for each command that is issued by the user. This permits audit trail information to be gathered.

Specifying When to Create Accounting Records

You can configure the switch to gather accounting information and create records. When you configure accounting (using the **set accounting command**), the switch can generate two types of records:

- Start records—Include partial information of the event (when the event started, type of service, and traffic statistics).
- Stop records—Include complete information of the event (when the event started, its duration, type of service, and traffic statistics).

Accounting records are created and sent to the server at two events:

- Start-stop—Accounting records are sent at both the start and stop of an action if the action has duration. If the NAS fails to send the accounting record at the start of the action, it still allows you to proceed with the action.
- Stop-only—Accounting records are sent only at the termination of the event. Commands are assumed to have zero duration, so only stop records are generated for command accounting. No users are associated with system events; therefore, the **start-stop** option in the **set accounting system** command is ignored for system events. The **stop-only** option in the **set accounting** commands provides complete accounting information.



Note Stop records include complete information of the event (when the event started, its duration, and traffic statistics). However, you might want redundancy and also to monitor both start and stop records of events occurring on the NAS.

Specifying RADIUS Servers

To specify one or more RADIUS servers, perform this task in privileged mode:

CISCO Confidential - DRAFT

	Task	Command
Step 1	Specify the IP address of up to three RADIUS servers. Specify the primary server using the primary keyword. Optionally, specify the destination UDP port to use on the server.	set radius server <i>ip_addr</i> [acct-port <i>port_number</i>] [primary]
Step 2	Verify the RADIUS server configuration.	show radius

This example shows how to specify a RADIUS server and verify the configuration:

```
Console> (enable) set radius server 172.20.52.3
172.20.52.3 with auth-port 1812 added to radius server table as primary server.
```

```
Console> (enable) show radius
```

```
Login Authentication: Console Session Telnet Session
-----
tacacs                disabled          disabled
radius                disabled          disabled
local                 enabled(primary) enabled(primary)
```

```
Enable Authentication: Console Session Telnet Session
-----
tacacs                disabled          disabled
radius                disabled          disabled
local                 enabled(primary) enabled(primary)
```

```
Radius Deadtime:           0 minutes
Radius Key:
Radius Retransmit:         2
Radius Timeout:            5 seconds
```

```
Radius-Server              Status Auth-port
-----
172.20.52.3                 primary 1812
Console> (enable)
```

Updating the Server

You can configure the switch to send accounting information to the TACACS+ server. There are two options:

- **Newinfo**—Sends accounting information to the server only when new accounting information becomes available.
- **Periodic**—Sends accounting update records at regular intervals. This option can be used to keep up-to-date connection and session information even if the NAS restarts and loses the initial start time. You must set a time lapse between periodic updates. Valid intervals are from 1 to 71582 minutes.

Suppressing Accounting

You can configure the system to suppress accounting when an unknown user with no username accesses the switch by using the **set accounting suppress null-username enable** command.

**Note**

RADIUS and TACACS+ accounting are the same, except that RADIUS does not do command accounting, periodic updates, or allow null-username suppression.

Configuring Accounting

The following sections describe how to configure accounting for both TACACS+ and RADIUS.

Accounting Default Configuration

Table 30-4 shows the default accounting configuration.

Table 30-4 Accounting Default Configuration

Feature	Default
Accounting	Disabled
Accounting events (EXEC, system, commands, and connect)	Disabled
Accounting records	Stop-only

Accounting Configuration Guidelines

This section lists the guidelines for configuring accounting on the switch:

- Configure RADIUS and TACACS+ servers before enabling accounting. See the “[Specifying TACACS+ Servers](#)” section on page 30-17 or the “[Specifying RADIUS Servers](#)” section on page 30-23, for more information on server setup.
- Configure RADIUS and TACACS+ keys to encrypt protocol packets before enabling accounting. See the “[Specifying the TACACS+ Key](#)” section on page 30-19 or the “[Specifying the RADIUS Key](#)” section on page 30-24, for more information on the key setup.

**Note**

The amount of DRAM that is allocated for one accounting event is approximately 500 bytes. The total amount of DRAM that is used by accounting depends on the number of concurrent accountable events occurring in the system.

Configuring Accounting

The next two sections describe how to configure RADIUS and TACACS+ accounting on the switch.

Enabling Accounting

To enable accounting on the switch, perform this task in privileged mode:

CISCO Confidential - DRAFT

	Task	Command
Step 1	Enable accounting for connection events.	set accounting connect enable {start-stop stop-only} {tacacs+ radius}
Step 2	Enable accounting for EXEC mode.	set accounting exec enable {start-stop stop-only} {tacacs+ radius}
Step 3	Enable accounting for system events.	set accounting system enable {start-stop stop-only} {tacacs+ radius}
Step 4	Enable accounting of configuration commands.	set accounting commands enable {config all} {stop-only} tacacs+
Step 5	Enable suppression of information for unknown users.	set accounting suppress null-username enable
Step 6	Configure accounting to be updated as new information is available.	set accounting update {new-info {periodic [interval]}}
Step 7	Verify the accounting configuration.	show accounting

This example shows how to enable stop-only TACACS+ accounting events:

```
Console> (enable) set accounting connect enable stop-only tacacs+
Accounting set to enable for connect events in stop-only mode.
Console> (enable)
```

```
Console> (enable) set accounting exec enable stop-only tacacs+
Accounting set to enable for exec events in stop-only mode.
Console> (enable)
```

```
Console> (enable) set accounting system enable stop-only tacacs+
Accounting set to enable for system events in stop-only mode.
Console> (enable)
```

```
Console> (enable) set accounting commands enable all stop-only tacacs+
Accounting set to enable for commands-all events in stop-only mode.
Console> (enable)
```

This example shows how to suppress accounting of unknown users:

```
Console> (enable) set accounting suppress null-username enable
Accounting will be suppressed for user with no username.
Console> (enable)
```

This example shows how to periodically update the server:

```
Console> (enable) set accounting update periodic 120
Accounting updates will be periodic at 120 minute intervals.
Console> (enable)
```

This example shows how to verify the configuration:

```
Console> (enable) show accounting
Event      Method  Mode
-----
exec:      tacacs+ stop-only
connect:   tacacs+ stop-only
system:    tacacs+ stop-only
commands:
config:    -      -
all:       tacacs+ stop-only
TACACS+ Suppress for no username: enabled
```


CISCO Confidential - DRAFT

Update Frequency: periodic, Interval = 120

Accounting information:

```
-----
Active Accounted actions on tty0, User (null) Priv 0
Active Accounted actions on tty288091924, User (null) Priv 0
Overall Accounting Traffic:
      Starts   Stops   Active
      -----
Exec           0       0       0
Connect        0       0       0
Command        0       0       0
System         1       0       0
Console> (enable)
```

Disabling Accounting

To disable accounting on the switch, perform this task in privileged mode:

	Task	Command
Step 1	Disable accounting for connection events.	set accounting connect disable
Step 2	Disable accounting for EXEC mode.	set accounting exec disable
Step 3	Disable accounting for system events.	set accounting system disable
Step 4	Disable accounting of configuration commands.	set accounting commands disable
Step 5	Disable suppression of information for unknown users.	set accounting suppress null-username disable
Step 6	Verify the accounting configuration.	show accounting

This example shows how to disable stop-only accounting:

```
Console> (enable) set accounting connect disable
Accounting set to disable for connect events.
Console> (enable)
```

```
Console> (enable) set accounting exec disable
Accounting set to disable for exec events.
Console> (enable)
```

```
Console> (enable) set accounting system disable
Accounting set to disable for system events.
Console> (enable)
```

```
Console> (enable) set accounting commands disable
Accounting set to disable for commands-all events.
Console> (enable)
```

This example shows how to disable suppression of unknown users:

```
Console> (enable) set accounting suppress null-username disable
Accounting will be not be suppressed for user with no username.
Console> (enable)
```

This example shows how to verify the configuration:

```
Console> (enable) show accounting
Event      Method  Mode
-----
```

CISCO Confidential - DRAFT

```

exec:      -      -
connect:   -      -
system:    -      -
commands:
config:    -      -
all:       -      -

TACACS+ Suppress for no username: disabled
Update Frequency: new-info

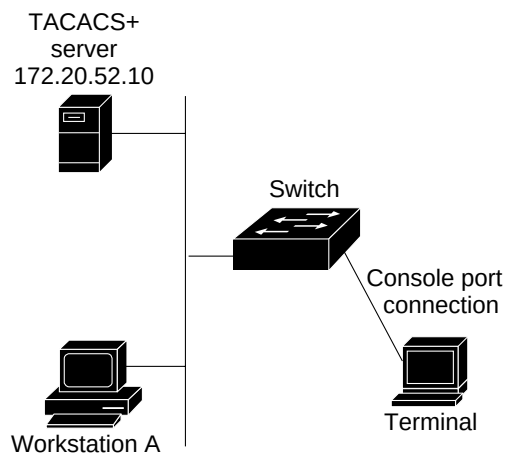
Accounting information:
-----
Active Accounted actions on tty0, User (null) Priv 0
Active Accounted actions on tty288091924, User (null) Priv 0
Overall Accounting Traffic:
      Starts   Stops   Active
      -----
Exec          0       0       0
Connect       0       0       0
Command       0       0       0
System        1       2       0
Console> (enable)

```

Accounting Example

Figure 30-5 shows a simple network topology using TACACS+. When Workstation A initiates an accountable event on the switch, the switch gathers event information and forwards the information to the server at the conclusion of the event. Accounting information is gathered at the conclusion of the event. Accounting is suspended for unknown users and the system is updated periodically every 120 minutes.

Figure 30-5 Example of a TACACS+ Network Topology



This example shows that TACACS+ accounting is enabled for connection, EXEC, system, and all command accounting:

```

Console> (enable) set accounting connect enable stop-only tacacs+
Accounting set to enable for connect events in stop-only mode.
Console> (enable) set accounting exec enable stop-only tacacs+
Accounting set to enable for exec events in stop-only mode.

```

CISCO Confidential - DRAFT

```

Console> (enable) set accounting commands enable all stop-only tacacs+
Accounting set to enable for commands-all events in stop-only mode.
Console> (enable) set accounting update periodic 120
Accounting updates will be periodic at 120 minute intervals.
Console> (enable) show accounting
Event      Method  Mode
-----
exec:      tacacs+ stop-only
connect:   tacacs+ stop-only
system:    tacacs+ stop-only
commands:
config:    -      -
all:       tacacs+ stop-only

TACACS+ Suppress for no username: enabled
Update Frequency: periodic, Interval = 120

Accounting information:
-----
Active Accounted actions on tty0, User (null) Priv 0
Active Accounted actions on tty288091924, User (null) Priv 0
Overall Accounting Traffic:
      Starts   Stops   Active
      -----
Exec           0         0         0
Connect        0         0         0
Command         0         0         0
System         1         0         0
Console> (enable)

```

CISCO Confidential - DRAFT

Configuring 802.1x Authentication

This chapter describes how to configure 802.1x authentication on the Catalyst 4000 family switches.

**Note**

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 4500 Series, Catalyst 2948G, and Catalyst 2980G Switches Command Reference* publication.

**Note**

For information on configuring ports to allow or restrict traffic based on host MAC addresses, see Chapter 16, [“Configuring Port Security.”](#)

**Note**

For information on configuring authentication, authorization, and accounting (AAA) to monitor and control access to the command-line interface (CLI) on the Catalyst 4000 family switches, see Chapter 30, [“Configuring the Switch Access Using AAA.”](#)

This chapter consists of these sections:

- [Understanding How 802.1x Authentication Works, page 31-1](#)
- [Authentication Default Configuration, page 31-7](#)
- [Authentication Configuration Guidelines, page 31-7](#)
- [Configuring 802.1x Authentication on the Switch, page 31-8](#)

Understanding How 802.1x Authentication Works

IEEE 802.1x is a client-server-based access control and authentication protocol that restricts unauthorized devices from connecting to a local area network (LAN) through publicly accessible ports. 802.1x authenticates each user device that is connected to a switch port before making available any services that are offered by the switch or the LAN. Until the device is authenticated, 802.1x access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the device is connected. After authentication is successful, normal traffic can pass through the port.

802.1x controls network access by creating two distinct virtual access points at each port. One access point is an uncontrolled port; the other is a controlled port. All traffic through the single port is available to both access points. Only EAPOL traffic is allowed to pass through the uncontrolled port, which is

CISCO Confidential - DRAFT

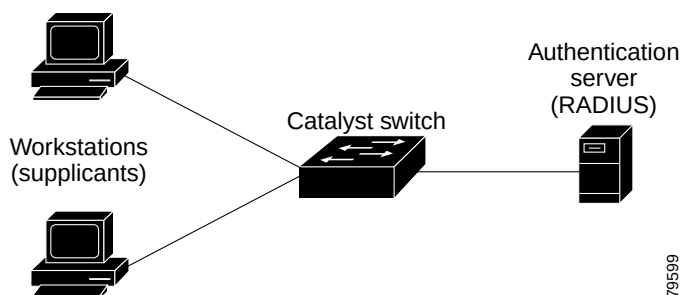
always open. The controlled port is open *only* when the device that is connected to the port has been authorized by 802.1x. After this authorization takes place, the controlled port opens, allowing normal traffic to pass. You can restrict traffic in both directions or just incoming traffic.

The following sections describe how 802.1x authentication work.

Device Roles

With 802.1x port-based authentication, the devices in the network have specific roles. (See [Figure 31-1](#).)

Figure 31-1 802.1x Device Roles



- **Host**—Requests access to the LAN and switch services and responds to requests from the switch. The workstation must be running 802.1x-compliant software.



Note

IEEE 802.1x uses the term *supplicant* for *client* or *host*. In this publication, we use *host* instead of *supplicant* because *host* is used in the Catalyst 4000 family CLI syntax.

- **Authentication server**—Performs the actual authentication of the host. The authentication server validates the identity of the host and notifies the switch whether or not the host is authorized to access the LAN and switch services. Because the switch acts as the proxy, the authentication service is transparent to the host. In this release, the Remote Authentication Dial-In User Service (RADIUS) security system with Extensible Authentication Protocol (EAP) extensions is the only supported authentication server; it is available in Cisco Secure Access Control Server version 3.0. RADIUS operates in a client/server model in which secure authentication information is exchanged between the RADIUS server and one or more RADIUS clients.
- **Switch**—Controls the physical access to the network based on the authentication status of the host. The switch acts as an intermediary (proxy) between the host and the authentication server, requesting identity information from the host, verifying that information with the authentication server, and relaying a response to the host. The switch interacts with the RADIUS client. The RADIUS client encapsulates and decapsulates the EAP frames and interacts with the authentication server.

When the switch receives Extensible Authentication Protocol over LAN (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 host.

CISCO Confidential - DRAFT

Authentication Initiation and Message Exchange

The switch or the host can initiate authentication. If you enable authentication on a port by using the **set port dot1x mod/port port-control auto** command, the switch must initiate authentication when it determines that the port link state transitions from down to up. The switch sends an EAP-request/identity frame to the host to request its identity (typically, the switch sends an initial identity/request frame that is followed by one or more requests for authentication information). When the host receives the frame, it sends an EAP-response/identity frame.

However, if during bootup, the host does not receive an EAP-request/identity frame from the switch, the host can initiate authentication by sending an EAPOL-start frame, which prompts the switch to request the host's identity.



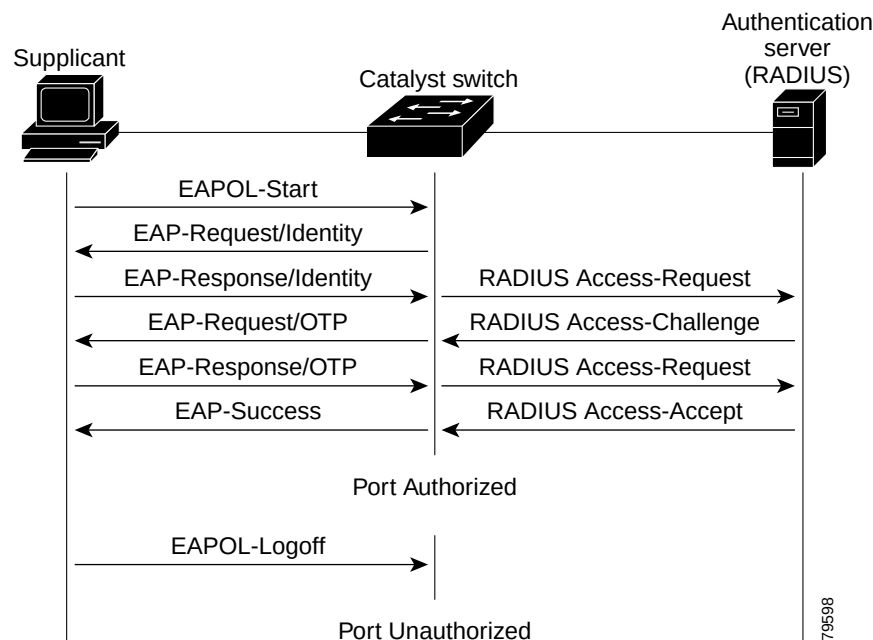
Note

If 802.1x is not enabled or supported on the network access device, any EAPOL frames from the host are dropped. If the host does not receive an EAP-request/identity frame after three attempts to start authentication, the host transmits frames as if the port is in the authorized state. A port that is in the authorized state means that the host has been successfully authenticated. For more information, see the [“Ports in Authorized and Unauthorized States”](#) section on page 31-4.

When the host supplies its identity, the switch acts as the intermediary, passing EAP frames between the host 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 31-4.

The specific exchange of EAP frames depends on the authentication method that is being used. [Figure 31-2](#) shows a message exchange that is initiated by the host using the One-Time-Password (OTP) authentication method with a RADIUS server.

Figure 31-2 Message Exchange



CISCO Confidential - DRAFT

Ports in Authorized and Unauthorized States

The switch port state determines if the host is granted access to the network. The port starts in the *unauthorized* state. In this state, the port disallows all ingress and egress traffic except for 802.1x protocol packets. When a host is successfully authenticated, the port transitions to the *authorized* state, allowing all traffic for the host to flow normally.

If a host that does not support 802.1x is connected to an unauthorized 802.1x port, the switch requests the host's identity. In this situation, the host does not respond to the request, the port remains in the unauthorized state, and the host is not granted access to the network.

When an 802.1x-enabled host connects to a port that is not running the 802.1x protocol, the host initiates the authentication process by sending the EAPOL-start frame. When no response is received, the host sends the request for a fixed number of times. Because no response is received, the host begins sending frames as if the port is in the authorized state.

You control the port authorization state by using the **set port dot1x mod/port port-control** command and these keywords:

- **force-authorized**—Disables 802.1x authentication and causes the port to transition to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1x-based authentication of the host. This is the default setting.
- **force-unauthorized**—Causes the port to remain in the unauthorized state, ignoring all attempts by the host to authenticate. The switch cannot provide authentication services to the host through the interface.
- **auto**—Enables 802.1x authentication and causes the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up or when an EAPOL-start frame is received. The switch requests the identity of the host and begins relaying authentication messages between the host and the authentication server. Each host attempting to access the network is uniquely identified by the switch by using the host's MAC address.

If the host is successfully authenticated (receives an Accept frame from the authentication server), the port state changes to authorized, and all frames from the authenticated host are allowed through the port. If the authentication fails, the port remains in the unauthorized state, but authentication can be retried. If the switch cannot reach the authentication server, it 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 host logs off, the server 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.

Table 31-1 defines the terms used in 802.1x.

*CISCO Confidential - DRAFT***Table 31-1 802.1x Terminology**

Term	Definition
Authenticator PAE	(Referred to as the “authenticator”) entity at one end of a point-to-point LAN segment that enforces host authentication. The authenticator is independent of the actual authentication method and functions only as a pass-through for the authentication exchange. It communicates with the host, submits the information from the host to the authentication server, and authorizes the host when instructed to do so by the authentication server.
Authentication server	Entity that provides the authentication service for the authenticator PAE. It checks the credentials of the host PAE, and then notifies its client, the authenticator PAE, whether the host PAE is authorized to access the LAN/switch services.
Authorized state	Status of the port after the host PAE is authorized.
Both	Bidirectional flow control, incoming and outgoing, at an unauthorized switch port.
Controlled port	Secured access point.
EAP	Extensible Authentication Protocol.
EAPOL ¹	Encapsulated EAP messages that can be handled directly by a LAN MAC service.
In	Flow control only on incoming frames in an unauthorized switch port.
Port	Single point of attachment to the LAN infrastructure (for example, MAC bridge ports).
PAE ²	Protocol object that is associated with a specific system port.
PDU	Protocol data unit.
RADIUS	Remote Access Dial In User Service.
PAE	(Referred to as the “host”) entity that requests access to the LAN/switch services and responds to information requests from the authenticator.
Unauthorized state	Status of the port before the host PAE is authorized.
Uncontrolled port	Unsecured access point that allows the uncontrolled exchange of PDUs.

1. EAPOL = Extensible Authorization Protocol over LAN

2. PAE = Port access entity

Authentication Server

The frames exchanged between the authenticator and the authentication server are dependent on the authentication mechanism, so they are not defined by the 802.1x standard. You can use other protocols, but we recommend RADIUS for authentication, particularly when the authentication server is located remotely, because RADIUS has extensions that support encapsulation of EAP frames built into it.

802.1x Parameters Configurable on the Switch

With 802.1x, you can do the following:

CISCO Confidential - DRAFT

- Specify force-authorized port control, force-unauthorized port control, or automatic 802.1x port control
- Enable or disable multiple hosts on a specific port
- Enable or disable system authentication control
- Specify the quiet time interval
- Specify the authenticator to host retransmission time interval
- Specify the back-end authenticator to host retransmission time interval
- Specify the back-end authenticator to authentication server retransmission time interval
- Specify the number of frames that are retransmitted from the back-end authenticator to host
- Specify the automatic host reauthentication time interval
- Specify the port shutdown timeout period after a security violation
- Enable or disable automatic host reauthentication

802.1x VLAN Assignment Using a RADIUS Server

In software release 6.3 or earlier releases, once the 802.1x host is authenticated, it joins an NVRAM-configured VLAN. With software release 7.2(1) and later releases, after authentication, an 802.1x host can receive its VLAN assignment from the RADIUS server.

The VLAN assignment feature allows you to restrict users to a specific VLAN. For example, you could put guest users in a VLAN with limited access to the network.

802.1x authenticated ports are assigned to a VLAN based on the username of the host that is connected to the port. The VLAN assignment feature works with the RADIUS server, which has a database of username-to-VLAN mappings.

After a successful 802.1x authentication of the port, the RADIUS server sends the VLAN in which the user needs to be given access. 802.1x port behavior with the VLAN assignment feature is summarized as follows:

- At linkup, the server places an 802.1x port in its original NVRAM-configured VLAN.
- After linkup, the server can put the port in the RADIUS-supplied VLAN if the RADIUS-supplied VLAN is valid and active in the management domain.
- If the port is currently in a different VLAN, the port is moved to the RADIUS-supplied VLAN.
- If the RADIUS-supplied VLAN is not active in the management domain, the server puts the port in an inactive state.
- If the RADIUS-supplied VLAN is invalid or there is a problem with the port hardware, the server moves the port to the 802.1x unauthorized state.
- If you enabled the multiple hosts option on an 802.1x port, the server places all hosts in the same RADIUS-supplied VLAN received by the first authenticated user.
- When an 802.1x-configured module goes down, the server clears all Enhanced Address Recognition Logic (EARL) entries for 802.1x ports.
- When an 802.1x-configured module comes up, the server configures all 802.1x ports in NVRAM-configured VLANs.
- If you clear an 802.1x-configured module's configuration, all the 802.1x ports are moved to the NVRAM-configured VLAN and all the EARL entries for the 802.1x ports are cleared.

CISCO Confidential - DRAFT

- If you move an 802.1x port from an authorized to an unauthorized state, the server moves the port to the NVRAM-configured VLAN.

In order for the 802.1x VLAN assignment using a RADIUS server to successfully complete, the RADIUS server must return the following three RFC 2868 attributes back to the authenticator (the Cisco switch to which the host attaches):

- [64] Tunnel-Type = VLAN
- [65] Tunnel-Medium-Type = 802
- [81] Tunnel-Private-Group-Id = VLAN NAME

Attribute [64] must contain the value “VLAN” (type 13). Attribute [65] must contain the value “802” (type 6). Attribute [81] specifies the VLAN name in which the successfully authenticated 802.1x host should be put.

**Note**

You must specify the VLAN by its name and not by its number.

Authentication Default Configuration

Table 31-2 shows the default configuration for authentication.

Table 31-2 802.1x Authentication Default Configuration

Feature	Default Value
802.1x port control	Force-Authorized
802.1x multiple hosts	Disabled
802.1x system authentication control	Enable
802.1x quiet period time	60 sec
802.1x authenticator to host retransmission time	30 sec
802.1x back-end authenticator to host retransmission time	30 sec
802.1x back-end authenticator to authentication server retransmission time	30 sec
802.1x number of frames retransmitted from back-end authenticator to host	2 frames
802.1x automatic host reauthentication time	3600 sec
802.1x automatic authenticator reauthentication of host	Disabled
802.1x shutdown timeout period	0 seconds

Authentication Configuration Guidelines

This section provides the guidelines for configuring 802.1x authentication on the switch:

CISCO Confidential - DRAFT

- 802.1x will work with other protocols, but we recommend that you use RADIUS with a remotely located authentication server.
- 802.1x is supported only on Ethernet ports.
- You cannot enable 802.1x on a trunk port until you turn off the trunking feature on that port. You cannot enable trunking on an 802.1x port.
- You cannot enable 802.1x on a dynamic port until you turn off the DVLAN feature on that port. You cannot enable DVLAN on an 802.1x port.
- You cannot enable 802.1x on a channeling port until you turn off the channeling feature on that port. You cannot enable channeling on an 802.1x port.
- You cannot enable 802.1x on a switched port analyzer (SPAN) destination port, and you cannot configure SPAN destination on an 802.1x port. However, you can configure an 802.1x port as a SPAN source port.

Configuring 802.1x Authentication on the Switch

The following sections describe how to configure 802.1x authentication on the switch.

Enabling 802.1x Globally

You must enable 802.1x authentication for the entire system before configuring it for individual ports. After you globally enable 802.1x authentication, you can configure individual ports for 802.1x authentication if they meet the specific requirements that are required by 802.1x. To enable 802.1x authentication for individual ports, see the [“Enabling and Initializing 802.1x Authentication for Individual Ports” section on page 31-9](#).

To globally enable 802.1x authentication, perform this task in privileged mode:

Task	Command
Globally enable 802.1x.	set dot1x system-auth-control enable

This example shows how to globally enable 802.1x authentication:

```
Console> (enable) set dot1x system-auth-control enable
dot1x system-auth-control enabled.
```

Disabling 802.1x Globally

When 802.1x authentication is enabled for the entire system, you can disable it globally. When 802.1x authentication is disabled globally, it is no longer available at any port, even ports that were previously configured for it.

To globally disable 802.1x authentication, perform this task in privileged mode:

Task	Command
Globally disable 802.1x.	set dot1x system-auth-control disable

CISCO Confidential - DRAFT

This example shows how to globally disable 802.1x authentication:

```
Console> (enable) set dot1x system-auth-control disable
dot1x system-auth-control disabled.
```

Enabling and Initializing 802.1x Authentication for Individual Ports

After 802.1x authentication is globally enabled, you can enable and initialize 802.1x authentication from the console only for individual ports. To globally enable 802.1x authentication, see the [“Enabling 802.1x Globally”](#) section on page 31-8.



Note

You must specify at least one RADIUS server before you can enable 802.1x authentication on the switch. For information on specifying a RADIUS server, see the [“Specifying RADIUS Servers”](#) section on page 30-23.

To enable and initialize 802.1x authentication for access to the switch, perform this task in privileged mode:

	Task	Command
Step 1	Enable 802.1x control on a specific port.	set port dot1x mod/port port-control auto
Step 2	Initialize 802.1x on the same port.	set port dot1x mod/port initialize
Step 3	Verify the 802.1x configuration.	show port dot1x mod/port

This example shows how to enable 802.1x authentication on port 1 in module 4, initialize 802.1x authentication on the same port, and verify the configuration:

```
Console> (enable) set port dot1x 4/1 port-control auto
Port 4/1 dot1x port-control is set to auto.
Trunking disabled for port 4/1 due to Dot1x feature.
Spanntree port fast start option enabled for port 4/1.
Console> (enable) set port dot1x 4/1 initialize
Port 4/1 initializing...
Port 4/1 dot1x initialization complete.
```

```
Console> show port dot1x 4/1
```

Port	Auth-State	BEnd-State	Port-Control	Port-Status
4/1	connecting	finished	auto	unauthorized

```
Port Multiple-Host Re-authentication
```

Port	Multiple-Host	Re-authentication
4/1	disabled	disabled

Setting and Enabling Automatic Reauthentication of the Host

You can specify how often 802.1x authentication reauthenticates the host if you do so prior to enabling automatic 802.1x host reauthentication. If you do not specify a time period prior to enabling host reauthentication, 802.1x defaults to 3600 seconds (the valid values are from 1 to 65,535 seconds).

You can enable automatic 802.1x host reauthentication for hosts that are connected to a specific port. To manually reauthenticate the host that is connected to a specific port, see the [“Manually Reauthenticating the Host”](#) section on page 31-10.

CISCO Confidential - DRAFT

To set how often 802.1x authentication reauthenticates the host and enable automatic 802.1x reauthentication, perform this task in privileged mode:

	Task	Command
Step 1	Set the time constant for reauthenticating the host.	set dot1x re-authperiod <i>seconds</i>
Step 2	Enable reauthentication.	set port dot1x <i>mod/port</i> re-authentication enable
Step 3	Verify the 802.1x configuration.	show port dot1x <i>mod/port</i>

This example shows how to set automatic reauthentication to 7200 seconds, enable 802.1x reauthentication, and verify the configuration:

```

Console> (enable) set dot1x re-authperiod 7200
dot1x re-authperiod set to 7200 seconds
Console> (enable) set port dot1x 4/1 re-authentication enable
Port 4/1 re-authentication enabled.
Console> (enable) show port dot1x 4/1
Port  Auth-State      BEnd-State Port-Control      Port-Status
-----
  4/1  connecting      finished   auto               unauthorized
Port  Multiple Host Re-authentication
-----
  4/1  disabled        enabled

```

Manually Reauthenticating the Host

You can manually reauthenticate the host that is connected to a specific port at any time. When you want to configure automatic 802.1x host reauthentication, see the [“Setting and Enabling Automatic Reauthentication of the Host” section on page 31-9](#).

To manually reauthenticate a host that is connected to a specific port, perform this task in privileged mode:

Task	Command
Manually reauthenticate the host that is connected to a specific port.	set port dot1x <i>mod/port</i> re-authenticate

This example shows how to manually reauthenticate the host that is connected to port 1 on module 4:

```

Console> (enable) set port dot1x 4/1 re-authenticate
Port 4/1 re-authenticating...
dot1x re-authentication successful...
dot1x port 4/1 authorized.

```

Enabling Multiple Hosts

You can enable a specific port to allow multiple-user access. When a port is enabled for multiple users, and a host that is connected to that port is authorized successfully, any host (with any MAC address) is allowed to send and receive traffic on that port. If you then connect multiple hosts to that port through a hub, you can reduce the security level on that port.

CISCO Confidential - DRAFT

To enable multiple-user access on a specific port, perform this task in privileged mode:

Task	Command
Enable multiple hosts on a specific port.	set port dot1x mod/port multiple-host enable

This example shows how to enable access for multiple hosts on port 1 on module 4:

```
Console> (enable) set port dot1x 4/1 multiple-host enable  
Port 4/1 multiple hosts allowed.
```

Disabling Multiple Hosts

You can disable multiple-user access on any port where it is enabled.

To disable multiple-user access on a specific port, perform this task in privileged mode:

Task	Command
Disable multiple hosts on a specific port.	set port dot1x mod/port multiple-host disable

This example shows how to disable access for multiple hosts on port 1 on module 4:

```
Console> (enable) set port dot1x 4/1 multiple-host disable  
Port 4/1 multiple hosts not allowed.
```

Setting the Quiet Period

When the authenticator cannot authenticate the host, it remains idle for a set period of time and then tries again. The idle time is determined by the quiet-period value. (The default is 60 seconds.) You may set the value from 0 to 65,535 seconds.

To set the value for the quiet period, perform this task in privileged mode:

Task	Command
Set the quiet-period value.	set dot1x quiet-period seconds

This example shows how to set the quiet period to 45 seconds:

```
Console> (enable) set dot1x quiet-period 45  
dot1x quiet-period set to 45 seconds.
```

Setting the Authenticator-to-Host Retransmission Time for EAP-Request/Identity Frames

The host notifies the authenticator that it received the EAP-request/identity frame. When the authenticator does not receive this notification, the authenticator waits a set period of time and then retransmits the frame. You may set the amount of time that the authenticator waits for notification from 1 to 65,535 seconds. The default is 30 seconds.

CISCO Confidential - DRAFT

To set the authenticator-to-host retransmission time for the EAP-request/identity frames, perform this task in privileged mode:

Task	Command
Set the authenticator-to-host retransmission time for EAP-request/identity frames.	set dot1x tx-period <i>seconds</i>

This example shows how to set the authenticator-to-host retransmission time for the EAP-request/identity frame to 15 seconds:

```
Console> (enable) set dot1x tx-period 15
dot1x tx-period set to 15 seconds.
```

Setting the Supplicant-to-Host Retransmission Time for EAP-Request Frames

The host notifies the back-end authenticator that it received the EAP-request frame. When the back-end authenticator does not receive this notification, the back-end authenticator waits a set period of time, and then retransmits the frame. You may set the amount of time that the back-end authenticator waits for notification from 1 to 65,535 seconds. The default is 30 seconds.

To set the back-end authenticator-to-host retransmission time for the EAP-request frames, perform this task in privileged mode:

Task	Command
Set the back-end authenticator-to-host retransmission time for EAP-request frame.	set dot1x supp-timeout <i>seconds</i>

This example shows how to set the back-end authenticator-to-host retransmission time for the EAP-request frame to 15 seconds:

```
Console> (enable) set dot1x supp-timeout 15
dot1x supp-timeout set to 15 seconds.
```

Setting the Back-End Authenticator-to-Authentication-Server Retransmission Time for Transport Layer Packets

The authentication server notifies the back-end authenticator each time it receives a transport layer packet. When the back-end authenticator does *not* receive a notification after sending a packet, the back-end authenticator waits a set period of time, and then retransmits the packet. You may set the amount of time that the back-end authenticator waits for notification from 1 to 65,535 seconds. The default is 30 seconds.

To set the value for the retransmission of transport layer packets from the back-end authenticator to the authentication server, perform this task in privileged mode:

Task	Command
Set the back-end authenticator-to-authentication-server retransmission time for transport layer packets.	set dot1x server-timeout <i>seconds</i>

CISCO Confidential - DRAFT

This example shows how to set the value for the retransmission time for transport layer packets that are sent from the back-end authenticator to the authentication server to 15 seconds:

```
Console> (enable) set dot1x server-timeout 15
dot1x server-timeout set to 15 seconds.
```

Setting the Back-End Authenticator-to-Host Frame-Retransmission Number

The authentication server notifies the back-end authenticator each time that it receives a specific number of frames. When the back-end authenticator does not receive this notification after sending the frames, the back-end authenticator waits a set period of time and then retransmits the frames. You may set the number of frames that the back-end authenticator retransmits from 1 to 10 (the default is 2).

To set the number of frames that are retransmitted from the back-end authenticator to the host, perform this task in privileged mode:

Task	Command
Set the back-end authenticator-to-host frame retransmission number.	set dot1x max-req count

This example shows how to set the number of retransmitted frames that are sent from the back-end authenticator to the host to 4:

```
Console> (enable) set dot1x max-req 4
dot1x max-req set to 4.
```

Setting the Shutdown Timeout Period

If a port is shut down because of a security violation, you must either manually re-enable it or configure the shutdown timeout period after which the port can be enabled again.

To set the period of time that a port will be disabled after a security violation, perform this task in privileged mode:

Task	Command
Set the shutdown timeout period.	set dot1x shutdown-timeout <i>1- 65535 seconds</i>

This example shows how to set the shutdown timeout period:

```
Console> (enable) set dot1x shutdown-timeout 300
dot1x shutdown-timeout set to 300 seconds.
Console> (enable)
```

Setting the Back-End Authenticator-to-Host Frame-Retransmission Number

The authentication server notifies the back-end authenticator each time that it receives a specific number of frames. When the back-end authenticator does not receive this notification after sending the frames, the back-end authenticator waits a set period of time and then retransmits the frames. You may set the number of frames that the back-end authenticator retransmits from 1 to 10 (the default is 2).

CISCO Confidential - DRAFT

To set the number of frames that are retransmitted from the back-end authenticator to the host, perform this task in privileged mode:

Task	Command
Set the back-end authenticator-to-host frame retransmission number.	set dot1x max-req count

This example shows how to set the number of retransmitted frames that are sent from the back-end authenticator to the host to 4:

```
console> (enable) set dot1x max-req 4
dot1x max-req count set to 4.
Console> (enable)
```

Setting the Back-End Authenticator-to-Host Frame-Retransmission Number

The authentication server notifies the back-end authenticator each time that it receives a specific number of frames. When the back-end authenticator does not receive this notification after sending the frames, the back-end authenticator waits a set period of time and then retransmits the frames. You may set the number of frames that the back-end authenticator retransmits from 1 to 10 (the default is 2).

To set the number of frames that are retransmitted from the back-end authenticator to the host, perform this task in privileged mode:

Task	Command
Set the back-end authenticator-to-host frame retransmission number.	set dot1x max-req count

This example shows how to set the number of retransmitted frames that are sent from the back-end authenticator to the host to 4:

```
Console> (enable) set dot1x max-req 4
dot1x max-req set to 4.
```

Resetting the 802.1x Configuration Parameters to the Default Values

You can reset the 802.1x configuration parameters to the default values with a single command, which also globally disables 802.1x.

To reset the 802.1x configuration parameters to the default values, perform this task in privileged mode:

	Task	Command
Step 1	Reset the 802.1x configuration parameters to the default values and globally disable 802.1x.	clear dot1x config
Step 2	Verify the 802.1x configuration.	show dot1x

This example shows how to reset the 802.1x configuration parameters to the default values:

```
Console> (enable) clear dot1x config
```

CISCO Confidential - DRAFT

```

This command will disable dot1x on all ports and take dot1x parameter values back to
factory defaults.
Do you want to continue (y/n) [n]?y
Dot1x config cleared.
Console> (enable) 2002 Sep 06 11:34:27 %SECURITY-1-DOT1X_BACKEND_SERVER:No Radiu
s servers configured

```

Setting the Trace Severity

You can alter the trace severity for 802.1x authentication. The number setting affects the number of trace messages that are displayed. Low numbers result in fewer messages; high numbers result in more messages.

To set the trace severity for 802.1x, perform this task in privileged mode:

Task	Command
Set the trace severity for 802.1x authentication.	set trace dot1x trace-level

This example shows how to set the trace severity for 802.1x authentication to 5:

```

Console> (enable) set trace dot1x 5
DOT1X tracing set to 5

```

Warning!! Turning on trace may affect the operation of the system.
Use with caution.

Using the show Commands

You can use these **show** commands to access information about 802.1x authentication and its configuration:

- **show port dot1x help**
- **show port dot1x**
- **show port dot1x statistics**
- **show dot1x**

To display the usage options for the **show port dot1x** command, perform this task in normal mode:

Task	Command
Display the usage options for the show port dot1x command.	show port dot1x help

This example shows how to display the usage options for the **show port dot1x** command:

```

Console> (enable) show port dot1x help
Usage: show port dot1x [<mod[/port]>]
       show port dot1x statistics [<mod[/port]>]

```

To display the values for all the parameters that are associated with the authenticator PAE and back-end authenticator on a specific port on a specific module, perform this task in normal mode:

CISCO Confidential - DRAFT

Task	Command
Display the values for all configurable and current state parameters that are associated with the authenticator PAE and back-end authenticator on a specific port on a specific module.	show port dot1x mod/port

This example shows how to display the values for all the parameters that are associated with the authenticator PAE and back-end authenticator on port 1 on module 4:

```

Console> (enable) show port dot1x 4/1
Port  Auth-State      BEnd-State Port-Control      Port-Status
-----
 4/1  connecting        finished   auto                unauthorized
Port  Multiple Host Re-authentication
-----
 4/1  disabled          enabled

```

To display the statistics for the different types of EAP frames that are transmitted and received by the authenticator on a specific port on a specific module, perform this task in normal mode:

Task	Command
Display the statistics for the different types of EAP frames that are transmitted and received by the authenticator on a specific port on a specific module.	show port dot1x statistics mod/port

This example shows how to display the statistics for the different types of EAP frames that are transmitted and received by the authenticator on port 1 on module 4:

```

Console> (enable) show port dot1x statistics 4/1
Port  Tx_Req/Id Tx_Req Tx_Total Rx_Start Rx_Logoff Rx_Resp/Id Rx_Resp
-----
 4/1   97      0    97      0        0        0        0
Port  Rx_Invalid Rx_Len_Err Rx_Total Last_Rx_Frm_Ver Last_Rx_Frm_Src_Mac
-----
 4/1    0        0        0        0              00-00-00-00-00-00

```

To display the global 802.1x parameters, perform this task in normal mode:

Task	Command
Display the PAE capabilities, protocol version, system-auth-control, and other global dot1x parameters.	show dot1x

CISCO Confidential - DRAFT

This example shows how to display the global 802.1x parameters:

```
Console> (enable) show dot1x
PAE Capability           Authenticator Only
Protocol Version         1
system-auth-control      enabled
re-authentication        disabled
max-req                  2
quiet-period             60 seconds
re-authperiod            3600 seconds
server-timeout           30 seconds
supp-timeout             30 seconds
tx-period                30 seconds
```

CISCO Confidential - DRAFT

Modifying the Switch Boot Configuration

This chapter describes how to modify the switch boot configuration, including the BOOT environment variable and the configuration register on the Catalyst enterprise LAN switches.

**Note**

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 4500 Series, Catalyst 2948G, and Catalyst 2980G Switches Command Reference*.

This chapter consists of these sections:

- [Understanding How the Switch Boot Configuration Works, page 32-1](#)
- [Default Switch Boot Configuration, page 32-4](#)
- [Setting the Configuration Register, page 32-4](#)
- [Setting the BOOT Environment Variable, page 32-6](#)
- [Setting and Clearing the CONFIG_FILE Environment Variable, page 32-7](#)
- [Displaying the Switch Boot Configuration, page 32-8](#)

Understanding How the Switch Boot Configuration Works

The following sections describe how the boot configuration works on the Catalyst 4000 family, 2948G, and 2980G switches.

Understanding the Boot Process

The boot process involves two software images: ROM monitor and supervisor engine system code. When you power up or reset the switch, the ROM-monitor code is executed. Depending on the nonvolatile RAM (NVRAM) configuration, the switch either stays in ROM-monitor mode or loads the supervisor engine system code.

Two user-configurable parameters determine how the switch boots: the configuration register and the BOOT environment variable. The configuration register is described in the [“Understanding the Configuration Register” section on page 32-2](#). The BOOT environment variable is described in the [“Understanding the BOOT Environment Variable” section on page 32-3](#).

CISCO Confidential - DRAFT

Understanding the ROM Monitor

The ROM monitor code executes upon switch power-up, reset, or when a fatal exception occurs. The system enters ROM-monitor mode if the switch does not find a valid system 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 system image from Flash memory, from a network server file, or from bootflash.

**Note**

For complete syntax and usage information for the ROM monitor commands, refer to the *Catalyst 4500 Series, Catalyst 2948G, and Catalyst 2980G Switches Command Reference*.

You can enter ROM-monitor mode by restarting the switch and then pressing **Ctrl-C** during the first 5 seconds of startup.

The following functionality is built into the ROM monitor:

- Power-on confidence test
- Hardware initialization
- Boot capability (allows manual boot and autoboot)
- Debug utility and crash analysis
- 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

Understanding the Configuration Register

The configuration register determines whether the switch loads an operating system image and where the system image is stored. The configuration register boot field determines if and how the ROM monitor loads a supervisor engine system image at startup. You can modify the boot field to force the switch to boot a particular system image at startup instead of using the default system image.

The lowest four bits (bits 3, 2, 1, and 0) of the 16-bit configuration register form the boot field. The default boot field value is 0x10F. The possible configuration register boot field settings are as follows:

- When the boot field equals 0000, the switch does not load a system image. The switch enters ROM-monitor mode from which you can enter ROM-monitor commands to manually load a system image.
- When the boot field equals 0001, the switch loads the first valid system image found in onboard Flash memory.
- When the boot field equals a value between 0010 and 1111, the switch loads the system image specified by **boot system** commands in the NVRAM configuration. It attempts to boot the image in the order in which you entered the **boot system** commands. If it cannot boot any image in the BOOT environment variable list, the switch remains in ROM-monitor mode. The exact booting sequence is defined by the ROM monitor.

The other bits in the configuration register function as follows when set:

- Bit 5 (0x0020): Enables CONFIG_FILE recurrence.
- Bit 6 (0x0040): Causes system software to clear NVRAM contents.
- Bit 7 (0x0080): Enables OEM bit (not used).

CISCO Confidential - DRAFT

- Bit 8 (0x0100): Disables break.
- Bit 9 (0x0200): Uses secondary bootstrap (not used by the ROM monitor).
- Bit 10 (0x0400): Provides IP broadcast with all zeros (not used).
- Bits 11/12 (0x0800/0x1000): These bits are always set to 0/0 (9600 baud).
- Bit 13 (0x2000): Boots default Flash software if network boot fails (not used).
- Bit 14 (0x4000): IP broadcasts do not have network numbers (not used).
- Bit 15 (0x8000): Enables diagnostic messages and ignores NVRAM contents (not used).

Understanding the BOOT Environment Variable

The BOOT environment variable specifies a list of image files on various devices from which the switch can boot at startup.

You can add several images to the BOOT environment variable to provide a fail-safe boot configuration. If the first file fails to boot the switch, subsequent images specified in the BOOT variable are tried until the switch boots or there are no additional images to attempt to boot. If there is no valid image to boot, the system enters ROM-monitor mode where you can manually specify an image to boot.

The system stores and executes images in the order in which you added them to the BOOT variable. If you want to change the order in which images are tried at startup, you can either prepend and clear images from the BOOT variable to attain the desired order or you can clear the entire BOOT environment variable and then redefine the list in the desired order.

Understanding the CONFIG_FILE Environment Variable

In software release 5.2 and later releases, you can use the CONFIG_FILE environment variable to specify a list of configuration files on various devices to use to configure the switch at startup. You can specify one of the following functions:

- Nonrecurring—When you add a list of configuration files to the CONFIG_FILE environment variable, the next time that the switch is restarted, the system erases the configuration in NVRAM and uses the specified files to configure the switch. The CONFIG_FILE variable is cleared before the switch is configured. Nonrecurring is the default setting.
- Recurring—When you add a list of configuration files to the CONFIG_FILE environment variable, the list is stored indefinitely in NVRAM. Each time the switch is restarted, the system erases the configuration in NVRAM and configures the switch using the configuration files specified. The CONFIG_FILE variable is not cleared.

**Note**

You can alter the CONFIG_FILE variable and change its recurrence properties by entering commands in the configuration files that are used to configure the switch at startup. For information, see the [“Setting CONFIG_FILE Recurrence”](#) section on page 32-5.

When the switch boots up, if any of the files specified in the CONFIG_FILE environment variable are valid configuration files, the configuration in NVRAM is erased and the system uses the specified configuration file to configure the switch. If multiple valid configuration files are specified, each configuration file is executed in the order in which it appears in the CONFIG_FILE environment variable.

CISCO Confidential - DRAFT

If any specified file is not a valid configuration file, the entry is skipped and subsequent files are tried until there are no additional images specified. If no valid configuration file is specified, the system retains the last configuration stored in NVRAM. For more information about using configuration files, see [Chapter 35, “Working with Configuration Files.”](#)

Default Switch Boot Configuration

[Table 32-1](#) shows the default switch boot configuration.

Table 32-1 Default Switch Boot Configuration

Feature	Default Configuration
Configuration register value	0x10f
Boot method	System boots from the image specified in the BOOT environment variable
ROM monitor console port baud rate	9600 baud ¹
ignore-config parameter	Disabled
BOOT environment variable	Empty
CONFIG_FILE environment variable	bootflash:switch.cfg
CONFIG_FILE recurrence configuration register parameter	Nonrecurring

1. The ROM monitor console port baud rate is always 9600 baud.

Setting the Configuration Register

The following sections describe how to modify the configuration register.

Setting the Boot Field in the Configuration Register

You can determine the boot method the switch will use at the next startup by setting the boot field in the configuration register. This command affects only the configuration register bits that control the boot field and leaves the remaining bits unaltered.

The following boot methods are supported:

- ROM monitor—Use the **rommon** keyword to keep the switch in ROM-monitor mode at startup.
- Bootflash—Use the **bootflash** keyword to cause the switch to boot from the first image stored in the onboard Flash memory.
- System—Use the **system** keyword to boot from the image specified in the BOOT environment variable (the default).

**Note**

We recommend that you use only the **rommon** and **system** options to the **set boot config-register boot** command.

To set the configuration register boot field, perform this task in privileged mode:

CISCO Confidential - DRAFT

Task	Command
Specify the boot field in the configuration register.	set boot config-register boot {rommon bootflash system} [mod_num]

This example shows how to force the switch to enter ROM-monitor mode at the next startup:

```
Console> (enable) set boot config-register boot rommon
Configuration register is 0x0
ignore-config: disabled
auto-config: non-recurring
console baud: 9600
boot: the ROM monitor
Console> (enable)
```

Setting CONFIG_FILE Recurrence

By default, when you set the CONFIG_FILE environment variable, the list of configuration files to use at startup is retained only until the next time the switch is restarted.

You can cause the system software to retain the CONFIG_FILE environment variable settings indefinitely so that each time the switch is restarted, the specified configuration files are used to configure the switch.

This command affects only the configuration register bit that controls whether the CONFIG_FILE environment variable settings are recurring or nonrecurring. The remaining configuration register bits are unaltered.



Caution

With the CONFIG_FILE environment variable set to **recurring**, the current configuration in NVRAM is erased each time the switch is restarted and the switch is configured using the specified configuration files. With the CONFIG_FILE environment variable set to **non-recurring**, the current configuration in NVRAM is erased at the next restart and the switch is configured using the specified configuration files. The NVRAM configuration is retained after subsequent restarts (unless you again set the CONFIG_FILE variable).

To set the switch to retain the current CONFIG_FILE environment variable indefinitely, perform this task in privileged mode:

Task	Command
Set the switch to retain the current CONFIG_FILE environment variable indefinitely.	set boot config-register auto-config {recurring non-recurring}

This example shows how to set the switch to retain the current CONFIG_FILE variable indefinitely:

```
Console> (enable) set boot config-register auto-config recurring
Configuration register is 0x1820
ignore-config: disabled
auto-config: recurring
console baud: 9600
boot: the ROM monitor
Console> (enable)
```

CISCO Confidential - DRAFT

Setting the Switch to Ignore the NVRAM Configuration

You can cause the system software to ignore the configuration information that is stored in NVRAM when the switch is restarted. This command affects only the configuration register bits that control whether the switch ignores the NVRAM configuration and leaves the remaining bits unaltered. This command only affects the next system restart.

**Caution**

Enabling the **ignore-config** parameter is the same as entering the **clear config all** command; that is, it clears the entire configuration stored in NVRAM the next time the switch is restarted.

To set the switch to ignore the NVRAM configuration at the next startup, perform this task in privileged mode:

Task	Command
Set the switch to ignore the contents of NVRAM at startup.	set boot config-register ignore-config enable

This example shows how to set the switch to ignore the NVRAM configuration at the next startup:

```
Console> (enable) set boot config-register ignore-config enable
Configuration register is 0x1860
ignore-config: enabled
auto-config: recurring
console baud: 9600
boot: the ROM monitor
Console> (enable)
```

Setting the BOOT Environment Variable

The next two sections describe how to modify the BOOT environment variable.

Setting the BOOT Environment Variable

To add a system image to the BOOT environment variable, perform this task in privileged mode:

Task	Command
Specify a system image to add to the BOOT environment variable.	set boot system flash device:[filename] [prepend] [mod_num]

This example shows how to add system images to the BOOT environment variable:

```
Console> (enable) set boot system flash bootflash:cat4000.5-1-1.bin
BOOT variable = bootflash:cat4000.5-1-1.bin,1;
Console> (enable) set boot system flash bootflash:cat4000.4-5-2.bin
BOOT variable = bootflash:cat4000.5-1-1.bin,1;bootflash:cat4000.4-5-2.bin,1;
Console> (enable) set boot system flash bootflash:cat4000.6-1-1.bin prepend
BOOT variable = bootflash:cat4000.6-1-1.bin,1;bootflash:cat4000.5-1-1.bin,1;
bootflash:cat4000.4-5-2.bin,1;
Console> (enable)
```

CISCO Confidential - DRAFT

Clearing the BOOT Environment Variable Settings

To clear entries from the BOOT environment variable, perform one of these tasks in privileged mode:

Task	Command
Clear a specific image from the BOOT environment variable.	clear boot system flash <i>device:[filename]</i> <i>[mod_num]</i>
Clear the entire BOOT environment variable.	clear boot system all <i>[mod_num]</i>

This example shows how to clear a specific entry from the BOOT environment variable:

```
Console> (enable) clear boot system flash bootflash:cat4000.5-1-1.bin
BOOT variable = bootflash:cat4000.5-2-1.bin,1;bootflash:cat4000.4-5-2.bin,1;
Console> (enable)
```

This example shows how to clear the entire BOOT environment variable:

```
Console> (enable) clear boot system all
BOOT variable =
Console> (enable)
```

Setting and Clearing the CONFIG_FILE Environment Variable

The next two sections describe how to set and clear the CONFIG_FILE environment variable.



Note

For more information about using configuration files, see [Chapter 35, “Working with Configuration Files.”](#)

Setting the CONFIG_FILE Environment Variable

You can specify multiple configuration files with the **set boot auto-config** command by separating them with a semicolon (;). You must specify both the device name and the filename for each configuration file.



Note

You cannot prepend or append configuration files to the CONFIG_FILE environment variable. Entering the **set boot auto-config** command erases any list of configuration files previously specified using the **set boot auto-config** command.

To set the CONFIG_FILE environment variable, perform this task in privileged mode (depending on your supervisor engine and switch type):

Task	Command
Set the list of configuration files to add to the CONFIG_FILE environment variable.	set boot auto-config <i>device:filename[;device:filename...]</i>

This example shows how to add a list of configuration files to the CONFIG_FILE environment variable:

```
Console> (enable) set boot auto-config bootflash:generic.cfg;bootflash:4003_1_noc.cfg
```

CISCO Confidential - DRAFT

```
CONFIG_FILE variable = bootflash:generic.cfg;bootflash:4003_1_noc.cfg
WARNING: nvram configuration may be lost during next bootup,
        and re-configured using the file(s) specified.
Console> (enable)
```

Clearing CONFIG_FILE Environment Variable Entries

To clear entries from the CONFIG_FILE environment variable, perform this task in privileged mode:

Task	Command
Clear entries in the CONFIG_FILE environment variable.	clear boot auto-config

This example shows how to clear the entries in the CONFIG_FILE environment variable:

```
Console> (enable) clear boot auto-config
CONFIG_FILE variable =
Console> (enable)
```

Displaying the Switch Boot Configuration

To display the current configuration register, BOOT environment variable, and CONFIG_FILE environment variable settings, perform this task in privileged mode:

Task	Command
Display the current configuration register, BOOT environment variable, and CONFIG_FILE environment variable settings.	show boot [<i>mod_num</i>]

This example shows how to display the current configuration register, BOOT environment variable, and CONFIG_FILE environment variable settings:

```
Console> (enable) show boot
BOOT variable = bootflash:cat4000.5-2-1.bin,1;
CONFIG_FILE variable = bootflash:generic.cfg;bootflash:4003_1_noc.cfg

Configuration register is 0x12f
ignore-config: disabled
auto-config: recurring
console baud: 9600
boot: image specified by the boot system commands

Console> (enable)
```

Working with System Software Images

This chapter describes how to work with system software image files on the Catalyst enterprise LAN switches.

**Note**

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 4500 Series, Catalyst 2948G, and Catalyst 2980G Switches Command Reference*.

This chapter consists of these sections:

- [Software Image Naming Conventions, page 33-1](#)
- [Downloading System Software Images to the Switch Using TFTP, page 33-1](#)
- [Uploading System Software Images to a TFTP Server, page 33-4](#)
- [Downloading System Software Images to the Switch Using rcp, page 33-5](#)
- [Uploading System Software Images to an rcp Server, page 33-8](#)
- [Upgrading the ROM Monitor, page 33-9](#)

Software Image Naming Conventions

The software images on the Catalyst 4000 family switches use the following naming conventions. Software release 6.1(3) is used in the examples:

- 6.1(3) Flash image (standard)—cat4000.6-1-3.bin
- 6.1(3) Flash image (CiscoView)—cat4000-**cv**.6-1-3.bin
- 6.1(3) Flash image (Secure Shell)—cat4000-**k9**.6-1-3.bin

Downloading System Software Images to the Switch Using TFTP

The following sections describe how to download system software images to the switch supervisor engine and to intelligent modules.

CISCO Confidential - DRAFT

Understanding How TFTP Software Image Downloads Work

You can download system software images to the switch using the Trivial File Transfer Protocol (TFTP). TFTP allows you to download system image files over the network from a TFTP server.

When you download a software image, the image file is downloaded to the supervisor engine Flash memory. You can store multiple image files on the Flash memory system devices.

For more information on working with system software image files on the Flash file system, see [Chapter 34, “Working With the Flash File System.”](#)

Preparing to Download an Image Using TFTP

Before you begin downloading a software image using TFTP, make sure of the following:

- Ensure that the workstation acting as the TFTP server is configured properly.
- Ensure that the switch has a route to the TFTP server. The switch and the TFTP server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the TFTP server using the **ping** command.
- Ensure that the software image to be downloaded is in the correct directory on the TFTP server (for example, /tftpboot on a UNIX workstation).
- Ensure that the permissions on the file are set correctly. Permissions on the file should be at least read for the specific username. If you are not using a Telnet session with a valid username, you can use the **set rcp username** command to specify a valid username.
- Ensure that a power interruption (or other problem) does not occur during the download procedure; this can corrupt the Flash code. If the Flash code is corrupted, you can connect to the switch through the console port. You can download the Flash code again through an enabled port in VLAN 1. By default, port 1/1 is enabled. You can use port 1/1 or enable another port.

Downloading Supervisor Engine Images Using TFTP

To download a supervisor engine software image to the switch from a TFTP server, follow these steps:

-
- Step 1** Copy the software image file to the appropriate TFTP directory on the workstation.
- Step 2** Log into the switch through the console port or through a Telnet session. If you log in using Telnet, your Telnet session disconnects when you reset the switch to run the new software.
- Step 3** Download the software image from the TFTP server using the **copy tftp flash** command. When prompted, enter the IP address or host name of the TFTP server and the name of the file to download. On those platforms that support the Flash file system, you are also prompted for the Flash device to which to copy the file and the destination filename.



Note The Catalyst 4000 family, 2948G, and 2980G switches have only one Flash device (**bootflash**).

The switch downloads the image file from the TFTP server, and the image is copied to the bootflash.



Note The switch remains operational while the image downloads.

Step 4	Modify the BOOT environment variable using the set boot system flash <i>device:filename</i> prepend command, so that the new image boots when you reset the switch. Specify the Flash device (<i>device:</i>) and the filename of the downloaded image (<i>filename</i>).
Step 5	Reset the switch using the reset system command. If you are connected to the switch through Telnet, your Telnet session disconnects.
Step 6	When the switch reboots, enter the show version command to check the version of the code on the switch.

Sample TFTP Download Procedures

```
Autoboot executing command: "boot bootflash:cat4000.6-1-1.bin"  
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC  
Uncompressing file: #####  
#####  
#####  
#####  
#####  
#####  
#####  
#####  
#####  
#####
```

CISCO Confidential - DRAFT

```
#####
#####
```

```
System Power On Diagnostics
NVRAM Size .. .....512KB
ID Prom Test .....Passed
DPRAM Size .....16KB
DPRAM Data 0x55 Test .....Passed
DPRAM Data 0xaa Test .....Passed
DPRAM Address Test .....Passed
Clearing DPRAM .....Done
System DRAM Memory Size .....32MB
DRAM Data 0x55 Test .....Passed
DRAM Data 0xaa Test .....Passed
DRAM Address Test .....Passed
Clearing DRAM .....Done
EARL++ .....Present
EARL RAM Test .....Passed
EARL Serial Prom Test .....Passed
Level2 Cache .....Present
Level2 Cache test.....Passed
```

```
Boot image: bootflash:cat4000.6-1-1.bin
```

```
Cisco Systems Console
```

```
Enter password:
07/21/2000,13:52:51:SYS-5:Module 1 is online
07/21/2000,13:53:11:SYS-5:Module 4 is online
07/21/2000,13:53:11:SYS-5:Module 5 is online
07/21/2000,13:53:14:PAGP-5:Port 1/1 joined bridge port 1/1.
07/21/2000,13:53:14:PAGP-5:Port 1/2 joined bridge port 1/2.
07/21/2000,13:53:40:SYS-5:Module 2 is online
07/21/2000,13:53:45:SYS-5:Module 3 is online
```

```
Console> show version 1
```

Mod	Port	Model	Serial #	Versions
1	0	WS-X4012	JAB03130104	Hw : 1.5 Gsp: 6.1(1.4) Nmp: 6.1(1)

```
Console>
```

Uploading System Software Images to a TFTP Server

The next two sections describe how to upload system software images from a switch to a TFTP server.

For more information on working with system software image files on the Flash file system, see [Chapter 34, “Working With the Flash File System.”](#)

Preparing to Upload an Image to a TFTP Server

Before you attempt to upload a software image to a TFTP server, do the following:

- Ensure that the workstation acting as the TFTP server is configured properly.

- Ensure that the switch has a route to the TFTP server. The switch and the TFTP server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the TFTP server using the **ping** command.
- If needed, create an empty file on the TFTP server before uploading the image. On a UNIX workstation, create an empty file by entering the **touch filename** command, where *filename* is the name of the file you will use when uploading the image to the server.
- If you are overwriting an existing file (including an empty file, if you had to create one), ensure that the permissions on the file are set correctly. Make sure that the permissions on the file are world-write.

Uploading Software Images to a TFTP Server

To upload a software image on a switch to a TFTP server for storage, follow these steps:

Step 1	Log in to the switch through the console port or a Telnet session.
Step 2	Upload the software image to the TFTP server using the copy flash tftp command. When prompted, specify the TFTP server address and destination filename. On platforms that support the Flash file systems, you are first prompted for the Flash device and source filename, If desired, you can use the copy file-id tftp command on these platforms. The software image is uploaded to the TFTP server.

This example shows how to upload the supervisor engine software image to a TFTP server:

```
Console> (enable) copy flash tftp
Flash device [bootflash]? bootflash
Name of file to copy from []? cat4000.6-1-1.bin
IP address or name of remote host [172.20.52.3]? 172.20.52.10
Name of file to copy to [cat4000.6-1-1.bin]?
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC|
File has been copied successfully.
Console> (enable)
```

Downloading System Software Images to the Switch Using rcp

The following sections describe how to download system software images to the switch supervisor engine and to intelligent modules using `scp`.

Understanding How rcp Software Image Downloads Work

You can download system software images to the switch using the remote copy protocol (rcp); rcp allows you to download system image files over the network from an rcp server.

You can store multiple image files in the Flash memory.

For more information on working with system software image files on the Flash file system, see to [Chapter 34, “Working With the Flash File System.”](#)

CISCO Confidential - DRAFT

Preparing to Download an Image Using rcp

Before you begin downloading a software image using rcp, make sure of the following:

- Ensure that the workstation acting as the rcp server supports the remote shell (rsh).
- Ensure that the switch has a route to the rcp server. The switch and the rcp server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the rcp server using the **ping** command.
- If you are accessing the switch through the console or a Telnet session without a valid username, make sure that the current rcp username is the one you want to use for the rcp download. You can enter the **show users** command to view the current valid username. If you do not want to use the current username, create a new rcp username using the **set rcp username** command. The new username will be stored in NVRAM. If you are accessing the switch through a Telnet session with a valid username, this username will be used and there is no need to set the rcp username.
- A power interruption (or other problem) during the download procedure can corrupt the Flash code. If the Flash code is corrupted, you can connect to the switch through the console port. You can download the Flash code again through an enabled port in VLAN 1. By default, port 1/1 is enabled. You can use port 1/1.

Downloading Supervisor Engine Images Using rcp

To download a supervisor engine software image to the switch from an rcp server, follow these steps:

-
- Step 1** Copy the software image file to the appropriate rcp directory on the workstation.
- Step 2** Log into the switch through the console port or through a Telnet session. If you log in using Telnet, your Telnet session disconnects when you reset the switch to run the new software.
- Step 3** Download the software image from the rcp server using the **copy rcp flash** command. When prompted, enter the IP address or host name of the rcp server and the name of the file to download. On those platforms that support the Flash file system, you are also prompted for the Flash device to which to copy the file and the destination filename.



Note The Catalyst 4000 family, 2948G, and 2980G switches have only one Flash device (**bootflash**).

The switch downloads the image file from the rcp server and copies the image to bootflash.



Note The switch remains operational while the image downloads.

- Step 4** Modify the BOOT environment variable using the **set boot system flash device:filename prepend** command, so that the new image boots when you reset the switch. Specify the Flash device (*device:*) and the filename of the downloaded image (*filename*).
- Step 5** Reset the switch using the **reset system** command. If you are connected to the switch through Telnet, your Telnet session disconnects.

During startup, the Flash memory on the supervisor engine is reprogrammed with the new Flash code.

Step 6 When the switch reboots, enter the **show version** command to check the version of the code on the switch.

Sample rcp Download Procedures

This example shows a complete rcp download procedure of a supervisor engine software image:

```
Console> (enable) show version 1
Mod Port Model Serial # Versions
-----
1 2 WS-X5530 007451586 Hw : 1.3
Fw : 3.1.2
Fw1: 3.1(2)
Sw : 4.1(2)

Console> (enable) copy rcp flash
IP address or name of remote host []? 172.20.52.3
Name of file to copy from []? cat4000.6-1-1.bin
Flash device [bootflash]?
Name of file to copy to [cat6000.6-1-1.bin]?

4369664 bytes available on device bootflash, proceed (y/n) [n]? y
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCC
File has been copied successfully.
Console> (enable) set boot system flash bootflash:cat4000.6-1-1.bin prepend
BOOT variable = bootflash:cat4000.6-1-1.bin,1;bootflash:cat4000.5-1-2.bin,1;
Console> (enable) reset system
This command will reset the system.
Do you want to continue (y/n) [n]? y
Console> (enable) 07/21/2000,13:51:39:SYS-5:System reset from Console//
```

```
System Bootstrap, Version 3.1(2)
Copyright (c) 1994-1997 by cisco Systems, Inc.
Presto processor with 32768 Kbytes of main memory
```

[illegible]

```
System Power On Diagnostics
NVRAM Size .. .....512KB
ID Prom Test .....Passed
DPRAM Size .....16KB
DPRAM Data 0x55 Test .....Passed
DPRAM Data 0xaa Test .....Passed
DPRAM Address Test .....Passed
```

CISCO Confidential - DRAFT

```

Clearing DPRAM .....Done
System DRAM Memory Size .....32MB
DRAM Data 0x55 Test .....Passed
DRAM Data 0xaa Test .....Passed
DRAM Address Test .....Passed
Clearing DRAM .....Done
EARL++ .....Present
EARL RAM Test .....Passed
EARL Serial Prom Test .....Passed
Level2 Cache .....Present
Level2 Cache test.....Passed

```

```
Boot image: bootflash:cat4000.6-1-1.bin
```

```
Cisco Systems Console
```

```

Enter password:
07/21/2000,13:52:51:SYS-5:Module 1 is online
07/21/2000,13:53:11:SYS-5:Module 4 is online
07/21/2000,13:53:11:SYS-5:Module 5 is online
07/21/2000,13:53:14:PAGP-5:Port 1/1 joined bridge port 1/1.
07/21/2000,13:53:14:PAGP-5:Port 1/2 joined bridge port 1/2.
07/21/2000,13:53:40:SYS-5:Module 2 is online
07/21/2000,13:53:45:SYS-5:Module 3 is online

```

```
Console> show version 1
```

Mod	Port	Model	Serial #	Versions
1	0	WS-X4012	JAB03130104	Hw : 1.5 Gsp: 6.1(1.4) Nmp: 6.1(0.104)

```
Console>
```

Uploading System Software Images to an rcp Server

The next two sections describe how to upload system software images from a switch to an rcp server.

For more information on working with system software image files on the Flash file system, see [Chapter 34, “Working With the Flash File System.”](#)

Preparing to Upload an Image to an rcp Server

Before you attempt to upload a software image to an rcp server, do the following:

- Ensure that the workstation acting as the rcp server is configured properly.
- Ensure that the switch has a route to the rcp server. The switch and the rcp server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the rcp server using the **ping** command.
- If you are overwriting an existing file (including an empty file, if you had to create one), ensure that the permissions on the file are set correctly. Make sure that the permissions on the file are set to write for the specific username.

CISCO Confidential - DRAFT

Uploading Software Images to an rcp Server

To upload a software image on a switch to an rcp server for storage, follow these steps:

-
- Step 1** Log in to the switch through the console port or a Telnet session.
- Step 2** Upload the software image to the rcp server using the **copy flash rcp** command. When prompted, specify the rcp server address and the destination filename. On platforms that support the Flash file systems, you are first prompted for the Flash device and source filename. If desired, you can use the **copy file-id rcp** command on these platforms.

The software image is uploaded to the rcp server.

This example shows how to upload the supervisor engine software image to an rcp server:

```
Console> (enable) copy flash rcp
Flash device [bootflash]? bootflash:
Name of file to copy from []? cat4000.6-1-1.bin
IP address or name of remote host [172.20.52.3]? 172.20.52.10
Name of file to copy to [cat4000.6-1-1.bin]?
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
```

```
File has been copied successfully.
Console> (enable)
```

Upgrading the ROM Monitor

If the ROM Monitor (ROMMON) loaded onto your switch is version 4.5(1) or earlier, you need to upgrade the ROMMON to version 6.1(4) in order to run software release 7.1 or later releases.

**Caution**

To avoid actions that might render your system unbootable, read this entire section before starting the upgrade.

You can do this procedure entirely over a Telnet connection, but if something fails, you will need to have access to the console serial port. If done improperly, the system can be rendered unbootable. It will then have to be returned to Cisco for repair.

This section describes an upgrade to ROMMON version 6.1(4). The same procedure applies to other ROMMON versions, but you will have to substitute appropriate version numbers in the upgrade image names.

To upgrade the ROMMON follow these steps:

-
- Step 1** Download the **promupgrade** program from Cisco.com and place it on a TFTP server in a directory that is accessible from the switch to be upgraded.

The **promupgrade** programs are available at the same location on cisco.com where you download Catalyst 4000 system images.

To upgrade to ROMMON version 6.1(4), download the **cat4000-promupgrade.6-1-4.bin** file.

CISCO Confidential - DRAFT

- Step 2** In privileged mode on your switch, use the **show version** command to verify the ROMMON version loaded on the switch.

The ROMMON version number is listed as the System Bootstrap Version. For example, the following system is running ROMMON version 6.1(2):

```
Console> (enable) show version
WS-C4003 Software, Version NmpSW:5.5(8)
Copyright (c) 1995-2001 by Cisco Systems, Inc.
NMP S/W compiled on May 24 2001, 21:12:09
GSP S/W compiled on May 24 2001, 18:39:50

System Bootstrap Version:6.1(2)

Hardware Version:1.0 Model:WS-C4003 Serial #:xxxxxxxxx

.
.
.
Console > (enable)
```

- Step 3** Use the **dir bootflash:** command to ensure that there is sufficient space in Flash memory to store the **promupgrade** image. If there is insufficient space, delete one or more images and then enter the **squeeze bootflash:** command to reclaim the space.

- Step 4** Download the **promupgrade** image into Flash using the **copy tftp** command.

This example shows how to download the **promupgrade** image **cat4000-promupgrade.6-1-4.bin** from the remote host **Lab_Server** to bootflash.

```
Console> (enable) copy tftp flash
IP address or name of remote host []? Lab_Server
Name of file to copy from []? /cat4000-promupgrade.6-1-4.bin
Flash device []? bootflash
Name of file to copy to []? cat4000-promupgrade.6-1-4.bin

9205592 bytes available on device bootflash, proceed (y/n) [n]? y
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
File has been copied successfully.
Console > (enable)
```

- Step 5** Ensure that the last line in the output of the **show boot** command is the following:

"boot:image specified by the boot system commands."

If the last line in the output of the **show boot** command does not say

"boot:image specified by the boot system commands," go to Step 6.

If the last line in the output of the **show boot** command is the following:

"boot:image specified by the boot system commands," go to Step 7.

This example shows the autoboot configuration:

```
Console> (enable) show boot
BOOT variable = bootflash:cat4000.5-5-8.bin,1;
CONFIG_FILE variable = bootflash:switch.cfg
```

Configuration register is 0x102

ignore-config:disabled

auto-config:non-recurring

console baud:9600

➔ boot:image specified by the boot system commands

Console > (enable)

CISCO Confidential - DRAFT

- Step 6** If the last line in the output of the **show boot** command does not say “boot:image specified by the boot system commands,” use the **set boot config-register** command to set the boot configuration.

This example shows how to set the boot configuration:

```
Console> (enable) set boot config-register boot system
Configuration register is 0x102
ignore-config:disabled
auto-config:non-recurring
console baud:9600
boot:image specified by the boot system commands
Console> (enable)
```

- Step 7** Use the **set boot system flash** command to prepend the **promupgrade** image to the boot string.

**Note**

Make sure that you use the **prepend** keyword with the **set boot system flash** command. The switch always boots the first image in the boot string, and you want the **promupgrade** image to boot first.

This example shows how to prepend the **promupgrade** image to the boot string:

```
Console> (enable) set boot system flash bootflash:cat4000-promupgrade.6-1-4.bin prepend
BOOT variable = bootflash:cat4000-promupgrade.6-1-4.bin,1;bootflash:cat4000.5-5-8.bin,1;
```

- Step 8** Reset the switch to boot the **promupgrade** program.

**Caution**

No intervention is necessary to complete the upgrade. Do not interrupt the boot process by performing a reset, power cycle, OIR of the supervisor engine, and so on, for at least 5 minutes. If the process is not allowed to complete, you might damage the switch and have to return it to Cisco for repair.

Upgrading the ROMMON may require up to 5 minutes because the switch boots the **promupgrade** image. This special program erases the current ROMMON from Flash and installs the new one. After you install the new ROMMON, the system resets again and boots the next image in the BOOT string. If the BOOT string was configured as described in Step 7 on page 33-11, the next image is the software image that the switch was originally configured to boot.

**Note**

A Telnet session is disconnected when you reset the switch; you will lose connectivity to the switch.

If you are connected to the console serial port, output similar to the following is displayed after you reset the switch:

```
0:00.530901:ig0:00:10:7b:aa:d3:fe is 172.20.59.203
0:00.531660:netmask:255.255.255.0
0:00.532030:broadcast:172.20.59.255
0:00.532390:gateway:172.20.59.1
WS-X4012 bootrom version 6.1(2), built on 2000.04.03 15:20:09
H/W Revisions:Meteor:2 Comet:8 Board:1
Supervisor MAC addresses:00:10:7b:aa:d0:00 through 00:10:7b:aa:d3:ff (1024 addresses)
Installed memory:64 MB
Testing LEDs.... done!
The system will autoboot in 5 seconds.
Type control-C to prevent autobooting.
rommon 1 >
The system will now begin autobooting.
Autobooting image:
```

CISCO Confidential - DRAFT

```
"bootflash:cat4000-promupgrade.6-1-4.bin"
```

```
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC#####
Replacing ROM version 6.1(2) with version 6.1(4)
```

```
Upgrading your PROM... DO NOT RESET the system
unless instructed or it may NOT be bootable!!!
Beginning erase of 524288 bytes at offset 0x0... Done!
Beginning write of system prom (467456 bytes at offset 0x0)...
This could take as little as 10 seconds or up to 2 minutes.
Please DO NOT RESET!
```

```
*****
```

```
Success!
System will reset in 2 seconds...
[ ... ]
```

The switch reboots back into the supervisor engine software:

```
0:00.530856:ig0:00:10:7b:aa:d3:fe is 172.20.59.203
0:00.531616:netmask:255.255.255.0
0:00.531967:broadcast:172.20.59.255
0:00.532342:gateway:172.20.59.1
WS-X4012 bootrom version 6.1(4), built on 2000.04.03 15:20:09
H/W Revisions:Meteor:2 Comet:8 Board:1
Supervisor MAC addresses:00:10:7b:aa:d0:00 through 00:10:7b:aa:d3:ff (1024 addresses)
Installed memory:64 MB
Testing LEDs.... done!
The system will autoboot in 5 seconds.
Type control-C to prevent autobooting.
rommon 1 >
The system will now begin autobooting.
Autobooting image:"bootflash:cat4000.5-5-8.bin"
```

```
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC#####
CCCCCCCCCCCCCCCCCCCC#####
```

- Step 9** In privileged mode on your switch, use the **show version** command to verify that the new ROMMON version is running on the switch.

The ROMMON version number is listed as the System Bootstrap Version. For example, the following system is running ROMMON version 6.1(4):

```
Console> (enable) show version
WS-C4003 Software, Version NmpSW:5.5(8)
Copyright (c) 1995-2001 by Cisco Systems, Inc.
NMP S/W compiled on May 24 2001, 21:12:09
GSP S/W compiled on May 24 2001, 18:39:50
```

```
System Bootstrap Version:6.1(4)
```

```
Hardware Version:1.0 Model:WS-C4003 Serial #:xxxxxxxx
```

```
.
.
.
```

```
Console > (enable)
```

- Step 10** Enter the **clear boot system flash promupgrade_image** command to remove the **promupgrade** program from the autoboot string.

CISCO Confidential - DRAFT**Caution**

When entering the **clear boot system flash cat.4000-promupgrade.6-1-4.bin** command, be sure to type the correct **promupgrade** image in the command syntax. If you enter only **clear boot system flash**, all images in the autoboot string are cleared, and the switch does not know which image to boot.

This example shows how to remove the **promupgrade** image **cat.4000-promupgrade.6-1-4.bin** from the boot sequence. Notice that the response message shows the system image for software release 5.5(8) in the autoboot string.

```
Console> (enable) clear boot system flash bootflash:cat4000-promupgrade.6-1-4.bin
BOOT variable = bootflash:cat4000.5-5-8.bin,1;
```

- Step 11** Enter **del** to delete the **promupgrade** program from Flash memory. Squeeze the flash memory to reclaim unused space.

This example shows how to delete the **promupgrade** image **cat.4000-promupgrade.6-1-4.bin** from Flash and reclaim unused space:

```
Console> (enable) del bootflash:cat4000-promupgrade.6-1-4.bin
Console> (enable) squeeze bootflash:
```

All deleted files will be removed, proceed (y/n) [n]? y

Squeeze operation may take some time, proceed (y/n) [n]? y
Console > (enable)

- Step 12** After removing the **promupgrade** image from the BOOT string, use the **show boot** command to verify that the BOOT string is set correctly.

CISCO Confidential - DRAFT



Working With the Flash File System

This chapter describes how to use the Flash file system on the Catalyst enterprise LAN switches.



For complete syntax and usage information for the commands used in this chapter, see *Catalyst 4500 Series, Catalyst 2948G, and Catalyst 2980G Switches Command Reference*.

The Flash file system provides a number of useful commands to help you manage system image and configuration files. The Catalyst 4000 family, 2948G, and 2980G switches have one Flash device: **bootflash**.

Working the Flash File System on the Switch

The following sections describe how to work with the Flash file system.

Setting the Default Flash Device

When you set the default Flash device for the system, the default device is assumed when you enter a Flash file system command without specifying the Flash device.

To set the default Flash device, perform this task:

	Task	Command
Step 1	Set the default Flash device for the system.	<code>cd [[m/]][bootflash:]</code>
Step 2	Verify the default Flash device for the system.	<code>pwd [mod_num]</code>

This example shows how to change the default Flash device to bootflash: and verify the default device:

```
Console> (enable) cd bootflash:
Console> (enable) pwd
bootflash
Console> (enable)
```

CISCO Confidential - DRAFT

Setting the Text File Configuration Mode

When you configure the switch to use text file configuration mode, the switch stores its configuration as a text file in nonvolatile storage, either in NVRAM or Flash memory. This text file consists of commands that are entered by you to configure various features. For example, if you disable a port, the command to disable that port will be in the text configuration file.

Because the text file contains only commands that you have used to configure your switch, it typically uses less NVRAM or Flash memory space than binary configuration mode. Because the text configuration file in most cases requires less space, NVRAM is a good place to store the file. If the text file exceeds NVRAM space, it can also be stored to Flash memory.

When the switch is operating in text file configuration mode, most user settings are not immediately saved to NVRAM. Configuration changes are written only to DRAM. You will need to enter the **write memory** command to store the configuration in nonvolatile storage.

**Note**

VLAN commands are not saved as part of the configuration file when the switch is operating in text mode with the VTP mode set to server.

To set the text file configuration mode, perform this task in privileged mode:

	Task	Command
Step 1	Set the file configuration mode for the system to text.	set config mode {binary text} [nvram device:file-id]
Step 2	Verify the file configuration mode for the system.	show config mode
Step 3	Save the text file configuration.	write memory
Step 4	Display the current runtime configuration.	show running-config all
Step 5	Display the startup configuration that will be used after the next reset.	show config

This example shows how to configure the system to save its configuration as a text file in NVRAM, verify the configuration mode, and display the current runtime configuration:

```
Console> (enable) set config mode text nvram
Console> (enable) show config mode
Console> (enable) show running-config all
Console> (enable) show config
Console> (enable)
```

Listing the Files on a Flash Device

To list the files on a Flash device, perform one of these tasks:

Task	Command
Display a list of files on a Flash device.	dir [[m/]device:][filename]
Display a list of only deleted files on a Flash device.	dir [[m/]device:][filename] deleted

CISCO Confidential - DRAFT

Task	Command
Display a list of all files on a Flash device, including deleted files.	dir <i>[[m/]device:][filename]</i> all
Display a detailed list of files on a Flash device.	dir <i>[[m/]device:][filename]</i> long

This example shows how to list the files on the default Flash device:

```
Console> (enable) dir
-#- -length- -date/time----- name
  1 3846376 Jun 14 2000 14:13:10 cat4000-k4.6-1-0-104-ORL.bin
  2 3761580 Jun 14 2000 14:16:05 cat4000.6-1-0-104-ORL.bin

3795052 bytes available (7608212 bytes used)
Console> (enable)
```

This example shows how to list the deleted files on the default Flash device:

```
Console> (enable) dir deleted
-#- ED --type-- --crc--- -seek-- nlen -length- -date/time----- name
  1 .D ffffffff 81a027ca 41bdc 22 7004 Apr 01 1998 15:27:45 4003.config.
4.1.98.cfg
  2 .D ffffffff ccce97a3 43644 23 6630 Apr 01 1998 15:36:47 4003.default
.config.cfg
  3 .D ffffffff 81a027ca 45220 15 7004 Apr 19 1998 10:05:59 4003_config.cfg

1213952 bytes available (6388224 bytes used)
Console> (enable)
```

Displaying the Contents of a File on a Flash Device

In software release 5.2 and later releases, you can display the contents of a file on a Flash device onscreen. Enter the **dump** keyword to display a hex dump of the file.

To display the contents of a file on a Flash device, perform this task in privileged mode:

Task	Command
Display the contents of a file on a Flash device.	show file <i>[device:]filename</i> [dump]

This example shows how to display the contents of a file in bootflash:

```
Console> (enable) show file bootflash:dns_config.cfg
begin

!
#dns
set ip dns server 172.16.10.70 primary
set ip dns server 172.16.10.140
set ip dns enable
set ip dns domain corp.com
end
Console> (enable)
```

CISCO Confidential - DRAFT

Copying Files

Enter the **copy** command to perform these tasks:

- Download a system image or configuration file from a TFTP or rcp server to a Flash device
- Upload a system image or configuration file from a Flash device to a TFTP or rcp server
- Configure the switch using a configuration file on a Flash device or on a TFTP or rcp server
- Copy the current configuration to a Flash device or to a TFTP or rcp server

To copy a file, perform one of these tasks in privileged mode:

Task	Command
Copy a Flash file to a TFTP server, Flash memory, or to the running configuration.	copy <i>file-id</i> { tftp rcp flash <i>file-id</i> config }
Copy a file from a TFTP server to Flash memory, or to the running configuration.	copy { tftp rcp } { flash <i>file-id</i> config }
Copy a file from Flash memory to a TFTP server, or to the running configuration.	copy flash { tftp rcp <i>file-id</i> config }
Copy the running configuration to Flash memory, or to a TFTP server.	copy config { flash <i>file-id</i> tftp rcp }

This example shows how to copy a file from a TFTP server to the running configuration:

```

Console> (enable) copy tftp config
IP address or name of remote host []? 172.20.52.3
Name of file to copy from []? dns_config.cfg

Configure using tftp:dns_config.cfg (y/n) [n]? y
/
Finished network download. (135 bytes)
>>
>> set ip dns server 172.16.10.70 primary
172.16.10.70 added to DNS server table as primary server.
>> set ip dns server 172.16.10.140
172.16.10.140 added to DNS server table as backup server.
>> set ip dns enable
DNS is enabled
>> set ip dns domain corp.com
Default DNS domain name set to corp.com
Console> (enable)

```

This example shows how to download a configuration file from a TFTP server for storage in bootflash:

```

Console> (enable) copy tftp flash
IP address or name of remote host []? 172.20.52.3
Name of file to copy from []? dns-config.cfg
Flash device [bootflash]?
Name of file to copy to [dns-config.cfg]?

9932056 bytes available on device slot0, proceed (y/n) [n]? y
/
File has been copied successfully.
Console> (enable)

```

This example shows how to copy the running configuration to Flash memory:

CISCO Confidential - DRAFT

```

Console> (enable) copy config flash
Flash device [bootflash]? bootflash:
Name of file to copy to []? 4012_config.cfg

Upload configuration to bootflash:4012_config.cfg
9942096 bytes available on device bootflash, proceed (y/n) [n]? y
.....
.....
.....

.....
.....
..

Configuration has been copied successfully.
Console> (enable)

```

This example shows how to upload a configuration file on bootflash to a TFTP server:

```

Console> (enable) copy bootflash:4012_config.cfg tftp
IP address or name of remote host []? 172.20.52.3
Name of file to copy to [4012_config.cfg]?
/
File has been copied successfully.
Console> (enable)

```

This example shows how to upload an image from a remote host into Flash memory using the **copy rcp flash** command:

```
Console> (enable) copy rcp flash  
IP address or name of remote host []? 172.20.52.3  
Name of file to copy from []? cat4000.6-1-1.bin  
Flash device [bootflash]?  
Name of file to copy to [cat4000.6-1-1.bin]?  
  
4369664 bytes available on device bootflash, proceed (y/n) [n]? y  
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC  
CCCCCCCCCCCCCCCCCCCC  
File has been copied successfully.  
Console> (enable)
```

Deleting Files

Enter the **delete** command to delete files from a Flash device.



Caution

If you enter the **squeeze** command on a Flash device, you cannot restore files that you deleted from that device before you entered the **squeeze** command.

To delete files from a Flash device, perform this task in privileged mode:

	Task	Command
Step 1	Delete a file from a Flash device.	delete <i>[[m/]device:]filename</i>
Step 2	If desired, permanently remove all deleted files on the Flash device (this operation can take a number of minutes to complete).	squeeze <i>[m/]device:</i>
Step 3	Verify that the files are deleted.	dir <i>[[m/]device:][filename]</i>

CISCO Confidential - DRAFT

This example shows how to delete a file from a Flash device:

```
Console> (enable) delete dns_config.cfg
Console> (enable)
```

This example shows how to permanently remove all deleted files from a Flash device:

```
Console> (enable) squeeze bootflash:
All deleted files will be removed, proceed (y/n) [n]? y
Squeeze operation may take a while, proceed (y/n) [n]? y
Erasing squeeze log
Console> (enable)
```

Restoring Deleted Files

You must specify the index number of a deleted file to restore it. The index number for each file appears in the first column of the **dir** command output. A file cannot be undeleted if a valid file with the same name already exists. Instead, you must delete the existing file and then undelete the desired file. A file can be deleted and undeleted up to 15 times.

To restore deleted files on a Flash device, perform this task in privileged mode:

	Task	Command
Step 1	Identify the index number of the deleted files on the Flash device.	dir <i>[[m/]device:][filename] deleted</i>
Step 2	Undelete a file on a Flash device.	undelete <i>index</i> <i>[[m/]device:]</i>
Step 3	Verify that the file is restored.	dir <i>[[m/]device:][filename]</i>

This example shows how to restore a deleted file:

```
Console> (enable) dir deleted
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time----- name
6 .D ffffffff 42da7f71 657a00 14 135 Jul 17 1999 11:30:05 dns_config.cfg

1213952 bytes available (3231989 bytes used)
Console> (enable) undelete 6
Console> (enable) dir
-#- -length- -----date/time----- name
5 3231989 Jun 24 1999 12:04:40 cat4000.4-4-0-28.bin
6 135 Jul 17 1999 11:30:05 dns_config.cfg

1213952 bytes available (3231989 bytes used)
Console> (enable)
```

Verifying a File Checksum

To verify the checksum of a file on a Flash device, perform this task in privileged mode:

Task	Command
Verify the checksum of a file on a Flash device.	verify <i>[[m/]device:] filename</i>

This example shows how to verify the checksum of a file:

CISCO Confidential - DRAFT

Working with Configuration Files

This chapter describes how to work with switch configuration files on the Catalyst enterprise LAN switches.

**Note**

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 4500 Series, Catalyst 2948G, and Catalyst 2980G Switches Command Reference*.

This chapter consists of these sections:

- [Creating and Using Configuration Files Guidelines, page 35-1](#)
- [Creating a Configuration File, page 35-2](#)
- [Configuring the Switch Using a File in Flash Memory, page 35-2](#)
- [Copying Configuration Files Using TFTP, page 35-3](#)
- [Copying Configuration Files Using rcp, page 35-5](#)
- [Clearing the Configuration, page 35-7](#)

**Note**

For more information on working with configuration files on the Flash file system, see [Chapter 34, “Working With the Flash File System.”](#)

Creating and Using Configuration Files Guidelines

Configuration files can help you configure your switch. Configuration files can contain some or all the commands needed to configure one or more switches. For example, you might want to download the same configuration file to several switches that have the same hardware configuration so that they have identical module and port configurations.

This section lists the guidelines for creating a configuration file:

- We recommend that you connect through the console port when using configuration files to configure the switch. If you configure the switch from a Telnet session, IP addresses are not changed, and ports and modules are not disabled.
- If no passwords have been set on the switch, you must set them on each switch by entering the **set password** and **set enablepass** commands. Enter a blank line after the **set password** and **set enablepass** commands. The passwords are saved in the configuration file as clear text.

CISCO Confidential - DRAFT

If passwords already exist, you cannot enter the **set password** and **set enablepass** commands because the password verification will fail. If you enter passwords in the configuration file, the switch mistakenly attempts to execute the passwords as commands as it executes the file.

- Some commands must be followed by a blank line in the configuration file. Without the blank line, these commands might disconnect your Telnet session. Before disconnecting a session, the switch prompts you for confirmation. The blank line acts as a carriage return, which indicates a negative response to the prompt, and retains the Telnet session.

Include a blank line after each occurrence of these commands in a configuration file:

- **set interface sc0** *ip_addr netmask*
- **set interface sc0** **disable**
- **set module disable** *mod_num*
- **set port disable** *mod_num/port_num*

Creating a Configuration File

When creating a configuration file, you must list commands in a logical way so that the system can respond appropriately. To create a configuration file, follow these steps:

-
Step 1	Download an existing configuration from a switch.
Step 2	Open the configuration file in a text editor, such as vi or emacs on UNIX or Notepad on a PC.
Step 3	Extract the portion of the configuration file with the desired commands and save it in a new file. Make sure the file begins with the word begin on a line by itself and ends with the word end on a line by itself.
Step 4	Copy the configuration file to the appropriate TFTP directory on the workstation (usually /tftpboot on a UNIX workstation).
Step 5	Ensure that the permissions on the file are set to username.
-

This example shows a sample configuration file. This file could be used to set the DNS configuration on multiple switches.

```
begin

!
#dns
set ip dns server 172.16.10.70 primary
set ip dns server 172.16.10.140
set ip dns enable
set ip dns domain corp.com
end
```

Configuring the Switch Using a File in Flash Memory

You can configure the switch using a file stored in Flash memory. The procedure varies depending on your switch platform.

To configure a switch using a configuration file stored on a Flash device in the Flash file system, follow these steps:

CISCO Confidential - DRAFT

-
- Step 1** Log in to the switch through the console port or a Telnet session.
- Step 2** Locate the configuration file using the **cd** and **dir** commands (for more information, see the [“Listing the Files on a Flash Device”](#) section on page 34-2).
- Step 3** Configure the switch using the configuration file stored on the Flash device using the **copy file-id config** command.
-

The commands are executed as the file is parsed line by line.

This example shows how to configure the switch using a configuration file stored on a Flash device:

```
Console> (enable) copy bootflash:dns-config.cfg config

Configure using bootflash:dns-config.cfg (y/n) [n]? y

Finished network download. (134 bytes)
>>
>> set ip dns server 172.16.10.70 primary
172.16.10.70 added to DNS server table as primary server.
>> set ip dns server 172.16.10.140
172.16.10.140 added to DNS server table as backup server.
>> set ip dns enable
DNS is enabled
>> set ip dns domain corp.com
Default DNS domain name set to corp.com
Console> (enable)
Console> (enable)
```

Copying Configuration Files Using TFTP

You can configure the switch using configuration files that you create or download from another switch. In addition, you can store configuration files on Flash devices on hardware that supports the Flash file system, configure the switch using a configuration stored on a Flash device, or upload the configuration to a TFTP server.

The following sections describe how to configure the switch using configuration files downloaded from a TFTP server or stored on a Flash device, and how to upload a configuration file to a TFTP server.

Downloading Configuration Files from a TFTP Server

The following sections describe how to download a configuration file on a TFTP server to the running configuration or to a Flash device.

Preparing to Download a Configuration File Using TFTP

Before you begin downloading a configuration file using TFTP, do the following:

- Ensure that the workstation acting as the TFTP server is configured properly.
- Ensure that the switch has a route to the TFTP server. The switch and the server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the TFTP server using the **ping** command.

CISCO Confidential - DRAFT

- Ensure that the configuration file to be downloaded is in the correct directory on the server (for example, /tftpboot on a UNIX workstation).
- Ensure that the permissions on the file are set correctly. Make sure that the permissions are set to world-read.

Configuring the Switch Using a File on a TFTP Server

To configure a switch using a configuration file downloaded from a TFTP server, follow these steps:

-
- Step 1** Copy the configuration file to the appropriate TFTP directory on the workstation.
- Step 2** Log in to the switch through the console port or a Telnet session.
- Step 3** Configure the switch using the configuration file downloaded from the TFTP server using the **copy tftp config** or the **configure network** command. Specify the IP address or host name of the TFTP server and the name of the file to download.

The configuration file downloads and the commands are executed as the file is parsed line by line.

This example shows how to configure a switch using a configuration file downloaded from a TFTP server:

```

Console> (enable) copy tftp config
IP address or name of remote host []? 172.20.52.3
Name of file to copy from []? dns-config.cfg

Configure using tftp:dns-config.cfg (y/n) [n]? y
/
Finished network download. (134 bytes)
>>
>> set ip dns server 172.16.10.70 primary
172.16.10.70 added to DNS server table as primary server.
>> set ip dns server 172.16.10.140
172.16.10.140 added to DNS server table as backup server.
>> set ip dns enable
DNS is enabled
>> set ip dns domain corp.com
Default DNS domain name set to corp.com
Console> (enable)

```

Uploading Configuration Files to a TFTP Server

The next two sections describe how to upload the running configuration or a configuration file stored on a Flash device to a TFTP server.

Preparing to Upload a Configuration File to a TFTP Server

Before you attempt to upload a configuration file to a TFTP server, do the following:

- Ensure that the workstation acting as the TFTP server is configured properly.
- Ensure that the switch has a route to the TFTP server. The switch and the TFTP server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the TFTP server using the **ping** command.

CISCO Confidential - DRAFT

- You might need to create an empty file on the TFTP server before uploading the configuration file. On a UNIX workstation, create an empty file by entering the **touch filename** command, where *filename* is the name of the file you will use when uploading the configuration to the server.
- If you are overwriting an existing file (including an empty file, if you had to create one), ensure that the permissions on the file are set correctly. Make sure the permissions on the file are set to world-write.

Uploading a Configuration File to a TFTP Server

To upload a configuration file from a switch to a TFTP server for storage, follow these steps:

-
- Step 1** Log in to the switch through the console port or a Telnet session.
- Step 2** Upload the switch configuration to the TFTP server using the **copy config tftp** or the **write network** command. Specify the IP address or host name of the TFTP server and the destination filename.
- The file is uploaded to the TFTP server.
-

This example shows how to upload the running configuration on a switch, to a TFTP server for storage:

```

Console> (enable) copy config tftp
IP address or name of remote host []? 172.20.52.3
Name of file to copy to []? cat4003_config.cfg

Upload configuration to tftp:cat4003_config.cfg, (y/n) [n]? y
.....
.....
.....

..
/
Configuration has been copied successfully.
Console> (enable)

```

Copying Configuration Files Using rcp

The Remote Copy Protocol (rcp) provides another way to download, upload, and copy config files between remote hosts and the switch. rcp uses the Transmission Control Protocol (TCP), a connection-oriented protocol; TFTP uses the User Datagram Protocol (UDP), which is a connectionless protocol.

To use rcp to copy files, the server from or to which you will be copying files must support rcp. The **rcp copy** commands rely on the remote shell (rsh) server (or daemon) on the remote system. To copy files using rcp, you do not need to create a server for file distribution, as you do with TFTP. You need only to have access to a server that supports rsh. (Most UNIX systems support rsh.) Because you are copying a file from one place to another, you must have read permission on the source file and write permission on the destination file. If the destination file does not exist, rcp creates it for you.

Downloading Configuration Files from an rcp Server

The next two sections describe how to download a configuration file from an rcp server to the running configuration or to a Flash device.

CISCO Confidential - DRAFT

Preparing to Download a Configuration File Using rcp

Before you begin downloading a configuration file using rcp, do the following:

- Ensure that the workstation acting as the rcp server supports the rsh.
- Ensure that the switch has a route to the rcp server. The switch and the server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the rcp server using the **ping** command.
- If you are accessing the switch through the console or a Telnet session without a valid username, make sure that the current rcp username is the one you want to use for the rcp download. You can enter the **show users** command to view the current valid username. If you do not want to use the current username, create a new rcp username using the **set rcp username** command. The new username will be stored in NVRAM. If you are accessing the switch through a Telnet session with a valid username, this username will be used and there is no need to set the rcp username.

Configuring the Switch Using a File on an rcp Server

To configure a switch using a configuration file downloaded from a rcp server, follow these steps:

-
- Step 1** Copy the configuration file to the appropriate rcp directory on the workstation.
 - Step 2** Log in to the switch through the console port or a Telnet session.
 - Step 3** Configure the switch using the configuration file downloaded from the rcp server using the **copy rcp config or the configure host file [rcp]** command. Specify the IP address or host name of the rcp server and the name of the file to download.

The configuration file downloads and the commands are executed as the file is parsed line-by-line.

This example shows how to configure a switch using a configuration file downloaded from an rcp server:

```
Console> (enable) copy rcp config
IP address or name of remote host []? 172.20.52.3
Name of file to copy from []? dns-config.cfg

Configure using rcp:dns-config.cfg (y/n) [n]? y
/
Finished network download. (134 bytes)
>>
>> set ip dns server 172.16.10.70 primary
172.16.10.70 added to DNS server table as primary server.
>> set ip dns server 172.16.10.140
172.16.10.140 added to DNS server table as backup server.
>> set ip dns enable
DNS is enabled
>> set ip dns domain corp.com
Default DNS domain name set to corp.com
Console> (enable)
```

Uploading Configuration Files to an rcp Server

The next two sections describe how to upload the running configuration or a configuration file stored on a Flash device to an rcp server.

CISCO Confidential - DRAFT

Preparing to Upload a Configuration File to an rcp Server

Before you attempt to upload a configuration file to an rcp server, do the following:

- Ensure that the workstation acting as the rcp server is configured properly.
- Ensure that the switch has a route to the rcp server. The switch and the rcp server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the rcp server using the **ping** command.
- If you are overwriting an existing file (including an empty file, if you had to create one), ensure that the permissions on the file are set correctly. Make sure that the permissions on the file are set to user write.

Uploading a Configuration File to an rcp Server

To upload a configuration file from a switch to an rcp server for storage, follow these steps:

-
- Step 1** Log in to the switch through the console port or a Telnet session.
- Step 2** Upload the switch configuration to the rcp server using either the **copy config rcp** or the **write host file [rcp]** command. Specify the IP address or host name of the rcp server and the destination filename. The file is uploaded to the rcp server.
-

This example shows how to upload the running configuration on a switch, to an rcp server for storage:

```

Console> (enable) copy config rcp
IP address or name of remote host []? 172.20.52.3
Name of file to copy to []? cat4000_config.cfg

Upload configuration to rcp:cat4000_config.cfg, (y/n) [n]? y
.....
.....
.....

.....
.....
..
/
Configuration has been copied successfully.
Console> (enable)
Console> (enable)

```

Clearing the Configuration

To clear the configuration on the entire switch, perform this task in privileged mode:

Task	Command
Clear the switch configuration.	clear config all

This example shows how to clear the configuration for the entire switch:

```

Console> (enable) clear config all

```

CISCO Confidential - DRAFT

This command will clear all configuration in NVRAM.
This command will cause ifIndex to be reassigned on the next system startup.
Do you want to continue (y/n) [n]? y
.....
.....

System configuration cleared.
Console> (enable)

To clear the configuration on an individual module, perform this task in privileged mode:

Task	Command
Clear the configuration for a specific module.	clear config <i>mod_num</i>



Note

If you remove a module and replace it with a module of another type (for example, if you remove a Fast Ethernet module and insert a Token Ring module), the module configuration is inconsistent. The output of the **show module** command indicates this problem. To resolve the inconsistency, clear the configuration on the problem module.

This example shows how to clear the configuration on a specific module:

Console> (enable) **clear config 2**
This command will clear module 2 configuration.
Do you want to continue (y/n) [n]? y
Module 2 configuration cleared.
Console> (enable)

Configuring Switch Acceleration

This chapter describes the Backplane Channel Module and the switch acceleration feature that are supported on the Catalyst 4000 family supervisor engine.

This chapter consists of these sections:

- [Understanding How Switch Acceleration Works, page 36-1](#)
- [Configuring Switch Acceleration on the Switch, page 36-2](#)
- [Backplane Channel Module, page 36-3](#)



Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 4500 Series, Catalyst 2948G, and Catalyst 2980G Switches Command Reference*.

Understanding How Switch Acceleration Works

The switch acceleration feature provides the following supervisor engine performance benefits:

- Increased bandwidth between switch engines
- Full-mesh connectivity between switch engines
- Reduced internal traffic congestion

The switch acceleration feature is supported on Catalyst 4006 switches with Supervisor Engine II and on the Catalyst 4000 family Backplane Channel Module. The switch acceleration feature reduces internal traffic congestion by creating a full-mesh connection between the switch engines (SEs). Supervisor Engine II has three switch engines that switch traffic to and from the modules and the uplink ports. This chapter refers to these switch engines as SE1, SE2, and SE3.

- SE1 handles traffic for Gigabit Ethernet uplink port 1/1 and traffic between modules installed in the chassis.
- SE3 handles traffic for Gigabit Ethernet uplink port 1/2 and traffic between modules installed in the chassis.
- SE2 switches internal traffic and forwards traffic bound for the uplink ports to the correct SE for that port.

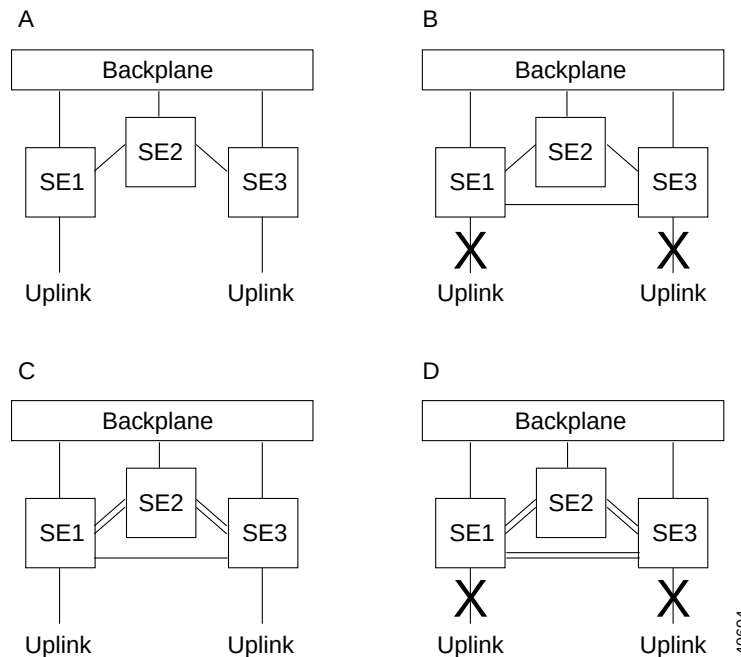
By default, there is no direct internal connection between SE1 and SE3. As a result, traffic coming in on SE1 destined for SE3, or vice versa, must go through SE2, which could potentially create congestion. To avoid such congestion, you can disable the uplink ports and create a direct internal link between SE1 and SE3.

CISCO Confidential - DRAFT

Switch acceleration is supported in different configuration modes. Supervisor Engine II supports a mesh configuration with no uplink connections. With the Backplane Channel Module installed, two additional modes are supported.

Figure 36-1 shows the possible configurations.

Figure 36-1 Switch Acceleration Configuration Modes



- Option A—No switch acceleration is configured (default).
- Option B—Fully meshed interconnections exist between SEs; there are no Gigabit Ethernet uplink port connections.

This mode requires that you enable switch acceleration on the supervisor engine.

- Option C—Fully meshed interconnections exist between SEs; there is dual-link load-balancing between SE1 and SE2 and between SE2 and SE3; Gigabit Ethernet uplink port connections.

This mode requires that the Backplane Channel Module is installed and that switch acceleration is not configured on the supervisor engine.

- Option D—Fully meshed interconnections and multi-link load balancing exist between all SEs; there are no Gigabit Ethernet uplink port connections.

This mode requires that the Backplane Channel Module is installed and that switch acceleration is configured on the supervisor engine.

Configuring Switch Acceleration on the Switch

By default, switch acceleration is disabled on the Supervisor Engine II. Before you enable switch acceleration, you need to disable the two front-panel Gigabit Ethernet uplink ports on Supervisor Engine II.

CISCO Confidential - DRAFT

Enabling Switch Acceleration

To enable switch acceleration, perform this task in privileged mode:

	Task	Command
Step 1	Disable front-panel Gigabit Ethernet ports.	set port disable <i>mod_num/port_num</i>
Step 2	Enable switch acceleration.	set switchacceleration {enable disable} <i>mod-num</i>

This example shows how to enable switch acceleration on the switch:

```
Console> (enable) set port disable 1/1-2
Port(s) 1/1-2 disabled.
Console> (enable) set switchacceleration enable 1
Enabling or Disabling switch acceleration may impact performance for 1-2 seconds.
Do you want to continue (y/n) [n]? y
Switch Acceleration on module 1 enabled.
Console> (enable)
```

This example shows how to disable switch acceleration on the switch:

```
Console> (enable) set switchacceleration disable 1
Enabling or Disabling switch acceleration may impact performance for 1-2 seconds.
Do you want to continue (y/n) [n]? y
Switch Acceleration on module 1 disabled.
Console> (enable)
```

Displaying Switch Acceleration Information

To display switch acceleration status, perform this task in privileged mode:

Task	Command
Display the current status of switch acceleration.	show switchacceleration <i>mod_num</i>

This example shows how to display the current status of the switch acceleration feature:

```
Console> show switchacceleration 1
Module 1 has switch acceleration enabled.
Console>
```

Backplane Channel Module

The Backplane Channel Module extends the benefits of switch acceleration by providing multilink load balancing between the switch engines. The Backplane Channel Module also allows you to retain the Gigabit Ethernet uplinks on the supervisor engine.

CISCO Confidential - DRAFT

The Backplane Channel Module provides the following benefits in the default configuration mode:

- Full-mesh connection between all three switch engines
- Multilink load balancing between SE1 and SE2 and between SE2 and SE3
- Supervisor engine Gigabit Ethernet uplink connections

As an alternative, you can configure switch acceleration on the supervisor engine to get dual-link load balancing between all three SEs.

**Note**

If you want to keep the uplink connections, do not enable switch acceleration on the supervisor engine.

You can insert or remove a Backplane Channel Module at any time. When you remove the Backplane Channel Module, traffic might be interrupted for a short time. For minimal disruption, disable the Backplane Channel Module for a short time, and then remove it.

You do not need to configure the Backplane Channel Module because it is enabled by default.

Configuring System Message Logging

This chapter describes how to configure system message logging on the Catalyst enterprise LAN switches.

**Note**

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 4500 Series, Catalyst 2948G, and Catalyst 2980G Switches Command Reference*.

This chapter consists of these major sections:

- [Understanding How System Message Logging Works, page 37-1](#)
- [System Log Message Format, page 37-4](#)
- [Default System Message Logging Configuration, page 37-3](#)
- [System Log Message Format, page 37-4](#)
- [Configuring System Message Logging on the Switch, page 37-4](#)

Understanding How System Message Logging Works

The system message logging software can save messages in a log file or direct the messages to other devices. With the system message logging facility, you can do the following:

- Get logging information for monitoring and troubleshooting
- Select the types of captured logging information
- Select the destination of captured logging information

By default, the switch logs normal but significant system messages to its internal buffer and sends these messages to the system console. You can specify which system messages should be saved based on the type of facility (see [Table 37-1](#)) and the severity level (see [Table 37-4](#)). Messages are time-stamped to enhance real-time debugging and management.

You can access logged system messages using the switch CLI or by saving them to a properly configured syslog server. The switch software saves syslog messages in an internal buffer that can store up to 1024 messages. You can monitor system messages remotely by accessing the switch through Telnet or the console port, or by viewing the logs on a syslog server.

**Note**

When the switch first initializes, the network is not connected until the initialization completes. Messages that are redirected to a syslog server are delayed up to 90 seconds.

CISCO Confidential - DRAFT

Table 37-1 describes the facility types that are supported by the system message logs.

Table 37-1 System Message Log Facilities

Facility Name	Definition
cdp	Cisco Discovery Protocol
dtp	Dynamic Trunking Protocol
drip	Dual Ring Protocol
dvlan	Dynamic VLAN
earl	Enhanced Address Recognition Logic
fddi	Fiber Distributed Data Interface
filesys	Flash file system
gvrp	GARP VLAN Registration Protocol
ip	IP permit list
kernel	Kernel
mgmt	Management messages
mcast	Multicast messages
pagp	Port Aggregation Protocol
protfilt	Protocol filtering
pruning	VTP pruning
qos	Quality of Service
radius	RADIUS authentication
rmon	Remote Monitoring
security	Port security
snmp	Simple Network Management Protocol
spantree	Spanning-Tree Protocol
sys	System
tac	TACACS+ authentication
tcp	Transmission Control Protocol
telnet	Terminal emulation protocol in the TCP/IP protocol stack
tftp	Trivial File Transfer Protocol
udld	UniDirectional Link Detection
vmpls	VLAN Membership Policy Server
vtp	VLAN Trunking Protocol

Table 37-2 describes the severity levels that are supported by the system message logs.

*CISCO Confidential - DRAFT***Table 37-2 Definitions of System Message Log Severity Levels**

Severity Level	Keyword	Description
0	emergencies	System unusable
1	alerts	Immediate action required
2	critical	Critical condition
3	errors	Error conditions
4	warnings	Warning conditions
5	notifications	Normal but significant conditions
6	informational	Informational messages
7	debugging	Debugging messages

System Log Message Format

System log messages begin with a percent sign (%) and can contain up to 80 characters. Messages are displayed in the following format:

mm/dd/yyyy:hh/mm/ss:facility-severity-MNEMONIC:description

Table 37-3 describes the elements of syslog messages.

Table 37-3 System Log Message Elements

Element	Description
<i>mm/dd/yyyy:hh/mm/ss</i>	Date and time of the error or event. This information appears only if you configure this with the set logging timestamp enable command.
<i>facility</i>	Indicates the facility to which the message refers (for example, SNMP, SYS, etc.).
<i>severity</i>	Single-digit code from 0 to 7 that indicates the severity of the message.
<i>MNEMONIC</i>	Text string that uniquely describes the error message.
<i>description</i>	Text string containing detailed information about the event being reported.

This example shows typical switch system messages (at system startup):

```
1999 Apr 16 10:01:26 %MLS-5-MLSENABLED:IP Multilayer switching is enabled
1999 Apr 16 10:01:26 %MLS-5-NDEDISABLED:Netflow Data Export disabled
1999 Apr 16 10:01:26 %SYS-5-MOD_OK:Module 1 is online
1999 Apr 16 10:01:47 %SYS-5-MOD_OK:Module 3 is online
1999 Apr 16 10:01:42 %SYS-5-MOD_OK:Module 6 is online
1999 Apr 16 10:02:27 %PAGP-5-PORTTOSTP:Port 3/1 joined bridge port 3/1
1999 Apr 16 10:02:28 %PAGP-5-PORTTOSTP:Port 3/2 joined bridge port 3/2
```

Default System Message Logging Configuration

Table 37-4 describes the severity levels that are supported by the system message logs.

*CISCO Confidential - DRAFT***Table 37-4 Definitions of System Message Log Severity Levels**

Severity Level	Keyword	Description
0	emergencies	System unusable
1	alerts	Immediate action required
2	critical	Critical condition
3	errors	Error conditions
4	warnings	Warning conditions
5	notifications	Normal but significant conditions
6	informational	Informational messages
7	debugging	Debugging messages

System Log Message Format

System log messages begin with a percent sign (%) and can contain up to 80 characters. Messages are displayed in the following format:

mm/dd/yyyy:hh/mm/ss:facility-severity-MNEMONIC:description

Table 37-5 describes the elements of syslog messages.

Table 37-5 System Log Message Elements

Element	Description
<i>mm/dd/yyyy:hh/mm/ss</i>	Date and time of the error or event. This information appears only if you configure this with the set logging timestamp enable command.
<i>facility</i>	Indicates the facility to which the message refers (for example, SNMP, SYS, etc.).
<i>severity</i>	Single-digit code from 0 to 7 that indicates the severity of the message.
<i>MNEMONIC</i>	Text string that uniquely describes the error message.
<i>description</i>	Text string containing detailed information about the event being reported.

This example shows typical switch system messages (at system startup):

```
1999 Apr 16 10:01:26 %MLS-5-MLSENABLED:IP Multilayer switching is enabled
1999 Apr 16 10:01:26 %MLS-5-NDEDISABLED:Netflow Data Export disabled
1999 Apr 16 10:01:26 %SYS-5-MOD_OK:Module 1 is online
1999 Apr 16 10:01:47 %SYS-5-MOD_OK:Module 3 is online
1999 Apr 16 10:01:42 %SYS-5-MOD_OK:Module 6 is online
1999 Apr 16 10:02:27 %PAGP-5-PORTTOSTP:Port 3/1 joined bridge port 3/1
1999 Apr 16 10:02:28 %PAGP-5-PORTTOSTP:Port 3/2 joined bridge port 3/2
```

Configuring System Message Logging on the Switch

The following sections describe how to configure system message logging on the switch.

CISCO Confidential - DRAFT

Configuring Session Logging Settings

By default, system logging messages are sent to console and Telnet sessions based on the default logging facility and severity values. If desired, you can disable logging to the console or logging to a given Telnet session.

When you disable or enable logging to console sessions, the enable state is applied to all future console sessions. For example, if you disable logging to the console, disconnect from the console port, and later reconnect, logging is still disabled for the console.

In contrast, when you disable or enable logging to a Telnet session, the enable state is applied only to that session. If you disable logging to a Telnet session, disconnect the session, and later reconnect, logging is enabled for the new session.

**Note**

If you enter the **set logging session** command while connected through the console port, the command has the same effect as entering the **set logging console** command. However, if you enter the **set logging console** command while connected through a Telnet session, the default console logging enable state is changed.

To configure the logging enable state for console sessions, perform this task in privileged mode:

	Task	Command
Step 1	Configure the default logging enable state for console sessions.	set logging console {enable disable}
Step 2	Verify the logging configuration.	show logging [noalias]

This example shows how to configure the logging disabled state for the current and future console sessions:

```
Console> (enable) set logging console disable
System logging messages will not be sent to the console.
Console> (enable)
```

To change the logging enable state for the current Telnet session, perform this task in privileged mode:

	Task	Command
Step 1	Change the logging enable state for a Telnet session.	set logging session {enable disable}
Step 2	Verify the logging configuration.	show logging [noalias]

This example shows how to disable logging to the current Telnet session:

```
Console> (enable) set logging session disable
System logging messages will not be sent to the current login session.
Console> (enable)
```

CISCO Confidential - DRAFT

Configuring the System Message Logging Levels

You can change the severity level for each logging facility using the **set logging level** command. Enter the **all** keyword to specify all facilities. Enter the **default** keyword to make the specified severity level the default for the specified facilities. If you do not use the **default** keyword, the specified severity level applies only to the current session.

To change the system message logging severity level setting for a logging facility, perform this task in privileged mode:

	Task	Command
Step 1	Set the severity level for logging facilities.	set logging level {all facility} severity [default]
Step 2	Verify the system message logging configuration.	show logging [noalias]

This example shows how to set the logging severity level to 5 for all facilities (for the current session only):

```
Console> (enable) set logging level all 5
All system logging facilities for this session set to severity 5(notifications)
Console> (enable)
```

This example shows how to set the default logging severity level to 3 for the **cdp** facility:

```
Console> (enable) set logging level cdp 3 default
System logging facility <cdp> set to severity 3(errors)
Console> (enable)
```

Enabling and Disabling the Logging Time Stamp

To enable or disable the logging time stamp, perform this task in privileged mode:

	Task	Command
Step 1	Specify the logging time stamp enable state.	set logging timestamp {enable disable}
Step 2	Verify the logging time stamp enable state.	show logging [noalias]

This example shows how to enable the time stamp display on system logging messages:

```
Console> (enable) set logging timestamp enable
System logging messages timestamp will be enabled.
Console> (enable)
```

Setting the Logging Buffer Size

To set the number of messages to log to the logging buffer, perform this task in privileged mode:

	Task	Command
Step 1	Set the number of messages to log to the logging buffer.	set logging buffer buffer_size
Step 2	Verify the system message logging configuration.	show logging [noalias]

CISCO Confidential - DRAFT

This example shows how to set the logging buffer size to 200 messages:

```
Console> (enable) set logging buffer 200
System logging buffer size set to <200>
Console> (enable)
```

Limiting the Number of syslog Messages

You can limit the number of syslog messages that are sent to the history table and the SNMP network management station based on severity. The default severity is set to warnings(4).

To limit the number of syslog messages, perform this task in privileged mode:

	Task	Command
Step 1	Limit the number of syslog messages.	set logging history severity <i>severity_level</i>
Step 2	Verify the system message logging configuration.	show logging

This example shows how to limit the number of syslog messages to messages with a severity level of notifications(5):

```
Console> (enable) set logging history severity 5
System logging history set to severity <5>
Console> (enable)
```

Configuring the syslog Daemon on a UNIX syslog Server

Before you can send system log messages to a UNIX syslog server, you must configure the syslog daemon on a UNIX server.

To configure the syslog daemon, follow these steps:

-
- Step 1** Log in to the UNIX server as root.
- Step 2** Add a line such as the following to the file `/etc/syslog.conf`:
- ```
user.debug /var/log/myfile.log
```



**Note** There must be five tab characters between **user.debug** and */var/log/myfile.log*. Refer to entries in the `/etc/syslog.conf` file for further examples.

---

The switch sends messages according to specified facility types and severity levels. The **user** keyword specifies the UNIX logging facility that is used. The messages from the switch are generated by user processes. The **debug** keyword specifies the severity level of the condition that is being logged. You can set UNIX systems to receive all messages from the switch.

- Step 3** Create the log file by entering these commands at the UNIX shell prompt:
- ```
$ touch /var/log/myfile.log
$ chmod 666 /var/log/myfile.log
```

Make sure that the syslog daemon reads the new changes by entering this command:

```
$ kill -HUP `cat /etc/syslog.pid`
```

Configuring syslog Servers

**Note**

Before you can send system log messages to a UNIX syslog server, you must configure the syslog daemon on the UNIX server as described in the [“Configuring the syslog Daemon on a UNIX syslog Server”](#) section on page 37-7.

To configure the switch to log messages to a syslog server, perform this task in privileged mode:

	Task	Command
Step 1	Specify the IP address of as many as three syslog servers.	set logging server <i>ip_addr</i>
Step 2	Set the facility and severity levels for syslog server messages.	set logging server facility <i>server_facility_parameter</i> set logging server severity <i>server_severity_level</i>
Step 3	Enable system message logging to configured syslog servers.	set logging server enable
Step 4	Verify the configuration.	show logging [noalias]

This example shows how to specify a syslog server, set the facility and severity levels, and enable logging to the server:

```
Console> (enable) set logging server 10.10.10.100
10.10.10.100 added to System logging server table.
Console> (enable) set logging server facility local5
System logging server facility set to <local5>
Console> (enable) set logging server severity 5
System logging server severity set to <5>
Console> (enable) set logging server enable
System logging messages will be sent to the configured syslog servers.
Console> (enable)
```

To delete a syslog server from the syslog server table, perform this task in privileged mode:

Task	Command
Delete a syslog server from the syslog server table.	clear logging server <i>ip_addr</i>

This example shows how to delete a syslog server from the syslog server table:

```
Console> (enable) clear logging server 10.10.10.100
System logging server 10.10.10.100 removed from system logging server table.
Console> (enable)
```

To disable logging to the syslog server, perform this task in privileged mode:

CISCO Confidential - DRAFT

Task	Command
Disable system message logging to configured syslog servers.	set logging server disable

This example shows how to disable logging to syslog servers:

```
Console> (enable) set logging server disable
System logging messages will not be sent to the configured syslog servers.
Console> (enable)
```

Displaying the Logging Configuration

Enter the **show logging** command to display the current system message logging configuration. Enter the **noalias** keyword to display the IP addresses instead of the host names of the configured syslog servers.

To display the current system message logging configuration, perform this task:

Task	Command
Display the current system message logging configuration.	show logging [noalias]

This example shows how to display the current system message logging configuration:

```
Console> (enable) show logging

Logging buffer size:      200
    timestamp option:    disabled
Logging history size:     1
    severity:            notifications(5)
Logging console:          enabled
Logging server:           enabled
{syslog.bigcorp.com}
    server facility:      LOCAL5
    server severity:      notifications(5)

Facility      Default Severity      Current Session Severity
-----
cdp            3                      3
drip           2                      5
dtp            5                      5
dvlan          2                      5
earl           2                      5
fddi           2                      5
filesys        2                      5
gvrp           2                      5
ip             2                      5
kernel         2                      5
mcast          2                      5
mgmt           5                      5
mls            5                      5
pagp           5                      5
protfilt       2                      5
pruning        2                      5
radius         2                      5
security       2                      5
snmp           2                      5
spantree       2                      5
sys            5                      5
```

CISCO Confidential - DRAFT

```

tac                2                5
tcp                2                5
telnet             2                5
tftp               2                5
udld               4                5
vmps               2                5
vtp                2                5

0(emergencies)     1(alerts)         2(critical)
3(errors)          4(warnings)       5(notifications)
6(information)     7(debugging)
Console> (enable)

```

Displaying System Messages

Use the **show logging buffer** command to display the messages in the switch logging buffer. If you do not specify *number_of_messages*, the default is to display the last 20 messages in the buffer.

To display the messages in the switch logging buffer, perform one of these tasks:

Task	Command
Display the first <i>number_of_messages</i> messages in the buffer.	show logging buffer [<i>number_of_messages</i>]
Display the last <i>number_of_messages</i> messages in the buffer.	show logging buffer -[<i>number_of_messages</i>]

This example shows how to display the first five messages in the buffer:

```

Console> (enable) show logging buffer 5
1999 Apr 16 08:40:11 %SYS-5-MOD_OK:Module 1 is online
1999 Apr 16 08:40:14 %SYS-5-MOD_OK:Module 3 is online
1999 Apr 16 08:40:14 %SYS-5-MOD_OK:Module 2 is online
1999 Apr 16 08:41:15 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1
1999 Apr 16 08:41:15 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/2

```

This example shows how to display the last five messages in the buffer:

```

Console> (enable) show logging buffer -5
%PAGP-5-PORTFROMSTP:Port 3/1 left bridge port 3/1
%SPANTREE-5-PORTDEL_SUCCESS:3/2 deleted from vlan 1 (PAgP_Group_Rx)
%PAGP-5-PORTFROMSTP:Port 3/2 left bridge port 3/2
%PAGP-5-PORTTOSTP:Port 3/1 joined bridge port 3/1-2
%PAGP-5-PORTTOSTP:Port 3/2 joined bridge port 3/1-2
Console> (enable)

```

Configuring DNS

This chapter describes how to configure the Domain Name System (DNS) on the Catalyst enterprise LAN switches.

**Note**

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 4500 Series, Catalyst 2948G, and Catalyst 2980G Switches Command Reference*.

This chapter consists of these sections:

- [Understanding How DNS Works, page 38-1](#)
- [Default DNS Configuration, page 38-1](#)
- [Configuring DNS on the Switch, page 38-2](#)

Understanding How DNS Works

DNS is a distributed database with which you can map host names to IP addresses through the DNS protocol from a DNS server. When you configure DNS on the switch, you can substitute the host name for the IP address with all IP commands, such as **ping**, **telnet**, **upload**, and **download**.

To use DNS, you must have a DNS name server on your network.

You can specify a primary DNS name server on the switch as well as two backup servers. The first server that is specified is the primary server unless you explicitly identify the primary server. The switch sends DNS queries to the primary server first. If the query to the primary server fails, the backup servers are queried.

Default DNS Configuration

[Table 38-1](#) shows the default DNS configuration.

Table 38-1 Default DNS Configuration

Feature	Default Value
DNS enable state	Disabled

*CISCO Confidential - DRAFT***Table 38-1 Default DNS Configuration (continued)**

Feature	Default Value
DNS default domain name	Null
DNS servers	None specified

Configuring DNS on the Switch

The following sections describe how to configure DNS:

- [Setting Up and Enabling DNS, page 38-2](#)
- [Clearing a DNS Server, page 38-3](#)
- [Clearing the DNS Domain Name, page 38-3](#)
- [Disabling DNS, page 38-3](#)

Setting Up and Enabling DNS

To set up and enable DNS on the switch, perform this task in privileged mode:

	Task	Command
Step 1	Specify the IP address of one or more DNS servers.	set ip dns server <i>ip_addr</i> [primary]
Step 2	Set the domain name.	set ip dns domain <i>name</i>
Step 3	Enable DNS.	set ip dns enable
Step 4	Verify the DNS configuration.	show ip dns [noalias]

This example shows how to set up and enable DNS on the switch and verify the configuration:

```

Console> (enable) set ip dns server 10.2.2.1
10.2.2.1 added to DNS server table as primary server.
Console> (enable) set ip dns server 10.2.24.54 primary
10.2.24.54 added to DNS server table as primary server.
Console> (enable) set ip dns server 10.12.12.24
10.12.12.24 added to DNS server table as backup server.
Console> (enable) set ip dns domain corp.com
Default DNS domain name set to corp.com
Console> (enable) set ip dns enable
DNS is enabled
Console> (enable) show ip dns
DNS is currently enabled.
The default DNS domain name is: corp.com

```

```

DNS name server                status
-----
dns_serv2
dns_serv1                    primary
dns_serv3
Console> (enable)

```

CISCO Confidential - DRAFT

Clearing a DNS Server

To clear DNS servers from the DNS server table, perform this task in privileged mode:

	Task	Command
Step 1	Clear one or all of the DNS servers from the table.	clear ip dns server [<i>ip_addr</i> all]
Step 2	Verify the DNS configuration.	show ip dns [noalias]

This example shows how to clear a DNS server from the DNS server table:

```
Console> (enable) clear ip dns server 10.12.12.24
10.12.12.24 cleared from DNS table
Console> (enable)
```

This example shows how to clear all of the DNS servers from the DNS server table:

```
Console> (enable) clear ip dns server all
All DNS servers cleared
Console> (enable)
```

Clearing the DNS Domain Name

To clear the default DNS domain name, perform this task in privileged mode:

	Task	Command
Step 1	Clear the default DNS domain name.	clear ip dns domain
Step 2	Verify the DNS configuration.	show ip dns [noalias]

This example shows how to clear the default DNS domain name:

```
Console> (enable) clear ip dns domain
Default DNS domain name cleared.
Console> (enable)
```

Disabling DNS

To disable DNS, perform this task in privileged mode:

	Task	Command
Step 1	Disable DNS on the switch.	set ip dns disable
Step 2	Verify the DNS configuration.	show ip dns [noalias]

This example shows how to disable DNS on the switch:

```
Console> (enable) set ip dns disable
DNS is disabled
Console> (enable)
```

CISCO Confidential - DRAFT

Configuring NTP

This chapter describes how to configure the Network Time Protocol (NTP) on the Catalyst enterprise LAN switches.

**Note**

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 4500 Series, Catalyst 2948G, and Catalyst 2980G Switches Command Reference*.

This chapter consists of these sections:

- [Understanding How NTP Works, page 39-1](#)
- [Default NTP Configuration, page 39-2](#)
- [Configuring NTP on the Switch, page 39-2](#)

Understanding How NTP Works

NTP synchronizes timekeeping among a set of distributed time servers and clients. With this synchronization, you can correlate events to the time that system logs were created and the time that other time-specific events occur. An NTP server must be accessible by the client switch.

NTP uses the User Datagram Protocol (UDP) as its transport protocol. All NTP communication uses Coordinated Universal Time (UTC), which is the same as Greenwich Mean Time. An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock that is attached to a time server. NTP distributes this time across the network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two machines to within a millisecond of one another.

NTP uses a stratum to describe how many NTP hops away a machine is from an authoritative time source. A stratum 1 time server has a radio or atomic clock that is directly attached, a stratum 2 time server receives its time from a stratum 1 time server, and so on. A machine running NTP automatically chooses as its time source the machine with the lowest stratum number that it is configured to communicate with through NTP. This strategy effectively builds a self-organizing tree of NTP speakers.

NTP has two ways to avoid synchronizing to a machine whose time might be ambiguous:

- NTP never synchronizes to a machine that is not synchronized itself.
- NTP compares the time that is reported by several machines and does not synchronize to a machine whose time is significantly different from the others, even if its stratum is lower.

CISCO Confidential - DRAFT

The communications between machines running NTP, known as associations, are usually statically configured; each machine is given the IP addresses of all machines with which it should form associations. An associated pair of machines can keep accurate timekeeping by exchanging NTP messages between each other. However, in a LAN environment, you can configure NTP to use IP broadcast messages. With this alternative, you can configure the machine to send or receive broadcast messages, but the accuracy of timekeeping is marginally reduced because the information flow is one-way only.

Cisco's implementation of NTP does not support stratum 1 service; it is not possible to connect to a radio or atomic clock. We recommend that you obtain the time service for your network from the public NTP servers available on the IP Internet.

If the network is isolated from the Internet, Cisco's NTP implementation allows a machine to be configured so that it acts as though it is synchronized using NTP, when it actually has determined the time using other methods. Other machines synchronize to that machine using NTP.

Default NTP Configuration

Table 39-1 shows the default NTP configuration.

Table 39-1 *Default NTP Configuration*

Feature	Default Value
Broadcast client mode	Disabled
Client mode	Disabled
Broadcast delay	3000 microseconds
Time zone	Not specified
Offset from UTC	0 hours
Summertime adjustment	Disabled
NTP server	None specified
Authentication mode	Disabled

Configuring NTP on the Switch

The following sections describe how to configure NTP.

Enabling NTP in Broadcast-Client Mode

Enable the switch in NTP broadcast-client mode if an NTP broadcast server, such as a router, regularly broadcasts time-of-day information on the network. To compensate for any server-to-client packet latency, you can specify an NTP broadcast delay (a time adjustment factor for the receiving of broadcast packets by the switch).

To enable NTP broadcast-client mode on the switch, perform this task in privileged mode:

CISCO Confidential - DRAFT

	Task	Command
Step 1	Enable NTP broadcast-client mode.	set ntp broadcastclient enable
Step 2	(Optional) Set the estimated NTP broadcast packet delay.	set ntp broadcast delay <i>microseconds</i>
Step 3	Verify the NTP configuration.	show ntp [noalias]

This example shows how to enable NTP broadcast-client mode on the switch, set a broadcast delay of 4000 microseconds, and verify the configuration:

```
Console> (enable) set ntp broadcastclient enable
NTP Broadcast Client mode enabled
Console> (enable) set ntp broadcastdelay 4000
NTP Broadcast delay set to 4000 microseconds
Console> (enable) show ntp
```

```
Current time: Tue Jun 23 1998, 20:25:43
Timezone: '', offset from UTC is 0 hours
Summertime: '', disabled
Last NTP update:
Broadcast client mode: enabled
Broadcast delay: 4000 microseconds
Client mode: disabled
```

NTP-Server

```
-----
Console> (enable)
```

Configuring NTP in Client Mode

Configure the switch in NTP client mode if you want the client switch to regularly send time-of day requests to an NTP server. You can configure up to ten server addresses per client.

To configure the switch in NTP client mode, perform this task in privileged mode:

	Task	Command
Step 1	Specify the IP address of the NTP server.	set ntp server <i>ip_addr</i>
Step 2	Enable NTP client mode.	set ntp client enable
Step 3	Verify the NTP configuration.	show ntp [noalias]

CISCO Confidential - DRAFT

This example shows how to configure the NTP server address, enable NTP client mode on the switch, and verify the configuration:

```
Console> (enable) set ntp server 172.20.52.65
NTP server 172.20.52.65 added.
Console> (enable) set ntp client enable
NTP Client mode enabled
Console> (enable) show ntp
```

```
Current time: Tue Jun 23 1998, 20:29:25
Timezone: '', offset from UTC is 0 hours
Summertime: '', disabled
Last NTP update: Tue Jun 23 1998, 20:29:07
Broadcast client mode: disabled
Broadcast delay: 3000 microseconds
Client mode: enabled
```

NTP-Server

172.16.52.65

Console> (enable)

Configuring Authentication in Client Mode

Authentication can enhance the security of a system running NTP. When you enable the authentication feature, the client switch sends time-of-day requests only to trusted NTP servers. The authentication feature is documented in RFC 1305.

You can configure up to ten authentication keys per client. Each authentication key is actually a pair of two keys:

- A public key number—A 32-bit integer that can range from 1 to 4,294,967,295
- A secret key string—An arbitrary string of 32 characters, including all printable characters and spaces

To authenticate the message, the client authentication key must match the key on the server. Therefore, the authentication key must be securely distributed in advance (the client administrator must get the key pair from the server administrator and configure it on the client).

To configure authentication, perform this task in privileged mode:

	Task	Command
Step 1	Configure an authentication key pair for NTP and specify whether the key will be trusted or untrusted.	set ntp key <i>public_key</i> [<i>trusted</i> <i>untrusted</i>] md5 <i>secret_key</i>
Step 2	Set the IP address of the NTP server and the public key.	set ntp server <i>ip_addr</i> [<i>key public_key</i>]
Step 3	Enable NTP client mode.	set ntp client enable
Step 4	Enable NTP authentication.	set ntp authentication enable
Step 5	Verify the NTP configuration.	show ntp [<i>noalias</i>]

This example shows how to configure the NTP server address, enable NTP client and authentication modes on the switch, and verify the configuration:

```
Console> (enable) set ntp server 172.20.52.65 key 879
NTP server 172.20.52.65 with key 879 added.
```

CISCO Confidential - DRAFT

```

Console> (enable) set ntp client enable
NTP Client mode enabled
Console> (enable) set ntp authentication enable
NTP authentication feature enabled
Console> (enable) show ntp

Current time: Tue Jun 23 1998, 20:29:25
Timezone: '', offset from UTC is 0 hours
Summertime: '', disabled
Last NTP update: Tue Jun 23 1998, 20:29:07
Broadcast client mode: disabled
Broadcast delay: 3000 microseconds
Client mode: enabled
Authentication: enabled

NTP-Server                               Server Key
-----
172.16.52.65

Key Number  Mode      Key String
-----

```

Console> (enable)

Setting the Time Zone

You can set a time zone for the switch to display the time in that time zone. You must enable NTP before you set the time zone. If NTP is not enabled, this command has no effect. If you enable NTP and do not specify a time zone, UTC is shown by default.

To set the time zone, perform this task in privileged mode:

	Task	Command
Step 1	Set the time zone.	set timezone zone hours [minutes]
Step 2	Verify the time zone configuration.	show timezone

This example shows how to set the time zone on the switch:

```

Console> (enable) set timezone Pacific -8
Timezone set to 'Pacific', offset from UTC is -8 hours
Console> (enable)

```

Enabling the Daylight Saving Time Adjustment

Following U.S. standards, you can have the switch advance the clock one hour at 2:00 a.m. on the first Sunday in April and move the clock back one hour at 2:00 a.m. on the last Sunday in October. You can also explicitly specify start and end dates and times and whether the time adjustment recurs every year.

To enable the daylight saving time clock adjustment following the U.S. standards, perform this task in privileged mode:

CISCO Confidential - DRAFT

	Task	Command
Step 1	Enable the daylight saving time clock adjustment.	set summertime enable <i>[zone_name]</i> set summertime recurring
Step 2	Verify the configuration.	show summertime

This example shows how to set the clock adjusted for Pacific Daylight Time following the U.S. standards:

```
Console> (enable) set summertime enable PDT
Console> (enable) set summertime recurring
Summertime is enabled and set to 'PDT'
Console> (enable)
```

To enable the daylight saving time clock adjustment that recurs every year on different days or with a different offset than the U.S. standards, perform this task in privileged mode:

	Task	Command
Step 1	Enable the daylight saving time clock adjustment.	set summertime recurring <i>week day month</i> <i>hh:mm week day month hh:mm offset</i>
Step 2	Verify the configuration.	show summertime

This example shows how to set the daylight saving time clock adjustment, repeating every year, starting on the third Monday of February at noon and ending on the second Saturday of August at 3:00 p.m. with a 30-minute offset forward in February and back in August.

```
Console> (enable) set summertime recurring 3 mon feb 3:00 2 saturday aug 15:00 30
Summer time is disabled and set to ''
  start: Sun Feb 13 2000, 03:00:00
  end: Sat Aug 26 2000, 14:00:00
  Offset: 30 minutes
  Recurring: yes, starting at 3:00am Sunday of the third week of February and ending
  14:00pm Saturday of the fourth week of August.
Console> (enable)
```

To enable the daylight saving time clock adjustment to a nonrecurring specific date, perform this task in privileged mode:

	Task	Command
Step 1	Enable the daylight saving time clock adjustment.	set summertime date <i>month date year hh:mm</i> <i>month date year hh:mm offset</i>
Step 2	Verify the configuration.	show summertime

This example shows how to set the nonrecurring daylight saving time clock adjustment on April 30, 2003, at 4.30 a.m., ending on February 1, 2004 at 5:30 a.m., with an offset of 1 day (1440 min):

```
Console> (enable) set summertime date apr 13 2003 4:30 jan 21 2004 5:30 50
Summertime is disabled and set to ''
Start : Thu Apr 13 2000, 04:30:00
End : Mon Jan 21 2002, 05:30:00
Offset: 1440 minutes (1 day)
Recurring: no
Console> (enable)
```

CISCO Confidential - DRAFT

Disabling the Daylight Saving Time Adjustment

To disable the daylight saving time clock adjustment, perform this task in privileged mode:

	Task	Command
Step 1	Disable the daylight saving time clock adjustment.	set summertime disable [zone_name]
Step 2	Verify the configuration.	show summertime

This example shows how to disable the daylight saving time adjustment:

```
Console> (enable) set summertime disable Arizona
Summertime is disabled and set to 'Arizona'
Console> (enable)
```

Clearing the Time Zone

To clear the time zone settings and return the time zone to UTC, perform this task in privileged mode:

Task	Command
Clear the time zone settings.	clear timezone

This example shows how to clear the time zone settings:

```
Console> (enable) clear timezone
Timezone name and offset cleared
Console> (enable)
```

Clearing NTP Servers

To clear an NTP server address from the NTP servers table on the switch, perform this task in privileged mode:

	Task	Command
Step 1	Clear an NTP server address from the NTP server table.	clear ntp server [ip_addr all]
Step 2	Verify the NTP configuration.	show ntp [noalias]

This example shows how to clear an NTP server address from the NTP server table:

```
Console> (enable) clear ntp server 172.16.64.10
NTP server 172.16.64.10 removed.
Console> (enable)
```

Disabling NTP

To disable NTP broadcast-client mode on the switch, perform this task in privileged mode:

CISCO Confidential - DRAFT

	Task	Command
Step 1	Disable NTP broadcast-client mode.	set ntp broadcastclient disable
Step 2	Verify the NTP configuration.	show ntp [noalias]

This example shows how to disable NTP broadcast-client mode on the switch:

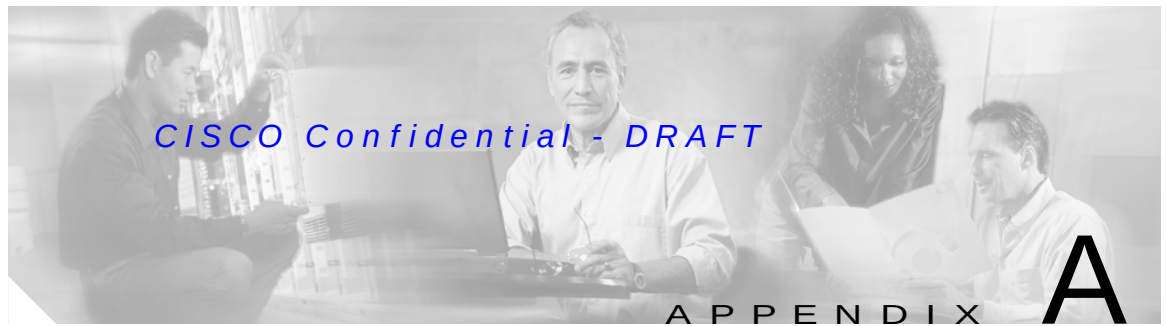
```
Console> (enable) set ntp broadcastclient disable
NTP Broadcast Client mode disabled
Console> (enable)
```

To disable NTP client mode on the switch, perform this task in privileged mode:

	Task	Command
Step 1	Disable NTP client mode.	set ntp client disable
Step 2	Verify the NTP configuration.	show ntp [noalias]

This example shows how to disable NTP client mode on the switch:

```
Console> (enable) set ntp client disable
NTP Client mode disabled
Console> (enable)
```



Acronyms

A

AAL	ATM adaptation layer
ACE	access control entry
ADM	add-drop multiplexer
AFI	Authority and Format Identifier
AMP	active monitor present
APaRT	automated packet recognition/translation
ARP	Address Resolution Protocol
ASP	ATM switch processor
ATM	Asynchronous Transfer Mode

B

BDPU	bridge protocol data unit
BRF	Bridge Relay Function
BUS	broadcast and unknown server

C

CAM	content-addressable memory
CAS	column address strobe
CBR	constant bit rate

CISCO Confidential - DRAFT

CDDI	Copper Distributed Data Interface
CDP	Cisco Discovery Protocol
CGMP	Cisco Group Management Protocol
CLI	command-line interface
COPS	Common Open Policy Service
CoS	class of service
CRC	Cyclic Redundancy Check
CRF	Concentrator Relay Function
 D	
DCC	Data Country Code
DEC	Digital Equipment Corporation
DFI	domain-specific part format identifier
DHCP	Dynamic Host Configuration Protocol
DISL	dynamic inter-switch link
DMP	data movement processor
DNS	Domain Name System
DoD	Department of Defense
DRiP	Dual Ring Protocol
DSAP	destination service access point
DTP	Dynamic Trunking Protocol
DTR	dedicated Token Ring; data terminal ready

E

EARL	Enhanced Address Recognition Logic
ECMA	European Computer Manufacturers Association
EEPROM	electrically erasable programmable read-only memory
EIA	Electronic Industries Association

CISCO Confidential - DRAFT

ELAN	emulated local area network
ESI	end-system identifier
F	
FCS	frame check sequence
FDDI	Fiber Distributed Data Interface
FDX	full duplex
FSSRP	Fast Simple Server Redundancy Protocol
FTP	foil twisted-pair
FTTH	fiber to the home

G

GARP	General Attribute Registration Protocol
GBIC	Gigabit Interface Converter
GMRP	GARP Multicast Registration Protocol
GSP	Gigabit Switch Platform
GVRP	GARP VLAN Registration Protocol

H

HDX	half duplex

I

ICD	International Code Designator
ICMP	Internet Control Message Protocol
IDP	Initial Domain Part
IGMP	Internet Group Management Protocol

CISCO Confidential - DRAFT

ILMI	Integrated Local Management Interface
IMPL	initial microprogram load
IP	Internet Protocol
IPC	interprocessor communication
IPX	Internetwork Packet Exchange
ISL	Inter-Switch Link
ISO	International Organization of Standardization

K

KDC	key distribution center

L

LAN	local-area network
LANE	LAN Emulation
LAT	local-area transport
LCP	Link Control Protocol
LEC	LAN Emulation Client
LECS	LAN Emulation Configuration Server
LEM	link error monitor
LER	link error rate
LES	LAN Emulation Server
LLC	logical link control

M

MAC	Media Access Control
MAP	Manufacturing Automation Protocol

CISCO Confidential - DRAFT

MBS	maximum burst size
MCP	Master Communication Processor
MIB	Management Information Base
MII	media-independent interface
MLS	Multilayer Switching
MLSP	Multilayer Switching Protocol
MLS-RP	multilayer switching-route processor
MM	multi-mode
MOP	Maintenance Operation Protocol
MOTD	message-of-the-day
MPC	Multiprotocol over ATM client
MPOA	multiprotocol over ATM
MPS	multiprotocol over ATM server
MTU	maximum transmission unit

N

NAUN	nearest available upstream neighbor
NBMA	non-broadcast multi-access
NBS	non-bused spare
NDE	NetFlow Data Export
NFFC	NetFlow Feature Card
NFFC II	Enhanced NetFlow Feature Card
NFLS	NetFlow LAN Switching
NHC	Next Hop Client
NHRP	Next Hop Resolution Protocol
NHS	Next Hop Server
NMP	Network Management Processor
NNI	Network-Network Interface

CISCO Confidential - DRAFT

NSAP	network service access point
NTP	Network Time Protocol
NVRAM	nonvolatile random-access memory

O

OAM	Operation, Administration, and Maintenance
OOB	out-of-band
OSI	Open System Interconnection
OTP	One-Time-Password

P

PAgP	Port Aggregation Protocol
PAM	port adapter module
PCM	pulse code modulation
PCMCIA	Personal Computer Memory Card International Association
PCR	peak cell rate
PDU	protocol data unit
PHY	physical sublayer
PIM	protocol independent multicast
PLCP	physical layer convergence procedure
PLIM	physical layer interface module
PPP	Point-to-Point Protocol
PVC	permanent virtual circuit (or permanent virtual connection in ATM terminology)

Q

QoS	quality of service

CISCO Confidential - DRAFT

R

RADIUS	Remote Authentication Dial-In User Service
RAS	row address strobe
RCD	RAS-to-CAS delay
RCP	remote copy protocol
RGMP	Router Group Management Protocol
RIF	routing information field
RMON	remote monitoring
ROM	read-only memory
RP	route processor
RSM	Route Switch Module

S

SAID	Security Association Identifier
SAMBA	synergy advanced multipurpose bus arbiter
SAP	service access point
SAR	segmentation and reassembly
SCP	Serial Control Protocol
SCR	sustainable cell rate
SDP	Session Description Protocol
SE	search engine
SLIP	Serial Line Internet Protocol
SM	single-mode
SMP	standby monitor present
SMT	station management
SNA	Systems Network Architecture
SNAP	Subnetwork Access Protocol

CISCO Confidential - DRAFT

SNMP	Simple Network Management Protocol
SPAN	Switched Port Analyzer
SRB	source-route bridging
SRT	source-route transparent bridging
SSCOP	Service-Specific Connection Oriented Protocol
SSRP	Simple Server Redundancy Protocol
STP	1) Spanning Tree Protocol 2) shielded twisted-pair
STPX	Spanning Tree Protocol Extensions (MIB)
SVC	switched virtual circuit

T

TACACS+	Terminal Access Controller Access Control System Plus
TCP/IP	Transmission Control Protocol/Internet Protocol
TFTP	Trivial File Transfer Protocol
TGT	ticket granting ticket
TIA	Telecommunications Industry Association
TLV	type-length value
TOS	type of service
TrBRF	Token Ring Bridge Relay Function
TrCRF	Token Ring Concentrator Relay Function
TRT	token rotation timer
TTL	time to live
TTY	teletype

U

UART	universal asynchronous receiver/transmitter
UBR	unspecified bit rate

CISCO Confidential - DRAFT

UDLD	Unidirectional Link Detection Protocol
UDP	User Datagram Protocol
UNI	User-Network Interface
UTC	Coordinated Universal Time
V	
VBR	variable bit rate
VC	virtual circuit
VCC	virtual channel connection
VCD	Virtual Channel Descriptor
VCI	1) virtual channel identifier; 2) virtual connection identifier
VCR	Virtual Configuration Register
VLAN	virtual LAN
VMPS	VLAN Membership Policy Server
VPI	virtual path identifier
VQP	VLAN Query Protocol
VTP	VLAN Trunking Protocol
W	
WRED	weighted random early detect
WRR	Weighted Round Robin

CISCO Confidential - DRAFT

Numerics

- 10/100 port speed, setting [4-4](#)
- 1400W DC power supply [28-5](#)
- 802.1Q
 - example [11-9, 11-19](#)
 - mapping VLANs to ISL [10-10](#)
 - overview [11-1](#)
 - restrictions [11-4](#)
 - supported switches (table) [11-3](#)
- 802.1x authentication
 - authentication server
 - defined [31-2](#)
 - client, defined [31-2](#)
 - configurable parameters [31-5](#)
 - overview [31-1](#)
 - using a RADIUS server for VLAN assignment [31-6](#)

A

- accelerator module, switch fabric
 - See switch fabric accelerator module
- accounting
 - configuration guidelines [30-49](#)
 - disabling [30-51](#)
 - enabling [30-49](#)
 - overview [30-46](#)
 - See also RADIUS accounting; TACACS+ accounting
- adding multicast filter profiles [15-19](#)
- addresses
 - See IP addresses; MAC addresses
- Address Resolution Protocol
 - See ARP

- administration
 - switch [27-1, 38-1](#)
- administrative groups, EtherChannel [6-6](#)
- advertisements
 - See VTP advertisements
- aliases
 - See command aliases; IP aliases
- aliases, command [2-7](#)
- ARP
 - configuring entries [27-8](#)
- assigning port filter associations [15-22](#)
- attempts, limiting telnet [30-9](#)
- audience [xxiii](#)
- authentication
 - See 802.1x authentication, Kerberos authentication; local authentication; login authentication; NTP authentication; RADIUS authentication; TACACS+ authentication
- authorization
 - overview [30-40](#)
 - See also TACACS+ authorization [30-42](#)
- authorized ports with 802.1X [31-4](#)
- autonegotiation
 - duplex [4-5](#)
 - speed [4-5](#)
 - trunks [11-2](#)
- auxiliary VLANs
 - configuring [10-12](#)
 - dynamic VLAN membership [12-13](#)
 - software support [10-5](#)

B

- BackboneFast

- adding a switch (figure) [8-7](#)
- disabling [8-18](#)
- displaying statistics [8-17](#)
- enabling [8-17](#)
- multiple spanning tree [7-14](#)
- overview [8-4](#)
- backplane channel module [36-3](#)
- banners
 - See login banners
- boot configuration
 - clearing system flash [32-7](#)
 - ignoring NVRAM [32-6](#)
- BOOT environment variables
 - clearing [32-7](#), [32-8](#)
 - default [32-4](#)
 - displaying [32-8](#)
 - overview [32-3](#)
 - setting [32-6](#), [32-7](#)
- boot field
 - overview [32-2](#)
 - setting [32-4](#)
- BPDU filter
 - multiple spanning tree [7-14](#)
- BPDU guard
 - disabling [8-14](#)
 - enabling [8-13](#)
 - multiple spanning tree [7-14](#)
- BPDU overview [7-2](#)
- BPDU skewing
 - configuring [7-53](#)
 - understanding [7-20](#)
- bridge identifiers
 - MAC addresses [7-12](#)
 - PVST+ [7-22](#)
- bridge protocol data unit
 - See BPDU

C

- Catalyst 2948G switches, overview (table) [1-2](#)
- Catalyst 2980G switches, overview (table) [1-3](#)
- CDP
 - default configuration [21-2](#)
 - disabling globally [21-2](#)
 - disabling on ports [21-2](#)
 - displaying neighbor information [21-5](#)
 - enabling globally [21-2](#)
 - enabling on ports [21-2](#)
 - overview [21-1](#)
 - setting holdtime [21-4](#)
 - setting message interval [21-4](#)
- CGMP
 - clearing multicast groups [15-17](#)
 - clearing multicast router ports [15-16](#)
 - configuring multicast groups [15-6](#), [15-16](#)
 - disabling [15-8](#)
 - disabling fast-leave processing [15-7](#)
 - displaying multicast groups [15-6](#)
 - enabling [15-4](#)
 - enabling fast-leave processing [15-5](#)
 - joining multicast groups [15-2](#)
 - leaving multicast groups [15-2](#)
 - overview [15-1](#)
 - specifying multicast router ports [15-15](#)
 - viewing statistics [15-7](#)
- channel modes, EtherChannel (table) [6-5](#)
 - LACP [6-16](#)
- checksum, verifying Flash file [34-6](#)
- CIDR
 - static routes and [27-9](#)
- Cisco Discovery Protocol
 - See CDP
- Cisco Group Management Protocol
 - See CGMP
- Cisco IP Phones
 - sound quality [29-2](#)

CISCO Confidential - DRAFT

- CiscoWorks2000 [24-17](#)
- CIST [7-14](#)
- classification
 - frames [14-3](#)
- classless interdomain routing
 - See CIDR
- class of service
 - See CoS
- clear boot system flash command [32-7](#)
- CLI
 - command aliases [2-7](#)
 - ROM monitor [2-9](#)
 - switch
 - accessing [2-2](#)
 - designating IP addresses [2-8](#)
 - designating IP aliases [2-8](#)
 - designating MAC addresses [2-8](#)
 - designating modules [2-7](#)
 - designating ports [2-7](#)
 - designating VLANs [2-7](#)
 - help [2-4](#)
 - history substitution [2-6](#)
 - operating [2-3](#)
- clock, setting [27-4](#)
- command aliases
 - creating [27-6](#)
 - using [2-7](#)
- command-line interface
 - See CLI
- Common and Internal Spanning Tree
 - See CIST [7-14](#)
- Common Spanning Tree
 - See CST [7-13](#)
- common spanning tree
 - See CST
- community ports
 - definition [10-15](#)
- community strings
 - defining [24-7](#)
- overview [24-5](#)
- CONFIG_FILE variable
 - setting recurrence [32-5](#)
- configuration
 - clearing the [35-7](#)
- configuration files
 - creating [35-2](#)
 - downloading via RCP [35-6](#)
 - downloading via TFTP [35-4](#)
 - guidelines [35-1](#)
 - uploading preparation [35-4](#), [35-7](#)
 - uploading to RCP server [35-7](#)
 - uploading to TFTP server [35-5](#)
- configuration guidelines
 - TACACS+ accounting [30-49](#)
- configuration register
 - default setting [32-4](#)
 - ignoring NVRAM at boot [32-6](#)
 - overview [32-2](#)
 - setting boot field [32-4](#)
 - setting CONFIG_FILE recurrence [32-5](#)
- configurations
 - IGMP traffic filtering [15-17](#)
- configuring
 - multicast filtering [15-19](#)
 - port IP multicast filtering [15-19](#)
- configuring a switch
 - using a file on an rcv server [35-6](#)
- console port
 - disconnecting user sessions [20-8](#)
 - establishing connections [2-2](#)
 - monitoring user sessions [20-7](#)
 - SLIP and [3-8](#)
 - system message logging settings [37-5](#)
- conventions, document [xxvi](#)
- CoS
 - configuring default switch values [14-5](#)
 - drop thresholds
 - mapping [14-6](#)

- transmitting [14-3](#)
- Layer 2 CoS values [14-2](#)
- reverting to default [14-5](#)
- CST [7-13](#)
- VLAN 1 [7-17](#)

D

- databases
 - downloading VMPS [12-9](#)
 - See also VMPS databases
- date, setting [27-4](#)
- daylight saving time
 - disabling adjustment [39-7](#)
 - enabling adjustment [39-5](#)
- default configurations
 - Ethernet [4-2](#)
 - Fast Ethernet [4-2](#)
 - TACACS+ accounting [30-49](#)
- default gateway, configuring [3-6](#)
- default IGMP filter configuration [15-18](#)
- denying filter match-action [15-20](#)
- DHCP
 - releasing lease [3-10](#)
 - renewing lease [3-10](#)
 - sc0 interface and [3-9](#)
- disabling IGMP multicast filtering [15-19](#)
- DISL
 - See DTP
- DNS
 - clearing domain names [38-3](#)
 - default configuration [38-1](#)
 - disabling [38-3](#)
 - enabling [38-2](#)
 - overview [38-1](#)
 - setting domain names [38-2](#)
 - setting up [38-2](#)
 - system name and [27-1](#)
 - system prompt and [27-1](#)

- DNS servers
 - clearing [38-3](#)
 - specifying [38-2](#)
- documentation
 - conventions [xxvi](#)
 - organization [xxiii](#)
 - related [xxv](#)
- domain names
 - clearing [38-3](#)
 - setting [38-2](#)
- Domain Name System
 - See DNS
- downloading
 - configuration files [35-4, 35-6](#)
 - software images [33-2, 33-5](#)
- drop thresholds
 - CoS mapping [14-6](#)
 - transmit queue [14-3](#)
- DTP
 - non-Cisco devices and [11-3](#)
 - overview [11-2](#)
- duplex mode
 - Fast Ethernet [4-5](#)
- Dynamic Host Configuration Protocol
 - See DHCP
- dynamic ports
 - troubleshooting [12-11](#)
- dynamic port VLAN membership
 - See VMPS
- Dynamic Trunking Protocol
 - See DTP

E

- enable mode, switch CLI [2-3](#)
- enable password
 - recovering lost [30-14](#)
 - setting [30-13](#)
- enabling IGMP multicast filtering [15-18](#)

CISCO Confidential - DRAFT

- enabling IGMP traffic filtering [15-19](#)
- encapsulation type descriptions, trunks (table) [11-2](#)
- encryption
 - See secure shell encryption
- environment variables
 - See BOOT environment variables
- errdisable timeout, configuring [4-7](#)
- error messages
 - system message logging (syslog) [37-1](#)
 - VMPS (table) [12-11](#)
- establishing multicast filter profiles [15-19](#)
- EtherChannel
 - administrative groups [6-6](#)
 - channel modes (table) [6-5](#)
 - LACP [6-16](#)
 - configuration guidelines [6-3](#)
 - configuring [6-6](#)
 - configuring administrative groups [6-7](#)
 - displaying PAgP statistics [6-12](#)
 - displaying statistics [6-11](#)
 - EtherChannel IDs [6-6](#)
 - frame distribution [6-2](#)
 - hardware support [6-2](#)
 - maximum number of channels supported [6-4](#)
 - modes [6-5](#)
 - modes, using LACP [6-16](#)
 - overview [6-1](#)
 - PAgP and [6-5](#)
 - port costs [6-8](#)
 - port-VLAN costs [6-9](#)
 - sample configuration [11-9](#)
 - See also Fast EtherChannel; Gigabit EtherChannel

Ethernet

- autonegotiation [4-5](#)
- checking connectivity [4-8](#)
- default configuration [4-2](#)
- overview [4-1](#)
- setting port duplex [4-5](#)
- setting port name [4-3](#)

- setting port priority [4-4](#)
- setting port speed [4-4](#)
 - See also protocol filtering
- examples, conventions [xxvi](#)
- extended-range VLANs
 - See VLANs

F

Fast EtherChannel

- example [6-12](#)
- overview [6-2](#)
 - See also EtherChannel; Gigabit EtherChannel

Fast Ethernet

- autonegotiation [4-5](#)
- checking connectivity [4-8](#)
- default configuration [4-2](#)
- overview [4-1](#)
- setting port duplex [4-5](#)
- setting port name [4-3](#)
- setting port priority [4-4](#)
- setting port speed [4-4](#)
 - See also protocol filtering

- fiber-optic cables, detecting unidirectional links [23-1](#)

filtering

- IGMP actions [15-17](#)

filters, protocol

- See protocol filtering

Flash file system

- copying files [34-4](#)
- deleting files [34-5](#)
- listing files [34-2, 34-3](#)
- restoring deleted files [34-6](#)
- setting configuration modes [34-2](#)
- setting default devices [34-1](#)
- verifying checksum [34-6](#)
- verifying file checksum [34-6](#)

flow control

- configuring [5-8](#)

overview [5-1](#)
 forward delay timer [7-40](#)
 frame classification
 overview [14-3](#)
 frame distribution, EtherChannel [6-2](#)

G

GARP Multicast Registration Protocol
 See GMRP
 GARP timers
 setting [13-6, 15-13](#)
 GARP VLAN Registration Protocol
 See GVRP
 Gigabit EtherChannel
 example [6-14](#)
 See also EtherChannel; Fast EtherChannel
 Gigabit Ethernet
 checking connectivity [5-10](#)
 configuring flow control [5-8](#)
 configuring port negotiation [5-9](#)
 default configuration [5-6](#)
 flow control [5-1](#)
 port negotiation [5-3](#)
 port negotiation link states (table) [5-3](#)
 setting port names [5-7](#)
 setting port priority [5-7](#)
 GMRP
 clearing statistics [15-14](#)
 default configuration [15-8](#)
 disabling forward-all option [15-11](#)
 disabling globally [15-15](#)
 disabling per-port [15-10](#)
 enabling forward-all option [15-11](#)
 enabling globally [15-9](#)
 enabling per-port [15-9](#)
 overview [15-3](#)
 registration [15-11 to 15-12](#)
 setting timers [15-13](#)

software requirements [15-8](#)
 viewing statistics [15-14](#)
 group profiles
 IGMP multicast [15-17](#)
 GVRP
 clearing statistics [13-8](#)
 configuring registration [13-4](#)
 disabling [13-8](#)
 enabling [13-2](#)
 registration [13-5](#)
 setting timers [13-6](#)
 viewing statistics [13-7](#)

H

hello time
 timer [7-40](#)
 history
 switch CLI [2-6](#)

I

I-BPDU [7-14](#)
 ICMP
 IP traceroute [20-12](#)
 time-exceeded messages [20-12](#)
 using ping [20-9 to 20-10](#)
 ID and MAC addresses, bridge [7-12](#)
 IEEE 802.1Q
 See 802.1Q
 IEEE 802.1x
 See 802.1x authentication
 IGMP
 configuration guidelines [15-4](#)
 joining multicast groups [15-2](#)
 leaving multicast groups [15-2](#)
 overview [15-1](#)
 using traffic filtering [15-17](#)

CISCO Confidential - DRAFT

- IGMP filtering
 - software requirements [15-18](#)
- IGMP filter match-action
 - denying and verifying [15-20](#)
 - permitting and verifying [15-20](#)
- IGMP multicast filtering
 - disabling and verifying [15-19](#)
 - enabling and verifying [15-18](#)
- IGMP traffic filtering [15-17](#)
- images
 - See software images; system images
- in-band (sc0) interface
 - See sc0 interface
- inferior BPDUs, BackboneFast and [8-4](#)
- Inline power
 - modes [28-12](#)
- inline power
 - configuring on Cisco IP phones [28-11, 29-3](#)
- interfaces
 - me1 (out-of-band management) [3-4, 3-6](#)
 - sc0 (in-band) [3-4, 10-2](#)
 - sl0 (SLIP)) [3-8](#)
- Internal Spanning Tree
 - See IST [7-13](#)
- Internet Control Message Protocol
 - See ICMP
- Internet Group Management Protocol
 - See IGMP
- Inter-Switch Link
 - See ISL
- IP addresses
 - adding to IP permit list [18-2](#)
 - automatic assignment [3-2](#)
 - CIDR [27-9](#)
 - clearing from IP permit list [18-4](#)
 - creating aliases [27-7](#)
 - default gateway [3-6](#)
 - designating [2-8](#)
 - DHCP and [3-9](#)
 - me1 interface and [3-6](#)
 - RARP and [3-9](#)
 - sc0 interface and [3-5](#)
 - sl0 interface and [3-9](#)
 - static routes [27-9](#)
 - VLANs and [10-2](#)
- IP aliases
 - creating [27-7](#)
 - designating [2-8](#)
- IP multicast
 - CGMP and [15-3](#)
 - GMRP and [15-8](#)
 - group entries [15-15](#)
 - overview [15-1](#)
 - router ports and group entries [15-15](#)
 - See also multicast groups; multicast routers
- IP permit lists
 - adding addresses [18-2](#)
 - clearing entries [18-4](#)
 - default configuration [18-2](#)
 - disabling [18-4](#)
 - enabling [18-3](#)
 - overview [18-1](#)
- IP Phones
 - See Cisco IP Phones [29-2](#)
- IP phones
 - detecting an IP phone [28-14](#)
 - powering off phones [28-13](#)
 - power requirements [28-12](#)
 - removing a phone from the network [28-13](#)
 - wall powered phones [28-13](#)
- IP traceroutes
 - executing [20-12](#)
 - overview [20-12](#)
- ISL
 - mapping 802.1Q VLANs [10-10](#)
 - overview [11-1](#)
 - supported switches (table) [11-3](#)
- isolated ports

definition [10-15](#)

IST

MST regions [7-13](#)

ISTP [7-13](#)

K

Kerberos authentication

configuration guidelines [30-9](#)

copying SRVTAB files [30-33](#)

defining realm [30-31](#)

disabling credentials forwarding [30-35](#)

enabling [30-31](#)

enabling credentials forwarding [30-34](#)

overview [30-5](#)

servers, specifying [30-32](#)

terminology [30-5, 31-5](#)

keys

See RADIUS keys; TACACS+ keys

L

LACP

configuration parameters [6-17](#)

configuration procedures [6-18](#)

modes [6-16](#)

Layer 2 traceroute

utility [20-11](#)

leave processing, CGMP

disabling [15-7](#)

enabling [15-5](#)

limiting telnet attempts [30-9](#)

Link Aggregation Control Protocol

See LACP

listing all multicast filters [15-21](#)

listing port filter associations [15-22](#)

load balancing [7-13](#)

load sharing, trunking and [11-12](#)

local authentication

configuration guidelines [30-9](#)

default configuration [30-8, 30-49](#)

disabling [30-13](#)

enabling [30-11](#)

overview [30-2](#)

password recovery [30-14](#)

setting enable password [30-13](#)

local user authentication

deleting an account [30-15, 30-16](#)

disabling [30-16](#)

enabling [30-15](#)

overview [30-3](#)

setting passwords [30-15](#)

location, setting [27-3](#)

login

limiting attempts [30-2](#)

login authentication

enabling [30-9, 30-10](#)

overview [30-2](#)

login banner

clearing [27-5](#)

configuring [27-4](#)

displaying or suppressing the "Cisco Systems Console"
login banner [27-5](#)

overview [27-4](#)

login passwords

recovering lost [30-14](#)

setting [30-12](#)

login timer

changing [20-6](#)

loop guard

multiple spanning tree [7-14](#)

M

MAC addresses

allocating [7-12](#)

blocking [16-1](#)

CISCO Confidential - DRAFT

- blocking unicast flood packets [17-1](#)
- bridge identifiers [7-12](#)
- designating [2-8](#)
- disabling notification [16-6](#)
- enabling notification [16-6](#)
- port security and [16-1](#)
- setting notification history log size [16-6](#)
- setting notification interval [16-6](#)
- management interfaces
 - overview [3-1](#)
- mapping VLANs [10-10](#)
- match-action filtering [15-20](#)
- maximum aging time timers [7-40](#)
- me1 interface
 - assigning IP addresses [3-6](#)
 - configuring [3-6](#)
 - overview [3-1](#)
- message-of-the-day
 - See login banner
- metric values, switch TopN reports (table) [22-2](#)
- MIBs
 - Network Analysis Module and [25-2](#)
 - overview [24-5](#)
- MISTP
 - bridge ID priority [7-30, 7-46](#)
 - configuring an instance [7-30](#)
 - conflicts, MISTP VLAN [7-35](#)
 - default configuration [7-28](#)
 - enabling an instance [7-33](#)
 - mapping VLANs to [7-34](#)
 - MISTP-PVST+ [7-28](#)
 - port cost [7-31](#)
 - port instance cost [7-32](#)
 - port instance priority [7-33](#)
 - port priority [7-32](#)
 - unmapping VLANs from [7-35](#)
- modes, switch CLI [2-3](#)
- modules
 - checking status [20-1](#)
 - configuring Ethernet [4-1, 19-1](#)
 - configuring Fast Ethernet [4-1, 6-1, 19-1](#)
 - configuring Gigabit Ethernet [5-1](#)
 - configuring supervisor engine [3-1](#)
 - designating on command line [2-7](#)
 - Ethernet
 - configuring [6-1](#)
 - Fast Ethernet
 - configuring [6-1](#)
 - Gigabit Ethernet
 - configuring [6-1](#)
- modules, switch fabric accelerator [36-3](#)
- MOTD
 - See login banner
- MST [7-13](#)
 - boundary ports [7-18](#)
 - bridge ID priority [7-46](#)
 - configuration guidelines [7-17](#)
 - configuring [7-42](#)
 - configuring bridge ID priority [7-46](#)
 - edge ports [7-18](#)
 - enabling [7-42](#)
 - hop count [7-19](#)
 - instances [7-17](#)
 - interoperability [7-16](#)
 - interoperability with PVST+ [7-14](#)
 - link type [7-19](#)
 - mapping VLANs to [7-50](#)
 - master [7-18](#)
 - message age [7-19](#)
 - port cost [7-47](#)
 - port instance cost [7-48](#)
 - port instance priority [7-49](#)
 - port priority [7-48](#)
 - regions [7-17](#)
 - understanding [7-13](#)
- MSTP
 - M-record [7-14](#)
 - M-tree [7-14](#)

multicast

See IP multicast

multicast filter profiles

establishing and verifying [15-19](#)

removing [15-20](#)

multicast filters

listing all [15-21](#)

removing all [15-21](#)

multicast groups

CGMP and [15-3](#)

clearing [15-17](#)

configuring [15-6, 15-16](#)

GMRP and [15-8](#)

joining [15-2](#)

leaving [15-2](#)

multicast port filter associations

removing [15-22](#)

multicast routers

clearing ports [15-16](#)

specifying port for [15-15](#)

multiple forwarding paths [7-13](#)

Multiple Instance Spanning Tree Protocol

See MSTP

Multiple Spanning Tree

See MST [7-13](#)

N

names, assigning port [5-7](#)

names, setting port [4-3](#)

native VLANs

802.1Q and [11-4](#)

neighbor devices, displaying [21-5](#)

NetFlow Feature Card

See NFFC/NFFCII

network fault tolerance [7-13](#)

network management

configuring [25-1](#)

See also RMON; SNMP

Network Time Protocol

See NTP

NFFC/NFFC II

IGMP snooping and [15-4](#)

protocol filtering and [19-1](#)

NMS

SPAN, configuring [26-1](#)

nonvolatile random-access memory

See NVRAM

normal mode, switch CLI [2-3](#)

normal-range VLANs

See VLANs

NTP

clearing time zone [39-7](#)

configuring broadcast-client mode [39-2](#)

configuring client mode [39-3](#)

default configuration [39-2](#)

disabling [39-7](#)

disabling broadcast-client mode [39-8](#)

disabling client mode [39-8](#)

disabling daylight saving time adjustment [39-7](#)

overview [39-1](#)

NTP authentication

configuring [39-4](#)

enabling daylight saving time adjustment [39-5](#)

setting time zone [39-5](#)

NTP servers

clearing [39-7](#)

specifying [39-3](#)

NVRAM

ignoring content at boot [32-6](#)

setting configuration modes [34-2](#)

O

organization, document [xxiii](#)

out-of-band management interface

See me1 interface

CISCO Confidential - DRAFT

P

PAgP

- displaying statistics [6-12](#)
- overview [6-5](#)

passwords

- recovering lost [30-14](#)
- setting enable [30-13](#)

permit lists

- See IP permit lists

permitting and verifying [15-20](#)

permitting filter match-action [15-20](#)

physical restrictions [15-18](#)

ping

- executing [20-10](#)
- overview [20-9](#)
- testing connectivity [4-8, 5-10](#)

Port Aggregation Protocol

- See PAgP

port-based authentication

- authentication server
 - RADIUS server [31-2](#)
- device roles [31-2](#)
- EAPOL-start frame [31-3](#)
- EAP-request/identity frame [31-3](#)
- EAP-response/identity frame [31-3](#)
- encapsulation [31-2](#)
- initiation and message exchange [31-3](#)

ports

- authorization state and dot1x port-control command [31-4](#)
- authorized and unauthorized [31-4](#)

switch

- as proxy [31-2](#)
- RADIUS client [31-2](#)

port cost

- EtherChannel [6-8](#)
- PVST+ [7-23](#)

port debounce timer

- disabling [4-6](#)

- displaying [4-6](#)

- enabling [4-6](#)

PortFast

- configuring [8-8](#)
- multiple spanning tree [7-14](#)

PortFast BPDU guard

- configuring [8-13](#)
- disabling [8-14](#)

port filter associations

- assigning and listing [15-22](#)

port IP multicast filtering [15-19](#)

port names

- Ethernet [4-3](#)
- Fast Ethernet [4-3](#)
- Gigabit Ethernet [5-7](#)
- setting [4-3, 5-7](#)

port negotiation

- configuring [5-9](#)
- overview [5-3](#)

port priority

- Ethernet [4-4](#)
- Fast Ethernet [4-4](#)
- Gigabit Ethernet [5-7](#)

ports

- assigning to VLAN [10-9](#)
- checking capabilities [20-5](#)
- checking status [20-2](#)
- designating on command line [2-7](#)
- dynamic VLAN membership overview [12-1](#)
- private VLAN [10-15](#)
- reconfirming VMPS [12-9](#)
- setting the debounce timer [4-6](#)
- speed
 - 10/100 Fast Ethernet [4-4](#)

port security

- configuring [16-1 to 16-11](#)
- clearing MAC addresses [16-5](#)
- guidelines for [16-3](#)

CISCO Confidential - DRAFT

- MAC address notification [16-6](#)
 - monitoring MAC addresses [16-6](#)
 - specifying age time [16-5](#)
 - specifying secure MAC addresses [16-4](#)
 - specifying security violation action [16-8](#)
 - specifying shutdown time [16-8](#)
 - disabling [16-9](#)
 - enabling [16-3](#)
 - monitoring [16-10](#)
 - overview [16-1](#)
 - restricting MAC address traffic [16-9](#)
 - port VLAN cost
 - configuring for PVST+ [7-25](#)
 - setting EtherChannel [6-9](#)
 - port VLAN priority
 - configuring [7-25](#)
 - power, inline [28-11, 29-3](#)
 - power budget
 - setting [28-16](#)
 - power management
 - Catalyst 4500 series [28-1, 28-6](#)
 - Catalyst 4500 series power supplies [28-3](#)
 - combined mode [28-2](#)
 - configuring combined mode [28-3](#)
 - configuring redundant mode [28-2](#)
 - redundancy [28-6](#)
 - redundant mode [28-2](#)
 - voice [28-11](#)
 - power supplies
 - fixed [28-1](#)
 - variable [28-2](#)
 - priority
 - See port priority
 - private VLANs
 - configuration guidelines [10-16](#)
 - creating [10-17](#)
 - deleting community VLANs [10-21](#)
 - deleting isolated VLANs [10-21](#)
 - deleting mapping [10-21](#)
 - deleting primary VLANs [10-20](#)
 - hardware interactions [10-16](#)
 - isolated VLAN [10-15](#)
 - overview [10-15](#)
 - primary VLAN [10-15](#)
 - software interactions [10-16](#)
 - privileged mode, switch CLI [2-3](#)
 - promiscuous ports
 - communicating [10-15](#)
 - prompts
 - configuring [27-2](#)
 - overview [27-1](#)
 - protocol filtering
 - configuring [19-2](#)
 - default configuration [19-2](#)
 - overview [19-1](#)
 - protocol support [19-1](#)
 - pruning, VTP
 - See VTP pruning
 - PVST+
 - configuring bridge ID priority [7-21](#)
 - default configuration [7-21](#)
 - default port cost mode [7-24](#)
 - disabling [7-26](#)
 - port cost [7-23](#)
 - port priority [7-23](#)
 - port VLAN cost [7-25](#)
-
- ## Q
- QoS
 - CoS
 - mapping drop thresholds [14-6](#)
 - reverting to port default [14-5](#)
 - transmitting drop thresholds [14-3](#)
 - values [14-2](#)
 - default configuration [14-4](#)
 - disabling [14-7](#)
 - displaying information [14-7](#)

CISCO Confidential - DRAFT

- enabling [14-5](#)
- frame classification [14-3](#)
- labels [14-2](#)
- overview [14-1](#)
- reverting to defaults [14-7](#)
- traffic flow (figure) [14-2](#)
- transmit queue
 - overview [14-3](#)
- quality of service
 - See QoS

R

RADIUS

- configuration guidelines [30-49](#)
- overview [30-47, 30-48](#)

RADIUS accounting

- accounting events [30-47](#)
- creating accounting records [30-47](#)
- disabling [30-51](#)
- enabling [30-49](#)
- overview [30-46](#)
- sample configuration [30-52](#)
- specifying servers [30-47](#)
- suppressing accounting [30-48](#)
- updating the server [30-48](#)

RADIUS authentication

- configuration guidelines [30-9](#)
- default configuration [30-8, 30-49](#)
- disabling [30-29](#)
- enabling [30-23](#)
- overview [30-4](#)
- servers, specifying optional attributes [30-27](#)
- setting deadtime [30-27](#)
- setting retransmit count [30-26](#)
- setting timeout [30-25](#)
- using a RADIUS server for 802.1x VLAN assignment [31-6](#)

RADIUS keys

- clearing [30-29](#)
- specifying [30-24](#)

RADIUS servers

- clearing [30-28](#)
- specifying [30-23, 30-47](#)

rapid-PVST+

- configuring [7-26](#)
- overview [7-11](#)

rapid Spanning Tree Protocol

- See RSTP [7-14](#)

RARP

- sc0 interface and [3-9](#)
- using [3-9](#)

rcp

- downloading configuration files [35-6](#)
- uploading configuration files [35-7](#)

related documentation [xxv](#)

remote copy protocol

- See RCP

Remote Monitoring

- See RMON

Remote Switched Port Analyzer

- See RSPAN

removing all multicast filters [15-21](#)

removing multicast filter profiles [15-20](#)

removing multicast port filter associations [15-22](#)

reports

- IGMP filtering [15-17](#)

reports, system status [27-12](#)

reserved-range VLANs

- See VLANs

restrictions

- IGMP traffic filtering [15-18](#)

Reverse Address Resolution Protocol

- See RARP

RMON

- enabling [25-2](#)
- overview [25-1](#)
- supported MIB objects [25-2](#)

- viewing data [25-2](#)
 - ROM monitor
 - BOOT environment variables and [32-3](#)
 - boot process and [32-2](#)
 - CLI [2-9](#)
 - configuration register and [32-2](#)
 - root guard
 - disabling [7-39](#)
 - enabling [7-39](#)
 - multiple spanning tree [7-14](#)
 - root switch
 - configuring primary [7-36](#)
 - configuring secondary [7-37](#)
 - overview [7-36](#)
 - See also root guard
 - router, multicast
 - See multicast routers
 - RSPAN
 - configuration examples [26-13 to 26-17](#)
 - configuration guidelines [26-9](#)
 - configuring from CLI [26-10](#)
 - configuring multiple RSPAN sessions [26-15](#)
 - configuring single RSPAN session [26-14](#)
 - disabling [26-13](#)
 - hardware requirements [26-8](#)
 - overview [26-1](#)
 - session limits [26-4](#)
 - See also SPAN; VSPAN
 - RSTP
 - overview [7-14](#)
 - port roles [7-15](#)
 - port states [7-15](#)
 - running configuration
 - downloading via rcp [35-6](#)
 - configuring [3-5](#)
 - DHCP and [3-9](#)
 - overview [3-1, 3-4](#)
 - RARP and [3-9](#)
 - VLAN assignment [10-2](#)
 - secure ports
 - disabling unicast flood blocking [16-5](#)
 - enabling unicast flood blocking [16-5](#)
 - secure shell encryption
 - See SSH
 - security
 - configuring [18-1](#)
 - configuring passwords [30-13](#)
 - IP permit list [18-1](#)
 - set spantree portcost command [7-23, 7-47](#)
 - set spantree priority command [7-46](#)
 - show port mac-address command [20-4](#)
 - Simple Network Management Protocol
 - See SNMP
 - Single Spanning Tree
 - See SST [7-13, 7-14](#)
 - sl0 interface
 - configuring [3-8](#)
 - console port and [3-8](#)
 - overview [3-1](#)
 - SLIP interface
 - See sl0 interface
 - SNMP
 - benefits [24-11](#)
 - clearing IP addresses associated with access numbers [24-10](#)
 - clearing SNMP community strings [24-9](#)
 - configuring [24-6](#)
 - default configuration [24-6](#)
 - defining community strings [24-7](#)
 - ifindex persistence feature [24-4](#)
 - overview [24-5](#)
 - setting access numbers for hosts [24-9](#)
 - setting multiple SNMP community strings [24-8](#)
-
- S
- sc0 interface
 - assigning IP address [3-5](#)

CISCO Confidential - DRAFT

- supported RMON MIB objects [25-2](#)
- SNMPv3
 - configuring [24-14](#)
 - definitions [24-14](#)
 - overview [24-11](#)
- software images
 - downloading using rcp [33-6](#)
 - downloading using TFTP [33-2](#)
 - supervisor engine, description [1-3](#)
 - uploading to rcp server [33-8](#)
 - uploading to TFTP server [33-4](#)
- software restraints [15-18](#)
- SPAN
 - configuration guidelines [26-5](#)
 - configuring [26-6](#)
 - destination port [26-2](#)
 - disabling [26-8](#)
 - egress [26-3](#)
 - ingress [26-3](#)
 - NMS and [26-1](#)
 - overview [26-4](#)
 - session limits [26-4](#)
 - sessions [26-1](#)
 - source ports [26-2](#)
 - traffic [26-4](#)
- spanning tree
 - dummy MAC addresses and [8-4](#)
 - EtherChannel port costs [6-8](#)
 - EtherChannel port-VLAN costs [6-9](#)
- spanning tree BackboneFast convergence
 - See BackboneFast
- spanning tree PortFast
 - See PortFast
- Spanning Tree Protocol
 - See STP
- spanning tree UplinkFast
 - See UplinkFast
- speed
 - setting 10/100 Fast Ethernet port [4-4](#)
- SSH [20-7](#)
 - configuring [20-7](#)
- SST [7-13, 7-14](#)
 - interoperability [7-16](#)
- static route, configuring [27-9](#)
- status reports, system [27-12](#)
- STP
 - BPDUs and [7-2](#)
 - forward delay timer [7-40](#)
 - hello time [7-40](#)
 - MAC address allocation [7-12](#)
 - MAC address reduction
 - enabling [10-5](#)
 - maximum age timer [7-40](#)
 - overview [7-2](#)
 - PortFast, configuring [8-8](#)
 - port states [7-4](#)
 - See also MISTP; PVST+
- supervisor engine
 - configuring [3-1](#)
 - connecting through console port [2-2](#)
 - default configuration [3-5](#)
 - default gateways [3-6](#)
 - me1 interface [3-6](#)
 - sc0 interface [3-5](#)
 - sl0 interface [3-8](#)
 - software description [1-3](#)
 - software images overview [1-3](#)
 - startup configuration [32-1](#)
 - static routes [27-9](#)
 - uploading software images [33-5, 33-9](#)
- switch acceleration [36-1](#)
 - configuring [36-1, 36-2](#)
- switch CLI
 - accessing [2-2](#)
 - command aliases [2-7](#)
 - designating IP addresses [2-8](#)
 - designating IP aliases [2-8](#)
 - designating MAC addresses [2-8](#)

CISCO Confidential - DRAFT

- designating modules [2-7](#)
 - designating ports [2-7](#)
 - designating VLANs [2-7](#)
 - help [2-4](#)
 - history substitution [2-6](#)
 - modes [2-3](#)
 - operating [2-3](#)
 - Switched Port Analyzer
 - See SPAN
 - switch management interfaces
 - See me1 interface; sc0 interface; sl0 interface
 - switch TopN reports
 - background option [22-2](#)
 - foreground execution [22-2, 22-3](#)
 - metric values (table) [22-2](#)
 - overview [22-1](#)
 - running [22-3](#)
 - viewing [22-3](#)
 - syslog
 - configuring [37-4](#)
 - configuring daemon [37-7](#)
 - configuring servers [37-8](#)
 - default configuration [37-3](#)
 - displaying configuration [37-9](#)
 - displaying message log [37-10](#)
 - facilities (table) [37-2](#)
 - limiting the number of syslog messages [37-7](#)
 - message format [37-3, 37-4](#)
 - overview [37-1](#)
 - setting buffer size [37-6](#)
 - setting logging levels [37-6](#)
 - setting session settings [37-5](#)
 - severity levels (table) [37-3, 37-4](#)
 - syslog servers
 - configuring [37-8](#)
 - system clock, setting [27-4](#)
 - system contact, setting [27-3](#)
 - system images
 - downloading using rcp [33-6](#)
 - downloading using TFTP [33-2](#)
 - switch
 - specifying startup [32-1](#)
 - uploading [33-9](#)
 - uploading [33-5](#)
 - system location, setting [27-3](#)
 - system message logging
 - changing enable state timestamp [37-6](#)
 - configuring [37-4](#)
 - configuring daemon [37-7](#)
 - configuring syslog daemon [37-7](#)
 - default configuration [37-3](#)
 - displaying configuration [37-9](#)
 - displaying message log [37-10](#)
 - facilities (table) [37-2](#)
 - message format [37-3, 37-4](#)
 - overview [37-1](#)
 - setting buffer size [37-6](#)
 - setting logging levels [37-6](#)
 - setting session settings [37-5](#)
 - severity levels (table) [37-3, 37-4](#)
 - system name
 - clearing [27-3](#)
 - configuring [27-2](#)
 - overview [27-1](#)
 - system prompt
 - configuring [27-2](#)
 - overview [27-1](#)
 - system reset
 - scheduling [27-10](#)
 - system status report
 - generating [27-12](#)
-
- T
- TACACS+ accounting
 - accounting events [30-47](#)
 - configuration guidelines [30-49](#)
 - creating accounting records [30-47](#)

CISCO Confidential - DRAFT

- disabling [30-51](#)
- enabling [30-49](#)
- overview [30-46](#)
- sample configuration [30-52](#)
- suppressing accounting [30-48](#)
- updating the server [30-48](#)
- TACACS+ authentication
 - configuration guidelines [30-9](#)
 - default configuration [30-8](#)
 - disabling [30-22](#)
 - enabling [30-18](#)
 - login attempts allowed [30-20](#)
 - overview [30-3](#)
 - sample configuration [30-39](#)
 - timeout interval [30-19](#)
- TACACS+ authorization
 - authorization events [30-40](#)
 - command authorization [30-41](#)
 - configuration guidelines [30-42](#)
 - default configuration [30-42](#)
 - disabling [30-44](#)
 - enabling [30-42](#)
 - fallback options [30-40](#)
 - overview [30-40](#)
 - primary options [30-40](#)
 - sample configuration [30-45](#)
- TACACS+ keys
 - clearing [30-21](#)
 - specifying [30-19](#)
- Telnet
 - disconnecting user sessions [20-8](#)
 - executing [20-6](#)
 - limiting attempts [30-9](#)
 - monitoring user sessions [20-7](#)
 - system message logging settings [37-5](#)
- text file configuration mode
 - setting the configuration mode [34-2](#)
- TFTP
 - downloading software images [33-2](#)
 - uploading configuration files [35-4, 35-5](#)
 - uploading software images [33-5](#)
- time, setting [27-4](#)
- time-exceeded messages [20-12](#)
- timers
 - configuring forward delay [7-40](#)
 - configuring hello time [7-40](#)
 - configuring maximum aging time [7-40](#)
 - GARP [13-6, 15-13](#)
 - login [20-6](#)
- time zone
 - clearing [39-7](#)
 - setting [39-5](#)
- TopN reports
 - See switch TopN reports
- traceroute
 - See IP traceroute
- traceroute utility, Layer 2 [20-11](#)
- traffic filtering
 - IGMP [15-17](#)
- transmit queue overview [14-3](#)
- troubleshooting
 - dynamic port VLAN membership [12-11](#)
 - system message logging and [37-1](#)
 - VMPS [12-10](#)
- trunks
 - 802.1Q restrictions [11-4](#)
 - allowed VLANs [11-6](#)
 - autonegotiation [11-2](#)
 - configuring IEEE 802.1Q [11-5](#)
 - default configuration [11-5](#)
 - disabling [11-7](#)
 - disabling VLAN 1 [11-8](#)
 - encapsulation types
 - descriptions (table) [11-2](#)
 - switch support matrix (table) [11-3](#)
 - modes (table) [11-2](#)
 - overview [11-1](#)
 - possible configurations (table) [11-3](#)

sample configurations

Gigabit [11-9](#)load sharing [11-12](#)nonnegotiate [11-19](#)software images [33-4](#), [33-8](#)supervisor [33-9](#)

user sessions

disconnecting [20-8](#)monitoring [20-7](#)using IGMP traffic filtering [15-17](#)

U

UDLD

default configuration [23-2](#)disabling globally [23-4](#)disabling on ports [23-4](#)displaying configuration [23-6](#)enabling aggressive mode [23-5](#)enabling globally [23-3](#)enabling on ports [23-4](#)hardware requirements [23-2](#)overview [23-1](#)software requirements [23-2](#)specifying message interval [23-5](#)unauthorized ports with 802.1X [31-4](#)unclassified frames [14-3](#)

unicast flood blocking

configuring [17-1 to 17-3](#)blocking MAC addresses [17-1](#)guidelines for [17-2](#)disabling [17-3](#)disabling on a secure port [16-5](#)displaying [17-3](#)enabling [17-2](#)enabling on a secure port [16-5](#)

UniDirectional Link Detection

See UDLD

UplinkFast

configuring [8-14](#)dummy MAC addresses [8-4](#)multiple spanning tree [7-14](#)overview [8-3](#)

uploading

configuration files [35-4](#), [35-7](#)

Vverifying disabled IGMP multicast filtering [15-19](#)verifying enabled IGMP multicast filtering [15-18](#)verifying IGMP filter match-action [15-20](#)verifying multicast filter profiles [15-19](#)

virtual LANs

See VLANs

VLAN-based SPAN

See VSPAN

VLAN filtering

trunk [26-4](#)

VLAN Membership Policy Server

See VMPS

VLANs

allowed on trunk [11-6](#)assigning switch ports to [10-9](#)auxiliary [10-12](#)configuration guidelines [10-4](#)default configuration [10-4](#)deleting [10-11](#)designating on command line [2-7](#)Ethernet [10-5](#), [10-6](#)extended range [10-3](#), [10-4](#)in-band (sc0) interface assignment [10-2](#)IP subnetworks and [10-2](#)mapping 802.1Q to ISL [10-10](#)mapping conflicts [7-35](#)normal range [10-3](#)overview [10-1](#)protocol filtering and [19-1](#)reserved range [10-3](#)

CISCO Confidential - DRAFT

- sc0 (in-band) interface assignment [10-2](#)
- See also auxiliary VLANs; native VLANs; private VLANs
- VLANs, private
 - See private VLANs
- VLAN Trunking Protocol
 - See VTP
- VMPS
 - administering [12-8](#)
 - clear VMPS server entries [12-9](#)
 - clear VMPS statistics [12-9](#)
 - configuration guidelines [12-3](#)
 - configuring [12-4](#)
 - configuring dynamic port membership [12-7](#)
 - configuring port statistics [12-10](#)
 - configuring VMPS clients [12-7](#)
 - configuring VMPS servers [12-7](#)
 - database [12-4](#)
 - default configuration [12-2](#)
 - disabling [12-10](#)
 - downloading VMPS database [12-9](#)
 - error messages (table) [12-11](#)
 - example [12-11](#)
 - for auxiliary VLANs [12-13](#)
 - monitoring [12-8](#)
 - overview [12-1](#)
 - reconfirm dynamic port assignments [12-9](#)
 - reconfirming membership [12-9](#)
 - troubleshooting [12-10](#)
 - troubleshooting dynamic ports [12-11](#)
- VMPS clients
 - configuring [12-7](#)
- VMPS database
 - creating [12-4](#)
 - downloading [12-9](#)
 - example configuration file [12-5](#)
 - global settings [12-4](#)
 - MAC addresses [12-4](#)
 - port groups [12-5](#)
 - VLAN groups [12-5](#)
 - VLAN port policies [12-5](#)
- VMPS servers
 - configuring [12-7](#)
- voice interfaces
 - configuring [29-1](#)
- Voice over IP
 - configuring [29-2](#)
- voice-over-IP network
 - auxiliary VLANs, configuring [10-12](#)
 - software and hardware requirements [29-1](#)
- voice traffic [28-11, 29-3](#)
- VSPAN
 - overview [26-3](#)
- VTP
 - "off" mode, configuring [9-8](#)
 - configuration guidelines [9-5](#)
 - configuring client [9-6](#)
 - configuring server [9-6](#)
 - configuring transparent mode [9-7](#)
 - default configuration [9-5](#)
 - disabling [9-7, 9-8](#)
 - domains [9-2](#)
 - monitoring [9-11](#)
 - overview [9-1](#)
 - statistics [9-11](#)
- VTP advertisements [9-2](#)
- VTP modes
 - client [9-2](#)
 - off [9-2](#)
 - server [9-2](#)
 - transparent [9-2](#)
- VTP pruning
 - configuring [9-9](#)
 - disabling [9-10](#)
 - overview [9-3](#)
- VTP version 2
 - disabling [9-9](#)
 - enabling [9-8](#)

CISCO Confidential - DRAFT

overview [9-3](#)

W

write tech support command [27-12](#)