

CISCO SYSTEMS



Catalyst 2950 Desktop Switch Command Reference

Cisco IOS Release 12.1(11) EA1 and
Cisco IOS Release 12.1(11) YJ
November 2002

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-7814984=
Text Part Number: 78-14984-01



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, the Cisco Arrow logo, the Cisco Powered Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, Internet Quotient, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARTnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That's Possible, 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, IOS, IP/TV, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, 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. (0208R)

Catalyst 2950 Desktop Switch Command Reference

Copyright © 2001–2002, Cisco Systems, Inc.

All rights reserved.



CONTENTS

Preface **xiii**

Audience **xiii**

Purpose **xiii**

Organization **xiv**

Conventions **xiv**

Related Publications **xv**

Obtaining Documentation **xvi**

 World Wide Web **xvi**

 Documentation CD-ROM **xvi**

 Ordering Documentation **xvi**

 Documentation Feedback **xvi**

Obtaining Technical Assistance **xvii**

 Cisco.com **xvii**

 Technical Assistance Center **xvii**

 Cisco TAC Web Site **xviii**

 Cisco TAC Escalation Center **xviii**

CHAPTER 1

Using the Command-Line Interface **1-1**

 Type of Memory **1-1**

 Platforms **1-1**

 CLI Command Modes **1-2**

 User EXEC Mode **1-3**

 Privileged EXEC Mode **1-3**

 Global Configuration Mode **1-4**

 Controller Configuration Mode **1-4**

 Interface Configuration Mode **1-4**

 Sequence Configuration Mode **1-5**

 config-vlan Mode **1-5**

 VLAN Configuration Mode **1-6**

 Line Configuration Mode **1-6**

 Command Summary **1-6**

CHAPTER 2**Cisco IOS Commands**

aaa authentication dot1x	2-1
access-list (IP extended)	2-3
access-list (IP standard)	2-6
archive download-sw	2-8
archive tar	2-10
archive upload-sw	2-14
auto qos voip	2-16
boot boothlpr	2-19
boot buffersize	2-20
boot config-file	2-21
boot enable-break	2-22
boot helper	2-23
boot helper-config-file	2-24
boot manual	2-25
boot private-config-file	2-26
boot system	2-27
channel-group	2-28
class	2-30
class-map	2-32
clear controllers ethernet-controller	2-34
clear controllers lre	2-36
clear controllers lre link monitor	2-37
clear controllers lre log	2-38
clear interface	2-39
clear lre rate selection	2-40
clear mac address-table	2-41
clear pagp	2-43
clear port-security dynamic	2-44
clear port-security sticky	2-45
clear spanning-tree detected-protocols	2-47
clear vmps statistics	2-48
clear vtp counters	2-49
cluster commander-address	2-50
cluster discovery hop-count	2-52

cluster enable **2-53**
cluster holdtime **2-54**
cluster management-vlan **2-55**
cluster member **2-56**
cluster run **2-58**
cluster standby-group **2-59**
cluster timer **2-61**
controller LongReachEthernet **2-62**
cpe duplex **2-63**
cpe protected **2-65**
cpe shutdown **2-66**
cpe speed **2-68**
cpe type **2-70**
define interface-range **2-71**
delete **2-73**
deny (access-list configuration) **2-74**
deny (MAC access-list configuration) **2-77**
dot1x default **2-80**
dot1x max-req **2-81**
dot1x multiple-hosts **2-82**
dot1x port-control **2-83**
dot1x re-authenticate **2-85**
dot1x re-authentication **2-86**
dot1x timeout quiet-period **2-87**
dot1x timeout re-authperiod **2-88**
dot1x timeout tx-period **2-89**
duplex **2-90**
errdisable detect **2-92**
errdisable recovery **2-94**
flowcontrol **2-96**
hw-module slot module-slot # upgrade lre **2-100**
interface **2-103**
interface port-channel **2-105**
interface range **2-106**
ip access-group **2-108**

ip access-list	2-110
ip address	2-112
ip igmp snooping	2-113
ip igmp snooping vlan	2-114
ip igmp snooping vlan immediate-leave	2-115
ip igmp snooping vlan mrouter	2-116
ip igmp snooping vlan static	2-118
link monitor	2-120
link monitor logging	2-121
link monitor threshold rserr	2-122
link monitor threshold snr	2-124
local duplex	2-126
local speed	2-127
logging lre	2-128
lre profile	2-130
lre rate selection sequence	2-132
lre sequence	2-134
lre upgrade default family device-family binary	2-136
mac access-group	2-138
mac access-list extended	2-140
mac address-table aging-time	2-142
mac address-table notification	2-144
mac address-table static	2-146
margin	2-148
match	2-150
media-type	2-152
mls qos cos	2-153
mls qos map	2-155
mls qos trust	2-157
monitor session	2-160
mvr	2-163
mvr immediate	2-166
mvr type	2-168
mvr vlan group	2-170
pagp learn-method	2-172

pag port-priority **2-174**
permit (access-list configuration) **2-175**
permit (MAC access-list configuration) **2-178**
persistence **2-180**
police **2-181**
policy-map **2-183**
port-channel load-balance **2-185**
profile (interface mode) **2-187**
profile (sequence mode) **2-189**
rate selection **2-191**
rate selection profile lock **2-192**
rate selection sequence **2-193**
rcommand **2-195**
remote-span **2-197**
rmon collection stats **2-199**
service-policy **2-201**
set **2-202**
show access-lists **2-204**
show auto qos **2-206**
show boot **2-209**
show class-map **2-211**
show cluster **2-213**
show cluster candidates **2-215**
show cluster members **2-217**
show controllers ethernet-controller **2-219**
show controllers lre cpe identity **2-223**
show controllers lre cpe mfg **2-225**
show controllers lre cpe protected **2-228**
show controllers lre cpe version **2-230**
show controllers lre *interface-id* actual **2-231**
show controllers lre *interface-id* admin **2-234**
show controllers lre link monitor errors **2-236**
show controllers lre link monitor parameters **2-238**
show controllers lre link monitor statistics **2-241**
show controllers lre log **2-243**

show controllers lre log level	2-245
show controllers lre profile names	2-246
show controllers lre profile details	2-248
show controllers lre sequence	2-250
show controllers lre status	2-253
show controllers lre version	2-257
show dot1x	2-258
show env	2-262
show errdisable recovery	2-263
show etherchannel	2-265
show file	2-268
show interfaces	2-271
show interfaces counters	2-278
show ip access-lists	2-281
show ip igmp snooping	2-283
show ip igmp snooping mrouter	2-285
show lre upgrade binaries	2-287
show lre upgrade status	2-289
show lre upgrade version	2-295
show mac access-group	2-298
show mac address-table	2-300
show mac address-table multicast	2-303
show mac address-table notification	2-305
show mls masks	2-307
show mls qos interface	2-309
show mls qos maps	2-311
show monitor	2-313
show mvr	2-315
show mvr interface	2-317
show mvr members	2-319
show pagp	2-321
show policy-map	2-323
show port-security	2-325
show remote lre	2-328
show rps	2-330

show running-config vlan **2-332**
show spanning-tree **2-334**
show storm-control **2-339**
show system mtu **2-342**
show udld **2-343**
show version **2-346**
show wlan **2-347**
show vmps **2-351**
show vtp **2-353**
show wrr-queue bandwidth **2-358**
show wrr-queue cos-map **2-359**
shutdown **2-360**
shutdown wlan **2-361**
snmp-server enable traps **2-362**
snmp-server host **2-364**
snmp trap mac-notification **2-367**
spanning-tree backbonefast **2-369**
spanning-tree bpdufilter **2-370**
spanning-tree bpduguard **2-372**
spanning-tree cost **2-374**
spanning-tree extend system-id **2-376**
spanning-tree guard **2-378**
spanning-tree link-type **2-380**
spanning-tree loopguard default **2-381**
spanning-tree mode **2-383**
spanning-tree mst configuration **2-384**
spanning-tree mst cost **2-386**
spanning-tree mst forward-time **2-388**
spanning-tree mst hello-time **2-389**
spanning-tree mst max-age **2-391**
spanning-tree mst max-hops **2-393**
spanning-tree mst port-priority **2-395**
spanning-tree mst priority **2-397**
spanning-tree mst root **2-398**
spanning-tree port-priority **2-400**

spanning-tree portfast (global configuration)	2-402
spanning-tree portfast (interface configuration)	2-404
spanning-tree stack-port	2-406
spanning-tree uplinkfast	2-408
spanning-tree vlan	2-410
speed	2-413
storm-control	2-416
switchport access	2-418
switchport mode	2-420
switchport nonegotiate	2-422
switchport port-security	2-424
switchport port-security aging	2-428
switchport priority extend	2-430
switchport protected	2-431
switchport trunk	2-432
switchport voice vlan	2-435
system mtu	2-437
udld (global configuration)	2-439
udld (interface configuration)	2-441
udld reset	2-443
upgrade binary	2-444
upgrade preserve	2-445
vlan (global configuration)	2-446
vlan (VLAN configuration)	2-452
vlan database	2-458
vmpls reconfirm (global configuration)	2-461
vmpls reconfirm (privileged EXEC)	2-462
vmpls retry	2-463
vmpls server	2-464
vtp (global configuration)	2-466
vtp (privileged EXEC)	2-470
vtp (VLAN configuration)	2-472
wrr-queue bandwidth	2-476
wrr-queue cos-map	2-477

APPENDIX A**Debug Commands A-1**

- debug dot1x A-2
- debug etherchannel A-3
- debug lre A-4
- debug pagp A-5
- debug pm A-6
- debug spanning-tree A-8
- debug spanning-tree backbonefast A-10
- debug spanning-tree bpdu A-11
- debug spanning-tree bpdu-opt A-12
- debug spanning-tree mstp A-13
- debug spanning-tree switch A-15
- debug spanning-tree uplinkfast A-17
- debug sw-vlan A-18
- debug sw-vlan ifs A-20
- debug sw-vlan notification A-21
- debug sw-vlan vtp A-22
- debug udld A-24

APPENDIX B**Boot Loader Commands B-1**

- boot B-2
- cat B-3
- copy B-6
- delete B-7
- dir B-8
- flash_init B-10
- format B-11
- fsck B-12
- help B-13
- load_helper B-14
- memory B-15
- mkdir B-17
- more B-18
- rename B-19
- reset B-20

rmdir	B-21
set	B-22
type	B-25
unset	B-26
version	B-28

INDEX



Preface

Audience

This guide is for the networking professional using the Cisco IOS command-line interface (CLI) to manage the Catalyst 2950 switch, hereafter referred to as *the switch*. Before using this guide, you should have experience working with the Cisco IOS and be familiar with the concepts and terminology of Ethernet and local area networking.

Purpose

The Catalyst 2950 switch is supported by either the standard software image (SI) or the enhanced software image (EI). The enhanced software image provides a richer set of features, including access control lists (ACLs), enhanced quality of service (QoS) features, the Secure Shell (SSH) Protocol, extended-range VLANs, the IEEE 802.1W Rapid Spanning Tree Protocol (STP), and the IEEE 802.1S Multiple STP.



Note

This guide describes the features for all Catalyst 2950 switches, including the Catalyst 2950 Long-Reach Ethernet (LRE) switches. Cisco IOS Release 12.1(11)EA1 is *not* for the LRE switches. Do not install Release 12.1(11)EA1 on the Catalyst 2950 LRE switches.

Release 12.1(11)YJ is for the Catalyst 2950 LRE switches only. Do not install Release 12.1(11)YJ on non-LRE switches.

The enhanced software image supports these switches:

- Catalyst 2950C-24
- Catalyst 2950G-12-EI
- Catalyst 2950G-24-EI
- Catalyst 2950G-24-EI-DC
- Catalyst 2950G-48-EI
- Catalyst 2950T-24
- Catalyst 2950ST-8-LRE
- Catalyst 2950ST-24-LRE

The standard software image supports these switches:

- Catalyst 2950-12
- Catalyst 2950-24
- Catalyst 2950SX-24

This guide provides the information you need about the CLI commands that have been created or changed for use with the Catalyst 2950 family of switches. For information about the standard IOS Release 12.1 commands, refer to the IOS documentation set available from the Cisco.com home page by selecting **Service and Support > Technical Documents**. On the Cisco Product Documentation home page, select **Release 12.1** from the Cisco IOS Software drop-down list.

This guide does not provide procedures for configuring your switch. For detailed configuration procedures, refer to the *Catalyst 2950 Desktop Switch Software Configuration Guide* for this release.

This guide does not describe system messages you might encounter. For more information, refer to the *Catalyst 2950 Desktop Switch System Message Guide* for this release.

Organization

This guide is organized into these chapters:

[Chapter 1, “Using the Command-Line Interface,”](#) describes how to access the command modes and use the switch CLI to configure software features. It also lists the commands that have the same function but different syntax in software releases earlier than Release 12.1(6)EA2 and in Release 12.1(6)EA2 or later.

[Chapter 2, “Cisco IOS Commands,”](#) describes in alphabetical order the IOS commands that you use to configure and monitor your switch.

[Appendix A, “Debug Commands,”](#) describes the **debug** privileged EXEC commands. Debug commands are helpful in diagnosing and resolving internetworking problems.

Conventions

This guide uses these conventions to convey instructions and information:

Command descriptions use these conventions:

- Commands and keywords are in **boldface** text.
- Arguments for which you supply values are in *italic*.
- Square brackets ([]) mean optional elements.
- Braces ({ }) group required choices, and vertical bars (|) separate the alternative elements.
- Braces and vertical bars within square brackets ({{ | }}) mean a required choice within an optional element.

Interactive examples use these conventions:

- Terminal sessions and system displays are in **screen** font.
- Information you enter is in **boldface screen** font.
- Nonprinting characters, such as passwords or tabs, are in angle brackets (< >).

Notes, cautions, and tips use these conventions and symbols:

**Note**

Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in this manual.

**Caution**

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

**Timesaver**

Means the following *will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information.

Related Publications

These documents provide complete information about the switch and are available from this URL:

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat2950/index.htm>

You can order printed copies of documents with a DOC-xxxxxx= number from the Cisco.com sites and from the telephone numbers listed in the “[Obtaining Documentation](#)” section on page xvi.

**Note**

Switch requirements and procedures for initial configurations and software upgrades tend to change and therefore appear only in the release notes. Before installing, configuring, or upgrading the switch, refer to the release notes on Cisco.com for the latest information.

- *Release Notes for the Catalyst 2950 Switches*, Cisco Release 12.1(11)EA1 (not orderable but is available on Cisco.com)
- *Release Notes for the Catalyst 2950 LRE Switches*, Cisco Release 12.1(11) YJ (not orderable but is available on Cisco.com)

**Note**

The *Release Notes for the Catalyst 2950 Switches* is for switches that are *not* LRE switches. For LRE switches, refer to the *Release Notes for the Catalyst 2950 LRE Switches*.

- *Catalyst 2950 Desktop Switch Software Configuration Guide* (order number DOC-7811380=)
- *Catalyst 2950 Desktop Switch Command Reference* (order number DOC-7811381=)
- *Catalyst 2950 Desktop Switch System Message Guide* (order number DOC-7814233=)
- *Catalyst 2950 Desktop Switch Hardware Installation Guide* (order number DOC-7811157=)
- *Catalyst GigaStack Gigabit Interface Converter Hardware Installation Guide* (order number DOC-786460=)
- Cluster Management Suite (CMS) online help (available only from the switch CMS software)
- *CWDM Passive Optical System Installation Note* (not orderable but is available on Cisco.com)
- *1000BASE-T Gigabit Interface Converter Installation Notes* (not orderable but is available on Cisco.com)

Obtaining Documentation

These sections explain how to obtain documentation from Cisco Systems.

World Wide Web

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

<http://www.cisco.com>

Translated documentation is available at 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 is 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.

Ordering Documentation

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/cgi-bin/order/order_root.pl
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:
<http://www.cisco.com/go/subscription>
- 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. In the Cisco Documentation home page, click the **Fax** or **Email** option in the “Leave Feedback” section at the bottom 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: Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

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

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that 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

If you want to obtain customized information and service, you can self-register on Cisco.com. To access Cisco.com, go to this URL:

<http://www.cisco.com>

Technical Assistance Center

The Cisco Technical Assistance Center (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 Web Site and the Cisco TAC Escalation Center.

Cisco TAC inquiries are categorized according to the urgency of the issue:

- 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.

The Cisco TAC resource that you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

You can use the Cisco TAC Web Site 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 Web Site, 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 Web Site. The Cisco TAC Web Site requires 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://www.cisco.com/register/>

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

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

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC Web Site.

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.



CHAPTER

1

Using the Command-Line Interface

The Catalyst 2950 switches are supported by Cisco IOS software. This chapter describes how to use the switch command-line interface (CLI) to configure the software features.

For a complete description of the commands that support these features, see [Chapter 2, “Cisco IOS Commands.”](#) For more information on Cisco IOS Release 12.1, refer to the Cisco IOS Release 12.1 Command Summary.

For task-oriented configuration steps, refer to the *Catalyst 2950 Desktop Switch Software Configuration Guide* for this release.

The switches are preconfigured and begin forwarding packets as soon as they are attached to compatible devices.

By default, all ports belong to virtual LAN (VLAN) 1. Access to the switch itself is also through VLAN 1, which is the default management VLAN. The management VLAN is configurable. You manage the switch by using Telnet, Secure Shell (SSH) Protocol, web-based management, and Simple Network Management Protocol (SNMP) through devices connected to ports assigned to the management VLAN.

Type of Memory

The switch Flash memory stores the Cisco IOS software image, the startup and private configuration files, and helper files.

Platforms

This IOS release runs on a variety of switches. For a complete list, refer to the *Release Notes for the Catalyst 2950 Switches* or the *Release Notes for the Catalyst 2950 LRE Switches*.



Note

This guide describes the features for all Catalyst 2950 switches, including the Catalyst 2950 Long-Reach Ethernet (LRE) switches. Cisco IOS Release 12.1(11)EA1 is *not* for the LRE switches. Do not install Release 12.1(11)EA1 on the Catalyst 2950 LRE switches.

Release 12.1(11)YJ is for the Catalyst 2950 LRE switches only. Do not install Release 12.1(11)YJ on non-LRE switches.

CLI Command Modes

This section describes the CLI command mode structure. Command modes support specific Cisco IOS commands. For example, the **interface type_number** command works only when entered in global configuration mode. These are the main command modes:

- User EXEC
- Privileged EXEC
- Global configuration
- Controller configuration
- Interface configuration
- Sequence configuration
- Config-vlan
- VLAN configuration
- Line configuration

Table 1-1 lists the command modes, how to access each mode, the prompt you see in that mode, and how to exit that mode. The prompts listed assume the default name *Switch*.

Table 1-1 Command Modes Summary

Command Mode	Access Method	Prompt	Exit or Access Next Mode
User EXEC	This is the first level of access. (For the switch) Change terminal settings, perform basic tasks, and list system information.	Switch>	Enter the logout command to exit from the switch. To enter privileged EXEC mode, enter the enable command.
Privileged EXEC	From user EXEC mode, enter the enable command.	Switch#	To exit to user EXEC mode, enter the disable command. To enter global configuration mode, enter the configure command.
Global configuration	From privileged EXEC mode, enter the configure command.	Switch(config)#	To exit to privileged EXEC mode, enter the exit or end command, or press Ctrl-Z . To enter interface configuration mode, enter the interface command.
Controller configuration	From the global configuration mode, enter the controller longreachethernet command (with a specific interface).	Switch(config-controller)#	To exit to global configuration mode, enter exit . To exit to privileged EXEC mode, enter Ctrl-Z or end .
Interface configuration	From the global configuration mode, enter the interface command (with a specific interface).	Switch(config-if)#	To exit to global configuration mode, enter exit . To exit to privileged EXEC mode, enter Ctrl-Z or end .

Table 1-1 Command Modes Summary (continued)

Command Mode	Access Method	Prompt	Exit or Access Next Mode
Sequence configuration	From the global configuration mode, specify the sequence by entering the lre sequence command (with a specific interface).	Switch(config-seq)#	To exit to global configuration mode, enter exit . To exit to privileged EXEC mode, enter Ctrl-Z or end .
Config-vlan	From the global configuration mode, enter the vlan vlan-id command.	Switch(config-vlan)#	To exit to global configuration mode, enter the exit command. To return to privileged EXEC mode, enter the end command, or press Ctrl-Z .
VLAN configuration	From privileged EXEC mode, enter the vlan database command.	Switch(vlan)#	To exit to privileged EXEC mode, enter the exit command.
Line configuration	From global configuration mode, specify a line by entering the line command.	Switch(config-line)#	To exit to global configuration mode, enter the exit command. To return to privileged EXEC mode, enter the end command, or press Ctrl-Z .

User EXEC Mode

After you access the device, you are automatically in user EXEC command mode. The EXEC commands available at the user level are a subset of those available at the privileged level. In general, use the user EXEC commands to change terminal settings temporarily, to perform basic tests, and to list system information.

The supported commands can vary depending on the version of IOS software in use. To view a comprehensive list of commands, enter a question mark (?) at the prompt.

```
Switch> ?
```

Privileged EXEC Mode

Because many of the privileged commands configure operating parameters, privileged access should be password-protected to prevent unauthorized use. The privileged command set includes those commands contained in user EXEC mode, as well as the **configure** command through which you access the remaining command modes.

If your system administrator has set a password, you are prompted to enter it before being granted access to privileged EXEC mode. The password does not appear on the screen and is case sensitive.

The privileged EXEC mode prompt is the device name followed by the pound sign (#).

```
Switch#
```

Enter the **enable** command to access privileged EXEC mode:

```
Switch> enable
Switch#
```

The supported commands can vary depending on the version of IOS software in use. To view a comprehensive list of commands, enter a question mark (?) at the prompt.

```
Switch# ?
```

To return to user EXEC mode, enter the **disable** command.

Global Configuration Mode

Global configuration commands apply to features that affect the device as a whole. Use the **configure** privileged EXEC command to enter global configuration mode. The default is to enter commands from the management console.

When you enter the **configure** command, a message prompts you for the source of the configuration commands:

```
Switch# configure
Configuring from terminal, memory, or network [terminal]?
```

You can specify either the terminal or nonvolatile RAM (NVRAM) as the source of configuration commands.

This example shows you how to access global configuration mode:

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

The supported commands can vary depending on the version of IOS software in use. To view a comprehensive list of commands, enter a question mark (?) at the prompt.

```
Switch(config)# ?
```

To exit global configuration command mode and to return to privileged EXEC mode, enter the **end** or **exit** command, or press **Ctrl-Z**.

Controller Configuration Mode

Controller configuration commands configure LRE switches for firmware updates, but are seldom used. The default behavior for upgrading firmware is sufficient for most operations.

Controller configuration commands always follow a global configuration command, which defines the interface type.

Use the **controller longreachethernet interface-id** command to access controller configuration mode. The new prompt shows controller configuration mode.

```
Switch(config-controller)#
```

To exit controller configuration mode and to return to global configuration mode, enter the **exit** command. To exit controller configuration mode and to return to privileged EXEC mode, enter the **end** command, or press **Ctrl-Z**.

Interface Configuration Mode

Interface configuration commands modify the operation of the interface. Interface configuration commands always follow a global configuration command, which defines the interface type.

Use the **interface type_number.subif** command to access interface configuration mode. The new prompt shows interface configuration mode.

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

The supported commands can vary depending on the version of IOS software in use. To view a comprehensive list of commands, enter a question mark (?) at the prompt.

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

To exit interface configuration mode and to return to global configuration mode, enter the **exit** command. To exit interface configuration mode and to return to privileged EXEC mode, enter the **end** command, or press **Ctrl-Z**.

Sequence Configuration Mode

Sequence configuration commands apply only to LRE interfaces. Use this command to create a sequence or to add profiles to an existing sequence. Sequence configuration commands always follow a global configuration command, which defines the interface.

Use the **lre sequence sequence-name** command to access sequence configuration mode. The new prompt shows sequence configuration mode.

```
Switch(config-seq)#
```

To exit sequence configuration mode and to return to global configuration mode, enter the **exit** command. To exit sequence configuration mode and to return to privileged EXEC mode, enter the **end** command, or press **Ctrl-Z**.

config-vlan Mode

Use this mode to configure normal-range VLANs (VLAN IDs 1 to 1005) or, when VTP mode is transparent, to configure extended-range VLANs (VLAN IDs 1006 to 4094) when the enhanced software image is installed. When VTP mode is transparent, the VLAN and VTP configuration is saved in the running configuration file, and you can save it to the switch startup configuration file by using the **copy running-config startup-config** privileged EXEC command. The configurations of VLAN IDs 1 to 1005 are saved in the VLAN database if VTP is in transparent or server mode. The extended-range VLAN configurations are not saved in the VLAN database.

Enter the **vlan vlan-id** global configuration command to access config-vlan mode:

```
Switch(config)# vlan 2000
Switch(config-vlan)#
```

The supported keywords can vary but are similar to the commands available in VLAN configuration mode. To view a comprehensive list of commands, enter a question mark (?) at the prompt.

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

For extended-range VLANs, all characteristics except MTU size must remain at the default setting.

To return to global configuration mode, enter **exit**; to return to privileged EXEC mode, enter **end**. All commands except **shutdown** take effect when you exit config-vlan mode.

VLAN Configuration Mode

You can use the VLAN configuration commands to create or modify VLAN parameters for VLANs 1 to 1005. Enter the **vlan database** privileged EXEC command to access VLAN configuration mode:

```
Switch# vlan database
Switch(vlan)#
```

The supported commands can vary depending on the version of IOS software in use. To view a comprehensive list of commands, enter a question mark (?) at the prompt.

```
Switch(vlan)# ?
```

To return to privileged EXEC mode, enter the **abort** command to abandon the proposed database. Otherwise, enter **exit** to implement the proposed new VLAN database and to return to privileged EXEC mode.

Line Configuration Mode

Line configuration commands modify the operation of a terminal line. Line configuration commands always follow a line command, which defines a line number. Use these commands to change terminal parameter settings line-by-line or for a range of lines.

Use the **line vty line_number [ending_line_number]** command to enter line configuration mode. The new prompt indicates line configuration mode.

This example shows how to enter line configuration mode for virtual terminal line 7:

```
Switch(config)# line vty 0 7
```

The supported commands can vary depending on the version of IOS software in use. To view a comprehensive list of commands, enter a question mark (?) at the prompt.

```
Switch(config-line)# ?
```

To exit line configuration mode and to return to global configuration mode, use the **exit** command. To exit line configuration mode and to return to privileged EXEC mode, enter the **end** command, or press **Ctrl-Z**.

Command Summary

Table 1-2 lists and describes commands that have the same function but different syntax in software releases earlier than Release 12.1(6)EA2 and in Release 12.1(6)EA2 or later. It lists the commands supported in releases earlier than Release 12.1(6)EA2, the equivalent commands in Release 12.1(6)EA2 or later, and command descriptions.

If you are running Release 12.1(6)EA2 or later, the switch supports the commands in the left column of **Table 1-2** only if they are in a saved configuration file. When you save the switch configuration after modifying it, the commands in **Table 1-2** are replaced by equivalent commands supported in Release 12.1(6)EA2 or later.

For information about commands listed in the left column of **Table 1-2**, refer to the *Catalyst 2950 Desktop Switch Command Reference, Cisco IOS Release 12.0(5.2)WC(1)* (April 2001). You can access this document at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat2950/2950_wc/index.htm

Table 1-2 Command Comparison

Command in IOS releases earlier than Release 12.1(6)EA2	Command in Release 12.1(6)EA2 or later	Description
mac-address-table secure	switchport port-security mac-address	Adds secure addresses to the MAC address table.
no negotiation auto	speed nonegotiate	Disables autonegotiation on 1000BASE-X, -LX, and -ZX Gigabit Interface Converter (GBIC) ports.
port group	channel-group	Assigns a port to a Fast EtherChannel or Gigabit EtherChannel port group.
port monitor	monitor session	Enables Switch Port Analyzer (SPAN) port monitoring on a port.
port protected	switchport protected	Isolates Layer 2 unicast, multicast, and broadcast traffic from other protected ports on the same switch.
port security	switchport port-security	Enables port security on a port and restricts the use of the port to a user-defined group of stations.
port security action	switchport port-security violation	Specifies the action to take when an address violation occurs on a secure port.
port security max-mac-count	switchport port-security maximum	Specifies the maximum number of secure addresses supported by a secure port.
port storm-control	storm-control	Enables unicast, multicast, or broadcast storm control on a port, and specifies storm-control parameters on a port.
show mac-address-table secure	show port-security	Displays the port security settings for an interface and the secure addresses in the MAC address table.
show port group	show etherchannel	Displays EtherChannel information for a channel.
show port monitor	show monitor	Displays SPAN session information.
show port protected	show interfaces switchport	Displays the port protection settings of a port.
show port security	show port-security	Displays the port security settings defined for a port.
show port storm-control	show storm-control	Displays the packet-storm control information.
spanning-tree rootguard	spanning-tree guard	Enables the root guard feature for all VLANs associated with a port.

Table 1-2 Command Comparison (continued)

Command in IOS releases earlier than Release 12.1(6)EA2	Command in Release 12.1(6)EA2 or later	Description
switchport priority	mls qos cos	Defines the default class of service (CoS) value of a port.
switchport priority override	mls qos cos override	Assigns the default CoS value to all incoming packets on a port.

Table 1-3 lists and describes the commands that are not supported in Release 12.1(6)EA2 or later. These commands are supported only in software releases earlier than Release 12.1(6)EA2. If you are running Release 12.1(6)EA2 or later, the switch supports the commands listed in **Table 1-3** only if they are in a saved configuration file.

Table 1-3 Commands Not Supported in Release 12.1(6)EA2 or Later

Command	Description
clear ip address	Deletes an IP address for a switch without disabling the IP processing.
clear mac-address-table static	Deletes static entries from the MAC address table.
management	Shuts down the current management VLAN interface and enables the new management VLAN interface.
show mac-address-table self	Displays the addresses added by the switch itself to the MAC address table.
spanning-tree protocol	Specifies the Spanning Tree Protocol (STP) to be used for specified spanning-tree instances. In Release 12.1(6)EA2 or later, the switch supports only IEEE Ethernet STP.

For detailed command syntax and descriptions, see [Chapter 2, “Cisco IOS Commands.”](#) For task-oriented configuration steps, refer to the software configuration guide for this release.



Cisco IOS Commands

aaa authentication dot1x

Use the **aaa authentication dot1x** global configuration command to specify one or more authentication, authorization, and accounting (AAA) methods for use on interfaces running IEEE 802.1X. Use the **no** form of this command to disable authentication.

aaa authentication dot1x {default} method1 [method2...]

no aaa authentication dot1x {default} method1 [method2...]

Syntax Description	default Use the listed authentication methods that follow this argument as the default list of methods when a user logs in.	
method1 [method2...]	At least one of these keywords: <ul style="list-style-type: none">• enable—Use the enable password for authentication.• group radius—Use the list of all Remote Authentication Dial-In User Service (RADIUS) servers for authentication.• line—Use the line password for authentication.• local—Use the local username database for authentication.• local-case—Use the case-sensitive local username database for authentication.• none—Use no authentication. The client is automatically authenticated by the switch without using the information supplied by the client.	
Defaults	No authentication is performed.	
Command Modes	Global configuration	
Command History	Release	Modification
	12.1(6)EA2	This command was introduced.

```
aaa authentication dot1x
```

Usage Guidelines

The *method* argument identifies the list of methods that the authentication algorithm tries in the given sequence to validate the password provided by the client. The only method that is truly 802.1X-compliant is the **group radius** method, in which the client data is validated against a RADIUS authentication server. The remaining methods enable AAA to authenticate the client by using locally configured data. For example, the **local** and **local-case** methods use the username and password that are saved in the IOS configuration file. The **enable** and **line** methods use the **enable** and **line** passwords for authentication.

If you specify **group radius**, you must configure the RADIUS server by entering the **radius-server host** global configuration command.

If you are not using a RADIUS server, you can use the **local** or **local-case** methods, which access the local username database to perform authentication. By specifying the **enable** or **line** methods, you can supply the clients with a password to provide access to the switch.

Use the **show running-config** privileged EXEC command to display the configured lists of authentication methods.

Examples

This example shows how to enable AAA and how to create an authentication list for 802.1X. This authentication first tries to contact a RADIUS server. If this action returns an error, the user is allowed access with no authentication.

```
Switch(config)# aaa new model
Switch(config)# aaa authentication dot1x default group radius none
```

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

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model. For syntax information, refer to Cisco IOS Security Command Reference for Release 12.1 > Authentication, Authorization, and Accounting > Authentication Commands .
show running-config	Displays the configuration information running on the switch. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 > Cisco IOS File Management Commands > Configuration File Commands .

access-list (IP extended)

Use the extended version of the **access-list** global configuration command to configure an extended IP access control list (ACL). Use the **no** form of the command to remove an extended IP ACL.

```
access-list access-list-number {deny | permit | remark} protocol {source source-wildcard |
    host source | any} [operator port] {destination destination-wildcard | host destination | any}
    [operator port] [dscp dscp-value] [time-range time-range-name]

no access-list access-list-number
```

This command is available on physical interfaces only if your switch is running the enhanced software image (EI).

Syntax Description	
<i>access-list-number</i>	Number of an ACL, from 100 to 199 or from 2000 to 2699.
<i>protocol</i>	Name of an IP protocol. <i>protocol</i> can be ip , tcp , or udp .
deny	Deny access if conditions are matched.
permit	Permit access if conditions are matched.
remark	ACL entry comment up to 100 characters.
<i>source source-wildcard host source any</i>	Define a source IP address and wildcard. The <i>source</i> is the source address of the network or host from which the packet is being sent, specified in one of these ways: <ul style="list-style-type: none"> The 32-bit quantity in dotted-decimal format. The <i>source-wildcard</i> applies wildcard bits to the source. The keyword host, followed by the 32-bit quantity in dotted-decimal format, as an abbreviation for <i>source</i> and <i>source-wildcard</i> of <i>source</i> 0.0.0.0. The keyword any as an abbreviation for <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255. You do not need to enter a source-wildcard.
<i>destination destination-wildcard host destination any</i>	Define a destination IP address and wildcard. The <i>destination</i> is the destination address of the network or host to which the packet is being sent, specified in one of these ways: <ul style="list-style-type: none"> The 32-bit quantity in dotted-decimal format. The <i>destination-wildcard</i> applies wildcard bits to the destination. The keyword host, followed by the 32-bit quantity in dotted-decimal format, as an abbreviation for <i>destination</i> and <i>destination-wildcard</i> of <i>destination</i> 0.0.0.0. The keyword any as an abbreviation for <i>destination</i> and <i>destination-wildcard</i> of 0.0.0.0 255.255.255.255. You do not need to enter a destination-wildcard.

access-list (IP extended)

<i>operator port</i>	(Optional) Define a source or destination port. The <i>operator</i> can be only eq (equal). If <i>operator</i> is after the source IP address and wildcard, conditions match when the source port matches the defined port. If <i>operator</i> is after the destination IP address and wildcard, conditions match when the destination port matches the defined port. The <i>port</i> is a decimal number or name of a Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) port. The number can be from 0 to 65535. Use TCP port names only for TCP traffic. Use UDP port names only for UDP traffic.
dscp <i>dscp-value</i>	(Optional) Define a Differentiated Services Code Point (DSCP) value to classify traffic. For the <i>dscp-value</i> , enter any of the 13 supported DSCP values (0, 8, 10, 16, 18, 24, 26, 32, 34, 40, 46, 48, and 56), or use the question mark (?) to see a list of available values.
time-range <i>time-range-name</i>	(Optional) For the time-range keyword, enter a meaningful name to identify the time range. For a more detailed explanation of this keyword, refer to the software configuration guide.

Defaults

The default extended ACL is always terminated by an implicit deny statement for all packets.

Command Modes

Global configuration

Command History

Release	Modification
12.1(6)EA2	This command was introduced.

Usage Guidelines

Plan your access conditions carefully. The ACL is always terminated by an implicit deny statement for all packets.

You can use ACLs to control virtual terminal line access by controlling the transmission of packets on an interface.

Extended ACLs support only the TCP and UDP protocols.

Use the **show ip access-lists** command to display the contents of IP ACLs.

Use the **show access-lists** command to display the contents of all ACLs.



Note For more information about configuring IP ACLs, refer to the “Configuring Network Security with ACLs” chapter in the *Catalyst 2950 Desktop Switch Software Configuration Guide* for this release.

Examples

This example shows how to configure an extended IP ACL that allows only TCP traffic to the destination IP address 128.88.1.2 with a TCP port number of 25 and how to apply it to an interface:

```
Switch(config)# access-list 102 permit tcp any host 128.88.1.2 eq 25
Switch(config)# interface fastethernet0/8
Switch(config-if)# ip access-group 102 in
```

This is an example of an extended ACL that allows TCP traffic only from two specified networks. The wildcard bits apply to the host portions of the network addresses. Any host with a source address that does not match the ACL statements is denied.

```
access-list 104 permit tcp 192.5.0.0 0.0.255.255 any
access-list 104 permit tcp 128.88.0.0 0.0.255.255 any
```



In these examples, all other IP access is implicitly denied.

You can verify your settings by entering the **show ip access-lists** or **show access-lists** privileged EXEC command.

Related Commands

Command	Description
access-list (IP standard)	Configures a standard IP ACL.
ip access-group	Controls access to an interface.
show access-lists	Displays ACLs configured on the switch.
show ip access-lists	Displays IP ACLs configured on the switch.

access-list (IP standard)

access-list (IP standard)

Use the standard version of the **access-list** global configuration command to configure a standard IP access control list (ACL). Use the **no** form of the command to remove a standard IP ACL.

```
access-list access-list-number {deny | permit | remark} {source source-wildcard | host source | any}
```

```
no access-list access-list-number
```

This command is available on physical interfaces only if your switch is running the enhanced software image (EI).

Syntax Description

<i>access-list-number</i>	Number of an ACL, from 1 to 99 or from 1300 to 1999.
deny	Deny access if conditions are matched.
permit	Permit access if conditions are matched.
remark	ACL entry comment up to 100 characters.
<i>source source-wildcard host source any</i>	<p>Define a source IP address and wildcard.</p> <p>The <i>source</i> is the source address of the network or host from which the packet is being sent, specified in one of these ways:</p> <ul style="list-style-type: none"> • The 32-bit quantity in dotted-decimal format. The <i>source-wildcard</i> applies wildcard bits to the source. • The keyword host, followed by the 32-bit quantity in dotted-decimal format, as an abbreviation for <i>source</i> and <i>source-wildcard</i> of <i>source</i> 0.0.0.0. • The keyword any as an abbreviation for <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255. You do not need to enter a source-wildcard.

Defaults

The default standard ACL is always terminated by an implicit deny statement for all packets.

Command Modes

Global configuration

Command History

Release	Modification
12.1(6)EA2	This command was introduced.

Usage Guidelines

Plan your access conditions carefully. The ACL is always terminated by an implicit deny statement for all packets.

You can use ACLs to control virtual terminal line access by controlling the transmission of packets on an interface.

Use the **show ip access-lists** command to display the contents of IP ACLs.

Use the **show access-lists** command to display the contents of all ACLs.

**Note**

For more information about configuring IP ACLs, refer to the “Configuring Network Security with ACLs” chapter in the *Catalyst 2950 Desktop Switch Software Configuration Guide* for this release.

Examples

This example shows how to configure a standard IP ACL that allows only traffic from the host network 128.88.1.10 and how to apply it to an interface:

```
Switch(config)# access-list 12 permit host 128.88.1.10
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip access-group 12 in
```

This is an example of a standard ACL that allows traffic only from three specified networks. The wildcard bits apply to the host portions of the network addresses. Any host with a source address that does not match the ACL statements is denied.

```
access-list 14 permit 192.5.34.0  0.0.0.255
access-list 14 permit 128.88.0.0  0.0.0.255
access-list 14 permit 36.1.1.0  0.0.0.255
```

**Note**

In these examples, all other IP access is implicitly denied.

You can verify your settings by entering the **show ip access-lists** or **show access-lists** privileged EXEC command.

Related Commands

Command	Description
access-list (IP extended)	Configures an extended IP ACL.
ip access-group	Controls access to an interface.
show access-lists	Displays ACLs configured on the switch.
show ip access-lists	Displays IP ACLs configured on the switch.

 archive download-sw

archive download-sw

Use the **archive download-sw** privileged EXEC command to download a new image to the switch and to overwrite or to keep the existing image.

```
archive download-sw {/force-reload | /imageonly | /leave-old-sw | /no-set-boot | /overwrite | /reload | /safe} source-url
```

Syntax Description	
/force-reload	Unconditionally force a system reload after successfully downloading the software image.
/imageonly	Download only the software image but not the HTML files associated with the Cluster Management Suite (CMS). The HTML files for the existing version are deleted only if the existing version is being overwritten or removed.
/leave-old-sw	Keep the old software version after a successful download.
/no-set-boot	Do not alter the setting of the BOOT environment variable to point to the new software image after it is successfully downloaded.
/overwrite	Overwrite the software image in Flash with the downloaded one.
/reload	Reload the system after successfully downloading the image unless the configuration has been changed and not been saved.
/safe	Keep the current software image; do not delete it to make room for the new software image before the new image is downloaded. The current image is deleted after the download.
source-url	<p>The source URL alias for a local or network file system. These options are supported:</p> <ul style="list-style-type: none"> • The syntax for the local Flash file system: flash: • The syntax for the File Transfer Protocol (FTP): ftp:[//username[:password]@location]/directory]/image-name.tar • The syntax for the Remote Copy Protocol (RCP): rcp:[//username@location]/directory]/image-name.tar • The syntax for the Trivial File Transfer Protocol (TFTP): tftp:[//location]/directory]/image-name.tar <p>The <i>image-name.tar</i> is the software image to download and install on the switch.</p>

Defaults

Both the software image and HTML files are downloaded.

The new image is downloaded to the flash: file system.

The BOOT environment variable is changed to point to the new software image on the flash: file system.

Image names are case sensitive; the image file is provided in tar format.

Command Modes

Privileged EXEC

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.

Usage Guidelines

Use the **/overwrite** option to overwrite the image on the Flash device with the downloaded one.

If the Flash device has sufficient space to hold two images and you want to overwrite one of these images with the same version, you must specify the **/overwrite** option.

If you specify the command without the **/overwrite** option, the download algorithm verifies that the new image is not the same as the one on the switch Flash device. If the images are the same, the download does not occur. If the images are different, the old image is deleted, and the new one is downloaded.

The **/imageonly** option removes the HTML files for the existing image if the existing image is being removed or replaced. Only the IOS image (without the HTML files) is downloaded.

Using the **/safe** or **/leave-old-sw** option can cause the new image download to fail if there is insufficient Flash space.

If you used the **/leave-old-sw** option and did not overwrite the old image when you downloaded the new one, you can remove the old image by using the **delete** privileged EXEC command. For more information, see the “[“delete” section on page 2-73](#)”.

If you leave the existing software in place before downloading the new image, an error results if the existing software prevents the new image from fitting onto Flash memory.

After downloading a new image, enter the **reload** privileged EXEC command to begin using the new image, or specify the **/reload** or **/force-reload** option in the **archive download-sw** command.

Examples

This example shows how to download a new image from a TFTP server at 172.20.129.10 and to overwrite the image on the switch:

```
Switch# archive download-sw /overwrite tftp://172.20.129.10/test-image.tar
```

This example shows how to download only the software image from a TFTP server at 172.20.129.10 to the switch:

```
Switch# archive download-sw /image-only tftp://172.20.129.10/test-image.tar
```

This example shows how to keep the old software version after a successful download:

```
Switch# archive download-sw /leave-old-sw tftp://172.20.129.10/test-image.tar
```

Related Commands

Command	Description
archive tar	Creates a tar file, lists the files in a tar file, or extracts the files from a tar file.
archive upload-sw	Uploads an existing image on the switch to a server.
delete	Deletes a file or directory on the Flash memory device.

archive tar

archive tar

Use the **archive tar** privileged EXEC command to create a tar file, to list files in a tar file, or to extract the files from a tar file.

```
archive tar {/create destination-url flash:/file-url} |{/table source-url} |{/xtract source-url  
flash:/file-url}
```

Syntax Description

/create destination-url flash:/file-url	<p>Create a new tar file on the local or network file system.</p> <p>For <i>destination-url</i>, specify the destination URL alias for the local or network file system and the name of the tar file to create. These options are supported:</p> <ul style="list-style-type: none"> • The syntax for the local Flash filesystem: flash: • The syntax for the File Transfer Protocol (FTP): ftp:[//username[:password]@location]/directory]/tar-filename.tar • The syntax for the Remote Copy Protocol (RCP) is: rcp:[//username@location]/directory]/tar-filename.tar • The syntax for the Trivial File Transfer Protocol (TFTP): tftp:[//location]/directory]/tar-filename.tar <p>The <i>tar-filename.tar</i> is the tar file to be created.</p> <p>For flash:/file-url, specify the location on the local Flash file system from which the new tar file is created.</p> <p>An optional list of files or directories within the source directory can be specified to write to the new tar file. If none are specified, all files and directories at this level are written to the newly created tar file.</p> <hr/>
--	---

/table source-url	<p>Display the contents of an existing tar file to the screen.</p> <p>For <i>source-url</i>, specify the source URL alias for the local or network file system. These options are supported:</p> <ul style="list-style-type: none"> • The syntax for the local Flash file system: flash: • The syntax for the File Transfer Protocol (FTP) ftp:[//username[:password]@location]/directory]/tar-filename.tar • The syntax for the Remote Copy Protocol (RCP): rcp:[//username@location]/directory]/tar-filename.tar • The syntax for the Trivial File Transfer Protocol (TFTP): tftp:[//location]/directory]/tar-filename.tar <p>The <i>tar-filename.tar</i> is the tar file to display.</p>
/xtract source-url flash:/file-url	<p>Extract files from a tar file to the local or network file system.</p> <p>For <i>source-url</i>, specify the source URL alias for the local or network file system. These options are supported:</p> <ul style="list-style-type: none"> • The syntax for the local Flash file system: flash: • The syntax for the File Transfer Protocol (FTP) ftp:[//username[:password]@location]/directory]/tar-filename.tar • The syntax for the Remote Copy Protocol (RCP): rcp:[//username@location]/directory]/tar-filename.tar • The syntax for the Trivial File Transfer Protocol (TFTP): tftp:[//location]/directory]/tar-filename.tar <p>The <i>tar-filename.tar</i> is the tar file from which to extract.</p> <p>For flash:/file-url, specify the location on the local Flash file system into which the tar file is extracted.</p> <p>An optional list of files or directories within the tar file can be specified for extraction. If none are specified, all files and directories are extracted.</p>

Defaults	None
-----------------	------

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

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.

Usage Guidelines	Filenames and directory names are case sensitive. Image names are case sensitive.
-------------------------	--

■ archive tar

Examples

This example shows how to create a tar file. The command writes the contents of the *new-configs* directory on the local Flash device to a file named *saved.tar* on the TFTP server at 172.20.136.9:

```
Switch# archive tar /create tftp:172.20.136.9/saved.tar flash:/new-configs
```

This example shows how to display the contents of the *saved.tar* file that is in Flash memory. The contents of the tar file appear on the screen:

```
Switch # archive tar /table tftp://172.20.136.9/saved.tar
Loading saved.tar from 172.20.136.9 (via Vlan1):!
info (247 bytes)
c2950lre-i612q4-mz.121/ (directory)
c2950lre-i612q4-mz.121/html/ (directory)
c2950lre-i612q4-mz.121/html/homepage.htm (3990 bytes)!!
c2950lre-i612q4-mz.121/html/not_supported.html (1392 bytes)
c2950lre-i612q4-mz.121/html/common.js (9449 bytes)!!
c2950lre-i612q4-mz.121/html/cms_splash.gif (22062 bytes)!!!!!
c2950lre-i612q4-mz.121/html/cms_13.html (1211 bytes)
c2950lre-i612q4-mz.121/html/cluster.html (2823 bytes)!
c2950lre-i612q4-mz.121/html/Redirect.jar (4226 bytes)!
c2950lre-i612q4-mz.121/html/c4v4_disc.sgz (11131 bytes)!!
c2950lre-i612q4-mz.121/html/CMS.sgz (1178465
bytes)!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
c2950lre-i612q4-mz.121/html/CiscoChartPanel.sgz (57732 bytes)!!!!!!!
c2950lre-i612q4-mz.121/html/cms_boot.jar (40976 bytes)!!!!!!!
c2950lre-i612q4-mz.121/c2950lre-i612q4-mz.121.bin (2769508
bytes)!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
c2950lre-i612q4-mz.121/lre-bin/ (directory)
c2950lre-i612q4-mz.121/lre-bin/CISCO2950-LRE_vdsloctl_02.50.00.bin (33480
bytes)!!!!!!!
c2950lre-i612q4-mz.121/lre-bin/CISCO2950-LRE_vdsloctl_02.51.00.bin (33480
bytes)!!!!!!!
c2950lre-i612q4-mz.121/lre-bin/CISCO2950-LRE_vdsloctl_02.60.00.bin (33480
bytes)!!!!!!!
c2950lre-i612q4-mz.121/lre-bin/CISCO575-LRE_vdsslsgl_50.00.00.bin (8896
bytes)!!
c2950lre-i612q4-mz.121/lre-bin/CISCO585-LRE_MC8051appl_01.02.00.bin (688
bytes)!
c2950lre-i612q4-mz.121/lre-bin/CISCO585-LRE_MC8051appl_01.03.00.bin (688
bytes)
c2950lre-i612q4-mz.121/lre-bin/CISCO585-LRE_MC8051boot_01.02.00.bin (688
bytes)
c2950lre-i612q4-mz.121/lre-bin/CISCO585-LRE_MC8051boot_01.03.00.bin (688
bytes)
c2950lre-i612q4-mz.121/lre-bin/CISCO585-LRE_vdsslsgl_51.00.00.bin (8896
bytes)!!
c2950lre-i612q4-mz.121/pef22824.bin (32768 bytes)!!!!!!!
c2950lre-i612q4-mz.121/info (247 bytes)
info.ver (247 bytes)
[OK - 4279808/8559616 bytes]
```

Related Commands

Command	Description
archive download-sw	Downloads a new image to the switch.
archive upload-sw	Uploads an existing image on the switch to a server.

 archive upload-sw

archive upload-sw

Use the **archive upload-sw** privileged EXEC command to upload an existing switch image to a server.

archive upload-sw [/version *version_string*] *destination-url*

Syntax Description	/version <i>version_string</i> (Optional) Specify the specify version string of the image to be uploaded. <i>destination-url</i> The destination URL alias for a local or network file system. These options are supported: <ul style="list-style-type: none"> The syntax for the local Flash file system: flash: The syntax for the File Transfer Protocol (FTP): ftp:[//username[:password]@location]/directory]/image-name.tar The syntax for the Remote Copy Protocol (RCP): rcp:[//username@location]/directory]/image-name.tar The syntax for the Trivial File Transfer Protocol (TFTP): tftp:[//location]/directory]/image-name.tar The <i>image-name.tar</i> is the name of software image to be stored on the server.
---------------------------	---

Defaults Uploads the currently running image from the flash: file system.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.

Usage Guidelines The upload feature is available only if the HTML files associated with the Cluster Management Suite (CMS) have been installed with the existing image.

The files are uploaded in this sequence: info, the IOS image, the HTML files, Long-Reach Ethernet (LRE) binary files and info.ver. After these files are uploaded, the software creates the tar file.

Image names are case sensitive.

Examples This example shows how to upload the currently running image to a TFTP server at 172.20.140.2:

```
Switch# archive upload-sw tftp://172.20.140.2/test-image.tar
```

Related Commands	Command	Description
	archive download-sw	Downloads a new image to the switch.
	archive tar	Creates a tar file, lists the files in a tar file, or extracts the files from a tar file.

■ **auto qos voip**

auto qos voip

Use the **auto qos voip** interface configuration command to configure automatic quality of service (auto-QoS) for Voice over IP (VoIP) within a QoS domain. Use the **no** form of this command to change the auto-QoS default settings to the standard-QoS defaults.

auto qos voip {cisco-phone | trust}

no auto qos voip

This command is available only if your switch is running the enhanced software image (EI).

Syntax Description	cisco-phone	Identify this interface as connected to a Cisco IP Phone, and automatically configure QoS for VoIP. The QoS labels of incoming packets are trusted only when the phone is detected.
	trust	Identify this interface as connected to a trusted switch or router. The QoS labels of incoming packets are trusted.

Defaults

Auto-QoS is disabled on all interfaces.

When auto-QoS is enabled, it uses the ingress packet label to categorize traffic, to assign Differentiated Services Code Point (DSCP) and class of service (CoS) packet labels, and to configure the egress queues as summarized in [Table 2-1](#).

Table 2-1 Traffic Types, Ingress Packet Labels, Assigned Packet Labels, and Egress Queues

	VoIP Data Traffic	VoIP Control Traffic	Routing Protocol Traffic	STP BPDU¹ Traffic	All Other Traffic
Ingress DSCP	46	26	—	—	—
Ingress CoS	5	3	6	7	—
Assigned DSCP	46	26	48	56	0
Assigned CoS	—	—	6	7	0
CoS-to-Queue Map	5	3, 4, 6, 7			0, 1, 2
Egress Queue	Expedite queue	80% WRR			20% WRR

1. BPDU = bridge protocol data unit

[Table 2-2](#) lists the default auto-QoS configuration for the egress queues.

Table 2-2 Default Auto-QoS Configuration for the Egress Queues

Egress Queue	Queue Number	CoS-to-Queue Map	Queue Weight
Expedite	4	5	—
80% WRR	3	3, 4, 6, 7	80%
20% WRR	1	0, 1, 2	20%

Command Modes Interface configuration

Command History

Release	Modification
12.1(11)EA1	This command was introduced.

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

Use the **cisco-phone** keyword on ports connected to Cisco IP Phones at the edge of the network. The switch detects the phone through the Cisco Discovery Protocol (CDP) and trusts the QoS labels in packets received from the phone.

Use the **trust** keyword on ports connected to the interior of the network. Because it is assumed that traffic has already been classified by other edge devices, the QoS labels in these packets from the interior of the network are trusted.

The first interface that you enable with the auto-QoS feature results in these automatic actions:

- The standard-QoS defaults for the egress queues are replaced with the auto-QoS defaults. For more information, refer to the software configuration guide for this release.
- The auto-QoS defaults for the egress queues are globally enabled on all interfaces.
- The auto-QoS defaults for the CoS-to-DSCP map are globally configured on all interfaces.
- When you enter the **auto qos voip cisco-phone** interface configuration command, the ingress classification on the interface is set to trust the CoS value received in the packet only if a Cisco IP Phone is detected.
- When you enter the **auto qos voip trust** interface configuration command, the ingress classification on the interface is set to trust the CoS value received in the packet.

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

The **auto qos voip** interface configuration command is mutually exclusive with interface ingress-classification commands. If you configure the **auto qos voip** command when the **mls qos cos override**, **mls qos trust [cos | device cisco-phone | dscp]**, or **service-policy** interface configuration commands are configured, an error message appears, and the existing configuration remains in effect.

If you previously configured the egress queues and then enable auto-QoS, the pre-existing configuration remains in effect.

If auto-QoS is enabled and you enter the **no** form of a standard-QoS command to return to the default, the auto-QoS default settings become the default settings.

auto qos voip**Examples**

This example shows how to enable auto-QoS and to trust the QoS labels received in incoming packets when the switch or router connected to Gigabit Ethernet interface 0/1 is a trusted device:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# auto qos voip trust
```

This example shows how to enable auto-QoS and to trust the QoS labels received in incoming packets when the device connected to Fast Ethernet interface 0/1 is detected and is a Cisco IP Phone:

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# auto qos voip cisco-phone
```

You can verify your settings by entering the **show auto qos voip interface *interface-id*** privileged EXEC command.

Related Commands

Command	Description
mls qos cos	Defines the default CoS value of a port or assigns the default CoS to all incoming packets on the port.
mls qos map	Defines the CoS-to-DSCP map or the DSCP-to-CoS map.
mls qos trust	Configures the port trust state.
show auto qos	Displays auto-QoS information.
show mls qos interface	Displays QoS information at the interface level.

boot boothlpr

Use the **boot boothlpr** global configuration command to load a special IOS image, which when loaded into memory, can load a second IOS image into memory and start it. This variable is used only for internal development and testing. Use the **no** form of this command to return to the default setting.

boot boothlpr *filesystem:/file-url*

no boot boothlpr

Syntax Description	<i>filesystem:</i> Alias for a Flash file system. Use flash: for the system board Flash device. <i>/file-url</i> The path (directory) and name of a bootable helper image.
---------------------------	--

Defaults	No helper image is loaded.
-----------------	----------------------------

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

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.

Usage Guidelines	Filenames and directory names are case sensitive.
-------------------------	---

This command changes the setting of the BOOTHLPR environment variable. For more information, see [Appendix B, “Boot Loader Commands.”](#)

Related Commands	Command	Description
	show boot	Displays the settings of the boot environment variables.

boot buffersize

boot buffersize

Use the **boot buffersize** global configuration command to specify the size of the file system-simulated nonvolatile RAM (NVRAM) in Flash memory. The buffer holds a copy of the configuration file in memory. Use the **no** form of this command to return to the default setting.

boot buffersize *size*

no boot buffersize

Syntax Description	<i>size</i>	The buffer allocation size in bytes. The range is 4096 to 524288 bytes.
---------------------------	-------------	---

Defaults	The default is 32 KB.
-----------------	-----------------------

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

Command History	Release	Modification
	12.1(11)YP	This command was introduced.

Usage Guidelines	The configuration file cannot be larger than the buffer size allocation.
-------------------------	--

You must reload the switch by using the **reload** privileged EXEC command for this command to take effect.

This command changes the setting of the CONFIG_BUFSIZE environment variable. For more information, see [Appendix B, “Boot Loader Commands.”](#)

Related Commands	Command	Description
	show boot	Displays the settings of the boot environment variables.

boot config-file

Use the **boot config-file** global configuration command to specify the filename that IOS uses to read and write a nonvolatile copy of the system configuration. Use the **no** form of this command to return to the default setting.

boot config-file flash:/file-url

no boot config-file

Syntax Description	flash:/file-url	The path (directory) and name of the configuration file.
Defaults	The default configuration file is flash:config.text.	
Command Modes	Global configuration	
Command History	Release	Modification
	12.1(11)YJ	This command was introduced.
Usage Guidelines	<p>Filenames and directory names are case sensitive.</p> <p>This command changes the setting of the CONFIG_FILE environment variable. For more information, see Appendix B, “Boot Loader Commands.”</p>	
Related Commands	Command	Description
	show boot	Displays the settings of the boot environment variables.

boot enable-break

boot enable-break

Use the **boot enable-break** global configuration command to enable interrupting the automatic boot process. Use the **no** form of this command to return to the default setting.

boot enable-break

no boot enable-break

Syntax Description This command has no arguments or keywords.

Defaults Disabled. The automatic start up process cannot be interrupted by pressing the **Break** key on the console.

Command Modes Global configuration

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.

Usage Guidelines When you enter this command, you can interrupt the automatic boot process by pressing the **Break** key on the console after the Flash file system is initialized.



Despite the setting of this command, you can interrupt the automatic boot process at any time by pressing the MODE button on the switch front panel.

This command changes the setting of the ENABLE_BREAK environment variable. For more information, see [Appendix B, “Boot Loader Commands.”](#)

Related Commands	Command	Description
	show boot	Displays the settings of the boot environment variables.

boot helper

Use the **boot helper** global configuration command to dynamically load files during boot loader initialization to extend or to patch the functionality of the boot loader. Use the **no** form of this command to return to the default.

boot helper *filesystem:/file-url ...*

no boot helper

Syntax Description	filesystem: Alias for a Flash file system. Use flash: for the system board Flash device. /file-url The path (directory) and a list of loadable files to dynamically load during loader initialization. Separate each image name with a semicolon.
---------------------------	---

Defaults	No helper files are loaded.
-----------------	-----------------------------

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

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.

Usage Guidelines	Filenames and directory names are case sensitive. This command changes the setting of the HELPER environment variable. For more information, see Appendix B, “Boot Loader Commands.”
-------------------------	--

Related Commands	Command	Description
	show boot	Displays the settings of the boot environment variables.

 boot helper-config-file

boot helper-config-file

Use the **boot helper-config-file** global configuration command to specify the name of the configuration file to be used by the IOS helper image. If this is not set, the file specified by the CONFIG_FILE environment variable is used by all version of IOS that are loaded. This variable is used only for internal development and testing. Use the **no** form of this command to return to the default setting.

boot helper-config-file *filesystem:/file-url*

no boot helper-config file

Syntax Description	<i>filesystem:</i>	Alias for a Flash file system. Use flash: for the system board Flash device.
	<i>/file-url</i>	The path (directory) and helper configuration file to load.

Defaults No helper configuration file is specified.

Command Modes Global configuration

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.

Usage Guidelines Filenames and directory names are case sensitive.

This command changes the setting of the `HELPER_CONFIG_FILE` environment variable. For more information, see [Appendix B, “Boot Loader Commands.”](#)

Related Commands	Command	Description
	show boot	Displays the settings of the boot environment variables.

boot manual

Use the **boot manual** global configuration command to enable starting the switch manually during the next power on cycle. Use the **no** form of this command to return to the default setting.

boot manual

no boot manual

Syntax Description This command has no arguments or keywords.

Defaults The default is **no boot manual**.

Command Modes Global configuration

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.

Usage Guidelines The next time you restart the system, the switch is in boot loader mode, which is shown by the `switch:` prompt. To power on the system, use the **boot** boot loader command, and specify the name of the bootable image.

This command changes the setting of the `MANUAL_BOOT` environment variable. For more information, see [Appendix B, “Boot Loader Commands.”](#)

Related Commands	Command	Description
	show boot	Displays the settings of the boot environment variables.

boot private-config-file

boot private-config-file

Use the **boot private-config-file** global configuration command to specify the filename that IOS uses to read and write a nonvolatile copy of the private configuration. Use the **no** form of this command to return to the default setting.

boot private-config-file *filename*

no boot private-config-file

Syntax Description	<i>filename</i>	The name of the private configuration file.
Defaults	The default configuration file is <i>private-config.text</i> .	
Command Modes	Global configuration	
Command History	Release	Modification
	12.1(11)YJ	This command was introduced.
Usage Guidelines	Filenames are case sensitive.	
Examples	<p>This example shows how to specify the name of the private configuration file to be <i>pconfig</i>:</p> <pre>Switch(config)# boot private-config-file pconfig</pre>	
Related Commands	Command	Description
	show boot	Displays the settings of the boot environment variables.

boot system

Use the **boot system** global configuration command to specify the IOS image to load during the next power on cycle. Use the **no** form of this command to return to the default setting.

boot system *filesystem:/file-url ...*

no boot system

Syntax Description	filesystem: Alias for a Flash file system. Use flash: for the system board Flash device. /file-url The path (directory) and name of a bootable image. Separate image names with a semicolon.
---------------------------	--

Defaults	The switch attempts to automatically power on the system by using information in the BOOT environment variable. If this variable is not set, the switch attempts to load and execute the first executable image it can by performing a recursive, depth-first search throughout the Flash file system. In a depth-first search of a directory, each encountered subdirectory is completely searched before the switch continues to search in the original directory.
-----------------	--

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

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.

Usage Guidelines	Filenames and directory names are case sensitive. If you are using the archive download-sw privileged EXEC command to maintain system images, you do not ever need to use the boot system command. The boot system command is automatically manipulated to load the downloaded image. This command changes the setting of the BOOT environment variable. For more information, see Appendix B, “Boot Loader Commands.”
-------------------------	---

Related Commands	Command	Description
	show boot	Displays the settings of the boot environment variables.

channel-group

channel-group

Use the **channel-group** interface configuration command to assign an Ethernet interface to an EtherChannel group. Use the **no** form of this command to remove an Ethernet interface from an EtherChannel group.

channel-group *channel-group-number* **mode** {**auto** [**non-silent**] | **desirable** [**non-silent**] | **on**}

no channel-group

Syntax Description

<i>channel-group-number</i>	Specify the channel group number. The range is 1 to 6.
mode	Specify the EtherChannel Port Aggregation Protocol (PAgP) mode of the interface.
auto	Enable PAgP only if a PAgP device is detected. Auto mode places an interface into a passive negotiating state, in which the interface 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. This setting is the default.
desirable	Unconditionally enable PAgP. Desirable mode places an interface into an active negotiating state, in which the interface initiates negotiations with other interfaces by sending PAgP packets. A channel is formed with another port group in either the desirable or auto mode.
non-silent	(Optional) Used with the auto or desirable keyword when traffic is expected from the other device.
on	Force the interface to channel without PAgP. With the on mode, a usable EtherChannel exists only when an interface group in the on mode is connected to another interface group in the on mode. This mode is not available for Long-Reach Ethernet (LRE), because LRE interfaces do not support an EtherChannel-only mode.

Defaults

No channel groups are assigned.

There is no default mode.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(6)EA2	This command was introduced. It replaced the port group command.

Usage Guidelines

You must specify the mode when entering this command. If the mode is not entered, an Ethernet interface is not assigned to an EtherChannel group, and an error message appears.

You do not have to create a port-channel interface before assigning a physical interface to a channel group. A port-channel interface is created automatically when the channel group gets its first physical interface.

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

You can create port channels by entering the **interface port-channel** global configuration command or when the channel group gets its first physical interface assignment. The port channels are not created at runtime or dynamically.

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

With the **on** mode, a usable EtherChannel exists only when a port group in **on** mode is connected to another port group in **on** mode.

If you do not specify **non-silent** with the **auto** or **desirable** mode, silent is assumed. The silent mode is used when the switch is connected to a device that is not PAgP-capable and seldom, if ever, transmits packets. An example of a silent partner is a file server or a packet analyzer that is not generating traffic. In this case, running PAgP on a physical port prevents that port from ever becoming operational; however, it allows PAgP to operate, to attach the interface to a channel group, and to use the interface for transmission. Both ends of the link cannot be set to silent.

**Caution**

You should exercise care when setting the mode to **on** (manual configuration). All ports configured in the **on** mode are bundled in the same group and are forced to have similar characteristics. If the group is misconfigured, packet loss or Spanning Tree Protocol (STP) loops might occur.

Examples

This example shows how to add an interface to the EtherChannel group specified as channel group 1:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# channel-group 1 mode on
```

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

Related Commands

Command	Description
interface port-channel	Accesses or creates the port channel.
port-channel load-balance	Sets the load distribution method among the ports in the EtherChannel.
show etherchannel	Displays EtherChannel information for a channel.
show running-config	Displays the configuration information running on the switch. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 > Cisco IOS File Management Commands > Configuration File Commands .

class

Use the **class** policy-map configuration command to define a traffic classification for the policy to act on using the class-map name or access group. Use the **no** form of this command to delete an existing class map.

class *class-map-name* [**access-group** **name** *acl-index-or-name*]

no class *class-map-name*

This command is available only if your switch is running the enhanced software image (EI).

Syntax Description

class-map-name	Name of the class map.
access-group name <i>acl-index-or-name</i>	(Optional) Number or name of an IP standard or extended access control list (ACL) or name of an extended MAC ACL. For an IP standard ACL, the index range is 1 to 99 and 1300 to 1999; for an IP extended ACL, the index range is 100 to 199 and 2000 to 2699.

Defaults

No policy-map class maps are defined.

Command Modes

Policy-map configuration

Command History

Release	Modification
12.1(6)EA2	This command was introduced.

Usage Guidelines

Before you use the **class** command, use the **policy-map** global configuration command to identify the policy map and to enter policy-map configuration mode. After you specify a policy map, you can configure a policy for new classes or modify a policy for any existing classes in that policy map. You attach the policy map to an interface by using the **service-policy** interface configuration command; however, you cannot attach one that uses an ACL classification to the egress direction.

The class name that you specify in the policy map ties the characteristics for that class to the class map and its match criteria as configured by using the **class-map** global configuration command.

The **class** command performs the same function as the **class-map** global configuration command. Use the **class** command when a new classification, which is not shared with any other ports, is needed. Use the **class-map** command when the map is shared among many ports.



Note In a policy map, the class named *class-default* is not supported. The switch does not filter traffic based on the policy map defined by the **class class-default** policy-map configuration command.

After entering the **class** command, you enter policy-map class configuration mode. These configuration commands are available:

- **default**: sets a command to its default.
- **exit**: exits policy-map class configuration mode and returns to policy-map configuration mode.
- **no**: returns a command to its default setting.
- **set**: specifies a Differentiated Services Code Point (DSCP) value to be assigned to the classified traffic. For more information, see the **set** command.
- **police**: defines a policer for the classified traffic. The policer specifies the bandwidth limitations and the action to take when the limits are exceeded. For more information, see the **police** command.

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



Note

For more information about configuring ACLs, refer to the “Configuring Network Security with ACLs” chapter in the *Catalyst 2950 Desktop Switch Software Configuration Guide* for this release.

Examples

This example shows how to create a policy map named *policy1*. When attached to the ingress port, it matches all the incoming traffic defined in *class1* and polices the traffic at an average rate of 1 Mbps and bursts at 131072 bytes. Traffic exceeding the profile is dropped.

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# police 1000000 131072 exceed-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)#
```

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

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to the class whose name you specify.
match	Defines the match criteria to classify traffic.
policy-map	Creates or modifies a policy map that can be attached to multiple interfaces to specify a service policy.
show policy-map	Displays quality of service (QoS) policy maps.

class-map

Use the **class-map** global configuration command to create a class map to be used for matching packets to the class whose name you specify and to enter class-map configuration mode. Use the **no** form of this command to delete an existing class map and to return to global configuration mode.

class-map *class-map-name* [**match-all**]

no class-map *class-map-name* [**match-all**]

This command is available only if your switch is running the enhanced software image (EI).

Syntax Description	<table border="0"> <tr> <td><i>class-map-name</i></td><td>Name of the class map.</td></tr> <tr> <td>match-all</td><td>(Optional) Perform a logical-AND of all matching statements under this class map. All criteria in the class map must be matched.</td></tr> </table>	<i>class-map-name</i>	Name of the class map.	match-all	(Optional) Perform a logical-AND of all matching statements under this class map. All criteria in the class map must be matched.
<i>class-map-name</i>	Name of the class map.				
match-all	(Optional) Perform a logical-AND of all matching statements under this class map. All criteria in the class map must be matched.				

Defaults	No class maps are defined.
-----------------	----------------------------

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

Command History	Release	Modification
	12.1(6)EA2	This command was introduced.

Usage Guidelines	Use this command to specify the name of the class for which you want to create or modify class-map match criteria and to enter class-map configuration mode. In this mode, you can enter one match command to configure the match criteria for this class.
-------------------------	---

The **class-map** command and its subcommands are used to define packet classification and marking as part of a globally named service policy applied on a per-interface basis.

In quality of service (QoS) class-map configuration mode, these configuration commands are available:

- **exit**: exits from QoS class-map configuration mode.
- **no**: removes a match statement from a class map.
- **match**: configures classification criteria. For more information, see the **match** class-map configuration command.

Only one match criterion per class map is supported. For example, when defining a class map, only one **match** command can be entered.

Only one access control list (ACL) can be configured in a class map. The ACL can have multiple access control entries (ACEs).



Note The switch does not support any deny conditions in an ACL configured in a class map.

**Note**

For more information about configuring ACLs, refer to the “Configuring Network Security with ACLs” chapter in the *Catalyst 2950 Desktop Switch Software Configuration Guide* for this release.

Examples

This example shows how to configure the class map named *class1*. *class1* has one match criteria, which is a numbered ACL.

```
Switch(config)# access-list 103 permit tcp any any eq 80
Switch(config)# class-map class1
Switch(config-cmap)# match access-group 103
Switch(config-cmap)# exit
```

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

Related Commands

Command	Description
class	Defines a traffic classification for the policy to act on by using the class-map name or access group.
match	Defines the match criteria to classify traffic.
policy-map	Creates or modifies a policy map that can be attached to multiple interfaces to specify a service policy.
show class-map	Displays QoS class maps.

■ clear controllers ethernet-controller

clear controllers ethernet-controller

Use the **clear controllers ethernet-controller** privileged EXEC command to delete the Ethernet link transmit and receive statistics for a switch port and for a Long-Reach Ethernet (LRE) customer premises equipment (CPE) device.

clear controllers ethernet-controller [FastEthernet | GE-WAN | Gigabit Ethernet | LongReach Ethernet] interface-id [cpe [port port-id]]

Syntax Description	
<i>interface-id</i>	(Optional) ID of the switch port.
cpe	This parameter only operates when Long-Reach Ethernet is specified as the interface. As a standalone keyword, it clears the Ethernet counters of the LRE chipset and all CPE Ethernet ports.
port	This parameter only operates when Long-Reach Ethernet is specified as the interface. The cpe port keywords clear the Ethernet counts of the designated CPE Ethernet port.
<i>port-id</i>	The CPE Ethernet port identifier. Valid values vary from 1 to 4, depending on CPE device model.

Defaults There is no default.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(11)YY	This command was introduced.

Usage Guidelines Using the **clear controllers ethernet-controller** command without specifying an interface-id clears the Ethernet link statistics for all ports on the switch. Without the port keyword, this command clears the statistics:

- Of the Ethernet port on the Cisco 575 LRE CPE
- Of all four Ethernet ports on the Cisco 585 LRE CPE

This command clears the switch Ethernet link statistics for all ports on the switch:

```
clear controllers ethernet-controller
```

This command clears the switch Ethernet link statistics for a specific port. It does not clear the CPE Ethernet port statistics on the CPE device:

```
clear controllers ethernet-controller LongReachEthernet 0/1
```

This command clears the Ethernet statistics for all the CPE Ethernet ports on the CPE device:

```
clear controllers ethernet-controller LongReachEthernet 0/1 cpe
```

**Note**

The Cisco 585 LRE CPE Ethernet ports cannot be cleared on a per-port basis, even by using the *port-id* argument.

The CPE Ethernet link is the connection between the CPE Ethernet port and the remote Ethernet device (such as a PC) connected to it. It is not the link between the switch LRE port and the LRE CPE device.

It takes the switch several seconds to clear the CPE Ethernet ports. The CPE Ethernet ports on CPE devices take longer to clear than all the other port types.

Examples

This example shows how to use the **clear controllers ethernet-controller** command to clear the Ethernet link statistics for LRE port 1:

```
Switch# clear controllers ethernet-controller lo0/1
Switch#
```

This example clears the Ethernet statistics for *all* the CPE Ethernet ports on a Cisco 585 LRE CPE:

```
Switch# clear controllers ethernet-controller lo0/1 cpe
Switch#
```

You can verify that information was deleted by entering the **show controllers ethernet-controller** user EXEC command.

Related Commands

Command	Description
show controllers ethernet-controller	Displays the Ethernet link transmit and receive statistics on a Fast Ethernet or a switch LRE port.

 clear controllers lre

clear controllers lre

Use the **clear controllers lre** user exec command to reset the switch Long-Reach Ethernet (LRE) or the Cisco LRE customer premises equipment (CPE) device interface.

clear controllers lre {local link | remote [link | micro]} interface-id

Syntax Description	
local link	Resets the LRE interfaces on the switch by performing a port reset.
remote link	Resets the LRE interface for the CPE device.
micro	Resets the Cisco 585 CPE device.

Defaults No default is defined.

Command Modes User Exec mode

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.

Usage Guidelines Use this command to reset a questionable local or remote interface.
The **clear controllers lre remote micro** command is not supported on the Cisco 575 LRE CPE device.

Examples This example shows how to reset the local LRE interfaces on the switch:

```
Switch> clear controllers lre local link
Switch>
```

This example shows how to reset all Cisco 575 LRE or Cisco 585 LRE CPE devices connected to the switch:

```
Switch> clear controllers lre remote link
Switch>
```

This example shows how to reset the Cisco 585 LRE CPE micro-controller connected to the switch:

```
Switch(> clear controllers lre remote micro
Switch>
```

Related Commands	Command	Description
	cpe shutdown	Disables one or more customer premises equipment (CPE) ports.
	shutdown	Disables the LRE transmitter of an LRE interface.

clear controllers lre link monitor

Use the **clear controllers lre link monitor** privileged EXEC command to delete LRE link monitor data.

clear controllers lre link monitor *interface-id*

Syntax Description	<i>interface-id</i>	ID of the switch LRE port.
---------------------------	---------------------	----------------------------

Defaults	There is no default.
-----------------	----------------------

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

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.

Usage Guidelines	This command clears all collected link monitor data. New entries are added when a new polling cycle starts.
-------------------------	---

Examples	This example shows how to clear link monitor data on LRE interface 0/2:
-----------------	---

```
Switch# clear controllers lre link monitor lo 0/2
Switch#
```

Related Commands	Command	Description
	link monitor	Enables the LRE link monitor on a port.
	link monitor logging	Enables link monitor event logging per port.
	link monitor threshold snr	Sets an signal-to-noise margin for the LRE link monitor.
	link monitor threshold rserr	Sets a Reed-Solomon error threshold for the LRE link monitor.
	show controllers lre link monitor errors	Displays Reed-Solomon and Ethernet errors captured by the LRE link monitor.
	show controllers lre link monitor parameters	Displays the switch or CPE device operating parameter data.
	show controllers lre link monitor statistics	Displays the switch or CPE device statistical data.

■ **clear controllers lre log**

clear controllers lre log

Use the **clear controllers lre log** privileged EXEC command to delete the history of link, configuration, and timer events for a specific Long-Reach Ethernet (LRE) port or for all switch LRE ports.

clear controllers lre log [interface-id]

Syntax Description	<i>interface-id</i> (Optional) ID of the switch LRE port.
---------------------------	--

Defaults	There is no default.
-----------------	----------------------

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

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.

Usage Guidelines	Using the clear controllers lre log command without specifying a switch LRE port deletes the history of events on all switch LRE ports.
-------------------------	--

Examples	This example shows how to use the clear controllers lre log command to delete the history of events on switch LRE port 3:
-----------------	--

```
Switch# clear controllers lre log longReachEthernet 0/3
Switch#
```

You can verify that information was deleted by entering the **show controllers lre log** privileged EXEC command.

Related Commands	Command	Description
	logging lre	Sets the LRE logging level to event, extended, or normal.
	show controllers lre log	Displays the history of link, configuration, and timer events for a specific switch LRE port or for all LRE ports on the switch.

clear interface

Use the **clear interface** privileged EXEC command to clear the hardware logic on an interface or a VLAN.

clear interface {interface-id | vlan vlan-id}

Syntax Description	<table border="0"> <tr> <td><i>interface-id</i></td><td>ID of the interface.</td></tr> <tr> <td><i>vlan-id</i></td><td>VLAN ID. Valid VLAN IDs are from 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1001 when the standard software image (SI) is installed. Do not enter leading zeros.</td></tr> </table>	<i>interface-id</i>	ID of the interface.	<i>vlan-id</i>	VLAN ID. Valid VLAN IDs are from 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1001 when the standard software image (SI) is installed. Do not enter leading zeros.
<i>interface-id</i>	ID of the interface.				
<i>vlan-id</i>	VLAN ID. Valid VLAN IDs are from 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1001 when the standard software image (SI) is installed. Do not enter leading zeros.				

Defaults	No default is defined.
-----------------	------------------------

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

Command History	Release	Modification
	12.1(6)EA2	This command was introduced.

Examples	This example shows how to clear the hardware logic on a Gigabit Ethernet interface:
-----------------	---

```
Switch# clear interface gigabitethernet0/1
```

This example shows how to clear the hardware logic on a Long-Reach Ethernet (LRE) interface:
--

```
Switch# clear interface lo0/5
```

This example shows how to clear the hardware logic on a specific VLAN:
--

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

You can verify that the interface-reset counter for an interface is incremented by entering the show interfaces privileged EXEC command.

 clear lre rate selection

clear lre rate selection

Use the **clear lre rate selection** privileged EXEC command to reset the current rate selection setting and to restart rate selection for a specific Long-Reach Ethernet (LRE) port or for all switch LRE ports.

clear lre rate selection [lock] [interface-id]

Syntax Description	lock <i>interface-id</i>	(Optional) Rate selection runs on all ports that have rate selection enabled, including ports that are locked. (Optional) ID of the switch LRE port.
---------------------------	--	---

Defaults	No default is defined.
-----------------	------------------------

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

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.

Usage Guidelines	Using the clear lre rate selection command without specifying a switch LRE port runs rate selection on all switch LRE ports that have rate selection enabled except those ports with locked profiles. Specifying the lock keyword runs rate selection on all profiles, including those that are locked.
-------------------------	---

Examples	This example shows how to use the clear lre rate selection command to reset the rate selection setting and to restart rate selection on port 1.
-----------------	--

```
Switch# clear lre rate selection lo0/1
Switch#
```

This example shows how to rerun rate selection on all ports, including any locked ports.

```
Switch# clear lre rate selection lock
Switch#
```

This example shows how to reset and to restart rate selection on port 2, overriding the locked status.

```
Switch# clear lre rate selection lock lo0/2
Switch#
```

Related Commands	Command	Description
	rate selection	Enables rate selection on a specific port
	rate selection sequence	Assigns a rate selection sequence for a specific port.
	lre rate selection sequence	Assigns a rate selection sequence for the entire switch.

clear mac address-table

Use the **clear mac address-table** privileged EXEC command to delete from the MAC address table a specific dynamic address, all dynamic addresses on a particular interface, or all dynamic addresses on a particular VLAN. This command also clears the MAC address notification global counters.

```
clear mac address-table {dynamic [address mac-addr | interface interface-id | vlan vlan-id] | notification}
```


Note

Beginning with Release 12.1(11)EA1, the **clear mac address-table** command replaces the **clear mac-address-table** command (with the hyphen). The **clear mac-address-table** command (with the hyphen) will become obsolete in a future release.

Syntax Description

dynamic	Delete all dynamic MAC addresses.
dynamic address <i>mac-addr</i>	(Optional) Delete the specified dynamic MAC address.
dynamic interface <i>interface-id</i>	(Optional) Delete all dynamic MAC addresses on the specified physical port or port channel.
dynamic vlan <i>vlan-id</i>	(Optional) Delete all dynamic MAC addresses for the specified VLAN. Valid IDs are from 1 to 4096 when the enhanced software image (EI) is installed and 1 to 1005 when the standard software image (SI) is installed. Do not enter leading zeros.
notification	Clear the notifications in the history table and reset the counters.

Defaults

No default is defined.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(6)EA2	This command was introduced.
12.1(9)EA1	The notification keyword was added.
12.1(11)EA1	The clear mac-address-table command was replaced by the clear mac address-table command.

Examples

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

```
Switch# clear mac address-table dynamic address 0008.0070.0007
```

You can verify that the information was deleted by entering the **show mac address-table** privileged EXEC command.

■ **clear mac address-table**

Related Commands	Command	Description
	mac address-table notification	Enables the MAC address notification feature.
	show mac address-table	Displays the MAC address table static and dynamic entries.
	show mac address-table notification	Displays the MAC address notification settings for all interfaces or the specified interface.
	snmp trap mac-notification	Enables the Simple Network Management Protocol (SNMP) MAC address notification trap on a specific interface.

clear pagp

Use the **clear pagp** privileged EXEC command to clear Port Aggregation Protocol (PAgP) channel-group information.

clear pagp {channel-group-number [counters] | counters}

Syntax Description	<i>channel-group-number</i> Channel group number. The range is 1 to 6. counters Clear traffic counters.
---------------------------	---

Defaults This command has no default setting.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(6)EA2	This command was introduced.

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

```
Switch# clear pagp 4
```

This example shows how to clear channel-group traffic counters:

```
Switch# clear pagp counters
```

You can verify that the information was deleted by entering the **show pagp** privileged EXEC command.

Related Commands	Command	Description
	show pagp	Displays PAgP channel-group information.

 clear port-security dynamic

clear port-security dynamic

Use the **clear port-security dynamic** privileged EXEC command to delete from the MAC address table a specific dynamic secure address or all the dynamic secure addresses on an interface.

clear port-security dynamic [address mac-addr | interface interface-id]

Syntax Description	address mac-addr (Optional) Delete the specified dynamic secure MAC address. interface interface-id (Optional) Delete all the dynamic secure MAC addresses on the specified physical port or port channel.
---------------------------	---

Defaults	No default is defined.
-----------------	------------------------

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

Command History	Release	Modification
	12.1(11)EA1	This command was introduced.

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

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

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

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

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

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

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

Related Commands	Command	Description
	switchport port-security	Enables port security on an interface.
	switchport port-security	Configures secure MAC addresses.
	mac-address mac-address	
	switchport port-security maximum <i>value</i>	Configures a maximum number of secure MAC addresses on a secure interface.
	show port-security	Displays the port security settings defined for an interface or for the switch.

clear port-security sticky

Use the **clear port-security sticky** privileged EXEC command to delete from the secure MAC address table a specific sticky secure address, all the sticky secure addresses on an interface, or all the sticky secure addresses on the switch.

clear port-security sticky [address mac-addr | interface interface-id]

Syntax Description	address mac-addr (Optional) Delete the specified sticky secure MAC address. interface interface-id (Optional) Delete all the sticky secure MAC addresses on the specified physical port.
---------------------------	---

Defaults No default is defined.

Command Modes Privileged EXEC

Usage Guidelines If you enter the **clear port-security sticky** privileged EXEC command without keywords, the switch removes all sticky secure MAC addresses from the secure MAC address table.
 If you enter the **clear port-security sticky address mac-addr** command, the switch removes the specified secure MAC address from the secure MAC address table.
 If you enter the **clear port-security sticky interface interface-id** command, the switch removes all sticky secure MAC addresses on an interface from the secure MAC address table.

Command History	Release	Modification
	12.1(11)EA1a	This command was introduced.

Examples This example shows how to remove a specific sticky secure address from the secure MAC address table:
 Switch# **clear port-security sticky address 0008.0070.0007**
 This example shows how to remove all the sticky secure addresses learned on a specific interface:
 Switch# **clear port-security sticky interface gigabitethernet0/1**
 This example shows how to remove all the sticky secure addresses from the secure MAC address table:
 Switch# **clear port-security sticky**
 You can verify that the information was deleted by entering the **show port-security address** privileged EXEC command.

■ **clear port-security sticky**

Related Commands	Command	Description
	show port-security address	Displays the port security settings defined for an interface or for the switch.
	switchport port-security	Enables port security on an interface.
	switchport port-security mac-address sticky	Enables the interface for sticky learning.
	switchport port-security mac-address sticky <i>mac-address</i>	Specifies a sticky secure MAC address
	switchport port-security maximum <i>value</i>	Configures a maximum number of secure MAC addresses on a secure interface.

clear spanning-tree detected-protocols

Use the **clear spanning-tree detected-protocols** privileged EXEC command to restart the protocol migration process (force the renegotiation with neighboring switches) on all interfaces or on the specified interface.

clear spanning-tree detected-protocols [interface *interface-id*]

This command is available only if your switch is running the enhanced software image (EI).

Syntax Description	interface <i>interface-id</i>	(Optional) Restart the protocol migration process on the specified interface. Valid interfaces include physical ports, VLANs, and port channels. The valid VLAN range is 1 to 4094; do not enter leading zeros. The valid port-channel range is 1 to 6.
---------------------------	--------------------------------------	---

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

Command History	Release	Modification
	12.1(9)EA1	This command was introduced.

Usage Guidelines	A switch running both the Multiple Spanning Tree Protocol (MSTP) and the Rapid Spanning Tree Protocol (RSTP) supports a built-in protocol migration mechanism that enables it to interoperate with legacy 802.1D switches. If an MSTP and RSTP switch receives a legacy 802.1D configuration bridge protocol data unit (BPDU) with the protocol version set to 0, it sends only 802.1D BPDUs on that port. A multiple spanning-tree (MST) switch can also detect that a port is at the boundary of a region when it receives a legacy BPDU, an MST BPDU (version 3) associated with a different region, or an RST BPDU (version 2).
-------------------------	---

However, the switch does not automatically revert to the MSTP mode if it no longer receives 802.1D BPDUs because it cannot determine whether the legacy switch has been removed from the link unless the legacy switch is the designated switch. Use the **clear spanning-tree detected-protocols** command in this situation.

Examples	This example shows how to restart the protocol migration process on Fast Ethernet interface 0/1:
	<pre>Switch# clear spanning-tree detected-protocols interface fastethernet0/1</pre>

 clear vmpls statistics

clear vmpls statistics

Use the **clear vmpls statistics** privileged EXEC command to clear the statistics maintained by the VLAN Query Protocol (VQP) client.

clear vmpls statistics

Syntax Description This command has no arguments or keywords.

Defaults No default is defined.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(6)EA2	This command was introduced.

Examples This example shows how to clear VLAN Membership Policy Server (VMPS) statistics:

```
Switch# clear vmpls statistics
```

You can verify that the information was deleted by entering the **show vmpls statistics** privileged EXEC command.

Related Commands	Command	Description
	show vmpls statistics	Displays the VQP version, reconfirmation interval, retry count, VMPS IP addresses, and the current and primary servers.

clear vtp counters

Use the **clear vtp counters** privileged EXEC command to clear the VLAN Trunking Protocol (VTP) and pruning counters.

clear vtp counters

Syntax Description This command has no arguments or keywords.

Defaults No default is defined.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.0(5.2)WC(1)	This command was introduced.

Examples This example shows how to clear the VTP counters:

```
Switch# clear vtp counters
```

You can verify that the information was deleted by entering the **show vtp counters** privileged EXEC command.

Related Commands	Command	Description
	show vtp counters	Displays general information about the VTP management domain, status, and counters.

 ■ cluster commander-address

cluster commander-address

You do not need to enter this command. The command switch automatically provides its MAC address to member switches when these switches join the cluster. The member switch adds this information and other cluster information to its running configuration file. Enter the **no** form of this global configuration command from the member switch console port to remove it from a cluster only during debugging or recovery procedures.

cluster commander-address *mac-address* [member *number* name *name*]

no cluster commander-address

Syntax Description

<i>mac-address</i>	MAC address of the cluster command switch.
<i>member number</i>	(Optional) Number of a configured member switch. The range is from 0 to 15.
<i>name name</i>	(Optional) Name of the configured cluster up to 31 characters.

Defaults

The switch is not a member of any cluster.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5.2)WC(1)	This command was introduced.

Usage Guidelines

A cluster member can have only one command switch.

The member switch retains the identity of the command switch during a system reload by using the *mac-address* parameter.

You can enter the **no** form on a member switch to remove it from the cluster during debugging or recovery procedures. You would normally use this command from the member switch console port only when the member has lost communication with the command switch. With normal switch configuration, we recommend that you remove member switches only by entering the **no cluster member *n*** global configuration command on the command switch.

When a standby command-switch becomes active (becomes the command switch), it removes the cluster commander-address line from its configuration.

Examples

This is an example of text from the running configuration of a cluster member:

```
Switch(config)# show running-config
<output truncated>
cluster commander-address 00e0.9bc0.a500 member 4 name my_cluster
<output truncated>
```

This example shows how to remove a member from the cluster by using the cluster member console:

```
Switch# configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Switch(config)# no cluster commander-address
```

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

Related Commands	Command	Description
	show cluster	Displays the cluster status and a summary of the cluster to which the switch belongs.
	show running-config	Displays the configuration information running on the switch. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 > Cisco IOS File Management Commands > Configuration File Commands .

 ■ cluster discovery hop-count

cluster discovery hop-count

Use the **cluster discovery hop-count** global configuration command on the command switch to set the hop-count limit for extended discovery of candidate switches. Use the **no** form of this command to set the hop count to the default value.

cluster discovery hop-count *number*

no cluster discovery hop-count

Syntax Description	<i>number</i>	Number of hops from the cluster edge that the command switch limits the discovery of candidates. The range is from 1 to 7.
---------------------------	---------------	--

Defaults	The hop count is set to 3.
-----------------	----------------------------

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

Command History	Release	Modification
	12.0(5.2)WC(1)	This command was introduced.

Usage Guidelines	Enter this command only on the command switch. This command does not operate on member switches. If the hop count is set to 1, it disables extended discovery. The command switch discovers only candidates that are one hop from the edge of the cluster. The edge of the cluster is the point between the last discovered member switch and the first discovered candidate switch.
-------------------------	--

Examples	This example shows how to set the hop count limit to 4. This command is entered on the command switch.
-----------------	--

```
Switch(config)# cluster discovery hop-count 4
```

You can verify your settings by entering the **show cluster** privileged EXEC command on the command switch.

Related Commands	Command	Description
	show cluster	Displays the cluster status and a summary of the cluster to which the switch belongs.
	show cluster candidates	Displays a list of candidate switches.

cluster enable

Use the **cluster enable** global configuration command on a command-capable switch to enable it as the cluster command switch, assign a cluster name, and optionally assign a member number to it. Use the **no** form of the command to remove all members and make the command switch a candidate switch.

cluster enable *name* [*command-switch-member-number*]

no cluster enable

Syntax Description	<i>name</i> <i>command-switch-member-number</i>	Name of the cluster up to 31 characters. Valid characters include only alphanumerics, dashes, and underscores. (Optional) Assign a member number to the command switch of the cluster. The range is from 0 to 15.
--------------------	--	--

Defaults The switch is not a command switch.

No cluster name is defined.

The member number is 0 when this is the command switch.

Command Modes Global configuration

Command History	Release	Modification
	12.0(5.2)WC(1)	This command was introduced.

Usage Guidelines This command runs on any command-capable switch that is not part of any cluster. This command fails if a device is already configured as a member of the cluster.

You must name the cluster when you enable the command switch. If the switch is already configured as the command switch, this command changes the cluster name if it is different from the previous name.

Examples This example shows how to enable the command switch, name the cluster, and set the command switch member number to 4:

```
Switch(config)# cluster enable Engineering-IDF4 4
```

You can verify your settings by entering the **show cluster** privileged EXEC command on the command switch.

Related Commands	Command	Description
	show cluster	Displays the cluster status and a summary of the cluster to which the switch belongs.

cluster holdtime

Use the **cluster holdtime** global configuration command on the command switch to set the duration in seconds before a switch (either the command or member switch) declares the other switch down after not receiving heartbeat messages. Use the **no** form of this command to set the duration to the default value.

cluster holdtime *holdtime-in-secs*

no cluster holdtime

Syntax Description	<i>holdtime-in-secs</i>	Duration in seconds before a switch (either a command or member switch) declares the other switch down. The range is from 1 to 300 seconds.
---------------------------	-------------------------	---

Defaults	The holdtime is 80 seconds.
-----------------	-----------------------------

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

Command History	Release	Modification
	12.0(5.2)WC(1)	This command was introduced.

Usage Guidelines Use this command with the **cluster timer** global configuration command only on the command switch. The command switch propagates the values to all its cluster members so that the setting is consistent among all switches in the cluster.

The holdtime is typically set as a multiple of the interval timer (**cluster timer**). For example, it takes (holdtime-in-secs divided by interval-in-secs) number of heartbeat messages to be missed in a row to declare a switch down.

Examples This example shows how to change the interval timer and the duration on the command switch:

```
Switch(config)# cluster timer 3
Switch(config)# cluster holdtime 30
```

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

Related Commands	Command	Description
	show cluster	Displays the cluster status and a summary of the cluster to which the switch belongs.

cluster management-vlan

Use the **cluster management-vlan** global configuration command on the command switch to change the management VLAN for the entire cluster. Use the **no** form of this command to change the management VLAN to VLAN 1.

cluster management-vlan *n*

no cluster management-vlan

Syntax Description	<i>n</i> VLAN ID of the new management VLAN. Valid VLAN IDs are from 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1001 when the standard software image (SI) is installed. Do not enter leading zeros.
---------------------------	---

Defaults	The default management VLAN is VLAN 1.
-----------------	--

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

Command History	Release	Modification
	12.0(5.2)WC(1)	This command was introduced.

Usage Guidelines	Enter this command only on the command switch. This command changes the management VLAN of the command switch and member switches. Member switches must have either a trunk connection or connection to the new command-switch management VLAN to maintain communication with the command switch.
	This command is not written to the configuration file.

Examples	This example shows how to change the management VLAN to VLAN 5 on the entire cluster:
	<pre>Switch(config)# cluster management-vlan 5</pre>

You can verify your settings by entering the **show interfaces vlan *vlan-id*** privileged EXEC command.

Related Commands	Command	Description
	show interfaces	Displays the administrative and operational status of a switching (nonrouting) port.

cluster member

Use the **cluster member** global configuration command on the command switch to add members to a cluster. Use the **no** form of the command to remove members from the cluster.

cluster member [n] mac-address H.H.H [password enable-password] [vlan vlan-id]

no cluster member n

Syntax Description	<table border="0"> <tr> <td>n</td><td>(Optional) The number that identifies a cluster member. The range is from 0 to 15.</td></tr> <tr> <td>mac-address H.H.H</td><td>MAC address of the member switch in hexadecimal format.</td></tr> <tr> <td>password enable-password</td><td>(Optional) Enable password of the candidate switch. The password is not required if there is no password on the candidate switch.</td></tr> <tr> <td>vlan vlan-id</td><td>(Optional) VLAN ID through which the candidate is added to the cluster by the command switch. The range is 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1001 when the standard software image (SI) is installed. Do not enter leading zeros.</td></tr> </table>	n	(Optional) The number that identifies a cluster member. The range is from 0 to 15.	mac-address H.H.H	MAC address of the member switch in hexadecimal format.	password enable-password	(Optional) Enable password of the candidate switch. The password is not required if there is no password on the candidate switch.	vlan vlan-id	(Optional) VLAN ID through which the candidate is added to the cluster by the command switch. The range is 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1001 when the standard software image (SI) is installed. Do not enter leading zeros.
n	(Optional) The number that identifies a cluster member. The range is from 0 to 15.								
mac-address H.H.H	MAC address of the member switch in hexadecimal format.								
password enable-password	(Optional) Enable password of the candidate switch. The password is not required if there is no password on the candidate switch.								
vlan vlan-id	(Optional) VLAN ID through which the candidate is added to the cluster by the command switch. The range is 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1001 when the standard software image (SI) is installed. Do not enter leading zeros.								

Defaults A newly enabled command switch has no associated cluster members.

Command Modes Global configuration

Command History	Release	Modification
	12.0(5.2)WC(1)	This command was introduced.

Usage Guidelines Enter this command only on the command switch to add a member to or remove a member from the cluster. If you enter this command on a switch other than the command switch, the switch rejects the command and displays an error message.

You must enter a member number to remove a switch from the cluster. However, you do not need to enter a member number to add a switch to the cluster. The command switch selects the next available member number and assigns it to the switch that is joining the cluster.

You must enter the enable password of the candidate switch for authentication when it joins the cluster. The password is not saved in the running or startup configuration. After a candidate switch becomes a member of the cluster, its password becomes the same as the command-switch password.

If a switch does not have a configured host name, the command switch appends a member number to the command-switch host name and assigns it to the member switch.

If you do not specify a VLAN ID, the command switch automatically chooses a VLAN and adds the candidate to the cluster.

Examples

This example shows how to add a switch as member 2 with MAC address 00E0.1E00.2222 and the password *key* to a cluster. The command **switch** adds the candidate to the cluster through VLAN 3.

```
Switch(config)# cluster member 2 mac-address 00E0.1E00.2222 password key vlan 3
```

This example shows how to add a switch with MAC address 00E0.1E00.3333 to the cluster. This switch does not have a password. The command **switch** selects the next available member number and assigns it to the switch joining the cluster:

```
Switch(config)# cluster member mac-address 00E0.1E00.3333
```

You can verify your settings by entering the **show cluster members** privileged EXEC command on the command switch.

Related Commands

Command	Description
show cluster	Displays the cluster status and a summary of the cluster to which the switch belongs.
show cluster candidates	Displays a list of candidate switches.
show cluster members	Displays information about the cluster members.

cluster run

cluster run

Use the **cluster run** global configuration command to enable clustering on a switch. Use the **no** form of this command to disable clustering on a switch.

cluster run

no cluster run

Defaults

Clustering is enabled on all switches.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5.2)WC(1)	This command was introduced.

Usage Guidelines

When you enter the **no cluster run** command on a command switch, the command switch is disabled. Clustering is disabled, and the switch cannot become a candidate switch.

When you enter the **no cluster run** command on a member switch, it is removed from the cluster. Clustering is disabled, and the switch cannot become a candidate switch.

When you enter the **no cluster run** command on a switch that is not part of a cluster, clustering is disabled on this switch. This switch cannot then become a candidate switch.

Examples

This example shows how to disable clustering on the command switch:

```
Switch(config)# no cluster run
```

You can verify that clustering is disabled by entering the **show cluster** privileged EXEC command.

Related Commands

Command	Description
show cluster	Displays the cluster status and a summary of the cluster to which the switch belongs.

cluster standby-group

Use the **cluster standby-group** global configuration command to enable command switch redundancy by binding the Hot Standby Router Protocol (HSRP) standby group to the cluster. Use the **no** form of this command to unbind the cluster from the HSRP standby group.

cluster standby-group *HSRP-group-name*

no cluster standby-group

Syntax Description	<i>HSRP-group-name</i>	Name of the HSRP group that is bound to the cluster. The group name is limited to 32 characters.
---------------------------	------------------------	--

Defaults The cluster is not bound to any HSRP group.

Command Modes Global configuration

Command History	Release	Modification
	12.0(5.2)WC(1)	This command was introduced.

Usage Guidelines You must enter this command only on the command switch. If you enter it on a member switch, an error message appears.

The command switch propagates the cluster-HSRP binding information to all members. Each member switch stores the binding information in its nonvolatile RAM (NVRAM).

The HSRP group name must be a valid standby group; otherwise, the command entry produces an error.

Use the same group name on all members of the HSRP standby group that is to be bound to the cluster. Use the same HSRP group name on all cluster-HSRP capable members for the HSRP group that is to be bound. (When not binding a cluster to an HSRP group, you can use different names on the cluster command and the member switches.)

Examples This example shows how to bind the HSRP group named *my_hsrp* to the cluster. This command is entered on the command switch.

```
Switch(config)# cluster standby-group my_hsrp
```

This example shows the error message when this command is entered on a command switch and the specified HSRP standby group does not exist:

```
Switch(config)# cluster standby-group my_hsrp
%ERROR:Standby (my_hsrp) group does not exist
```

cluster standby-group

This example shows the error message when this command is entered on a member switch:

```
Switch(config)# cluster standby-group my_hsrp
%ERROR:This command runs on a cluster command switch
```

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

Related Commands	Command	Description
	show cluster	Displays the cluster status and a summary of the cluster to which the switch belongs.
	show standby	Displays standby group information.
	standby ip	Enables HSRP on the interface.

cluster timer

Use the **cluster timer** global configuration command on the command switch to set the interval in seconds between heartbeat messages. Use the **no** form of this command to set the interval to the default value.

cluster timer *interval-in-secs*

no cluster timer

Syntax Description	<i>interval-in-secs</i>	Interval in seconds between heartbeat messages. The range is from 1 to 300 seconds.
---------------------------	-------------------------	---

Defaults	The interval is 8 seconds.
-----------------	----------------------------

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

Command History	Release	Modification
	12.0(5.2)WC(1)	This command was introduced.

Usage Guidelines	Use this command with the cluster holdtime global configuration command only on the command switch. The command switch propagates the values to all its cluster members so that the setting is consistent among all switches in the cluster.
-------------------------	---

The holdtime is typically set as a multiple of the heartbeat interval timer (**cluster timer**). For example, it takes (holdtime-in-secs divided by the interval-in-secs) number of heartbeat messages to be missed in a row to declare a switch down.

Examples	This example shows how to change the heartbeat interval timer and the duration on the command switch.
-----------------	---

```
Switch(config)# cluster timer 3
Switch(config)# cluster holdtime 30
```

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

Related Commands	Command	Description
	show cluster	Displays the cluster status and a summary of the cluster to which the switch belongs.

■ controller LongReachEthernet

controller LongReachEthernet

Use the **controller LongReachEthernet** global configuration command to enter controller configuration mode.

controller LongReachEthernet *ctrlr#*

Syntax Description	<i>ctrlr#</i>	The Long-Reach Ethernet (LRE) controller number. Controller numbers are device specific. Valid entries are 0 to 2 on a 24-port LRE switch and 0 on a 8-port LRE switch.
---------------------------	---------------	---

Defaults	There is no default.
-----------------	----------------------

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

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.

Usage Guidelines	You can use this command to enter controller submode. An LRE controller is the LRE chipset in the switch.
-------------------------	---

Examples	This example shows how to enter controller configuration mode for controller 0.
-----------------	---

```
Switch(config)# controller Lo 0
Switch(config-controller)#
```

Related Commands	Command	Description
	upgrade binary	Configures upgrades on either end of an LRE link.
	upgrade preserve	Prevents an upgrade of the local CPE controller and all remote CPE devices connected to it.

cpe duplex

Use the **cpe duplex** interface configuration command to specify the duplex mode of operation for all customer premises equipment (CPE) ports. Use the **no** form of this command to return the port to its default value.

cpe duplex {auto / full / half} [port id]

no cpe duplex {auto / full / half} [port id]

Syntax Description		
	<i>auto</i>	The port automatically detects whether to run in full- or half- duplex mode.
	<i>full</i>	The port is in full-duplex mode.
	<i>half</i>	The port is in half-duplex mode.
	<i>id</i>	(Optional) The CPE Ethernet port identifier. Valid values vary from 1 to 4, depending on CPE device.

Defaults The default is half.

Command Modes

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.

Usage Guidelines The **cpe duplex full** command sets the duplex mode to full for all the CPE Ethernet ports. A setting of **auto** places the CPE Ethernet ports in an auto-negotiate state, and a setting of **half** forces the duplex to half for all the CPE Ethernet ports.

If the keyword **port** is not specified, the value is applied globally to all the CPE Ethernet ports. If the keyword **port** is specified, the value is applied to the specified CPE Ethernet port and overrides any global speed settings.

The **cpe duplex full port 2** command sets the duplex mode of port 2 of a CPE device to full duplex. If you entered both the **cpe duplex full** command and the **cpe duplex full port 2** command, they would both be added to the configuration file, and the port specific command would take priority over the base **cpe** command.

Specifying **no cpe duplex** sets all the CPE Ethernet ports to the default setting of half duplex.

This example show how to set the CPE device to auto:

```
Switch# configure terminal  
Switch(config)# interface long 0/2  
Switch(config-if)# cpe duplex auto  
Switch(config-if)#
```

cpe duplex

This example shows how to set port 3 of a Cisco 585 LRE CPE to full duplex:

```
Switch# configure terminal
Switch(config)# interface long 0/3
Switch(config-if)# cpe duplex full port 3
Switch(config-if)#
```

This example shows how to restore port 3 of a Cisco 585 LRE CPE to the default mode of half duplex:

```
Switch# configure terminal
Switch(config)# interface long 0/3
Switch(config-if)# no cpe duplex full port 3
Switch(config-if)#
```

This example shows how the port-specific command works with the base-cpe command. Port 1 is set to full duplex, port 2 is set to half duplex, and the remainder of the ports have autonegotiation.

```
Switch# configure terminal
Switch(config)# interface long 0/4
Switch(config-if)# cpe duplex auto
Switch(config-if)# cpe duplex full port 1
Switch(config-if)# cpe duplex half port 2
```

If you enter the following command, port 1 is set to autonegotiation because the CPE device base command has a value of auto.

```
Switch(config-if)# no cpe duplex full port
```

Related Commands

Command	Description
cpe speed	Specifies the CPE port speed settings.
show interfaces	Displays CPE Ethernet ports connection, speed, or duplex status when the cpe parameter is specified.

cpe protected

Use the **cpe protected** interface configuration command to restrict data traffic to individual ports on Cisco 585 LRE customer premises equipment (CPE) ports. Use the **no** form of this command to allow different ports on the same CPE device to exchange data directly.

cpe protected [port id]

no cpe protected [port id]

Syntax Description	port id (Optional) The CPE Ethernet port identifier. Valid values vary from 1 to 4, depending on CPE device.
---------------------------	--

Defaults The default is **no cpe protected**.

Command Modes Interface configuration

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.

Usage Guidelines Even though you can protect an LRE interface using the **switchport protected** command, that command does not protect individual CPE Ethernet ports. To ensure that data traffic from one CPE port is not accessed on any of the other three ports, use the **cpe protected** command. The **cpe protected** command restricts CPE traffic, either at the CPE device level or at the individual port level for data security. By specifying the **cpe protected** command without a CPE port, data is protected for all applicable CPE ports. By specifying the additional **port id** parameters, you can protect an individual CPE Ethernet port.

When protecting individual CPE ports, always specify a minimum of two ports. A single port that is configured as protected has no effect. Data traffic does not flow between two ports that are protected.

Examples This example shows how to protect CPE port 1 on Long-Reach Ethernet 0/1:

```
Switch# configure terminal
Switch(config)# interface long 0/2
Switch(config-if)# cpe protected port 1
Switch(config-if)#

```

Related Commands	Command	Description
	show controllers lre	Shows CPE protected port information.
	cpe protected	
	switchport protected	Isolates unicast, multicast, and broadcast traffic at Layer 2 from other protected ports on the same switch.

cpe shutdown

cpe shutdown

Use the **cpe shutdown** interface configuration command to disable one or more customer premises equipment (CPE) ports. Use the **no** form of this command to enable a port.

cpe shutdown [port id]

no cpe shutdown [port id]

Syntax Description	<i>id</i>	(Optional) The CPE Ethernet port identifier. Valid values vary from 1 to 4, depending on the CPE device.
---------------------------	-----------	--

Defaults	The default is that the ports are enabled.
-----------------	--

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

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.

Usage Guidelines	The cpe shutdown command operates in a similar method as the speed and duplex commands. The CPE Ethernet ports can be shut down at the CPE device level and the port level. If you add a configuration at the CPE device level and at the port level, you must request the no form of the command for both configurations to return the port to the default state.
-------------------------	--

If the keyword **port** is not specified, the value is applied globally to all the CPE Ethernet ports. If the keyword **port** is specified, the value is applied to the specified CPE Ethernet port and overrides any global speed settings.

Examples	This example shows how to disable all ports on the CPE device:
-----------------	--

```
Switch# configure terminal
Switch(config)# interface long 0/2
Switch(config-if)# cpe shutdown
Switch(config-if)#
```

This example shows how to disable port 2 on the CPE device:

```
Switch# configure terminal
Switch(config)# interface long 0/2
Switch(config-if)# cpe shutdown port 2
Switch(config-if)#
```

This example shows how to enable all CPE Ethernet ports that do not have a port-specific shutdown configured. If you followed this **no cpe shutdown** command after the previous example, port 2 continues to be shutdown because a port -specific shutdown command was entered. The **no cpe shutdown port 2** is the only way to enable the port.

```
Switch# configure terminal
Switch(config)# interface long 0/2
Switch(config-if)# no cpe shutdown
Switch(config-if)#
```

Related Commands

Command	Description
show interfaces	Displays CPE Ethernet ports connection, speed, or duplex status when the cpe parameter is specified.
shutdown	Disables the LRE transmitter of an LRE interface.

cpe speed

cpe speed

Use the **cpe speed** interface configuration command to set the speed of an customer premises equipment (CPE) port. Use the **no** form of this command to return a CPE port to the default setting.

cpe speed [auto | 10 | 100] [port id]

no cpe speed [auto | 10 | 100] [port id]

Syntax Description	auto	The port automatically detects whether it should run at 10 or 100 Mbps.
	10	The port runs at 10 Mbps.
	100	The port runs at 100 Mbps.
	port id	(Optional) The CPE Ethernet port identifier. Valid values vary from 1 to 4, depending on the CPE device.

Defaults

The default speed is **auto**.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(11)YJ	This command was introduced.

Usage Guidelines

If the keyword **port** is not specified, the value is applied globally to all the CPE Ethernet ports. If the keyword **port** is specified, the value is applied to the specified CPE Ethernet port and overrides any global speed settings.

Examples

This example shows how to set port 1 on a CPE to 100 Mbps:

```
Switch# configure terminal
Switch(config)# interface long 0/2
Switch(config-if)# cpe speed 100 port 1
Switch(config-if)#
```

This example shows how to restore the default setting of auto to all CPE Ethernet ports that do not have a port-specific speed configured:

```
Switch# configure terminal
Switch(config)# interface long 0/2
Switch(config-if)# no cpe speed 100
Switch(config-if)#
```

This example shows how the port-specific command works with the base CPE command. Port 1 is set to 10 Mbps, port 2 is set to 100 Mbps, and the remainder of the ports have autonegotiation.

```
Switch# configure terminal
Switch(config)# interface long 0/4
Switch(config-if)# cpe speed auto
Switch(config-if)# cpe speed 10 port 1
Switch(config-if)# cpe speed 100 port 2
```

If you enter this command, port 1 is set to autonegotiation because the CPE device base command has a value of auto.

```
Switch(config-if)# no cpe speed 10 port
```

Related Commands

Command	Description
show interfaces	Displays connection, speed, and duplex settings for CPE Ethernet ports attached to the specified LRE switch port.
local duplex	Sets the port speed for LRE ports.

cpe type

cpe type

Use the **cpe type** interface configuration command to set the type of an customer premises equipment (CPE) port that is connected to a Long-Reach Ethernet (LRE) switch.

cpe type [CISCO575-LRE | CISCO585-LRE | unknown]

Syntax Description This command has no arguments or keywords.

Defaults The default is **unknown**.

Command Modes Interface configuration

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.

Usage Guidelines This command can only be configured when the port is shut down. If the link is active on a CPE device port, the switch detects the CPE device type and automatically modifies the configuration. You cannot change the CPE device type on active links. For example, if the active CPE device type is **CISCO575-LRE**, you cannot change the type to **CISCO585-LRE** or **unknown**.

Examples This example shows how to set the CPE device type to CISCO585-LRE while the link is down:

```
Switch# configure terminal
Switch(config)# interface long 0/2
Switch(config-if)# cpe type CISCO585-LRE
Switch(config-if)#
```

Related Commands	Command	Description
	show interfaces	Displays connection, speed, and duplex settings for CPE Ethernet ports attached to the specified LRE switch port.

define interface-range

Use the **define interface-range** global configuration command to create an interface-range macro. Use the **no** form of this command to delete the defined macro.

define interface-range *macro-name* *interface-range*

no define interface-range *macro-name* *interface-range*

Syntax Description

<i>macro-name</i>	Name of the interface-range macro; up to 32 characters.
<i>interface-range</i>	Interface range; for valid values for interface ranges, see “Usage Guidelines.”

Defaults

This command has no default setting.

Command Modes

Global configuration

Command History

Release	Modification
12.1(6)EA2	This command was introduced.

Usage Guidelines

The macro name is a 32-character maximum character string.

A macro can contain up to five ranges.

All interfaces in a range must be the same type; that is, all Fast Ethernet ports, all Gigabit Ethernet ports, all EtherChannel ports, or all VLANs, but you can combine multiple interface types in a macro.

When entering the *interface-range*, use this format:

- *type* {*first-interface*} - {*last-interface*}
- You must add a space between the first interface number and the hyphen when entering an *interface-range*. For example, **gigabitethernet 0/1 -2** is a valid range; **gigabitethernet 0/1-2** is not a valid range.

Valid values for *type* and *interface*:

- **vlan** *vlan-id*, where *vlan-id* is from 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1001 when the standard software image (SI) is installed.
- **port-channel** *port-channel-number*, where *port-channel-number* is from 1 to 6
- **fastethernet** *interface-id*
- **gigabitethernet** *interface-id*

VLAN interfaces must have been configured with the **interface vlan** command (the **show running-config** privileged EXEC command displays the configured VLAN interfaces). VLAN interfaces not displayed by the **show running-config** command cannot be used in *interface-ranges*.

■ define interface-range

For physical interfaces, the *interface-id* is defined as a slot/number (where slot is always 0 for the switch), and the range can be entered as *type 0/number - number* (for example, **gigabitethernet0/1 - 2**). You can also enter multiple ranges.

When you define a range, you must enter a space before and after the hyphen (-):

```
interface range gigabitethernet0/1 - 2
```

When you define multiple ranges, you must enter a space before and after the comma (,):

```
interface range fastethernet0/3 - 7 , gigabitethernet0/1 - 2
```

Examples

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

```
Switch(config)# define interface-range macro1 fastethernet 0/3 -7 , gigabitethernet 0/2
```

Related Commands

Command	Description
interface range	Executes a command on multiple ports at the same time.
show running-config	Displays the current operating configuration, including defined macros. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 > Cisco IOS File Management Commands > Configuration File Commands .

delete

Use the **delete** privileged EXEC command to delete a file or directory on the Flash memory device.

delete [/force] [/recursive] filesystem:/file-url

Syntax Description

/force	(Optional) Suppress the prompt that confirms the deletion.
/recursive	(Optional) Delete the named directory and all subdirectories and the files contained in it.
filesystem:	Alias for a Flash file system. Use flash: for the system board Flash device.
/file-url	The path (directory) and filename to delete.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5.2)WC(1)	This command was introduced.
12.1(6)EA2	The /force and /recursive keywords were added.

Usage Guidelines

If you use the **/force** keyword, you are prompted once at the beginning of the deletion process to confirm the deletion.

If you use the **/recursive** keyword without the **/force** keyword, you are prompted to confirm the deletion of every file.

The prompting behavior depends on the setting of the **file prompt** global configuration command. By default, the switch prompts for confirmation on destructive file operations. For more information about this command, refer to the *Cisco IOS Command Reference for Release 12.1*.

Examples

This example shows how to delete a file from the switch Flash memory:

```
Switch# delete flash:filename
```

You can verify that the directory was removed by entering the **dir filesystem:** privileged EXEC command.

Related Commands

Command	Description
copy	Downloads a file from a source, such as a TFTP server, to a destination, such as the Flash memory.
dir filesystem:	Displays a list of files on a file system.
rename	Renames a file.

■ deny (access-list configuration)

deny (access-list configuration)

Use the **deny** access-list configuration command to configure conditions for a named or numbered IP access control list (ACL). Use the **no** form of the command to remove a deny condition from the IP ACL.

Use these commands with standard IP ACLs:

deny {*source source-wildcard* | **host** *source* | **any**}

no deny {*source source-wildcard* | **host** *source* | **any**}

Use these commands with extended IP ACLs:

deny *protocol* {*source source-wildcard* | **host** *source* | **any**} [*operator port*] {*destination destination-wildcard* | **host** *source* | **any**} [*operator port*] [**dscp** *dscp-value*] [**time-range** *time-range-name*]

no deny *protocol* {*source source-wildcard* | **host** *source* | **any**} [*operator port*] {*destination destination-wildcard* | **host** *source* | **any**} [*operator port*] [**dscp** *dscp-value*] [**time-range** *time-range-name*]

This command is available on physical interfaces only if your switch is running the enhanced software image (EI).

Syntax Description	protocol	Name of an IP protocol. <i>protocol</i> can be ip , tcp , or udp .
source source-wildcard host source any		Define a source IP address and wildcard. The <i>source</i> is the source address of the network or host from which the packet is being sent, specified in one of these ways: <ul style="list-style-type: none"> The 32-bit quantity in dotted-decimal format. The <i>source-wildcard</i> applies wildcard bits to the source. The keyword host, followed by the 32-bit quantity in dotted-decimal format, as an abbreviation for <i>source</i> and <i>source-wildcard</i> of <i>source</i> 0.0.0.0. The keyword any as an abbreviation for <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255. You do not need to enter a source-wildcard.
destination		Define a destination IP address and wildcard.
destination-wildcard host destination any		The <i>destination</i> is the destination address of the network or host to which the packet is being sent, specified in one of these ways: <ul style="list-style-type: none"> The 32-bit quantity in dotted-decimal format. The <i>destination-wildcard</i> applies wildcard bits to the destination. The keyword host, followed by the 32-bit quantity in dotted-decimal format, as an abbreviation for <i>destination</i> and <i>destination-wildcard</i> of <i>destination</i> 0.0.0.0. The keyword any as an abbreviation for <i>destination</i> and <i>destination-wildcard</i> of 0.0.0.0 255.255.255.255. You do not need to enter a destination-wildcard.

<i>operator port</i>	(Optional) Define a source or destination port. The <i>operator</i> can be only eq (equal). If <i>operator</i> is after the source IP address and wildcard, conditions match when the source port matches the defined port. If <i>operator</i> is after the destination IP address and wildcard, conditions match when the destination port matches the defined port. The <i>port</i> is a decimal number or name of a Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) port. The number can be from 0 to 65535. Use TCP port names only for TCP traffic. Use UDP port names only for UDP traffic.
dscep <i>dscep-value</i>	(Optional) Define a Differentiated Services Code Point (DSCP) value to classify traffic. For the <i>dscep-value</i> , enter any of the 13 supported DSCP values (0, 8, 10, 16, 18, 24, 26, 32, 34, 40, 46, 48, and 56), or use the question mark (?) to see a list of available values.
time-range <i>time-range-name</i>	(Optional) For the time-range keyword, enter a meaningful name to identify the time range. For a more detailed explanation of this keyword, refer to the software configuration guide.

Defaults

There are no specific conditions that deny packets in the named or numbered IP ACL.
The default ACL is always terminated by an implicit deny statement for all packets.

Command Modes

Access-list configuration

Command History

Release	Modification
12.1(6)EA2	This command was introduced.

Usage Guidelines

Use this command after the **ip access-list** global configuration command to specify deny conditions for an IP ACL. You can specify a source IP address, destination IP address, IP protocol, TCP port, or UDP port. Specify the TCP and UDP port numbers only if *protocol* is **tcp** or **udp** and *operator* is **eq**.



Note For more information about configuring IP ACLs, refer to the “Configuring Network Security with ACLs” chapter in the *Catalyst 2950 Desktop Switch Software Configuration Guide* for this release.

Examples

This example shows how to create an extended IP ACL and to configure deny conditions for it:

```
Switch(config)# ip access-list extended Internetfilter
Switch(config-ext-nacl)# deny tcp host 190.5.88.10 any
Switch(config-ext-nacl)# deny tcp host 192.1.10.10 any
```

■ deny (access-list configuration)

This is an example of a standard ACL that sets a deny condition:

```
ip access-list standard Acclist1
deny 192.5.34.0 0.0.0.255
deny 128.88.10.0 0.0.0.255
deny 36.1.1.0 0.0.0.255
```



Note In these examples, all other IP access is implicitly denied.

You can verify your settings by entering the **show ip access-lists** or **show access-lists** privileged EXEC command.

Related Commands

Command	Description
ip access-list	Defines an IP ACL.
permit (access-list configuration)	Sets conditions for an IP ACL.
ip access-group	Controls access to an interface.
show ip access-lists	Displays IP ACLs configured on the switch.
show access-lists	Displays ACLs configured on a switch.

deny (MAC access-list configuration)

Use the **deny** MAC access-list configuration command to prevent Layer 2 traffic from being forwarded if the conditions are matched. Use the **no** form of the command to remove a deny condition from the MAC named access control list (ACL).

```
{permit | deny} {any | host src-MAC-addr} {any | host dst-MAC-addr} [aarp | amber | appletalk | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 | etype-8042 | lat | lavc-sca | mop-console | mop-dump | msdos | mumps | netbios | vines-echo |vines-ip | xns-idp]

no {permit | deny} {any | host src-MAC-addr} {any | host dst-MAC-addr} [aarp | amber | appletalk | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 | etype-8042 | lat | lavc-sca | mop-console | mop-dump | msdos | mumps | netbios | vines-echo |vines-ip | xns-idp]
```

This command is available only if your switch is running the enhanced software image (EI).

Syntax Description

any	Keyword to deny any source or destination MAC address.
host src-MAC-addr	Define a host MAC address. If the source address for a packet matches the defined address, traffic from that address is denied. MAC address-based subnets are not allowed.
host dst-MAC-addr	Define a destination MAC address. If the destination address for a packet matches the defined address, traffic to that address is denied. MAC address-based subnets are not allowed.
aarp	Select EtherType AppleTalk Address Resolution Protocol that maps a data-link address to a network address.
amber	Select EtherType DEC-Amber.
appletalk	Select EtherType AppleTalk/EtherTalk.
dec-spanning	Select EtherType Digital Equipment Corporation (DEC) spanning tree.
decnet-iv	Select EtherType DECnet Phase IV protocol.
diagnostic	Select EtherType DEC-Diagnostic.
dsm	Select EtherType DEC-DSM.
etype-6000	Select EtherType 0x6000.
etype-8042	Select EtherType 0x8042.
lat	Select EtherType DEC-LAT.
lavc-sca	Select EtherType DEC-LAVC-SCA.
mop-console	Select EtherType DEC-MOP Remote Console.
mop-dump	Select EtherType DEC-MOP Dump.
msdos	Select EtherType DEC-MSDOS.
mumps	Select EtherType DEC-MUMPS.

■ deny (MAC access-list configuration)

netbios	Select EtherType DEC-Network Basic Input/Output System (NETBIOS).
vines-echo	Select EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems.
vines-ip	Select EtherType VINES IP.
xns-idp	Select EtherType Xerox Network Systems (XNS) protocol suite (from 0 to 65535), an arbitrary Ethertype in decimal, hexadecimal, or octal.

Defaults

This command has no defaults. However, the default action for a MAC named ACL is to deny.

Command Modes

MAC access-list configuration

Command History

Release	Modification
12.1(6)EA2	This command was introduced.

Usage Guidelines

When an access control entry (ACE) is added to an ACL, an implied **deny-any-any** condition exists at the end of the list. That is, if there are no matches, the packets are denied. However, before the first ACE is added, the list permits all packets.

These options are not allowed:

- Class of service (CoS)
- Ethertype number of a packet with Ethernet II or Subnetwork Access Protocol (SNAP) encapsulation
- Link Service Access Point (LSAP) number of a packet with 802.2 encapsulation

**Note**

For more information about configuring MAC extended ACLs, refer to the “Configuring Network Security with ACLs” chapter in the *Catalyst 2950 Desktop Switch Software Configuration Guide* for this release.

Examples

This example shows how to define the MAC named extended ACL to deny NETBIOS traffic from any source to MAC address 00c0.00a0.03fa. Traffic matching this list is denied.

```
Switch(config-ext-macl)# deny any host 00c0.00a0.03fa netbios
```

This example shows how to remove the deny condition from the named MAC extended ACL:

```
Switch(config-ext-macl)# no deny any host 00c0.00a0.03fa netbios
```

You can verify your settings by entering the **show access-lists** privileged EXEC command.

Related Commands

Command	Description
mac access-list extended	Creates an ACL based on MAC addresses for non-IP traffic.
permit (MAC access-list configuration)	Permits Layer 2 traffic to be forwarded if conditions are matched.
show access-lists	Displays ACLs configured on a switch.

dot1x default

dot1x default

Use the **dot1x default** global configuration command to reset the global 802.1X parameters to their default values.

dot1x default

Syntax Description This command has no arguments or keywords.

Defaults This command has no default setting.

Command Modes Global configuration

Command History	Release	Modification
	12.1(6)EA2	This command was introduced.

Examples This example shows how to reset the global 802.1X parameters:

```
Switch(config)# dot1x default
```

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

Related Commands	Command	Description
	dot1x max-req	Sets the maximum number of times that the switch sends an Extensible Authentication Protocol (EAP)-request/identity frame before restarting the authentication process.
	dot1x re-authentication	Enables periodic re-authentication of the client.
	dot1x timeout quiet-period	Sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange.
	dot1x timeout re-authperiod	Sets the number of seconds between re-authentication attempts.
	dot1x timeout tx-period	Sets the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request.
	show controllers lre version	Displays the 802.1X statistics, administrative status, and operational status for the switch or for the specified interface.

dot1x max-req

Use the **dot1x max-req** global configuration command to set the maximum number of times that the switch sends an Extensible Authentication Protocol (EAP)-request/identity frame (assuming that no response is received) before restarting the authentication process. Use the **no** form of this command to return to the default setting.

dot1x max-req *count*

no dot1x max-req

Syntax Description	<i>count</i>	Number of times that the switch sends an EAP-request/identify frame before restarting the authentication process. The range is 1 to 10.
Defaults	The default is 2 times.	
Command Modes	Global configuration	
Command History	Release	Modification
	12.1(6)EA2	This command was introduced.
Usage Guidelines	You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers.	
Examples	This example shows how to set the number of times that the switch sends an EAP-request/identity frame to 5 before restarting the authentication process: Switch(config)# dot1x max-req 5	
	You can verify your settings by entering the show dot1x privileged EXEC command.	
Related Commands	Command	Description
	dot1x timeout tx-period	Sets the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request.
	show controllers lre version	Displays the 802.1X statistics, administrative status, and operational status for the switch or for the specified interface.

dot1x multiple-hosts

dot1x multiple-hosts

Use the **dot1x multiple-hosts** interface configuration command to allow multiple hosts (clients) on an 802.1X-authorized port that has the **dot1x port-control** interface configuration command set to **auto**. Use the **no** form of this command to return to the default setting.

dot1x multiple-hosts

no dot1x multiple-hosts

Syntax Description This command has no arguments or keywords.

Defaults Multiple hosts are disabled.

Command Modes Interface configuration

Command History	Release	Modification
	12.1(6)EA2	This command was introduced.

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

Examples This example shows how to enable 802.1X on Fast Ethernet interface 0/1 and to allow multiple hosts:

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x multiple-hosts
```

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

Related Commands	Command	Description
	dot1x port-control	Enables manual control of the authorization state of the port.
	show controllers lre version	Displays 802.1X statistics, administrative status, and operational status for the switch or for the specified interface.

dot1x port-control

Use the **dot1x port-control** interface configuration command to enable manual control of the authorization state of the port. Use the **no** form of this command to return to the default setting.

dot1x port-control {auto | force-authorized | force-unauthorized}

no dot1x port-control

Syntax Description	auto	Enable 802.1X authentication on the interface and cause the port to transition to the authorized or unauthorized state based on the 802.1X authentication exchange between the switch and the client.
	force-authorized	Disable 802.1X authentication on the interface and cause the port to transition to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1X-based authentication of the client.
	force-unauthorized	Deny all access through this interface by forcing the port to transition to the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the interface.

Defaults

The authorization state is **force-authorized**.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(6)EA2	This command was introduced.

Usage Guidelines

The 802.1X protocol is supported on Layer 2 static-access ports.

You can use the **auto** keyword only if the port is not configured as one of these:

- Trunk port—If you try to enable 802.1X on a trunk port, an error message appears, and 802.1X is not enabled. If you try to change the mode of an 802.1X-enabled port to trunk, the port mode is not changed.
- Dynamic port—A port in dynamic mode can negotiate with its neighbor to become a trunk port. If you try to enable 802.1X on a dynamic port, an error appears, and 802.1X is not enabled. If you try to change the mode of an 802.1X-enabled port to dynamic, the port mode is not changed.
- Dynamic-access port—if you try to enable 802.1X on a dynamic-access (VLAN Query Protocol [VQP]) port, an error appears, and 802.1X is not enabled. If you try to change an 802.1X-enabled port to dynamic VLAN assignment, an error appears, and the VLAN configuration is not changed.
- EtherChannel port—Before enabling 802.1X on the port, you must first remove it from the EtherChannel. If you try to enable 802.1X on an EtherChannel or on an active port in an EtherChannel, an error appears, and 802.1X is not enabled. If you enable 802.1X on a not-yet active port of an EtherChannel, the port does not join the EtherChannel.

dot1x port-control

- Secure port—You cannot configure a secure port as an 802.1X port. If you try to enable 802.1X on a secure port, an error appears, and 802.1X is not enabled. If you try to change an 802.1X-enabled port to a secure port, an error appears, and the security settings are not changed.
- Switch Port Analyzer (SPAN) destination port—You can enable 802.1X on a port that is a SPAN destination port; however, 802.1X is disabled until the port is removed as a SPAN destination. You can enable 802.1X on a SPAN source port.

To globally disable 802.1X on the switch, you must disable it on each port. There is no global configuration command for this task.

Examples

This example shows how to enable 802.1X on Fast Ethernet interface 0/1:

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# dot1x port-control auto
```

You can verify your settings by entering the **show dot1x** privileged EXEC command and checking the Status column in the 802.1X Port Summary section of the output. An *enabled* status means the port-control value is set either to **auto** or to **force-unauthorized**.

Related Commands	Command	Description
	show controllers lre version	Displays 802.1X statistics, administrative status, and operational status for the switch or for the specified interface.

dot1x re-authenticate

Use the **dot1x re-authenticate** privileged EXEC command to manually initiate a re-authentication of all 802.1X-enabled ports or the specified 802.1X-enabled port.

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

Syntax Description	interface <i>interface-id</i> (Optional) Slot and port number of the interface to re-authenticate.
---------------------------	---

Defaults	There is no default setting.
-----------------	------------------------------

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

Command History	Release	Modification
	12.1(6)EA2	This command was introduced.

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

Examples	This example shows how to manually re-authenticate the device connected to Fast Ethernet interface 0/1:
	Switch# dot1x re-authenticate interface fastethernet0/1 Starting reauthentication on FastEthernet0/1.

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

Related Commands	Command	Description
	show controllers lre version	Displays 802.1X statistics, administrative status, and operational status for the switch or for the specified interface.

dot1x re-authentication

dot1x re-authentication

Use the **dot1x re-authentication** global configuration command to enable periodic re-authentication of the client. Use the **no** form of this command to return to the default setting.

dot1x re-authentication

no dot1x re-authentication

Syntax Description This command has no arguments or keywords.

Defaults Periodic re-authentication is disabled.

Command Modes Global configuration

Command History	Release	Modification
	12.1(6)EA2	This command was introduced.

Usage Guidelines You configure the amount of time between periodic re-authentication attempts by using the **dot1x timeout re-authperiod** global configuration command.

Examples This example shows how to disable periodic re-authentication of the client:

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

This example shows how to enable periodic re-authentication and set the number of seconds between re-authentication attempts to 4000 seconds:

```
Switch(config)# dot1x re-authentication
Switch(config)# dot1x timeout re-authperiod 4000
```

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

Related Commands

Command	Description
dot1x timeout re-authperiod	Sets the number of seconds between re-authentication attempts.
show controllers lre version	Displays 802.1X statistics, administrative status, and operational status for the switch or for the specified interface.

dot1x timeout quiet-period

Use the **dot1x timeout quiet-period** global configuration command to set the number of seconds that the switch remains in the quiet state following a failed authentication exchange (for example, the client provided an invalid password). Use the **no** form of this command to return to the default setting.

dot1x timeout quiet-period *seconds*

no dot1x timeout quiet-period

Syntax Description	<i>seconds</i>	Time in seconds that the switch remains in the quiet state following a failed authentication exchange with the client. The range is 0 to 65535 seconds.
---------------------------	----------------	---

Defaults The default time is 60 seconds.

Command Modes Global configuration

Command History	Release	Modification
	12.1(6)EA2	This command was introduced.

Usage Guidelines During the quiet period, the switch does not accept or initiate any authentication requests.

You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers.

If you want to provide a faster response time to the user, enter a smaller number than the default.

Examples This example shows how to set the quiet time on the switch to 30 seconds:

```
Switch(config)# dot1x timeout quiet-period 30
```

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

Related Commands	Command	Description
	show controllers lre version	Displays 802.1X statistics, administrative status, and operational status for the switch or for the specified interface.

dot1x timeout re-authperiod

dot1x timeout re-authperiod

Use the **dot1x timeout re-authperiod** global configuration command to set the number of seconds between re-authentication attempts. Use the **no** form of this command to return to the default setting.

dot1x timeout re-authperiod *seconds*

no dot1x timeout re-authperiod

Syntax Description	<i>seconds</i>	Number of seconds between re-authentication attempts. The range is 1 to 4294967295.						
Defaults	The default is 3600 seconds.							
Command Modes	Global configuration							
Command History	Release	Modification						
	12.1(6)EA2	This command was introduced.						
Usage Guidelines	<p>The dot1x timeout re-authperiod global configuration command affects the behavior of the switch only if you have enabled periodic re-authentication by using the dot1x re-authentication global configuration command.</p> <p>You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients or authentication servers.</p>							
Examples	<p>This example shows how to enable periodic re-authentication and set the number of seconds between re-authentication attempts to 4000 seconds:</p> <pre>Switch(config)# dot1x re-authentication Switch(config)# dot1x timeout re-authperiod 4000</pre> <p>You can verify your settings by entering the show dot1x privileged EXEC command.</p>							
Related Commands	<table border="1"> <thead> <tr> <th>Command</th><th>Description</th></tr> </thead> <tbody> <tr> <td>dot1x re-authentication</td><td>Enables periodic re-authentication of the client.</td></tr> <tr> <td>show controllers 1re version</td><td>Displays 802.1X statistics, administrative status, and operational status for the switch or for the specified interface.</td></tr> </tbody> </table>		Command	Description	dot1x re-authentication	Enables periodic re-authentication of the client.	show controllers 1re version	Displays 802.1X statistics, administrative status, and operational status for the switch or for the specified interface.
Command	Description							
dot1x re-authentication	Enables periodic re-authentication of the client.							
show controllers 1re version	Displays 802.1X statistics, administrative status, and operational status for the switch or for the specified interface.							

dot1x timeout tx-period

Use the **dot1x timeout tx-period** global configuration command to set the number of seconds that the switch waits for a response to an Extensible Authentication Protocol (EAP)-request/identity frame from the client before retransmitting the request. Use the **no** form of this command to return to the default setting.

dot1x timeout tx-period *seconds*

no dot1x timeout tx-period

Syntax Description	<i>seconds</i> Time in seconds that the switch should wait for a response to an EAP-request/identity frame from the client before retransmitting the request. The range is 1 to 65535 seconds.						
Defaults	The default is 30 seconds.						
Command Modes	Global configuration						
Command History	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>12.1(6)EA2</td><td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification	12.1(6)EA2	This command was introduced.		
Release	Modification						
12.1(6)EA2	This command was introduced.						
Usage Guidelines	You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients or authentication servers.						
Examples	<p>This example shows how to set 60 as the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request:</p> <pre>Switch(config)# dot1x timeout tx-period 60</pre> <p>You can verify your settings by entering the show dot1x privileged EXEC command.</p>						
Related Commands	<table border="1"> <thead> <tr> <th>Command</th><th>Description</th></tr> </thead> <tbody> <tr> <td>dot1x max-req</td><td>Sets the maximum number of times that the switch sends an EAP-request/identity frame before restarting the authentication process.</td></tr> <tr> <td>show controllers lre version</td><td>Displays 802.1X statistics, administrative status, and operational status for the switch or for the specified interface.</td></tr> </tbody> </table>	Command	Description	dot1x max-req	Sets the maximum number of times that the switch sends an EAP-request/identity frame before restarting the authentication process.	show controllers lre version	Displays 802.1X statistics, administrative status, and operational status for the switch or for the specified interface.
Command	Description						
dot1x max-req	Sets the maximum number of times that the switch sends an EAP-request/identity frame before restarting the authentication process.						
show controllers lre version	Displays 802.1X statistics, administrative status, and operational status for the switch or for the specified interface.						

■ duplex

duplex

Use the **duplex** interface configuration command to specify the duplex mode of operation for non-Long Reach Ethernet (LRE) switch ports. Use the **no** form of this command to return the port to its default value.

duplex {auto | full | half}

no duplex

Syntax Description	
auto	Port automatically detects whether it should run in full- or half-duplex mode.
full	Port is in full-duplex mode.
half	Port is in half-duplex mode.

Defaults For Fast Ethernet and 10/100/1000 ports, the default is **auto**.

For 100BASE-FX ports, the default is **full**.

For the default duplex mode of the Gigabit Interface Converter (GBIC)-module ports, refer to the documentation that came with your GBIC module.

For small, form-factor pluggable (SFP) Gigabit ports, the default is **auto**.

Command Modes Interface configuration

Command History	Release	Modification
	12.0(5.2)WC(1)	This command was introduced.

Usage Guidelines Applicability of this command is hardware-dependent.

Non-LRE Switches:

Certain ports, such as GBIC module ports, can be configured as either full duplex or half duplex. The applicability of this command depends on the device to which the switch is attached.

The 100BASE-FX ports on Catalyst 2950C-24 switches do not support the **duplex** command. These ports only operate in full-duplex and 100-Mbps mode.

For Fast Ethernet ports, setting the port to **auto** has the same effect as specifying **half** if the attached device does not autonegotiate the duplex parameter.

If the speed is set to **auto**, the switch negotiates with the device at the other end of the link for the speed setting and then forces the speed setting to the negotiated value. The duplex setting remains as configured on each end of the link, which could result in a duplex setting mismatch.



Note The 10/100/1000 ports can operate only in the full-duplex mode.

If both the speed and duplex are set to specific values, autonegotiation is disabled.

LRE Switches:

For Long-Reach Ethernet (LRE) switches, this command configures both the MAC and LRE chipset.

In the default configurations, LRE Gigabit ports are set to **auto**. A copper connection (10|100|1000) autonegotiates with the device at the other end of the link for the duplex setting and then forces the duplex setting to the negotiated value. A fiber-optic connection (SFP) also autonegotiates with the device at the other end of the link but only accepts a connection at full duplex.

The duplex setting for a Gigabit Ethernet port has a close relationship to the setting for speed. Fiber is always forced to 1000 Mbps full duplex. Copper can run at either full duplex or half duplex for 10|100 Mbps but is forced to full duplex for 1000 Mbps. When you force speed and duplex settings, autonegotiation is disabled, and speed and duplex settings can cause a mismatch.

**Note**

For guidelines on setting the switch speed and duplex parameters, refer to the *Catalyst 2950 Desktop Switch Hardware Installation Guide*.

Examples

This example shows how to set a Fast Ethernet port to half duplex:

```
Switch(config)# interface fastethernet0/11
Switch(config-if)# duplex half
```

This example shows how to set a Gigabit Ethernet port to full duplex:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# duplex full
```

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

Related Commands

Command	Description
show running-config	Displays the configuration information running on the switch. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 > Cisco IOS File Management Commands > Configuration File Commands .
local duplex	Specifies the LRE port speed.
cpe duplex	Sets the duplex setting for customer premises equipment (CPE) Ethernet ports.

errdisable detect

errdisable detect

Use the **errdisable detect** global configuration command to enable error disable detection. Use the **no** form of this command to disable this feature.

```
errdisable detect cause {all | dtp-flap | gbic-invalid | link-flap | pagp-flap}
```

```
no errdisable detect cause {all | dtp-flap | gbic-invalid | link-flap | pagp-flap}
```

Syntax Description	all Enable detection for all error disable causes.
dtp-flap	Enable detection for the Dynamic Trunking Protocol (DTP)- flap cause.
gbic-invalid	Enable error detection for an invalid GBIC error-disable cause.
link-flap	Enable detection for the link flap cause.
pagp-flap	Enable detection for the Port Aggregation Protocol (PAgP)-flap cause.

Defaults The default is **all**, enabled for all causes.

Command Modes Global configuration

Command History	Release	Modification
	12.1(6)EA2	This command was introduced.
	12.1(9)EA1	The bpduguard , rootguard , and udld keywords were removed. The gbic-invalid keyword was added.

Usage Guidelines A cause (**dtp-flap**, **gbic-invalid**, **link-flap**, and **pagp-flap**) is the reason why the error-disabled state occurred. When a cause is detected on an interface, the interface is placed in error-disabled state, an operational state similar to link-down state. If you do not enable errdisable recovery for the cause, the interface stays in the error-disabled state until you enter the **shutdown** and **no shutdown** interface configuration commands. If you enable the recovery for a cause, the interface is brought out of the error-disabled state and allowed to retry the operation again when all the causes have timed out.

You must enter the **shutdown** and then the **no shutdown** commands to manually recover an interface from the error-disabled state.

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

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

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

Related Commands

Command	Description
errdisable recovery	Configures the recovery mechanism variables.
show errdisable detect	Displays errdisable detection status.
show interfaces trunk	Displays interface status or a list of interfaces in error-disabled state.

errdisable recovery

errdisable recovery

Use the **errdisable recovery** global configuration command to configure the recover mechanism variables. Use the **no** form of this command to return to the default setting.

```
errdisable recovery {cause {all | bpduguard | dtp-flap | gbic-invalid | link-flap | pagp-flap | psecure-violation | udld} | {interval interval}}
no errdisable recovery {cause {all | bpduguard | dtp-flap | gbic-invalid | link-flap | pagp-flap | psecure-violation | udld} | {interval interval}}
```

Syntax Description	
cause	Enable error disable to recover from a specific cause.
all	Enable the timer to recover from all error-disable causes.
bpduguard	Enable the timer to recover from the bridge protocol data unit (BPDU)-guard error-disable state.
dtp-flap	Enable the timer to recover from the Dynamic Trunking Protocol (DTP)-flap error-disable state.
gbic-invalid	Enable the timer to recover from an invalid GBIC error disable state.
link-flap	Enable the timer to recover from the link-flap error-disable state.
pagp-flap	Enable the timer to recover from the Port Aggregation Protocol (PAgP)-flap error-disable state.
psecure-violation	Enable the timer to recover from a port security violation disable state.
udld	Enable the timer to recover from the UniDirectional Link Detection (UDLD) error-disable state.
interval <i>interval</i>	Specify the time to recover from specified error-disable state. The range is 30 to 86400 seconds. The same interval is applied to all causes. The default interval is 300 seconds.
Note The errdisable recovery timer initializes at a random differential from the configured interval value. The difference between the actual timeout value and the configured value can be up to 15 percent of the configured interval.	



Though visible in the command-line help string, the **channel-misconfig** keyword is not supported.

Defaults

Recovery is disabled for all causes.

The default interval is 300 seconds.

Command Modes

Global configuration

Command History	Release	Modification
	12.1(6)EA2	This command was introduced.
	12.1(9)EA1	The gbic-invalid and psecure-violation keywords were added. The rootguard keyword was removed.

Usage Guidelines

A cause (**bpduguard**, **dtp-flap**, **gbic-invalid**, **link-flap**, **pagg-flap**, **psecure-violation**, and **udld**) is defined as the reason why the error-disabled state occurred. When a cause is detected on an interface, the interface is placed in error-disabled state, an operational state similar to link-down state. If you do not enable errdisable recovery for the cause, the interface stays in error-disabled state until you enter a **shutdown** and **no shutdown** interface configuration command. If you enable the recovery for a cause, the interface is brought out of the error-disabled state and allowed to retry the operation again when all the causes have timed out.

Otherwise, you must enter the **shutdown** then **no shutdown** commands to manually recover an interface from the error-disabled state.

Examples

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

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

This example shows how to set the timer to 500 seconds:

```
Switch(config)# errdisable recovery interval 500
```

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

Related Commands

Command	Description
show errdisable recovery	Displays errdisable recovery timer information.
show interfaces status	Displays interface status.

flowcontrol

Use the **flowcontrol** interface configuration command to set the receive or send flow-control value for an interface. When flow control **send** is on for a device and it detects any congestion at its end, it notifies the link partner or the remote device of the congestion by sending a pause frame. When flow control **receive** is on for the remote device and it receives a pause frame, it stops sending any data packets. This prevents any loss of data packets during the congestion period.

Use the **receive off** and **send off** keywords to disable flow control.

flowcontrol {receive | send} {desired | off | on}



Note This **flowcontrol** command applies only to 10/100/1000 ports and Gigabit Interface Converter (GBIC)-module ports on the switches.

Syntax Description

receive	Sets whether the interface can receive flow-control packets from a remote device.
send	Sets whether the interface can send flow-control packets to a remote device.
desired	When used with receive , allows an interface to operate with an attached device that is required to send flow-control packets or with an attached device that is not required to but can send flow-control packets. When used with send , the interface sends flow-control packets to a remote device if the remote device supports it.
off	When used with receive , turns off an attached device's ability to send flow-control packets to an interface. When used with send , turns off the local port's ability to send flow-control packets to a remote device.
on	When used with receive , allows an interface to operate with an attached device that is required to send flow-control packets or with an attached device that is not required to but can send flow-control packets. When used with send , the interface sends flow-control packets to a remote device if the remote device supports it.

Defaults

The defaults for 10/100/1000 and GBIC-module ports are **flowcontrol receive off** and **flowcontrol send desired**.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5.2)WC(1)	This command was introduced.
12.1(6)EA2	The asymmetric and symmetric keywords were replaced with the receive , send , off , on , and desired keywords.

Usage Guidelines

Use the **flowcontrol** command only on 10/100/1000 and GBIC-module ports.

We strongly recommend that you do not configure IEEE 802.3X flowcontrol when quality of service (QoS) is configured on the switch. Before configuring flowcontrol on an interface, make sure to disable QoS on the switch.

Note that when used with **receive**, the **on** and **desired** keywords have the same result.

When you use the **flowcontrol** command to set a port to control traffic rates during congestion, you are setting flow control on a port to one of these conditions:

- **receive on and send on:** Flow control operates in both directions; pause frames can be sent by both the local device and the remote device to show link congestion.
- **receive on and send desired:** The port can receive pause frames and is able to send pause frames if the attached device supports them.
- **receive on and send off:** The port cannot send pause frames, but can operate with an attached device that is required to or is able to send pause frames; the port is able to receive pause frames.
- **receive off and send on:** The port sends pause frames if the remote device supports them, but cannot receive pause frames from the remote device.
- **receive off and send desired:** The port cannot receive pause frames, but can send pause frames if the attached device supports them.
- **receive off and send off:** Flow control does not operate in either direction. In case of congestion, no indication is given to the link partner, and no pause frames are sent or received by either device.

Table 2-3 shows the flow control resolution achieved on local and remote ports by a combination of settings. The table assumes that for **receive**, using the **desired** keyword has the same results as using the **on** keyword.

Table 2-3 Flow Control Settings and Local and Remote Port Flow Control Resolution

Flow Control Settings		Flow Control Resolution	
Local Device	Remote Device	Local Device	Remote Device
send on/receive on	send on/receive on	Sends and receives	Sends and receives
	send on/receive off	Does not send or receive	Does not send or receive
	send desired/receive on	Sends and receives	Sends and receives
	send desired/receive off	Does not send or receive	Does not send or receive
	send off/receive on	Sends and receives	Receives only
	send off/receive off	Does not send or receive	Does not send or receive
send on/receive off	send on/receive on	Does not send or receive	Does not send or receive
	send on/receive off	Does not send or receive	Does not send or receive
	send desired/receive on	Sends only	Receives only
	send desired/receive off	Does not send or receive	Does not send or receive
	send off/receive on	Sends only	Receives only
	send off/receive off	Does not send or receive	Does not send or receive

■ flowcontrol**Table 2-3 Flow Control Settings and Local and Remote Port Flow Control Resolution (continued)**

Flow Control Settings		Flow Control Resolution	
Local Device	Remote Device	Local Device	Remote Device
send desired/receive on	send on/receive on	Sends and receives	Sends and receives
	send on/receive off	Receives only	Sends only
	send desired/receive on	Sends and receives	Sends and receives
	send desired/receive off	Receives only	Sends only
	send off/receive on	Sends and receives	Receives only
	send off/receive off	Does not send or receive	Does not send or receive
send desired/receive off	send on/receive on	Does not send or receive	Does not send or receive
	send on/receive off	Does not send or receive	Does not send or receive
	send desired/receive on	Sends only	Receives only
	send desired/receive off	Does not send or receive	Does not send or receive
	send off/receive on	Sends only	Receives only
	send off/receive off	Does not send or receive	Does not send or receive
send off/receive on	send on/receive on	Receives only	Sends and receives
	send on/receive off	Receives only	Sends only
	send desired/receive on	Receives only	Sends and receives
	send desired/receive off	Receives only	Sends only
	send off/receive on	Receives only	Receives only
	send off/receive off	Does not send or receive	Does not send or receive
send off/receive off	send on/receive on	Does not send or receive	Does not send or receive
	send on/receive off	Does not send or receive	Does not send or receive
	send desired/receive on	Does not send or receive	Does not send or receive
	send desired/receive off	Does not send or receive	Does not send or receive
	send off/receive on	Does not send or receive	Does not send or receive
	send off/receive off	Does not send or receive	Does not send or receive

Examples

This example shows how to configure the local port to not support any level of flow control by the remote port:

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

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

Related Commands	Command	Description
	show interfaces counters	Displays the interface settings on a switch, including input and output flow control.

```
■ hw-module slot module-slot # upgrade lre
```

hw-module slot *module-slot* # upgrade lre

Use the **hw-module slot *module-slot* # lre upgrade lre** privileged EXEC command to perform firmware upgrades on Long-Reach Ethernet (LRE) systems.

```
hw-module slot module-slot # upgrade lre [force] [{local ctrlr unit # | remote interface-id}]
```

Syntax Description	
<i>module-slot</i> #	Physical slot that connects the local (LRE switch) and remote (customer premises equipment [CPE] device) of the upgrade.
force	(Optional) LRE binaries update by force, even when the version of the LRE binary on the switch Flash memory and the LRE binary in use are the same.
local ctrlr unit #	(Optional) The single LRE chipset for a controller at the local end of the LRE Ethernet link.
remote interface-id	(Optional) One or more chipsets on a single CPE device at the remote end of the LRE Ethernet link.

Defaults	No default is defined.
----------	------------------------

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

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.

Usage Guidelines Use the **hw-module slot *module-slot* # upgrade lre** command to start an LRE upgrade. An LRE upgrade can be started in one of these ways:

- Upgrade all LRE local chipsets (controllers) and remote CPE devices by entering the **hw-module slot *module-slot* # upgrade lre** command with no additional parameters.
- Upgrade a single local LRE controller by entering the **hw-module slot *module-slot* # lre upgrade** command with the local parameter.
- Upgrade a single remote LRE CPE device by entering the **hw-module slot *module-slot* # lre upgrade** command with the remote parameter.

You can use the **force** option to upgrade an LRE binary on a local LRE controller or a remote LRE CPE device, even though the device is already running the version of the desired LRE binary. The default behavior is not to upgrade LRE binaries that are already up to date.

During an upgrade, users on the LRE links being upgraded experience a temporary disruption of Ethernet connectivity. All LRE local and remote upgrades run concurrently and take 3 to 6 minutes to complete.

The IOS CLI remains available while an LRE upgrade is in progress.

Once started, an LRE upgrade can only be stopped by physically changing the remote CPE device or by reloading the IOS software on the Ethernet switch.

Under most circumstances, configuration for upgrades is not necessary.

Examples

This example shows how to start a system-wide LRE upgrade:

```
Switch# hw-module slot 0 upgrade lre
```

You are about to start an LRE upgrade on all LRE interfaces.
Users on LRE links being upgraded will experience a temporary
disruption of Ethernet connectivity.

Start LRE upgrade ? [yes]:

```
Starting remote upgrade on CPE Lo0/1.
Starting remote upgrade on CPE Lo0/2
Starting remote upgrade on CPE Lo0/3
Starting remote upgrade on CPE Lo0/4
Starting remote upgrade on CPE Lo0/5
Starting remote upgrade on CPE Lo0/6
Starting remote upgrade on CPE Lo0/7
Starting remote upgrade on CPE Lo0/8
Starting upgrade on local controller LongReachEthernet 0
Starting remote upgrade on CPE Lo0/9
Starting remote upgrade on CPE Lo0/10
Starting remote upgrade on CPE Lo0/11
Starting remote upgrade on CPE Lo0/12
Starting remote upgrade on CPE Lo0/13
Starting remote upgrade on CPE Lo0/14
Starting remote upgrade on CPE Lo0/15
Starting remote upgrade on CPE Lo0/16
Starting upgrade on local controller LongReachEthernet 1
Starting remote upgrade on CPE Lo0/17
Starting remote upgrade on CPE Lo0/18
Starting remote upgrade on CPE Lo0/19
Starting remote upgrade on CPE Lo0/20
Starting remote upgrade on CPE Lo0/21
Starting remote upgrade on CPE Lo0/22
Starting remote upgrade on CPE Lo0/23
Starting remote upgrade on CPE Lo0/24
Starting upgrade on local controller LongReachEthernet 2
```

This example shows how to start an LRE upgrade on a single LRE controller in a switch. In this example, LongRangeEthernet 0 causes an LRE upgrade to run on controller 0 in the switch.

```
Switch# hw-module slot 0 upgrade lre local lo 0
```

You are about to start an LRE upgrade on local controller LongReachEthernet 0.
Users on LRE links being upgraded will experience a temporary
disruption of Ethernet connectivity.

Start LRE upgrade ? [yes]:

```
Starting Upgrade on local controller LongReachEthernet 0
```

This example shows how to start an LRE upgrade on a single CPE device. In this example, LongRangeEthernet 0/1 causes an LRE upgrade to run on the CPE device connected to LRE link LongRangeEthernet 0/1.

```
Switch# hw-module slot 0 upgrade lre remote lo 0/1
```

You are about to start an LRE upgrade on CPE Lo0/1.
Users on LRE links being upgraded will experience a temporary

```
■ hw-module slot module-slot# upgrade lre
```

disruption of Ethernet connectivity.

Start LRE upgrade ? [yes]:

Starting remote upgrade on CPE Lo0/1

This example shows what happens when you attempt to update current firmware without using the **force** option.

```
Switch# hw-module slot 0 upgrade lre remote lo 0/1
```

You are about to start an LRE upgrade on CPE Lo0/1.
Users on LRE links being upgraded will experience a temporary
disruption of Ethernet connectivity.

Start LRE upgrade ? [yes]:

No upgrade required on CPE Lo0/1

This example shows the **force** option when attempting to update current firmware on a CPE:

```
Switch# hw-module slot 0 upgrade lre force remote lo 0/1
```

You are about to start an LRE upgrade on CPE Lo0/1.
Users on LRE links being upgraded will experience a temporary
disruption of Ethernet connectivity.

Start LRE upgrade ? [yes]:

Starting remote upgrade on CPE Lo0/1

Switch#

Related Commands

Command	Description
controller LongReachEthernet	Allows you to enter controller sub-mode.
show lre upgrade binaries	Displays the Long-Reach Ethernet (LRE) binaries present on the system Flash memory
show lre upgrade status	Displays the upgrade status on all ports in the switch.
show lre upgrade version	Displays the versions of binaries on local and remote ends on all ports.

interface

Use the **interface** global configuration command to configure an interface type, to create a switch virtual interface to be used as the management VLAN interface, and to enter interface configuration mode.

interface {interface-id | vlan number}

no interface {interface-id | vlan number}

Syntax Description	interface-id	Specify the interface type (Fast Ethernet, Gigabit Ethernet, Long-Reach Ethernet) and number.
	vlan number	VLAN number from 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1001 when the standard software image (SI) is installed to be used as the management VLAN. Do not enter leading zeroes.

Defaults The default management VLAN interface is VLAN 1.

Command Modes Global configuration

Command History	Release	Modification
	12.0(5.2)WC(1)	This command was introduced.

Usage Guidelines When creating a management VLAN interface, a space between **vlan** and **number** is accepted.

Only one management VLAN interface can be active.

You cannot delete the management VLAN 1 interface.

You can use the **no shutdown** interface configuration command to shut down the active management VLAN interface and to enable a new one.

You can configure the management VLAN interface on static-access and trunk ports.

Examples This example shows how to enable the switch to configure interface 2:

```
Switch(config)# interface fastethernet0/2
Switch(config-if)#
```

This example shows how to change the management VLAN from the default management VLAN to VLAN 3. Enter this series of commands only from the console. If these commands are entered through a Telnet session, the **shutdown** command disconnects the session, and there is no way to use IP to access the system.

```
Switch# configure terminal
Switch(config)# interface vlan 3
Switch(config-if)# ip address 172.20.128.176 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

■ interface

You can verify your settings by entering the **show interfaces** and **show interfaces vlan *vlan-id*** privileged EXEC commands.

Related Commands

Command	Description
show interfaces	Displays the administrative and operational status of a switching (nonrouting) port.
shutdown	Disables a port and shuts down the management VLAN.

interface port-channel

Use the **interface port-channel** global configuration command to access or create the port-channel logical interface for Layer 2 interfaces. Use the **no** form of this command to remove the port channel.

interface port-channel *port-channel-number*

no interface port-channel *port-channel-number*

Syntax Description	<i>port-channel-number</i> Port-channel number. The range is 1 to 6.									
Defaults	No port-channel logical interfaces are defined.									
Command Modes	Global configuration									
Command History	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>12.1(6)EA2</td><td>This command was introduced.</td></tr> </tbody> </table>		Release	Modification	12.1(6)EA2	This command was introduced.				
Release	Modification									
12.1(6)EA2	This command was introduced.									
Usage Guidelines	<p>Only one port channel in a channel group is allowed.</p> <p>Follow these guidelines when you use the interface port-channel command:</p> <ul style="list-style-type: none"> • If you want to use the Cisco Discovery Protocol (CDP), you must configure it only on the physical interface and not on the port-channel interface. • On the port-channel interface, if you do not assign a static MAC address or if you assign a static MAC address and then later remove it, the switch automatically assigns a MAC address to the interface. 									
Examples	<p>This example shows how to create a port-channel interface with a port-channel number of 5:</p> <pre>Switch(config)# interface port-channel 5</pre> <p>You can verify your settings by entering the show running-config or show etherchannel channel-group-number detail privileged EXEC command.</p>									
Related Commands	<table border="1"> <thead> <tr> <th>Command</th><th>Description</th></tr> </thead> <tbody> <tr> <td>channel-group</td><td>Assigns an Ethernet interface to an EtherChannel group.</td></tr> <tr> <td>show etherchannel</td><td>Displays EtherChannel information for a channel.</td></tr> <tr> <td>show running-config</td><td>Displays the configuration information running on the switch. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 > Cisco IOS File Management Commands > Configuration File Commands</td></tr> </tbody> </table>		Command	Description	channel-group	Assigns an Ethernet interface to an EtherChannel group.	show etherchannel	Displays EtherChannel information for a channel.	show running-config	Displays the configuration information running on the switch. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 > Cisco IOS File Management Commands > Configuration File Commands
Command	Description									
channel-group	Assigns an Ethernet interface to an EtherChannel group.									
show etherchannel	Displays EtherChannel information for a channel.									
show running-config	Displays the configuration information running on the switch. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 > Cisco IOS File Management Commands > Configuration File Commands									

■ interface range

interface range

Use the **interface range** global configuration command to enter interface range configuration mode and to execute a command on multiple ports at the same time. Use the **no** form of this command to remove an interface range.

interface range {port-range / macro name}

no interface range {port-range / macro name}

Syntax Description	port-range Port range. For a list of valid values for <i>port-range</i> , see the “Usage Guidelines” section.
	macro name Specify the name of a macro.

Defaults This command has no default setting.

Command Modes Global configuration

Command History	Release	Modification
	12.1(6)EA2	This command was introduced.

Usage Guidelines From the interface range configuration mode, all interface parameters that you enter are applied to all interfaces within the range.

For VLANs, you can use the **interface range** command only on existing VLAN interfaces. To display VLAN interfaces, enter the **show running-config** privileged EXEC command. VLANs not displayed cannot be used in the **interface range** command. The commands that you enter under the **interface range** command are applied to all existing VLAN interfaces in the range.

All configuration changes made to an interface range are saved to nonvolatile RAM (NVRAM), but the interface range itself is not saved to NVRAM.

You can enter the interface range in two ways:

- Specifying up to five interface ranges
- Specifying a previously defined interface-range macro

You can define up to five interface ranges with a single command, with each range separated by a comma (,).

All interfaces in a range must be the same type; that is, all Fast Ethernet ports, all Gigabit Ethernet ports, all EtherChannel ports, or all VLANs.

These are the valid values for *port-range* type and interface:

- **vlan** *vlan-id*, where *vlan-id* is from 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1001 when the standard software image (SI) is installed.
- **port-channel** *port-channel-number*, where *port-channel-number* is from 1 to 6
- **fastethernet** *interface-id*
- **gigabitethernet** *interface-id*

For physical interfaces, the *interface-id* is defined as a slot/number (where slot is always 0 for the switch), and the range is entered as *type 0/number - number* (for example, **gigabitethernet0/1 - 2**). You can also enter multiple ranges.

When you define a range, you must enter a space before and after the hyphen (-):

```
interface range gigabitethernet0/1 - 2
```

When you define multiple ranges, you must enter a space before and after the comma (,):

```
interface range fastethernet0/3 - 7 , gigabitethernet0/1 - 2
```

You cannot specify both a macro and an interface range in the same command.

A single interface can also be specified in *port-range*. (The command is then similar to the **interface interface-id** global configuration command.)



Note

For more information about configuring interface ranges, refer to the *Catalyst 2950 Desktop Switch Software Configuration Guide* for this release.

Examples

This example shows how to use the **interface range** command to enter interface range configuration mode and to enter commands for two ports:

```
Switch(config)# interface range gigabitethernet0/1 - 2
Switch(config-if-range)#
```

This example shows how to use the **interface range** command to enter interface range configuration mode and to enter commands for two Long-Reach Ethernet (LRE) ports:

```
Switch(config)# interface range lo0/1 - 2
Switch(config-if-range)#
```

This example shows how to use a port-range macro *macro1* for the same function. The advantage is that you can reuse the *macro1* until you delete it.

```
Switch(config)# define interface-range macro gigabitethernet0/1 - 2
Switch(config)# interface range macro macro1
Switch(config-if-range)#
```

Related Commands

Command	Description
show running-config	Displays the configuration information running on the switch. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 > Cisco IOS File Management Commands > Configuration File Commands .

ip access-group

ip access-group

Use the **ip access-group** interface configuration command to control access to an interface. Use the **no** form of this command to remove an access group from an interface.

ip access-group {access-list-number / name} in

no ip access-group {access-list-number / name} in

This command is available on physical interfaces only if your switch is running the enhanced software image (EI).

Syntax Description

<i>access-list-number</i>	Number of the IP access control list (ACL), from 1 to 199 or from 1300 to 2699.
<i>name</i>	Name of an IP ACL, specified in the ip access-list command.

Defaults

No ACL is applied to the interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(6)EA2	This command was introduced.

Usage Guidelines

You can apply IP ACLs only to ingress interfaces. If a MAC access group is already defined for an interface, you cannot apply this command to the interface.

The ACLs can be standard or extended.

For standard ACLs, after receiving a packet, the switch checks the packet source address. If the source address matches a defined address in the ACL and the list permits the address, the switch forwards the packet.

For extended ACLs, after receiving the packet, the switch checks the match conditions in the ACL. If the conditions are matched, the switch forwards the packet.

If the specified ACL does not exist, the switch forwards all packets.

IP access groups can be separated on Layer 2 and Layer 3 interfaces.



Note For more information about configuring IP ACLs, refer to the “Configuring Network Security with ACLs” chapter in the *Catalyst 2950 Desktop Switch Software Configuration Guide* for this release.

Examples

This example shows how to apply a numbered ACL to an interface:

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# ip access-group 101 in
```

You can verify your settings by entering the **show access-lists** or **show ip access-lists** privileged EXEC command.

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP ACL.
access-list (IP standard)	Defines a standard IP ACL.
deny (access-list configuration)	Configures conditions for an IP ACL.
ip access-list	Defines an IP ACL.
permit (access-list configuration)	Configures conditions for an IP ACL.
show access-lists	Displays ACLs configured on the switch.
show ip access-lists	Displays IP ACLs configured on the switch.

ip access-list

ip access-list

Use the **ip access-list** global configuration command to create an IP access control list (ACL) to be used for matching packets to an ACL whose name or number you specify and to enter access-list configuration mode. Use the **no** form of this command to delete an existing IP ACL and return to global configuration mode.

ip access-list {extended | standard} {access-list-number / name}

no ip access-list {extended | standard} {access-list-number / name}

This command is available on physical interfaces only if your switch is running the enhanced software image (EI).

Syntax Description

<i>access-list-number</i>	Number of an ACL. For standard IP ACLs, the range is from 1 to 99 and 1300 to 1999. For extended IP ACLs, the range from 100 to 199 and from 2000 to 2699.
<i>name</i>	Name of an ACL. Note The ACL name must begin with an alphabetic character to prevent ambiguity with numbered ACLs. A name also cannot contain a space or quotation mark.

Defaults

No named or numbered IP ACLs are defined.

Command Modes

Global configuration

Command History

Release	Modification
12.1(6)EA2	This command was introduced.

Usage Guidelines

Use this command to enter access-list configuration mode and to specify the name or number of the IP ACL for which you want to create or modify ACL match criteria. In this mode, you must enter the **permit** and **deny** commands to configure the permit and deny access conditions for this list.

Use the **ip access-list** command and its subcommands to define packet classification and marking as part of a globally-named service policy applied on a per-interface basis or as an IP access group applied on a per-interface basis.

Specifying **standard** or **extended** with the **ip access-list** command determines the prompt that you get when you enter access-list configuration mode.


Note

For more information about configuring IP ACLs, refer to the “Configuring Network Security with ACLs” chapter in the *Catalyst 2950 Desktop Switch Software Configuration Guide* for this release.

Examples

This example shows how to configure a standard ACL named *Internetfilter1*:

```
Switch(config)# ip access-list standard Internetfilter1
Switch(config-std-nacl)# permit 192.5.34.0 0.0.0.255
Switch(config-std-nacl)# permit 192.5.32.0 0.0.0.255
Switch(config-std-nacl)# exit
```

This example shows how to configure an extended ACL named *Internetfilter2*:

```
Switch(config)# ip access-list extended Internetfilter2
Switch(config-ext-nacl)# permit any 128.8.10.0 0.0.0.255 eq 80
Switch(config-ext-nacl)# permit any 128.5.8.0 0.0.0.255 eq 80
Switch(config-ext-nacl)# exit
```



Note In these examples, all other IP access is implicitly denied.

You can verify your settings by entering the **show access-lists** or **show ip access-lists** privileged EXEC command.

Related Commands

Command	Description
deny (access-list configuration)	Configures conditions for an IP ACL.
ip access-group	Controls access to an interface.
permit (access-list configuration)	Configures conditions for an IP ACL.
service-policy	Applies a policy map to the input of an interface.
show access-lists	Displays ACLs configured on the switch.
show ip access-lists	Displays IP ACLs configured on the switch.

ip address

ip address

Use the **ip address** interface configuration command to set an IP address for a switch. Use the **no** form of this command to remove an IP address or to disable IP processing.

ip address ip-address subnet-mask

no ip address ip-address subnet-mask

Syntax Description	<i>ip-address</i> IP address. <i>subnet-mask</i> Mask for the associated IP subnet.
---------------------------	--

Defaults No IP address is defined for the switch.

Command Modes Interface configuration

Command History	Release	Modification
	12.0(5.2)WC(1)	This command was introduced.

Usage Guidelines A switch can have one IP address.

The IP address of the switch can be accessed only by nodes connected to ports that belong to the management VLAN. By default, the management VLAN is VLAN 1, but you can configure a different VLAN as the management VLAN.

If you remove the IP address through a Telnet or Secure Shell (SSH) session, your connection to the switch is lost.

If your switch receives its IP address from a Bootstrap Protocol (BOOTP) or a Dynamic Host Configured Protocol (DHCP) server and you remove the switch IP address by using the **no ip address** command, IP processing is disabled, and the BOOTP or DHCP server cannot reassign the address.

Examples This example shows how to configure the IP address for the switch on a subnetted network:

```
Switch(config)# interface vlan 1
Switch(config-if)# ip address 172.20.128.2 255.255.255.0
```

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

Related Commands	Command	Description
	show running-config	Displays the configuration information running on the switch. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 > Cisco IOS File Management Commands > Configuration File Commands .

ip igmp snooping

Use the **ip igmp snooping** global configuration command to globally enable Internet Group Management Protocol (IGMP) snooping. Use the **no** form of this command to disable IGMP snooping.

ip igmp snooping

no ip igmp snooping

Syntax Description This command has no arguments or keywords.

Defaults By default, IGMP snooping is globally enabled.

Command Modes Global configuration

Command History	Release	Modification
	12.0(5.2)WC(1)	This command was introduced.

Usage Guidelines When IGMP snooping is globally enabled, it enables IGMP snooping on all the existing VLAN interfaces. When IGMP snooping is globally disabled, it disables IGMP snooping on all the existing VLAN interfaces.

The configuration is saved in nonvolatile RAM (NVRAM).

Examples This example shows how to globally enable IGMP snooping:

```
Switch(config)# ip igmp snooping
```

This example shows how to globally disable IGMP snooping:

```
Switch(config)# no ip igmp snooping
```

You can verify your settings commands by entering the **show ip igmp snooping** privileged EXEC command.

Related Commands	Command	Description
	ip igmp snooping vlan	Enables IGMP snooping on a VLAN interface.
	ip igmp snooping vlan immediate-leave	Enables IGMP Immediate-Leave processing.
	ip igmp snooping vlan mrouter	Configures a Layer 2 port as a multicast router port.
	ip igmp snooping vlan static	Configures a Layer 2 port as a member of a group.
	show ip igmp snooping	Displays the IGMP snooping configuration.

ip igmp snooping vlan

ip igmp snooping vlan

Use the **ip igmp snooping vlan** global configuration command to enable Internet Group Management Protocol (IGMP) snooping on a specific VLAN. Use the **no** form of this command to disable IGMP snooping on a VLAN interface.

ip igmp snooping vlan *vlan-id*

no ip igmp snooping vlan *vlan-id*

Syntax Description	<i>vlan-id</i>	VLAN ID. The range is from 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1001 when the standard software image (SI) is installed. Do not enter leading zeros.
---------------------------	----------------	---

Defaults By default, IGMP snooping is enabled when each VLAN is created.

Command Modes Global configuration

Command History	Release	Modification
	12.0(5.2)WC(1)	This command was introduced.

Usage Guidelines This command automatically configures the VLAN if it is not already configured. The configuration is saved in nonvolatile RAM (NVRAM).

Examples This example shows how to enable IGMP snooping on VLAN 2:

```
Switch(config)# ip igmp snooping vlan 2
```

This example shows how to disable IGMP snooping on VLAN 2:

```
Switch(config)# no ip igmp snooping vlan 2
```

You can verify your settings by entering the **show ip igmp snooping vlan** privileged EXEC command.

Related Commands	Command	Description
	ip igmp snooping	Globally enables IGMP snooping. IGMP snooping must be globally enabled in order to be enabled on a VLAN.
	ip igmp snooping vlan immediate-leave	Enables IGMP Immediate-Leave processing.
	ip igmp snooping vlan mrouter	Configures a Layer 2 port as a multicast router port.
	ip igmp snooping vlan static	Configures a Layer 2 port as a member of a group.
	show ip igmp snooping	Displays the IGMP snooping configuration.

ip igmp snooping vlan immediate-leave

Use the **ip igmp snooping immediate-leave** global configuration command to enable Internet Group Management Protocol (IGMP) Immediate-Leave processing on a VLAN interface. Use the **no** form of this command to disable Immediate-Leave processing on the VLAN interface.

ip igmp snooping vlan *vlan-id* immediate-leave

no ip igmp snooping vlan *vlan-id* immediate-leave

Syntax Description	<i>vlan-id</i>	VLAN ID value. The range is between 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1001 when the standard software image (SI) is installed. Do not enter leading zeros.
---------------------------	----------------	--

Defaults	By default, IGMP Immediate-Leave processing is disabled.
-----------------	--

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

Command History	Release	Modification
	12.0(5.2)WC(1)	This command was introduced.

Usage Guidelines	Use the Immediate-Leave feature only when there is only one IP multicast receiver present on every port in the VLAN. The Immediate-Leave configuration is saved in nonvolatile RAM (NVRAM).
-------------------------	---

The Immediate-Leave feature is supported only with IGMP version 2 hosts.

Examples	This example shows how to enable IGMP Immediate-Leave processing on VLAN 1: Switch(config)# ip igmp snooping vlan 1 immediate-leave
	This example shows how to disable IGMP Immediate-Leave processing on VLAN 1: Switch(config)# no ip igmp snooping vlan 1 immediate-leave

You can verify your settings by entering the **show ip igmp snooping vlan** privileged EXEC command.

Related Commands	Command	Description
	ip igmp snooping	Enables IGMP snooping.
	ip igmp snooping vlan mrouter	Configures a Layer 2 port as a multicast router port.
	show ip igmp snooping	Displays the IGMP snooping configuration.
	ip igmp snooping vlan static	Configures a Layer 2 port as a member of a group.
	show mac address-table multicast	Displays the Layer 2 multicast entries for a VLAN.

 ■ ip igmp snooping vlan mrouter

ip igmp snooping vlan mrouter

Use the **ip igmp snooping vlan mrouter** global configuration command to add a multicast router port and to configure the multicast router learning method. Use the **no** form of this command to remove the configuration.

```
ip igmp snooping vlan vlan-id mrouter {interface interface-id | learn {cgmp | pim-dvmrp}}
```

```
no ip igmp snooping vlan vlan-id mrouter {interface interface-id | learn {cgmp | pim-dvmrp}}
```

Syntax Description	vlan <i>vlan-id</i> Specify the VLAN ID. The range is from 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1001 when the standard software image (SI) is installed. Do not enter leading zeros. interface <i>interface-id</i> Specify the interface of the member port that is configured to a static router port. learn Specify the multicast router learning method. cgmp Set the switch to learn multicast router ports by snooping on Cisco Group Management Protocol (CGMP) packets. pim-dvmrp Set the switch to learn multicast router ports by snooping on IGMP queries and Protocol-Independent Multicasting-Distance Vector Multicast Routing Protocol (PIM-DVMRP) packets.
---------------------------	---

Defaults	The default learning method is pim-dvmrp .
-----------------	---

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

Command History	Release	Modification
	12.0(5.2)WC(1)	This command was introduced.

Usage Guidelines	The CGMP learning method is useful for controlling traffic in Cisco router environments. The configured learning method is saved in nonvolatile RAM (NVRAM). Static connections to multicast routers are supported only on switch ports.
-------------------------	--

Examples	This example shows how to configure Fast Ethernet interface 0/6 as a multicast router port:
-----------------	---

```
Switch(config)# ip igmp snooping vlan 1 mrouter interface fastethernet0/6
```

This example shows how to specify the multicast router learning method as CGMP:

```
Switch(config)# no ip igmp snooping vlan 1 mrouter learn cgmp
```

You can verify your settings by entering the **show ip igmp snooping mrouter** privileged EXEC command.

Related Commands	Command	Description
	ip igmp snooping	Globally enables Internet Group Management Protocol (IGMP) snooping.
	ip igmp snooping vlan	Enables IGMP snooping on the VLAN interface.
	ip igmp snooping vlan immediate-leave	Configures IGMP Immediate-Leave processing.
	ip igmp snooping vlan static	Configures a Layer 2 port as a member of a group.
	show ip igmp snooping mrouter	Displays the statically and dynamically learned multicast router ports.

■ ip igmp snooping vlan static

ip igmp snooping vlan static

Use the **ip igmp snooping vlan *vlan-id* static** global configuration command to add a Layer 2 port as a member of a multicast group. Use the **no** form of this command to remove the configuration.

ip igmp snooping vlan *vlan-id* static *mac-address* **interface *interface-id***

no ip igmp snooping vlan *vlan-id* static *mac-address* **interface *interface-id***

Syntax Description	vlan <i>vlan-id</i> Specify the VLAN ID. The range is 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1001 when the standard software image (SI) is installed. Do not enter leading zeros. static <i>mac-address</i> Specify the static group MAC address. interface <i>interface-id</i> Specify the interface configured to a static router port.
---------------------------	---

Defaults None configured.

Command Modes Global configuration

Command History	Release	Modification
	12.0(5.2)WC(1)	This command was introduced.

Usage Guidelines The command is used to statically configure the IP multicast group member ports. The static ports and groups are saved in nonvolatile RAM (NVRAM). Static connections to multicast routers are supported only on switch ports.

Examples This example shows how to statically configure a host on an interface:

```
Switch(config)# ip igmp snooping vlan 1 static 0100.5e02.0203 interface fastethernet0/6
Configuring port FastEthernet 0/6 on group 0100.5e02.0203
```

You can verify your settings by entering the **show mac address-table multicast** privileged EXEC command.

Related Commands	Command	Description
	ip igmp snooping	Enables Internet Group Management Protocol (IGMP) snooping.
	ip igmp snooping vlan	Enables IGMP snooping on the VLAN interface.
	ip igmp snooping vlan immediate-leave	Configures IGMP Immediate-Leave processing.
	ip igmp snooping vlan mrouter	Configures a Layer 2 port as a multicast router port.
	show mac address-table multicast	Displays the Layer 2 multicast entries for a VLAN.

link monitor

link monitor

Use the **link monitor** interface configuration command to enable Long-Reach Ethernet (LRE) link monitoring on a port. Use the **no** form of the command to disable LRE link monitoring on a port.

link monitor

no link monitor

Syntax Description This command has no arguments or keywords.

Defaults The default is **link monitor**.

Command Modes Interface configuration

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.

Usage Guidelines If the link is shut down, link monitor data is not collected.

Examples This example shows how to enable LRE link monitoring on port 1.

```
Switch# configure terminal
Switch(config)# interface long 0/1
Switch(config-if)# link monitor
Switch(config-if)#
```

Related Commands	Command	Description
	clear controllers lre link monitor	Deletes LRE link monitor data.
	link monitor logging	Enables link monitor event logging per port.
	link monitor threshold snr	Sets an signal-to-noise margin for the LRE link monitor.
	link monitor threshold rserr	Sets a Reed-Solomon error threshold for the LRE link monitor.
	show controllers lre link monitor errors	Displays Reed-Solomon and Ethenet errors captured by the LRE link monitor.
	show controllers lre link monitor parameters	Displays the switch or customer premises equipment (CPE) device operating parameter data.
	show controllers lre link monitor statistics	Displays the switch or CPE device statistical data.

link monitor logging

Use the **link monitor logging** interface configuration command to enable Long-Reach Ethernet (LRE) link monitoring event logging. Use the **no** form of the command to disable LRE link monitor logging.

link monitor logging

no link monitor logging

Syntax Description This command has no arguments or keywords.

Defaults The default is **no link monitor logging**.

Command Modes Interface configuration

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.

Usage Guidelines Events are logged in the system log when a configured threshold is crossed.

Examples This example shows how to enable LRE link monitoring logging on port 2.

```
Switch# configure terminal
Switch(config)# interface long 0/2
Switch(config-if)# link monitor logging
Switch(config-if)#
```

Command History	Command	Description
	clear controllers lre link monitor	Deletes LRE link monitor data.
	link monitor	Enables the LRE link monitor on a port.
	link monitor threshold snr	Sets an signal-to-noise margin for the LRE link monitor.
	link monitor threshold rserr	Sets a Reed-Solomon error threshold for the LRE link monitor.
	show controllers lre link monitor errors	Displays Reed-Solomon and Ethenet errors captured by the LRE link monitor.
	show controllers lre link monitor parameters	Displays the switch or CPE device operating parameter data.
	show controllers lre link monitor statistics	Displays the switch or CPE device statistical data.

 link monitor threshold rserr

link monitor threshold rserr

Use the **link monitor threshold rserr** interface configuration command to establish threshold values for Reed-Solomon errors. Use the **no** form of the command to reset the threshold values to their defaults.

link monitor threshold rserr {downstream value | upstream value}

no link monitor threshold rserr {downstream value | upstream value}

Syntax Description	<i>value</i>	The number of the Reed Solomon errors allowed per second. The valid range is from 0 to 25000.
---------------------------	--------------	---

Defaults	The default is 1000 errors per second.
-----------------	--

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

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.

Usage Guidelines	To compute threshold values, calculate the number of frames that can be sent for a particular bandwidth based on the Long-Reach Ethernet (LRE) profile. Use the show controller lre status profile command to determine the downstream and upstream data rates. Divide the downstream data rate by the length of an LRE frame (216 bytes) multiplied by 8 (8 bits per byte).
-------------------------	---

For example, a link is running LRE-10, which has a downstream data rate of 12.5 Mbps.

$((12500000)/(261*8))=598$

If you configure the downstream Reed-Solomon error threshold to 598, an alarm counter increments when the threshold is exceeded.

Examples	This example shows how to configure a threshold for Reed-Solomon errors at 4000 errors per second downstream and 3000 errors per second upstream.
-----------------	---

```
Switch# configure terminal
Switch(config)# interface long 0/1
Switch(config-if)# link monitor threshold rserr downstream 4000
Switch(config-if)# link monitor threshold rserr upstream 3000
Switch(config-if)#
```

Related Commands	Command	Description
	clear controllers lre link monitor	Deletes LRE link monitor data.
	link monitor	Enables the LRE link monitor on a port.

Command	Description
link monitor logging	Enables link monitor event logging per port.
link monitor threshold snr	Sets a signal-to-noise margin for the LRE link monitor.
show controllers lre link monitor errors	Displays Reed-Solomon and Ethenet errors captured by the LRE link monitor.
show controllers lre link monitor parameters	Displays the switch or CPE device operating parameter data.
show controllers lre link monitor statistics	Displays the switch or CPE device statistical data.
show controllers lre status	Displays the Long-Reach Ethernet (LRE) link statistics and profile information on a switch LRE port, including link state, link duration, profile name, and data rates.

 link monitor threshold snr

link monitor threshold snr

Use the **link monitor threshold snr** interface configuration command to establish threshold values for signal-to-noise ratio (SNR) errors. Use the **no** form of the command reset the threshold values to their defaults.

link monitor threshold snr {downstream *value* | upstream *value*}

no link monitor threshold snr {downstream *value* | upstream *value*}

Syntax Description	<i>value</i>	The value of the SNR, measured in dB. The valid range is from 0 to 10.
Defaults	The default is 2 dB.	
Command Modes	Interface configuration	
Command History	Release	Modification
	12.1(11)YJ	This command was introduced.
Usage Guidelines	The default theoretical SNR value added to the threshold value is compared to the value in the LRE chipset.	
Examples	This example shows how to configure the SNR threshold as 6 dB downstream and 4 dB upstream.	
	<pre>Switch# configure terminal Switch(config)# interface long 0/1 Switch(config-if)# link monitor threshold snr downstream 6 Switch(config-if)# link monitor threshold snr upstream 4 Switch(config-if)#</pre>	
Related Commands	Command	Description
	clear controllers lre link monitor	Deletes LRE link monitor data.
	link monitor	Enables the LRE link monitor on a port.
	link monitor logging	Enables link monitor event logging per port.
	link monitor threshold rserr	Sets a Reed-Solomon error threshold for the LRE link monitor.
	show controllers lre link monitor errors	Displays Reed-Solomon and Ethernet errors captured by the LRE link monitor.

Command	Description
show controllers lre link monitor parameters	Displays the switch or CPE device operating parameter data.
show controllers lre link monitor statistics	Displays the switch or CPE device statistical data.

local duplex

local duplex

Use the **local duplex** interface configuration command to specify the duplex mode of operation for a Long-Reach Ethernet (LRE) port. Use the **no** form of this command to return the port to its default value.

local duplex {half | full}

no local duplex

Syntax Description	full Port is in full-duplex mode. half Port is in half-duplex mode.
---------------------------	--

Defaults	The default is half .
-----------------	------------------------------

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

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.

Usage Guidelines	This command only sets the duplex mode on an LRE link. To set the duplex mode on a customer premises equipment (CPE) Ethernet link, use the cpe duplex command; to set the duplex mode of the Gigabit ports, use the duplex command.
-------------------------	--

Examples	This example shows how to set LRE port 1 to full duplex:
-----------------	--

```
Switch(config)# interface longrangethernet1/1
Switch(config-if)# local duplex full
Switch(config-if)#
```

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

Related Commands	Command	Description
	cpe duplex	Specifies the duplex mode of CPE Ethernet ports.
	cpe speed	Sets the speed of an customer premises equipment (CPE) port
	duplex	Specifies the duplex mode of Gigabit Ethernet ports.
	local speed	Specifies the speed of LRE ports.
	speed	Specifies the speed of LRE Gigabit Ethernet ports.

local speed

Use the **local speed** interface configuration command to specify the speed of a Long-Reach Ethernet (LRE) port and LRE interface. Use the **no** form of this command to return to the default value.

local speed {10 | 100}

no local speed

Syntax Description	10 LRE port runs at 10 Mbps. 100 LRE port runs at 100 Mbps.
---------------------------	--

Defaults	The default is 100 Mbps .
-----------------	----------------------------------

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

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.

Usage Guidelines	This command only sets the speed on an LRE link. To set the speed on a customer premises equipment (CPE) Ethernet link, use the cpe speed command; to set the speed of the Gigabit ports, use the speed command.
-------------------------	--

Examples	This example shows how to set LRE port 1 to 100 Mbps:
-----------------	---

```
Switch(config)# interface longrangethernet1/1
Switch(config-if)# local speed 100
Switch(config-if)#
```

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

Related Commands	Command	Description
	cpe duplex	Specifies the duplex mode of CPE Ethernet ports.
	cpe speed	Specifies the speed of CPE Ethernet ports.
	duplex	Specifies the duplex mode of Gigabit Ethernet ports.
	local duplex	Specifies the duplex mode of operation for LRE ports.
	speed	Specifies the speed of Gigabit Ethernet ports.

logging lre

logging lre

Use the **logging lre** interface configuration command to specify the mode in which to log Long-Reach Ethernet (LRE) events. Use the **no** form of the command to turn off logging of events.

logging lre { event | extended | normal}

no logging lre { event | extended | normal}

Syntax Description

event	Logs events only.
extended	Logs events and all possible parameters.
normal	Logs events and some typical parameters.

Defaults

The default is **normal**.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(11)YJ	This command was introduced.

Usage Guidelines

This command is not needed for normal operation of the switch. However, it can be used as a diagnostic tool to analyze activity on the switch.

The maximum number of events that can be logged on a per-port basis is 50. Eventually, the log overwrites itself when full.

Examples

This example shows how to disable the log:

```
Switch (config)# interface lo0/1
Switch(config-if)# no logging lre
Switch (config-if)#+
```

This example shows how to set logging for events:

```
Switch (config)# interface lo0/1
Switch(config-if)# logging lre event
Switch (config-if)#+
```

This example shows how to extend event logging to include all possible parameters:

```
Switch (config)# interface lo0/1
Switch(config-if)# logging lre extended
Switch (config-if)#+
```

This example shows how to add some typical parameters to logging events:

```
Switch (config)# interface lo0/1
Switch(config-if)# logging lre normal
Switch (config-if)#
```

Related Commands

Command	Description
clear controllers lre log	Deletes the history of link, configuration, and timer events for a specific LRE port or for all switch LRE ports.
show controllers lre log	Displays the history of link, configuration, and timer events for a specific LRE port or all switch LRE ports.

lre profile

lre profile

Use the **lre profile** global configuration command to assign a Long-Reach Ethernet (LRE) profile to all switch LRE ports.

lre profile *profile-name*

no lre profile *profile-name*

Syntax Description	<i>profile-name</i>	Name of the profile. The profile name can be a Cisco-supplied profile or a user-created profile. See the <i>Catalyst 2950 Series Software Configuration Guide</i> for further details on Cisco-supplied profiles.
---------------------------	---------------------	---

Defaults

The default is LRE-10.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(11)YJ	This command was introduced.

Usage Guidelines

Unless you assign a profile, the switch uses the default LRE-10 global profile. This profile allows the upstream and downstream transmission rate on the LRE link to be 12.5 Mbps. Profiles assigned at the port level have priority over profiles that are assigned at the global level.

When assigning profiles to LRE ports, keep these considerations in mind:

- The default profile, LRE-10, may not be the best choice for your environment.
- When you assign a different profile to a port, the port applies and uses the newly assigned profile.
- If the switch is used with equipment directly connected to a public switched telephone network (PSTN) without a public branch exchange (PBX) between the LRE switch and the public telephone lines, Cisco recommends that you use either the LRE-998-15-4-M2 or LRE-997-10-4-M2 profiles globally.

Examples

This example shows how to specify the **profile** command:

```
Switch# configure t
Switch(config)# lre profile LRE-8
Switch(config)#
```

You can verify your settings by entering the **show controllers lre profile details** privileged EXEC command.

Related Commands	Command	Description
	profile (sequence mode)	Adds an LRE profile to a rate selection sequence.
	show controllers lre profile names	Displays information about the LRE profiles available on the switch.
	show controllers lre profile details	Displays how the profiles are assigned to the switch LRE ports.

Ire rate selection sequence

Ire rate selection sequence

Use the **Ire rate selection sequence** global configuration command to assign the rate selection sequence for the entire switch. Use the **no** form of the command to delete the assigned sequence.

Ire rate selection sequence *sequenceName*

no Ire rate selection sequence *sequenceName*

Syntax Description	<i>sequenceName</i>	Name of the rate selection sequence being applied.
---------------------------	---------------------	--

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

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.

Usage Guidelines	This command applies a sequence to all ports that have rate selection enabled. The command is rejected if the sequence is not configured with a profile.
-------------------------	--

When rate selection is enabled, profiles and sequences follow a predefined priority scheme that determines the rate for a port or for the entire switch. In general, sequences have priority over standalone profiles, and port configurations have priority over switch-wide configurations. Specifically, these are the priority levels with rate selection enabled, from highest to lowest:

1. Per-port sequence
2. Global sequence
3. Port profile
4. Global profile

For further details on profiles, sequences, and their priority scheme, see *Catalyst 2950 Series Software Configuration Guide*.

Examples	This example shows how to specify the sequence named Ire-seq-upstream:
-----------------	--

```
Switch(config)# ire rate selection sequence ire-seq-upstream
Switch(config)#
```

Related Commands	Command	Description
	Ire rate selection sequence	Assigns a sequence to the entire switch.
	Ire sequence	Creates user-defined rate selection sequences.
	rate selection	Enables rate selection on a specific port.

Command	Description
rate selection sequence	Assigns a rate selection sequence for a specific port.
show controllers ire sequence	Displays the list of sequences.

lre sequence

lre sequence

Use the **lre sequence** global configuration command to define a new sequence and to enter sequence configuration mode. Use the **no** form of the command to delete a user-configured sequence.

lre sequence *sequence-name*

no lre sequence *sequence-name*

Syntax Description	<i>sequence-name</i>	The name of the sequence being created or modified.
---------------------------	----------------------	---

Defaults	No default is defined.
-----------------	------------------------

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

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.

Usage Guidelines	This command creates a new sequence when the sequence name specified in the command does not match any of the existing configured sequences. When the sequence-name specified in the command matches a configured sequence, a new sequence is not created.
-------------------------	--

The profiles can be edited from the sequence configuration mode. However, the system-defined sequences cannot be edited. If the sequence specified in this command is a system-defined sequence, the command is rejected. An error message appears if the sequence name matches the name of a system-defined sequence. Use the **exit** command to return to global configuration mode.

Examples	This example shows how to specify the a user-defined sequence called myseq.
-----------------	---

```
Switch# configure t
Switch(config)# lre sequence myseq
Switch(config-seq)#

```

This example shows how to create a user-defined sequence called corpseq, with two profiles in that sequence.

```
Switch# configure t
Switch(config)# lre sequence corpseq
Switch(config-seq)# profile lre-15-5
Switch(config-seq)# profile lre-15-3
Switch(config-seq)# exit
Switch(config)#

```

This example shows the error message when trying to edit a system-defined sequence.

```
switch(config)# lre sequence lre-seq-complete-reach
Error:Sequence LRE-SEQ-COMPLETE-REACH is a system defined sequence. Cannot edit
      this sequence
Switch>(config)#

```

This example shows how to delete a user-defined sequence.

```
Switch# configure t
Switch(config)# no lre sequence myseq
Switch(config-seq)# exit
Switch(config)#

```

Related Commands	Command	Description
	lre rate selection sequence	Assigns sequences globally.
	profile	Adds a profile to a sequence.

lre upgrade default family device-family binary

lre upgrade default family *device-family* binary

Use the **lre upgrade default family** global configuration command to define a map between a Long-Reach Ethernet (LRE) device and an LRE binary.

lre upgrade default family *device-family* [model** *model*] [**revision** *revision*]
binary *LRE binary*]**

no lre upgrade default family *device-family* [model** *model*] [**revision** *revision*]
binary *LRE binary*]**

Syntax Description	<i>device-family</i>	Type of device that contains the chipset to be upgraded. Valid values are CISCO575-LRE, CISCO585-LRE, and CISCO2950-LRE.
	<i>model</i>	(Optional) Model number of the device family, for example, a model could be CISCO585-LRE.
	<i>revision</i>	(Optional) Revision of the target device.
	<i>LRE binary</i>	LRE binary file being applied.

Defaults No default is defined. The system selects the binary file.

Command Modes Global configuration mode

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.

Usage Guidelines Use the **lre upgrade default family *device-family* binary** configuration command to override the default behavior for upgrading LRE firmware. This command is useful when you want to upgrade all CPE devices or local controllers of a given family to an LRE binary version.



Note The name of the LRE binary must be entered as it appears on Flash memory. Use the **show lre upgrade binaries** command to determine the Flash filename of an LRE binary.

Examples This example configures all CISCO585-LRE CPE devices to upgrade with the LRE binary file CISCO-585-LRE_vdlsngl_51.00.00:

```
Switch(config)# lre upgrade default family CISCO585-LRE binary
      CISCO585-LRE_vdlsngl_51.00.00.bin
Switch(config)#
```

Related Commands	Command	Description
	controller	Allows you to enter controller submode.
	LongReachEthernet	
	show lre upgrade binaries	Displays the LRE binaries present on the system Flash memory.
	show lre upgrade version	Displays the version of binaries on local and remote ports in the switch.
	upgrade binary	Configures upgrades on either end of an LRE link.
	upgrade preserve	Prevents an upgrade of the local CPE controller and all remote CPE devices connected to it.

mac access-group

mac access-group

Use the **mac access-group** interface configuration command to apply a named extended MAC access control list (ACL) to an interface. Use the **no** form of this command to remove a MAC ACL from an interface.

mac access-group name in

no mac access-group name in

This command is available only if your switch is running the enhanced software image (EI).

Syntax Description	<i>name</i>	Name of the MAC extended ACL.
---------------------------	-------------	-------------------------------

Defaults	No MAC ACL is applied to the interface.
-----------------	---

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

Command History	Release	Modification
	12.1(6)EA2	This command was introduced.

Usage Guidelines	You can apply MAC ACLs only to ingress interfaces. If an IP access group is already defined for an interface, you cannot apply this command to the interface.
-------------------------	---

After receiving the packet, the switch checks the match conditions in the ACL. If the conditions are matched, the switch forwards the packet.

If the specified ACL does not exist, the switch forwards all packets.


Note

For more information about configuring MAC extended ACLs, refer to the “Configuring Network Security with ACLs” chapter in the *Catalyst 2950 Desktop Switch Software Configuration Guide* for this release.

Examples	This example shows how to apply a MAC extended ACL named <i>macacl2</i> to an interface:
-----------------	--

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# mac access-group macacl2 in
```

You can verify your settings by entering the **show mac access-group** privileged EXEC command.

Related Commands	Command	Description
	{ deny (MAC access-list configuration) permit (MAC access-list configuration) }	Configures a MAC ACL.
	show access-lists	Displays the ACLs configured on the switch.
	show mac access-group	Displays the MAC ACLs configured on the switch.

mac access-list extended

mac access-list extended

Use the **mac access-list extended** global configuration command to create an access control list (ACL) based on MAC addresses. Using this command changes the mode to extended MAC access-list configuration mode. Use the **no** form of this command to return to the default setting.

mac access-list extended name

no mac access-list extended name

This command is available only if your switch is running the enhanced software image (EI).

Syntax Description	name	Assign a name to the MAC extended ACL.
Defaults	No MAC ACLs are created.	
Command Modes	Global configuration	
Command History	Release	Modification
	12.1(6)EA2	This command was introduced.
Usage Guidelines	MAC-named extended ACLs are used with the mac access-group interface configuration command and class maps.	
Note	For more information about configuring MAC extended ACLs, refer to the “Configuring Network Security with ACLs” chapter in the <i>Catalyst 2950 Desktop Switch Software Configuration Guide</i> for this release.	
Examples	<p>This example shows how to enter extended MAC access-list configuration mode and to create a MAC extended ACL named <i>mac1</i>:</p> <pre>Switch(config)# mac access-list extended mac1 Switch(config-ext-macl)# </pre> <p>This example shows how to delete the MAC extended ACL named <i>mac1</i>:</p> <pre>Switch(config)# no mac access-list extended mac1 </pre> <p>You can verify your settings by entering the show access-lists privileged EXEC command.</p>	

Related Commands	Command	Description
	class-map	Creates a class map to be used for matching packets to the class whose name you specify and to enter class-map configuration mode.
	{deny (MAC access-list configuration) permit (MAC access-list configuration)}	Configures a MAC ACL.
	mac access-group	Applies a MAC ACL to an interface.
	show access-lists	Displays the ACLs configured on the switch.

mac address-table aging-time

mac address-table aging-time

Use the **mac address-table aging-time** global configuration command to set the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated. Use the **no** form of this command to return to the default setting. The aging time applies to all VLANs.

mac address-table aging-time [0 | 10–1000000]

no mac address-table aging-time [0 | 10–1000000]



Note Beginning with Release 12.1(11)EA1, the **mac address-table aging-time** command replaces the **mac-address-table aging-time** command (with the hyphen). The **mac-address-table aging-time** command (with the hyphen) will become obsolete in a future release.

Syntax Description	0	This value disables aging. Static address entries are never aged or removed from the table.
	<i>10–100000</i>	Aging time in seconds. The range is 10 to 1000000 seconds.

Defaults	The default is 300 seconds.
-----------------	-----------------------------

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

Command History	Release	Modification
	12.0(5.2)WC(1)	This command was introduced.
	12.1(6)EA2	The aging-time values were modified.
	12.1(11)EA1	The mac-address-table aging-time command was replaced by the mac address-table aging-time command.

Usage Guidelines	If hosts do not send continuously, increase the aging time to record the dynamic entries for a longer time. This reduces the possibility of flooding when the hosts send again.
-------------------------	---

Examples	This example shows how to set the aging time to 200 seconds:
-----------------	--

```
Switch(config)# mac address-table aging-time 200
```

This example shows how to disable aging in VLAN 1.

```
Switch(config)# mac address-table aging-time 0
```

This example shows how to set aging time to 450 seconds for all VLANs for which the user did not specify aging time.

```
Switch(config)# mac address-table aging-time 450
```

You can verify your settings by entering the **show mac address-table** privileged EXEC command.

Related Commands

Command	Description
clear mac address-table	Deletes dynamic entries from the MAC address table.
show mac address-table	Displays the MAC address table.
show mac address-table aging-time	Displays the MAC address table aging time for all VLANs or the specified VLAN.

mac address-table notification

Use the **mac address-table notification** global configuration command to enable the MAC notification feature and configure the notification-trap interval or history table. Use the **no** form of this command to disable this feature.

mac address-table notification [history-size size / interval interval]

no mac address-table notification [history-size size / interval interval]


Note

Beginning with Release 12.1(11)EA1, the **mac address-table notification** command replaces the **mac-address-table notification** command (with the hyphen). The **mac-address-table notification** command (with the hyphen) will become obsolete in a future release.

Syntax Description

history-size size	(Optional) Configures the maximum number of entries in the MAC notification history table; valid values are 0 to 500.
--------------------------	---

interval interval	(Optional) Configures the notification-trap interval in seconds; valid values are from 0 to 2147483647. The switch sends the notification traps when this amount of time has elapsed.
--------------------------	---

Defaults

The MAC notification feature is disabled.

The default trap-interval value is 1 second.

The default number of entries in the history table is 1.

Command Modes

Global configuration

Command History

Release	Modification
12.1(6)EA2	This command was introduced.
12.1(11)EA1	The mac-address-table notification command was replaced by the mac address-table notification command.

Usage Guidelines

The MAC address notification feature sends Simple Network Management Protocol (SNMP) traps to the network management system (NMS) whenever a MAC address is added or deleted from the forwarding tables. MAC notifications are generated only for dynamic and secure MAC addresses. Events are not generated for self addresses, multicast addresses, or other static addresses.

When you configure the **history-size** option, the existing MAC address history table is deleted, and a new table is created.

You enable the MAC address notification feature by using the **mac address-table notification** command. You must also enable MAC address notification traps on an interface by using the **snmp trap mac-notification** interface configuration command, and configure the switch to send MAC address traps to the NMS by using the **snmp-server enable traps mac-notification** global configuration command.

Examples

This example shows how to enable the MAC notification feature:

```
Switch(config)# mac address-table notification
```

This example shows how to set the notification-trap interval to 60 seconds:

```
Switch(config)# mac address-table notification interval 60
```

This example shows how to set the number of entries in the history table to 32:

```
Switch(config)# mac address-table notification history-size 32
```

You can verify your settings by entering the **show mac address-table notification** privileged EXEC command.

Related Commands

Command	Description
clear mac address-table notification	Clears the MAC address notification global counters.
show mac address-table notification	Displays the MAC address notification settings for all interfaces or the specified interface.
snmp-server enable traps	Sends the SNMP MAC notification traps when the mac-notification keyword is appended.
snmp trap mac-notification	Enables the SNMP MAC notification trap on a specific interface.

mac address-table static

mac address-table static

Use the **mac address-table static** global configuration command to add static addresses to the MAC address table. Use the **no** form of this command to remove static entries from the MAC address table.

mac address-table static mac-addr vlan vlan-id interface interface-id

no mac address-table static mac-addr vlan vlan-id interface interface-id

**Note**

Beginning with Release 12.1(11)EA1, the **mac address-table static** command replaces the **mac-address-table static** command (with the hyphen). The **mac-address-table static** command (with the hyphen) will become obsolete in a future release.

Syntax Description

mac-addr	Destination MAC address (unicast or multicast) to add to the address table. Packets with this destination address received in the specified VLAN are forwarded to the specified interface.
vlan vlan-id	Specify the VLAN for which the packet with the specified MAC address is received. Valid VLAN IDs are 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1005 when the standard software image (SI) is installed. Do not enter leading zeros.
interface interface-id	Interface to which the received packet is forwarded. Valid interfaces include physical ports and port channels.

Defaults

None configured.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5.2)WC(1)	This command was introduced.
12.1(6)EA2	The interface keyword and parameters were changed.
12.1(11)EA1	The mac-address-table static command was replaced by the mac address-table static command.

Examples

This example shows how to add the static address 0004.5600.67ab to the MAC address table:

```
Switch(config)# mac address-table static 0004.5600.67ab vlan 1 interface fastethernet0/2
```

This example shows how to add the static address c2f3.220a.12f4 to the MAC address table. When a packet is received in VLAN 4 with this MAC address as its destination, the packet is forwarded to the specified interface:

```
Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 interface  
gigabitethernet0/1
```

You can verify your settings by entering the **show mac address-table** privileged EXEC command.

Related Commands	Command	Description
	clear mac address-table	Deletes entries from the MAC address table.
	mac address-table aging-time	Sets the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated.
	show mac address-table	Displays the MAC address table.
	show mac address-table static	Displays static MAC address table entries only.

margin

margin

Use the **margin** interface configuration command to specify the margin value used to determine link quality during Long-Reach Ethernet (LRE) rate selection. Use the **no** form of this command to restore the default value.

margin {downstream value | upstream value}

no margin {downstream value | upstream value}

Syntax Description

downstream value	Value at the remote end of the link. Valid entries are from 0 to 10 dB.
upstream value	Value at the local end of the link. Valid entries are from 0 to 10 dB.

Defaults

The default is 0 dB.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(11)YJ	This command was introduced.

Usage Guidelines

When rate selection is running, the signal-to-noise ratio (SNR) shows the link quality. The switch does not provide any internal mechanism to assure link quality. There can be different requirements for link quality, depending on the required bit-error rate and the noise level of the environment. A noisier environment would require a higher SNR in order to provide a stable link. A lower bit-error rate would require a higher SNR. Typically a 6-dB margin provides an error rate of 10^{-21} bits.

To provide link stability, you should add a margin to the required SNR. You can configure your margins to an amount that is appropriate for the noise level of your environment. Increasing the margin requirement can cause the system to choose a lower profile, which would in turn translate to a lower rate but with a longer reach.

The switch does not guarantee any margins after a link is activated. Margins are only guaranteed when the link is established. When a link is activated, if the SNR requirements do not match the configured margin level, the link is not established.

Downstream means the remote end of the link and upstream the local end. The link has to satisfy both the local and remote margin requirements. If either one is not met, the link is advertised as down. This command has no significance if rate selection is not running on this interface.



Note Setting a margin requirement might cause the system to choose another profile, which might translate to a lower rate but a longer reach.

For a full discussion of link stability and margins, refer to the *Catalyst 2950 Series Software Configuration Guide*.

Examples

This example shows how to specify a margin of 2 dB for both upstream and downstream. If the SNR is 2 dB above the theoretical minimum for the chosen profile when the link is established, the link is classified as down and the next profile in the sequence is attempted.

```
Switch(config-if)# margin upstream 2 downstream 2  
Switch(config-if)#{}
```

This example shows how to specify a margin of 1 dB for downstream:

```
Switch(config-if)# margin downstream 1  
Switch(config-if)#{}
```

Related Commands

Command	Description
lre rate selection sequence	Assigns a rate selection sequence for the entire switch.
rate selection	Enables rate selection on a specific port.
rate selection sequence	Assigns a rate selection sequence for a specific port.

match

match

Use the **match** class-map configuration command to define the match criteria to classify traffic. Use the **no** form of this command to remove the match criteria.

match {access-group *acl-index* | access-group name *acl-name* | ip dscp *dscp-list*}

no match {access-group *acl-index* | access-group name *acl-name* | ip dscp}

This command is available only if your switch is running the enhanced software image (EI).

Syntax Description

access-group <i>acl-index</i>	Number of an IP standard or extended access control list (ACL). For an IP standard ACL, the ACL index range is 1 to 99 and 1300 to 1999. For an IP extended ACL, the ACL index range is 100 to 199 and 2000 to 2699.
access-group name <i>acl-name</i>	Name of an IP standard or extended ACL or name of an extended MAC ACL. Note The ACL name must begin with an alphabetic character to prevent ambiguity with numbered ACLs. A name also cannot contain a space or quotation mark.
ip dscp <i>dscp-list</i>	List of up to eight IP Differentiated Services Code Point (DSCP) values for each match statement to match against incoming packets. Separate each value with a space. The supported DSCP values are 0, 8, 10, 16, 18, 24, 26, 32, 34, 40, 46, 48, and 56.

Defaults

No match criteria are defined.

Command Modes

Class-map configuration

Command History

Release	Modification
12.1(6)EA2	This command was introduced.

Usage Guidelines

Use the **match** command to specify which fields in the incoming packets are examined to classify the packets. Only IP access groups, MAC access groups, and classification based on DSCP values are supported.

Only one **match** command per class map is supported.



Note For more information about configuring ACLs, refer to the “Configuring Network Security with ACLs” chapter in the *Catalyst 2950 Desktop Switch Software Configuration Guide* for this release.

Examples

This example shows how to classify traffic on an interface by using the access group named *acl2*:

```
Switch(config)# class-map class2
Switch(config-cmap)# match access-group name acl2
Switch(config-cmap)# exit
```

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

Related Commands

Command	Description
class	Defines a traffic classification for a policy to act on using the class-map name or access group.
class-map	Creates a class map to be used for matching packets to the class whose name you specify.
ip access-group	Controls access to an interface.
mac access-group	Applies a named extended MAC ACL to an interface.
show class-map	Displays quality of service (QoS) class maps.
show policy-map	Displays QoS policy maps.

media-type

Use the **media-type** interface configuration command to enable or disable fiber-optic or copper connections on a Long-Reach Ethernet (LRE) switch. It also allows you to manually set the port to select a small form-factor pluggable (SFP) connector or an RJ-45 connector. Use the **no** form of this command to return to the default setting of SFP-preferred.

```
media-type {auto-select | sfp | rj45}
no media-type {auto-select | sfp | rj45}
```

Syntax Description	
auto-select	First media-type detected makes the link.
sfp	SFP fiber-optic connection makes the link even when a link is already established with copper.
rj45	RJ-45 copper connection makes the link even when a link is already established with fiber-optic.

Defaults	The default is SFP-preferred.
-----------------	-------------------------------

Command Modes	Interface Configuration
----------------------	-------------------------

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.

Usage Guidelines	If an LRE switch detects an SFP connector inserted into the switch, whether or not fiber-optic is connected to that connector, it attempts to link by using SFP as the media-type. This preference of fiber-optic over copper connection is called <i>SFP-preferred</i> . To physically connect both fiber-optic and copper and to override the SFP preferred setting, use the auto-select parameter or force the setting to RJ45 or SFP .
-------------------------	---

You can check your settings using the **show interfaces** command with the **media** or **media interface-id** parameters.

Examples	This example of the media-type command forces the connection to a copper RJ-45 connection:
	<pre>Switch# configure t Switch(config)# interface gi0/1 Switch(config-if)# media-type rj45 Switch(config-if)</pre>

Related Commands	Command	Description
	show interfaces	Shows the status or resolution of the link.

mls qos cos

Use the **mls qos cos** interface configuration command to define the default class of service (CoS) value of a port or to assign the default CoS to all incoming packets on the port. Use the **no** form of this command to return to the default setting.

mls qos cos {default-cos | override}

no mls qos cos {default-cos | override}

Syntax Description	default-cos Assign a default CoS value to a port. If the port is CoS trusted and packets are untagged, the default CoS value becomes a CoS value used to select one output queue to index into the CoS-to-Differentiated Services Code Point (DSCP) map. The CoS range is 0 to 7. override Override the CoS of the incoming packets, and apply the default CoS value on the port to all incoming packets.
--------------------	--

Defaults The default CoS value for a port is 0.

CoS override is disabled.

Command Modes Interface configuration

Command History	Release	Modification
	12.1(6)EA2	This command was introduced.

Usage Guidelines You can use the default value to assign CoS and DSCP values to all packets entering a port if the port has been configured by using the **override** keyword.

Use the **override** keyword when all incoming packets on certain ports deserve higher or lower priority than packets entering from other ports. Even if a port was previously set to trust DSCP or CoS, this command overrides that trust state, and all the incoming CoS values are assigned the default CoS value configured with the **mls qos cos** command. If an incoming packet is tagged, the CoS value of the packet is modified with the default CoS of the port at the ingress port.

Examples This example shows how to configure the default port CoS to 4:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# mls qos trust cos
Switch(config-if)# mls qos cos 4
```

■ mls qos cos

This example shows how to assign all the packets entering a port to the default port CoS value of 4:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# mls qos cos 4
Switch(config-if)# mls qos cos override
```

You can verify your settings by entering the **show mls qos interface** privileged EXEC command.

Related Commands

Command	Description
mls qos map	Defines the CoS-to-DSCP map or the DSCP-to-CoS map.
mls qos trust	Configures the port trust state.
show mls qos interface	Displays quality of service (QoS) information.

mls qos map

Use the **mls qos map** global configuration command to define the class of service (CoS)-to-Differentiated Services Code Point (DSCP) map or DSCP-to-CoS map. Use the **no** form of this command to return to the default map.

mls qos map {cos-dscp *dscp1...dscp8* / dscp-cos *dscp-list to cos*}

no mls qos map {cos-dscp | dscp-cos}

This command is available only if your switch is running the enhanced software image (EI).

Syntax Description

cos-dscp *dscp1...dscp8* Define the CoS-to-DSCP map.

For *dscp1...dscp8*, enter eight DSCP values that correspond to CoS values 0 to 7. Separate each DSCP value with a space.

The supported DSCP values are 0, 8, 10, 16, 18, 24, 26, 32, 34, 40, 46, 48, and 56.

dscp-cos *dscp-list to cos* Define the DSCP-to-CoS map.

For *dscp-list*, enter up to 13 DSCP values separated by spaces. Then enter the **to** keyword. The supported DSCP values are 0, 8, 10, 16, 18, 24, 26, 32, 34, 40, 46, 48, and 56.

For *cos*, enter the CoS value to which the DSCP values correspond. The CoS range is 0 to 7.

Defaults

Table 2-4 shows the default CoS-to-DSCP map:

Table 2-4 Default CoS-to-DSCP Map

CoS Value	0	1	2	3	4	5	6	7
DSCP Value	0	8	16	24	32	40	48	56

Table 2-5 shows the default DSCP-to-CoS map:

Table 2-5 Default DSCP-to-CoS Map

DSCP Values	0	8, 10	16, 18	24, 26	32, 34	40, 46	48	56
CoS Value	0	1	2	3	4	5	6	7

Command Modes

Global configuration

Command History

Release Modification

12.1(6)EA2 This command was introduced.

mls qos map**Usage Guidelines**

All the maps are globally defined. You apply all maps to all ports.

If you enter the **mls qos trust cos** command, the default CoS-to-DSCP map is applied.

If you enter the **mls qos trust dscp** command, the default DSCP-to-CoS map is applied.

After a default map is applied, you can define the CoS-to-DSCP or DSCP-to-CoS map by entering consecutive **mls qos map** commands.

The supported DSCP values are 0, 8, 10, 16, 18, 24, 26, 32, 34, 40, 46, 48, and 56. If the **mls qos trust dscp** command is entered and a packet with an untrusted DSCP value is at an ingress port, the packet CoS value is set to 0.

**Note**

The switches do not support the **dscp-mutation**, **dscp-switch-priority**, **ip-prec-dscp**, and **policed-dscp** options.

Examples

This example shows how to define the DSCP-to-CoS map. DSCP values 16, 18, 24, and 26 are mapped to CoS 1. DSCP values 0, 8, and 10 are mapped to CoS 0.

```
Switch# configure terminal
Switch(config)# mls qos map dscp-cos 16 18 24 26 to 1
Switch(config)# mls qos map dscp-cos 0 8 10 to 0
```

This example shows how to define the CoS-to-DSCP map. CoS values 0 to 7 are mapped to DSCP values 8, 8, 8, 8, 24, 32, 56, and 56.

```
Switch# configure terminal
Switch(config)# mls qos map cos-dscp 8 8 8 8 24 32 56 56
```

You can verify your settings by entering the **show mls qos maps** privileged EXEC command.

Related Commands

Command	Description
mls qos cos	Defines the default CoS value of a port or assigns the default CoS to all incoming packets on the port.
mls qos trust	Configures the port trust state.
show mls qos maps	Displays quality of service (QoS) mapping information.

mls qos trust

Use the **mls qos trust** interface configuration command to configure the port trust state. Ingress traffic can be trusted, and classification is performed by examining the class of service (CoS) or the Differentiated Services Code Point (DSCP) value. Use the **no** form of this command to return a port to its untrusted state.

mls qos trust [cos [pass-through dscp] | device cisco-phone | dscp]

no mls qos trust [cos [pass-through dscp] | device cisco-phone | dscp]

Syntax Description	cos (Optional) Classify ingress packets with packet CoS values. For untagged packets, the port default CoS value is used.
cos pass-through dscp	(Optional) Configure the interface to classify ingress packets by trusting the CoS value and to send packets without modifying the DSCP value (pass-through mode).
device cisco-phone	(Optional) Classify ingress packets by trusting the value sent from the Cisco IP Phone (trusted boundary).
dscp	(Optional) Classify ingress packets with packet DSCP values (most significant 6 bits of the 8-bit service-type field). For non-IP packets, the packet CoS value is set to 0. This keyword is available only if your switch is running the enhanced software image (EI).

Defaults

The port is not trusted.

Pass-through mode is disabled.

Trusted boundary is disabled.

If no keyword is specified and the switch is running the EI, the default is **dscp**.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(6)EA2	This command was introduced.
12.1(11)EA1	The device cisco-phone and pass-through dscp keywords were added.

Usage Guidelines

Packets entering a quality of service (QoS) domain are classified at the edge of the QoS domain. When the packets are classified at the edge, the switch port within the QoS domain can be configured to one of the trusted states because there is no need to classify the packets at every switch within the domain. Use this command to specify whether the port is trusted and which fields of the packet to use to classify traffic.

When a port is configured with trust DSCP and the incoming packet is a tagged non-IP packet, the CoS value for the packet is set to 0, and the DSCP-to-CoS map is not applied. For an untagged non-IP packet, the default port CoS value is used.

■ mls qos trust

If DSCP is trusted, the DSCP field of the IP packet is not modified. However, it is still possible that the CoS value of the packet is modified (according to the DSCP-to-CoS map).

If CoS is trusted, the CoS of the packet is not modified, but DSCP can be modified (according to the CoS-to-DSCP map) if it is an IP packet.

To return a port to the untrusted state, use the **no mls qos trust** interface configuration command.

The trusted boundary feature prevents security problems if users disconnect their PCs from networked Cisco IP Phones and connect them into the switch port to take advantage of trusted CoS settings. You must globally enable the Cisco Discovery Protocol (CDP) on both the switch and on the interface connected to the IP phone. If the phone is not detected, trusted boundary disables the trust setting on the switch port and prevents misuse of a high-priority queue.

If trusted boundary is enabled and the **no mls qos trust** command is entered, the port returns to the untrusted state and cannot be configured to trust if it is connected to a Cisco IP Phone.

To disable trusted boundary, use the **no mls qos trust device** interface configuration command.

In software releases earlier than Release 12.1(11)EA1, the switch is in pass-through mode. It uses the CoS value of incoming packets without modifying the DSCP value and sends the packets from one of the four egress queues. You cannot enable or disable pass-through mode if your switch is running a software release earlier than Release 12.1(11)EA1.

In Release 12.1(11)EA1 or later, pass-through mode is disabled by default. The switch assigns a CoS value of 0 to all incoming packets without modifying the packets. It offers best-effort service to each packet regardless of the packet contents or size and sends it from a single egress queue.

You can enable pass-through mode on a switch running Release 12.1(11)EA1 or later by using the **mls qos trust cos pass-through dscp** interface configuration command. To disable pass-through mode, use the **no mls qos trust cos pass-through** interface configuration command.

**Note**

In software releases earlier than Release 12.1(11)EA1, the **mls qos trust** command is available only when the switch is running the EI.

Examples

This example shows how to configure a port to be a DSCP-trusted port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# mls qos trust dscp
```

**Note**

The **mls qos trust dscp** command is available only when the switch is running the EI.

This example shows how to specify that the Cisco IP Phone is a trusted device:

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# mls qos trust device cisco-phone
```

This example shows how to configure the interface to trust the CoS of incoming packets and to send them without modifying the DSCP field:

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# mls qos trust cos pass-through dscp
```

You can verify your settings by entering the **show mls qos interface** privileged EXEC command.

Related Commands	Command	Description
	mls qos cos	Defines the default CoS value of a port or assigns the default CoS to all incoming packets on the port.
	mls qos map	Defines the CoS-to-DSCP map or the DSCP-to-CoS map.
	show mls qos interface	Displays QoS information.

monitor session

monitor session

Use the **monitor session** global configuration command to start a new Switch Port Analyzer (SPAN) or Remote SPAN (RSPAN) session. Use the **no** form of this command to remove the SPAN or the RSPAN session or to remove source or destination interfaces from the SPAN or RSPAN session.

```
monitor session session_number {destination {interface interface-id [encapsulation {dot1q}] | remote vlan vlan-id reflector-port interface-id} | source {interface interface-id [, | -] [both] rx | tx] | remote vlan vlan-id}}

no monitor session session_number {destination {interface interface-id [encapsulation {dot1q}] | remote vlan vlan-id reflector-port interface-id} | source {interface interface-id [, | -] [both] rx | tx] | remote vlan vlan-id}}

no monitor session {session_number | all | local | remote}
```

To use the RSPAN feature, you must have the enhanced software image (EI) installed on your switch.

Syntax Description

session_number	Specify the session number identified with the SPAN or RSPAN session.
destination interface <i>interface-id</i>	Specify the destination interface for a local SPAN session. Valid interfaces are physical ports.
encapsulation	(Optional) Specify the encapsulation header for outgoing packets through a destination port. If encapsulation type is not specified, packets are sent in native form. To reconfigure a destination port in native form, enter the command without the encapsulation keyword.
dot1q	Specify the encapsulation type as 802.1Q.
destination remote vlan <i>vlan-id</i>	Specify the destination remote VLAN for an RSPAN source session.
reflector-port <i>interface-id</i>	Specify the reflector port used for a source RSPAN session.
source interface <i>interface-id</i>	Specify the SPAN source interface type, slot, and port number. Valid interfaces include physical ports and port channels.
,	Note (Optional) Specify a series of interfaces, or separate a range of interfaces from a previous range. Enter a space after the comma.
-	Note (Optional) Specify a range of interfaces. Enter a space before and after the hyphen.
both, rx, tx	(Optional) Specify the traffic direction for each source.
source remote vlan <i>vlan-id</i>	Specify the source RSPAN VLAN for an RSPAN destination session.
all, local, remote	Specify all , local , or remote to clear a SPAN or RSPAN session.

Defaults

On a source interface, the default is to monitor both received and transmitted traffic.

If encapsulation type is not specified on a destination port, packets are sent in native form with no encapsulation.

Command Modes	Global configuration
Command History	
Release	Modification
12.1(6)EA1	This command was introduced.
12.1(11)EA1	These RSPAN keywords were added: encapsulation, destination remote vlan reflector-port, source remote vlan, all, local, remote .

Usage Guidelines Traffic that enters or leaves source ports can be monitored by using SPAN or RSPAN. Traffic routed to source ports cannot be monitored.

You can configure (and store in NVRAM) one local SPAN session or multiple RSPAN sessions on a switch. The number of active sessions and combinations are subject to these restrictions:

- SPAN or RSPAN source (**rx, tx, both**): one active session limit. (SPAN and RSPAN are mutually exclusive on a source switch).
- RSPAN source sessions have one destination per session with an RSPAN VLAN associated for that session.
- Each RSPAN destination session has one or more destination interfaces for each RSPAN VLAN that it supports.
- RSPAN destination sessions are limited to two, or one if a local SPAN or a source RSPAN session is configured on the same switch.

You can monitor traffic on a single port or on a series or range of ports. You select a series or range of interfaces by using the **[, | -]** options.

If you specify a series of interfaces, you must enter a space after the comma. If you specify a range of interfaces, you must enter a space before and after the hyphen (-).

EtherChannel ports cannot be configured as SPAN or RSPAN destination or reflector ports. A physical port that is a member of an EtherChannel group can be used as a source or destination port. It does not participate in the EtherChannel group while it is configured for SPAN or RSPAN.

A port used as a reflector port cannot be a SPAN or RSPAN source or destination port, nor can a port be a reflector port for more than one session at a time.

A port used as a destination port cannot be a SPAN or RSPAN source or reflector port, nor can a port be a destination port for more than one session at a time.

You can enable 802.1X on a port that is a SPAN or RSPAN destination port; however, 802.1X is disabled until the port is removed as a SPAN destination. (If 802.1X is not available on the port, the switch will return an error message.) You can enable 802.1X on a SPAN or RSPAN source port.

Examples This example shows how to create SPAN session 1 to monitor both sent and received traffic on source interface 0/1 on destination interface 0/8:

```
Switch(config)# monitor session 1 source interface longreachethernet 0/1 both
Switch(config)# monitor session 1 destination interface longreachethernet 0/8
```

This example shows how to delete a destination port from an existing SPAN session:

```
Switch(config)# no monitor session 2 destination fastEthernet0/4
```

■ monitor session

This example shows how to configure RSPAN session 1 to monitor multiple source interfaces and to configure the destination RSPAN VLAN and the reflector-port.

```
Switch(config)# monitor session 1 source interface fastEthernet0/10 tx
Switch(config)# monitor session 1 source interface fastEthernet0/2 rx
Switch(config)# monitor session 1 source interface port-channel 102 rx
Switch(config)# monitor session 1 destination remote vlan 901 reflector-port
fastEthernet 0/1
Switch(config)# end
```

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

Related Commands	Command	Description
	remote-span	Configures an RSPAN VLAN in vlan configuration mode.
	show mvr	Displays SPAN and RSPAN session information.

mvr

Use the **mvr** global configuration command without keywords to enable the multicast VLAN registration (MVR) feature on the switch. Use the **no** form of this command to disable MVR and its options. Use the command with keywords to set the MVR mode for a switch, to configure the MVR IP multicast address, to set the maximum time to wait for a query reply before removing a port from group membership, and to specify the MVR multicast VLAN. Use the **no** form of the command to return the switch to the default settings.

```
mvr [group ip-address [count] | mode {compatible | dynamic} | querytime value | vlan vlan-id]
no mvr [group ip-address | mode {compatible | dynamic} | querytime value | vlan vlan-id]
```

Syntax Description		
	group ip-address	(Optional) Statically configure an MVR group IP multicast address on the switch. Use the no form of this command to remove a statically configured IP multicast address or contiguous addresses or, when no IP address is entered, to remove all statically configured MVR IP multicast addresses.
	count	(Optional) Configure multiple contiguous MVR group addresses. The range is from 1 to 256. The default is 1.
	mode	(Optional) Specify the MVR mode of operation. The default is compatible mode.
	compatible	Set MVR mode to provide compatibility with Catalyst 2900 XL and 3500 XL switches. This mode does not allow dynamic membership joins on source ports.
	dynamic	Set MVR mode to allow dynamic MVR membership on source ports.
	querytime value	(Optional) Set the maximum time to wait for Internet Group Management Protocol (IGMP) report memberships on a receiver port. This time applies only to receiver-port leave processing. When an IGMP query is sent from a receiver port, the switch waits for the default or configured MVR query time for an IGMP group membership report before removing the port from multicast group membership. The value is the response time in units of tenths of a second. The default is 5 tenths or one-half second. The range is 1 to 100 tenths of a second. Use the no form of the command to return to the default setting.
	vlan vlan-id	(Optional) Specify the VLAN on which MVR multicast data is expected to be received. This is also the VLAN to which all the source ports belong. The default is VLAN 1. Valid VLAN IDs are 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1001 when the standard software image (SI) is installed. Do not enter leading zeros.

Defaults

MVR is disabled by default.

The default MVR mode is compatible mode.

No IP multicast addresses are configured on the switch by default.

The default group IP address count is 0.

The default query response time is 5 tenths of or one-half second.

The default multicast VLAN for MVR is VLAN 1.

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

Command History	Release	Modification
	12.1(6)EA2	This command was introduced.

Usage Guidelines	A maximum of 256 MVR multicast groups can be configured on a switch.
-------------------------	--

Use the **mvr group** command to statically configure all the IP multicast addresses that will take part in MVR. Any multicast data sent to a configured multicast address is sent to all the source ports on the switch and to all receiver ports registered to receive data on that IP multicast address.



Note The **mvr group** command prevents adding IP multicast addresses that cause address aliasing between MVR multicast groups or with the reserved IP multicast addresses (in the range 224.0.0.xx). Each IP multicast address translates to a multicast 48-bit MAC address. If the IP address being configured translates (aliases) to the same 48-bit MAC address as a previously configured IP multicast address or the reserved MAC multicast addresses, the command fails.

The **mvr querytime** parameter applies only to receiver ports.

The **mvr group** and **mvr vlan** commands only apply to ports configured as receiver ports.

If the switch MVR is interoperating with Catalyst 2900 XL or Catalyst 3500 XL switches, set the multicast mode to compatible.

When in compatible mode, MVR does not support IGMP dynamic joins on MVR source ports.

Examples	This example shows how to enable MVR:
-----------------	---------------------------------------

```
Switch(config)# mvr
```

This example shows how to disable MVR:

```
Switch(config)# no mvr
```

This example shows how to configure 228.1.23.4 as an IP multicast address:

```
Switch(config)# mvr group 228.1.23.4
```

This command fails because of address aliasing:

```
Switch(config)# mvr group 230.1.23.4
```

Cannot add this IP address - aliases with previously configured IP address 228.1.23.4.

This example shows how to configure ten contiguous IP multicast groups with multicast addresses from 228.1.23.1 to 228.1.23.10:

```
Switch(config)# mvr group 228.1.23.1 10
```

This example shows how to delete the previously configured ten IP multicast addresses:

```
Switch(config)# no mvr group 228.1.23.1 10
```

This example shows how to delete all previously configured IP multicast addresses:

```
Switch(config)# no mvr group
```

This example shows how to set the maximum query response time as 1 second (10 tenths):

```
Switch(config)# mvr querytime 10
```

This example shows how to return the maximum query response time to the default setting of one-half second:

```
Switch(config)# no mvr querytime
```

This example shows how to set VLAN 2 as the multicast VLAN:

```
Switch(config)# mvr vlan 2
```

Use the **show mvr members** privileged EXEC command to display the IP multicast group addresses configured on the switch.

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

Related Commands

Command	Description
mvr immediate	Enables the Immediate-Leave feature on an interface.
mvr type	Configures a port as a receiver or source port.
mvr vlan group	Configures a receiver port as a member of an MVR group.
show mvr	Displays MVR global parameters or port parameters.
show mvr interface	Displays the configured MVR interfaces with their type, status, and Immediate-Leave configuration.
show mvr interface <i>interface-id</i> member	Displays all MVR groups of which the interface is a member.
show mvr members	Displays all ports that are members of an MVR multicast group; if the group has no members, its status is shown as Inactive.

mvr immediate

mvr immediate

Use the **mvr immediate** interface configuration command to enable the Immediate-Leave feature on an interface. Use the **no** form of this command to disable the feature on the interface.

mvr immediate

no mvr immediate

Syntax Description This command has no keywords or arguments.

Defaults The Immediate-Leave feature is disabled.

Command Modes Interface configuration

Command History	Release	Modification
	12.1(6)EA2	This command was introduced.

Usage Guidelines The Immediate-Leave feature applies only to receiver ports. When the Immediate-Leave feature is enabled, a receiver port leaves a multicast group more quickly. When the switch receives an Internet Group Management Protocol (IGMP) leave message from a group on a receiver port, it sends an IGMP query on that port and waits for IGMP group membership reports. If no reports are received in a configured time period, the receiver port is removed from multicast group membership. With the Immediate-Leave feature, an IGMP query is not sent from the receiver port on which the IGMP leave was received. As soon as the leave message is received, the receiver port is removed from multicast group membership, thus speeding up leave latency.

The Immediate-Leave feature should only be enabled on receiver ports to which a single receiver device is connected.

Examples This example shows how to enable the Immediate-Leave feature on a port:

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

This example shows how to disable the Immediate-Leave feature on a port:

```
Switch(config-if)# no mvr immediate
```

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

Related Commands	Command	Description
	mvr	Enables multicast VLAN registration (MVR).
	mvr type	Configures a port as a receiver or source port.
	mvr vlan group	Configures a receiver port as a member of an MVR group.
	show mvr	Displays MVR global parameters or port parameters.

mvr type

Use the **mvr type** interface configuration command to configure a port as a multicast VLAN registration (MVR) receiver or source port. Use the **no** form of the command to return the port to the default settings.

mvr type {receiver | source}

no mvr type {receiver | source}

Syntax Description	receiver	Port that receives multicast data and cannot send multicast data to multicast groups.
	source	Port that can send and receive multicast data to multicast groups.

Defaults By default, a port is configured as neither receiver nor source.

Command Modes Interface configuration

Command History	Release	Modification
	12.1(6)EA2	This command was introduced.

Usage Guidelines Configure a port as a source port if that port should be able to both send and receive multicast data bound for the configured multicast groups. Multicast data is received on all ports configured as source ports.

Configure a port as a receiver port if that port should only be able to receive multicast data and should not be able to send multicast data to the configured multicast groups. None of the receiver ports receives multicast data unless it sends an Internet Group Management Protocol (IGMP) group join message for a multicast group.

A receiver port configured as a static member of a multicast group remains a member until statically removed from membership.



Note All receiver ports must not be trunk ports and must not belong to the MVR source VLAN.

A port that is not taking part in MVR should not be configured as an MVR receiver port or source port. This port is a normal switch port and is able to send and receive multicast data with normal switch behavior.

Examples

This example shows how to configure a port as an MVR receiver port:

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# mvr type receiver
```

This example shows how to configure a port as an MVR source port:

```
Switch(config)# interface fastethernet0/3
Switch(config-if)# mvr type source
```

This example shows how to return a port to the default setting:

```
Switch(config)# interface fastethernet0/5
Switch(config-if)# no mvr type receiver
```

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

Related Commands

Command	Description
mvr	Enables MVR.
mvr immediate	Enables the Immediate-Leave feature on an interface.
mvr vlan group	Configures a receiver port as a member of an MVR group.
show mvr	Displays MVR global parameters or port parameters.

mvr vlan group

mvr vlan group

Use the **mvr vlan group** interface configuration command to statically configure a receiver port as a member of a multicast VLAN registration (MVR) group in a particular VLAN. Use the **no** form of the command to remove the port from the MVR group.

mvr vlan *vlan-id* group *ip-address*

no mvr vlan *vlan-id* group *ip-address*

Syntax Description	vlan <i>vlan-id</i> Specify the VLAN ID to which the receiver port belongs. Valid IDs are from 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1005 when the standard software image (SI) is installed. Do not enter leading zeros. group <i>ip-address</i> Specify the MVR group address for which the interface is statically configured to be a member.
---------------------------	---

Defaults By default, a port is configured as neither receiver nor source.

Command Modes Interface configuration

Command History	Release	Modification
	12.1(6)EA2	This command was introduced.

Usage Guidelines The receiver port belongs to a multicast VLAN.
The group address is configured as a MVR group address.

Examples This example shows how to configure a static MVR group entry on port 0/1 in VLAN 10:

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# mvr vlan 10 group 225.1.1.1
```

This example shows how to remove an entry on port 0/3 in VLAN 10:

```
Switch(config)# interface fastethernet0/3
Switch(config-if)# no mvr 10 group 255.1.1.2
```

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

Related Commands	Command	Description
	mvr	Enables MVR.
	mvr immediate	Enables the Immediate-Leave feature on an interface.
	mvr type	Configures a port as a receiver or source port.
	show mvr	Displays MVR global parameters or port parameters.

pagp learn-method

pagp learn-method

Use the **pagp learn-method** interface configuration command to set the source-address learning method of incoming packets received from an EtherChannel port. Use the **no** form of this command to return to the default setting.

pagp learn-method aggregation-port

no pagp learn-method

Syntax Description	aggregation-port	Specify address learning on the logical port-channel. The switch transmits packets to the source by using any of the interfaces in the EtherChannel. This setting is the default. With aggregate-port learning, it is not important on which physical port the packet arrives.
---------------------------	-------------------------	--



Note Though visible in the command-line help strings, the **physical-port** keyword is not supported.

Defaults	The default is aggregation-port (logical port channel).
-----------------	--

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

Command History	Release	Modification
	12.1(6)EA2	This command was introduced.

Usage Guidelines	The switch supports address learning only on aggregate ports even though the physical-port keyword is provided in the command-line interface (CLI). The pagp learn-method and the pagp port-priority interface configuration commands have no affect on the switch hardware.
-------------------------	---



Note You should not set the learn method to **physical-port** because the switch is an aggregate-learning device.

If the link partner to the switch is a physical learner that has the **channel-group** interface configuration command set to **auto** or **desirable**, the switch automatically uses the load-distribution method based on the source MAC address, regardless of the configured load-distribution method.

If the link partner to the switch is a physical learner that has the **channel-group** interface configuration command set to **on**, set the load-distribution method based on the source MAC address by using the **port-channel load-balance src-mac** global configuration command.

Examples

This example shows how to set the learning method to **aggregation-port** (the default):

```
Switch(config-if)# pagp learn-method aggregation-port
```

You can verify your settings by entering the **show running-config** or **show pagp channel-group-number internal** privileged EXEC command.

Related Commands

Command	Description
channel-group	Assigns an Ethernet interface to an EtherChannel group.
pagp port-priority	Selects an interface through which all Port Aggregation Protocol (PAgP) traffic through the EtherChannel is sent.
show pagp	Displays PAgP channel-group information.
show running-config	Displays the configuration information running on the switch. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 > Cisco IOS File Management Commands > Configuration File Commands .

■ pagp port-priority

pagp port-priority

You do not need to enter this command. It is documented for informational purposes only. Though visible in the command-line help strings, the switch does not support the **pagp port-priority** command.

Use the **pagp port-priority** interface configuration command to select an interface through which all Port Aggregation Protocol (PAgP) traffic through the EtherChannel is sent. Use the **no** form of this command to return to the default value.

pagp port-priority *priority*

no pagp port-priority

Syntax Description	<i>priority</i>	A priority number ranging from 0 to 255.
---------------------------	-----------------	--

Defaults	The default value is 128.
-----------------	---------------------------

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

Command History	Release	Modification
	12.1(6)EA2	This command was introduced.

Usage Guidelines	The pagp learn-method and the pagp port-priority interface configuration commands have no affect on the switch hardware.
-------------------------	--



Note You should not change the port priority because the switch does not support this command.

Related Commands	Command	Description
	pagp learn-method	Sets the source-address learning method of incoming packets received from an EtherChannel port.
	show pagp	Displays PAgP channel-group information.
	show running-config	Displays the configuration information running on the switch. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 > Cisco IOS File Management Commands > Configuration File Commands .

permit (access-list configuration)

Use the **permit** access-list configuration command to configure conditions for a named or numbered IP access control list (ACL). Use the **no** form of the command to remove a permit condition from the IP ACL.

Use these commands with standard IP ACLs:

```
permit {source source-wildcard | host source | any}
```

```
no permit {source source-wildcard | host source | any}
```

Use these commands with extended IP ACLs:

```
permit protocol {source source-wildcard | host source | any} [operator port] {destination destination-wildcard | host source | any} [operator port] [dscp dscp-value] [time-range time-range-name]
```

```
no permit protocol {source source-wildcard | host source | any} [operator port] {destination destination-wildcard | host source | any} [operator port] [dscp dscp-value] [time-range time-range-name]
```

This command is available on physical interfaces only if your switch is running the enhanced software image (EI).

Syntax Description		
	<i>protocol</i>	Name of an IP protocol. <i>protocol</i> can be ip , tcp , or udp .
	<i>source source-wildcard / host source any</i>	Define a source IP address and wildcard. The <i>source</i> is the source address of the network or host from which the packet is being sent, specified in one of these ways: <ul style="list-style-type: none"> The 32-bit quantity in dotted-decimal format. The <i>source-wildcard</i> applies wildcard bits to the source. The keyword host, followed by the 32-bit quantity in dotted-decimal format, as an abbreviation for <i>source</i> and <i>source-wildcard</i> of <i>source</i> 0.0.0.0. The keyword any as an abbreviation for <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255. You do not need to enter a <i>source-wildcard</i>.

■ permit (access-list configuration)

<i>destination</i>	Define a destination IP address and wildcard.
<i>destination-wildcard / host</i>	The <i>destination</i> is the destination address of the network or host to which the packet is being sent, specified in one of these ways:
	<ul style="list-style-type: none"> • The 32-bit quantity in dotted-decimal format. The <i>destination-wildcard</i> applies wildcard bits to the destination. • The keyword host, followed by the 32-bit quantity in dotted-decimal format, as an abbreviation for <i>destination</i> and <i>destination-wildcard</i> of <i>destination</i> 0.0.0.0. • The keyword any as an abbreviation for <i>destination</i> and <i>destination-wildcard</i> of 0.0.0.0 255.255.255.255. You do not need to enter a destination-wildcard.
<i>operator port</i>	(Optional) Define a source or destination port. The <i>operator</i> can be only eq (equal). If <i>operator</i> is after the source IP address and wildcard, conditions match when the source port matches the defined port. If <i>operator</i> is after the destination IP address and wildcard, conditions match when the destination port matches the defined port. The <i>port</i> is a decimal number or name of a Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) port. The number can be from 0 to 65535. Use TCP port names only for TCP traffic. Use UDP port names only for UDP traffic.
dscp <i>dscp-value</i>	(Optional) Define a Differentiated Services Code Point (DSCP) value to classify traffic. For the <i>dscp-value</i> , enter any of the 13 supported DSCP values (0, 8, 10, 16, 18, 24, 26, 32, 34, 40, 46, 48, and 56), or use the question mark (?) to see a list of available values.
time-range <i>time-range-name</i>	(Optional) For the time-range keyword, enter a meaningful name to identify the time range. For a more detailed explanation of this keyword, refer to the software configuration guide.

Defaults

There are no specific conditions that permit packets in a named or numbered IP ACL.

The default ACL is always terminated by an implicit deny statement for all packets.

Command Modes

Access-list configuration

Command History

Release	Modification
12.1(6)EA2	This command was introduced.

Usage Guidelines

Use this command after the **ip access-list** global configuration command to specify permit conditions for a named or numbered IP ACL. You can specify a source IP address, destination IP address, IP protocol, TCP port, or UDP port. Specify the TCP and UDP port numbers only if *protocol* is **tcp** or **udp** and *operator* is **eq**.

**Note**

For more information about configuring IP ACLs, refer to the “Configuring Network Security with ACLs” chapter in the *Catalyst 2950 Desktop Switch Software Configuration Guide* for this release.

Examples

This example shows how to create an extended IP ACL and configure permit conditions for it:

```
Switch(config)# ip access-list extended Internetfilter2
Switch(config-ext-nacl)# permit host 36.10.10.5 any
Switch(config-ext-nacl)# permit host 192.1.10.8 any
```

This is an example of a standard ACL that sets permit conditions:

```
ip access-list standard Acclist1
permit 192.5.34.0 0.0.0.255
permit 128.88.10.0 0.0.0.255
permit 36.1.1.0 0.0.0.255
```

**Note**

In these examples, all other IP access is implicitly denied.

You can verify your settings by entering the **show ip access-lists** or **show access-lists** privileged EXEC command.

Related Commands

Command	Description
deny (access-list configuration)	Sets deny conditions for an IP ACL.
ip access-group	Controls access to an interface.
ip access-list	Defines an IP ACL.
show access-lists	Displays ACLs configured on a switch.
show ip access-lists	Displays IP ACLs configured on the switch.

■ **permit (MAC access-list configuration)**

permit (MAC access-list configuration)

Use the **permit** MAC access-list configuration command to allow Layer 2 traffic to be forwarded if the conditions are matched. Use the **no** form of the command to remove a permit condition from the named MAC access control list (ACL).

```
{permit | deny} {any | host src-MAC-addr} {any | host dst-MAC-addr} [aarp | amber | appletalk
| dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 | etype-8042 | lat | lave-sca |
mop-console | mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-idp]

no {permit | deny} {any | host src-MAC-addr} {any | host dst-MAC-addr} [aarp | amber |
appletalk | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 | etype-8042 | lat |
lave-sca | mop-console | mop-dump | msdos | mumps | netbios | vines-echo | vines-ip |
xns-idp]
```

This command is available only if your switch is running the enhanced software image (EI).

Syntax Description

any	Keyword to specify to permit any source or destination MAC address.
host src-MAC-addr	Define a host MAC address. If the source address for a packet matches the defined address, traffic from that address is permitted. MAC address-based subnets are not allowed.
host dst-MAC-addr	Define a destination MAC address. If the destination address for a packet matches the defined address, traffic to that address is permitted. MAC address-based subnets are not allowed.
aarp	Select EtherType AppleTalk Address Resolution Protocol that maps a data-link address to a network address.
amber	Select EtherType DEC-Amber.
appletalk	Select EtherType AppleTalk/EtherTalk.
dec-spanning	Select EtherType Digital Equipment Corporation (DEC) spanning tree.
decnet-iv	Select EtherType DECnet Phase IV protocol.
diagnostic	Select EtherType DEC-Diagnostic.
dsm	Select EtherType DEC-DSM.
etype-6000	Select EtherType 0x6000.
etype-8042	Select EtherType 0x8042.
lat	Select EtherType DEC-LAT.
lave-sca	Select EtherType DEC-LAVC-SCA.
mop-console	Select EtherType DEC-MOP Remote Console.
mop-dump	Select EtherType DEC-MOP Dump.
msdos	Select EtherType DEC-MSDOS.
mumps	Select EtherType DEC-MUMPS.
netbios	Select EtherType DEC- Network Basic Input/Output System (NETBIOS).
vines-echo	Select EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems.

vines-ip	Select EtherType VINES IP.
xns-idp	Select EtherType Xerox Network Systems (XNS) protocol suite (from 0 to 65535), an arbitrary Ethertype in decimal, hexadecimal, or octal.

Defaults

This command has no defaults. However, the default action for a MAC-named ACL is to deny.

Command Modes

MAC access-list configuration

Command History

Release	Modification
12.1(6)EA2	This command was introduced.

Usage Guidelines

When an access control entry (ACE) is added to an ACL, an implied **deny-any-any** condition exists at the end of the list. That is, if there are no matches, the packets are denied. However, before the first ACE is added, the list permits all packets.

These options are not allowed:

- Class of service (CoS)
- Ethertype number of a packet with Ethernet II or Subnetwork Access Protocol (SNAP) encapsulation
- Link Service Access Point (LSAP) number of a packet with 802.2 encapsulation



Note For more information about configuring MAC extended ACLs, refer to the “Configuring Network Security with ACLs” chapter in the *Catalyst 2950 Desktop Switch Software Configuration Guide* for this release.

Examples

This example shows how to define the named MAC extended ACL to deny NETBIOS traffic from any source to MAC address 00c0.00a0.03fa. Traffic matching this list is allowed.

```
Switch(config-ext-macl)# permit any host 00c0.00a0.03fa netbios
```

This example shows how to remove the permit condition from the named MAC extended ACL:

```
Switch(config-ext-macl)# no permit any host 00c0.00a0.03fa netbios
```

You can verify your settings by entering the **show access-lists** privileged EXEC command.

Related Commands

Command	Description
deny (MAC access-list configuration)	Prevents Layer 2 traffic from being forwarded if conditions are matched.
mac access-list extended	Creates an ACL based on MAC addresses.
show access-lists	Displays ACLs configured on a switch.

persistence

persistence

Use the **persistence** interface configuration command to set the amount of delay before the link reports a link failure. Use the **no** form of the command to return to the default setting.

persistence delay

no persistence delay

Syntax Description	<i>delay</i> The amount of time delay; valid values can be 1 to 20 seconds.				
Defaults	The default is enabled and the duration is 3 seconds.				
Command Modes	Interface configuration mode				
Command History	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>12.1(11)YJ</td><td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification	12.1(11)YJ	This command was introduced.
Release	Modification				
12.1(11)YJ	This command was introduced.				
Usage Guidelines	Enter the persistence command before the link enters the profile link-up mode. If the link is already in the profile link-up mode when you enter the persistence value, the new value does not go into effect immediately. Instead, it becomes effective after the profile link goes down and comes back up.				
Examples:	This example of the persistence command establishes a delay of 1 second before the link reports a failure:				
	<pre>Switch(config)# interface lo0/1 Switch(config-if)# persistence 1 Switch(config-if)#</pre>				
Related Commands	<table border="1"> <thead> <tr> <th>Command</th><th>Description</th></tr> </thead> <tbody> <tr> <td>show controllers lre status</td><td>Displays the status of persistence.</td></tr> </tbody> </table>	Command	Description	show controllers lre status	Displays the status of persistence.
Command	Description				
show controllers lre status	Displays the status of persistence.				

police

Use the **police** policy-map class configuration command to define a policer for classified traffic. Use the **no** form of this command to remove an existing policer.

police rate-bps burst-byte [exceed-action {drop | dscp dscp-value}]

no police rate-bps burst-byte [exceed-action {drop | dscp dscp-value}]

This command is available only if your switch is running the enhanced software image (EI).

Syntax Description	<p><i>rate-bps</i> Specify average traffic rate in bits per second (bps). For 10/100 ports, the range is 1000000 to 100000000, and the granularity is 1 Mbps. For Gigabit-capable Ethernet ports, the range is 8000000 to 1016000000, and the granularity is 8 Mbps.</p> <p><i>burst-byte</i> Specify the normal burst size in bytes. For 10/100 ports, the burst size values are 4096, 8192, 16384, 32768, and 65536. For Gigabit-capable Ethernet ports, the burst size values are 4096, 8192, 16384, 32768, 65536, 131072, 262144, and 524288.</p> <p>exceed-action drop (Optional) When the specified rate is exceeded, specify that the switch drops the packet.</p> <p>exceed-action dscp <i>dscp-value</i> (Optional) When the specified rate is exceeded, specify that the switch changes the Differentiated Services Code Point (DSCP) of the packet to the specified <i>dscp-value</i> and then sends the packet.</p>
---------------------------	---

Defaults	No policers are defined.
-----------------	--------------------------

Command Modes	Policy-map class configuration
----------------------	--------------------------------

Command History	Release	Modification
	12.1(6)EA2	This command was introduced.

Usage Guidelines	You can configure up to six policers on ingress Fast Ethernet ports. You can configure up to 60 policers on ingress Gigabit-capable Ethernet ports. Policers cannot be configured on egress Fast Ethernet and Gigabit-capable Ethernet ports. To return to policy-map configuration mode, use the exit command. To return to privileged EXEC mode, use the end command.
-------------------------	--

police**Note**

For more information about configuring access control lists (ACLs), refer to the “Configuring Network Security with ACLs” chapter in the *Catalyst 2950 Desktop Switch Software Configuration Guide* for this release.

Examples

This example shows how to configure a policer that sets the DSCP value to 46 if traffic does not exceed a 1-Mbps average rate with a burst size of 65536 bytes and drops packets if traffic exceeds these conditions:

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# set ip dscp 46
Switch(config-pmap-c)# police 1000000 65536 exceed-action drop
Switch(config-pmap-c)# exit
```

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

Related Commands

Command	Description
policy-map	Creates or modifies a policy map that can be attached to multiple interfaces, and enters policy-map configuration mode.
show policy-map	Displays quality of service (QoS) policy maps.

policy-map

Use the **policy-map** global configuration command to create or modify a policy map that can be attached to multiple interfaces and to enter policy-map configuration mode. Use the **no** form of this command to delete an existing policy map and return to global configuration mode.

policy-map *policy-map-name*

no policy-map *policy-map-name*

This command is available only if your switch is running the enhanced software image (EI).

Syntax Description	<i>policy-map-name</i>	Name of the policy map.
---------------------------	------------------------	-------------------------

Defaults	No policy maps are defined.
-----------------	-----------------------------

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

Command History	Release	Modification
	12.1(6)EA2	This command was introduced.

Usage Guidelines	Entering the policy-map command enables the policy-map configuration mode. These configuration commands are available:
-------------------------	---

- **class**: defines the classification match criteria for the specified class map. For more information, see the **class** command.
- **description**: describes the policy map (up to 200 characters).
- **exit**: exits policy-map configuration mode and returns to global configuration mode.
- **no**: removes a previously defined policy map.
- **rename**: renames the policy map.



In a policy map, the class named *class-default* is not supported. The switch does not filter traffic based on the policy map defined by the **class class-default** policy-map configuration command.

To return to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

Before you can configure policies for classes whose match criteria are defined in a class map, use the **policy-map** command to specify the name of the policy map to be created or modified. Entering this command also enables the policy-map configuration mode in which you can configure or modify the class policies for that policy map.

■ policy-map

You can configure class policies in a policy map only if the classes have match criteria defined for them. Use the **class-map** and **match** commands to configure the match criteria for a class. Only one **match** command per class map is supported.

Only one policy map per interface per direction is supported. You can apply the same policy map to multiple interfaces but only in the ingress direction.

**Note**

For more information about configuring access control lists (ACLs), refer to the “Configuring Network Security with ACLs” chapter in the *Catalyst 2950 Desktop Switch Software Configuration Guide* for this release.

Examples

This example shows how to create a policy map called *policy1*. When attached to the ingress direction, it matches all the incoming traffic defined in *class1* and polices the traffic at an average rate of 1 Mbps and bursts at 65536 bytes. Traffic exceeding the profile is dropped.

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# police 1000000 65536 exceed-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)#

```

This example shows how to delete *policymap2*:

```
Switch(config)# no policy-map policymap2
```

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

Related Commands

Command	Description
class	Defines the default CoS value of a port or assigns the default CoS to all incoming packets on the port.
class-map	Creates a class map to be used for matching packets to the class whose name you specify.
police	Defines a policer for classified traffic.
set	Classifies IP traffic by setting a DSCP value in the packet.
show policy-map	Displays quality of service (QoS) policy maps.

port-channel load-balance

Use the **port-channel load-balance** global configuration command to set the load distribution method among the ports in the EtherChannel. Use the **no** form of this command to reset the load distribution to the default.

port-channel load-balance *method*

no port-channel load-balance

Syntax Description	<i>method</i>	Load distribution method. These are the <i>method</i> values: <ul style="list-style-type: none">• dst-mac—Load distribution using the destination MAC address• src-mac—Load distribution using the source MAC address
Defaults	The default method is src-mac .	
Command Modes	Global configuration	
Command History	Release	Modification
	12.1(6)EA2	This command was introduced.
Usage Guidelines	If the link partner to the switch is a physical learner that has the channel-group interface configuration command set to auto or desirable , the switch automatically uses the load-distribution method based on the source MAC address regardless of the configured load-distribution method. If the link partner to the switch is a physical learner that has the channel-group interface configuration command set to on , set the load-distribution method based on the source MAC address by using the port-channel load-balance src-mac global configuration command.	
Examples	This example shows how to set the load-distribution method to dst-mac : Switch(config)# port-channel load-balance dst-mac You can verify your settings by entering the show etherchannel privileged EXEC command.	

port-channel load-balance

Related Commands	Command	Description
	channel-group	Assigns an Ethernet interface to an EtherChannel group.
	show etherchannel	Displays EtherChannel information for a channel.
	show running-config	Displays the configuration information running on the switch. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 > Cisco IOS File Management Commands > Configuration File Commands .

profile (interface mode)

Use the **profile** interface configuration command to add a Long-Reach Ethernet (LRE) profile to a port. Use the **no** form of this command to delete a profile from the sequence.

profile *profile-name*

no profile *profile-name*

Syntax Description	<i>profile-name</i>	Name of the profile. The profile name can be a Cisco-supplied profile or a user-created profile. See the <i>Catalyst 2950 Series Software Configuration Guide</i> for further details on Cisco-supplied profiles.
---------------------------	---------------------	---

Defaults	The default is not defined.
-----------------	-----------------------------

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

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.

Usage Guidelines	This command can be used to assign a profile to a specific LRE port. The profile command in interface mode has a higher precedence than the profile specified in global scope using the lre profile profile command. If the profile command is not specified, the profile specified in global scope applies to this port.
-------------------------	--

For a complete list of considerations for using LRE profiles and profile sequences, refer to the “LRE Links and LRE Profiles” section in the *Catalyst 2950 Series Software Configuration Guide*.

Examples	This example shows how to assign the LRE-8 profile to LRE port 1:
-----------------	---

```
Switch(config)# interface lo0/1
Switch(config-if)# profile lre-8
Switch(config-if)#
```

This example shows how to return port 1 to global scope from the previous example.

```
Switch(config)# interface lo0/1
Switch(config-if)# no profile lre-8
Switch(config-if)#
```

Related Commands	Command	Description
	lre rate selection sequence	Assigns the rate selection sequence for the entire switch.
	lre sequence	Defines a new sequence.

■ profile (interface mode)

Command	Description
rate selection	Enables rate selection on a specific port.
rate selection sequence	Assigns a rate selection sequence for a specific port.
show controllers lre profile names	Displays information about the LRE profiles available on the switch.
show controllers lre profile details	Displays information about the LRE profiles and sequences available on the switch.

profile (sequence mode)

Use the **profile** sequence configuration command to add a Long-Reach Ethernet (LRE) profile to a sequence. Use the **no** form of this command to delete a profile from the sequence.

profile *profile-name*

no profile *profile-name*

Syntax Description	<i>profile-name</i>	Name of the profile. The profile name can be a Cisco-supplied profile or a user-created profile. See the <i>Catalyst 2950 Series Software Configuration Guide</i> for further details on Cisco-supplied profiles.
---------------------------	---------------------	---

Defaults	The default is LRE-10.
-----------------	------------------------

Command Modes	Sequence mode
----------------------	---------------

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.

Usage Guidelines	When you add an LRE profile to a sequence, the profile is added as in a first-in, first-out (FIFO) queue. Rate selection attempts to establish a link with the first profile in the sequence. If the link is not established in that profile, rate selection uses the next profile in the queue.
-------------------------	--

You cannot add a profile in the middle of the sequence. To add a profile to a user-defined sequence in the middle of a sequence, you need to delete the most-recent profiles first.

Although you can delete a profile from a sequence, you cannot change a sequence's configuration if it is in use by an interface.

You cannot add or delete a profile from a system-defined sequence.

For a complete list of considerations for using LRE profiles and profile sequences, refer to the "LRE Links and LRE Profiles" section in the *Catalyst 2950 Series Software Configuration Guide*.

Examples	This example shows how to assign the LRE-4 profile to the seq2downsym sequence:
-----------------	---

```
Switch(config)# lre sequence seq2downsym
Switch(config-seq)# profile LRE-4
Switch(config-seq)#
```

■ profile (sequence mode)

Related Commands	Command	Description
	lre rate selection sequence	Assigns the rate selection sequence for the entire switch.
	lre sequence	Defines a new sequence.
	rate selection	Enables rate selection on a specific port.
	rate selection sequence	Assigns a sequence for a specific port.

rate selection

Use the **rate selection** interface configuration command to enable rate selection on a port. Use the **no** form of this command to disable rate selection on ports already configured for rate selection.

rate selection

no rate selection

Syntax Description This command has no arguments or keywords.

Defaults The default is enabled.

Command Modes Interface configuration mode

Command History	Release	Modification
	12.1(11)YJ and 12.1(11)WC6	This command was introduced.

Usage Guidelines Use this command to enable rate selection on a port. The **rate selection** command does not cause rate selection to start. To start rate selection, you need to assign a sequence to a port. This command does not specify a sequence. Use the **rate selection sequence** command or the **lre rate selection sequence** command.

If a global sequence is configured and rate selection is disabled on the port, rate selection runs on the entire switch except on the port where rate selection is disabled.

Examples This example disables the rate selection feature on a port:

```
Switch(config-if)# no rate selection
Switch(config-if)#
```

Related Commands	Command	Description
	rate selection sequence	Assigns a sequence on a port.
	lre rate selection sequence	Assigns a sequence for the entire switch.

 ■ **rate selection profile lock**

rate selection profile lock

Use the **rate selection profile lock** interface configuration command to lock a profile in a port that is enabled for rate selection. Use the **no** form of the command to unlock a profile in a port.

rate selection profile lock

no rate selection profile lock

Syntax Description This command has no arguments or keywords.

Command Modes Interface configuration mode

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.

Usage Guidelines This command does not enable rate selection. It only has significance when a sequence is assigned to a port.

If rate selection is already converged on the port, this command causes the profile chosen by rate selection to immediately lock. During the lock process, the name of the profile appends to the end of this command. For example, if rate selection converges on LRE-15 and you enter this command, the resulting locked configuration looks like this:

rate selection profile lock LRE-15

If rate selection is not already converged on the port, this command has no immediate effect. However, when rate selection converges for that port, the profile is locked immediately, and the output of the running configuration is saved as in the example.

Examples This example locks a profile to a port that is running rate selection:

```
Switch(config-if)# rate selection profile lock
Switch(config-if)#
```

Related Commands	Command	Description
	rate selection sequence	Assigns a sequence on a port.
	lre rate selection sequence	Assigns a sequence for the entire switch.
	show controllers lre status	Displays information about the profiles and sequences when the sequence parameter is specified.

rate selection sequence

Use the **rate selection sequence** interface configuration command to assign a sequence to a port and to start rate selection. The **no** form of the command removes a specific rate selection sequence on a port.

rate selection sequence *sequenceName*

no rate selection sequence *sequenceName*

Syntax Description	<i>sequenceName</i>	The name of the sequence being applied to the port. Refer to the <i>Catalyst 2950 Series Software Configuration Guide</i> for a names of system-supplied sequences.
---------------------------	---------------------	---

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

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.

Usage Guidelines	A sequence is a list of profiles. Using this command overrides the default profile of LRE-10 and assigns a sequence of your choice.
-------------------------	---

When rate selection is enabled, profiles and sequences follow a predefined priority scheme that determines the rate for a port or for the entire switch. In general, sequences have priority over standalone profiles, and per-port configurations have priority over switch-wide configurations. Specifically, these are the priority levels with rate selection enabled, from highest to lowest:

1. Per-port sequence
2. Global sequence
3. Port profile
4. Global profile

Cisco provides a set of preconfigured sequences, called *system-defined* sequences. System-defined sequences cannot be modified. Users can create and modify their own sequences by using the **profile** command.

The rate selection sequence command is rejected if the specified sequence does not exist or is a null sequence. A null sequence is a sequence that does not have any profiles.

For further details on profiles, sequences and their priority scheme, see *Catalyst 2950 Series Software Configuration Guide*.

Examples	This example applies the sequence, CISCO-COMPLETE-SEQUENCE to the port:
-----------------	---

```
Switch(config-if)# rate selection sequence CISCO-COMPLETE-SEQUENCE
Switch(config-if)#

```

■ rate selection sequence

Related Commands	Command	Description
	rate selection	Enables rate selection on ports already configured for rate selection.
	show controllers lre sequence	Displays the list of sequences.

rcommand

Use the **rcommand** user EXEC command to start a Telnet session and to enter commands from the command switch for a member switch. To end the session, enter the **exit** command.

```
rcommand {n | commander | mac-address hw-addr}
```

Syntax Description	<table border="0"> <tr> <td>n</td><td>Provide the number that identifies a cluster member. The range is from 0 to 15.</td></tr> <tr> <td>commander</td><td>Provide access to the command switch from a member switch.</td></tr> <tr> <td>mac-address hw-addr</td><td>MAC address of the member switch.</td></tr> </table>	n	Provide the number that identifies a cluster member. The range is from 0 to 15.	commander	Provide access to the command switch from a member switch.	mac-address hw-addr	MAC address of the member switch.
n	Provide the number that identifies a cluster member. The range is from 0 to 15.						
commander	Provide access to the command switch from a member switch.						
mac-address hw-addr	MAC address of the member switch.						

Command Modes	User EXEC
----------------------	-----------

Command History	Release	Modification
	12.0(5.2)WC(1)	This command was introduced.

Usage Guidelines	If the switch is the command switch but the member switch <i>n</i> does not exist, an error message appears. To obtain the switch number, enter the show cluster members privileged EXEC command on the command switch.
-------------------------	--

You can use this command to access a member switch from the command-switch prompt or to access a command switch from the member-switch prompt.

For Catalyst 2900 XL, 2950, 3500 XL, and 3550 switches, the Telnet session accesses the member-switch command-line interface (CLI) at the same privilege level as on the command switch. For example, if you enter this command at user level on the cluster command switch, the member switch is accessed at user level. If you use this command on the command switch at privileged level, the command accesses the remote device at privileged level. If you use an intermediate enable-level lower than *privileged*, access to the member switch is at user level.

For Catalyst 1900 and 2820 switches running standard edition software, the Telnet session accesses the menu console (the menu-driven interface) if the command switch is at privilege level 15. If the command switch is at privilege level 1, you are prompted for the password before being able to access the menu console. Command switch privilege levels map to the member switches running standard edition software as follows:

- If the command switch privilege level is from 1 to 14, the member switch is accessed at privilege level 1.
- If the command switch privilege level is 15, the member switch is accessed at privilege level 15.

The Catalyst 1900 and 2820 CLI is available only on switches running Enterprise Edition Software.

This command does not work if the vty lines of the command switch have access-class configurations.

You are not prompted for a password because the member switches inherited the password of the command switch when they joined the cluster.

rcommand**Examples**

This example shows how to start a session with member 3. All subsequent commands are directed to member 3 until you enter the **exit** command or close the session.

```
Switch# rcommand 3
Switch-3# show version
Cisco Internet Operating System Software ...
...
Switch-3# exit
Switch#
```

Related Commands

Command	Description
show cluster members	Displays information about the cluster members.

remote-span

Use the **remote-span** VLAN configuration command to add the Remote Switched Port Analyzer (RSPAN) feature to a VLAN. Use the **no** form of this command to remove the RSPAN feature from the VLAN.

remote-span

no remote-span

This command is available only if your switch is running the enhanced software image (EI).

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

Defaults	No RSPAN VLANs are defined.
-----------------	-----------------------------

Command Modes	VLAN configuration
----------------------	--------------------

Command History	Release	Modification
	12.1(11)EA1	This command was introduced.

Usage Guidelines	When a VLAN is converted from a normal VLAN to an RSPAN VLAN (or the reverse), the VLAN is first deleted and is then recreated with the new configuration. The RSPAN feature is propagated by VLAN Trunking Protocol (VTP) for VLAN-IDs that are lower than 1005.
-------------------------	---

Before you configure the RSPAN **remote-span** feature, use the **vlan** (global configuration) command to create the VLAN.

Examples	This example shows how to configure an RSPAN VLAN.
-----------------	--

```
Switch(config)# vlan 901
Switch(config-vlan)# remote-span
```

This example shows how to remove the RSPAN feature from a VLAN.

```
Switch(config)# vlan 901
Switch(config-vlan)# no remote-span
```

You can verify your settings by entering the **show vlan** user EXEC command.

remote-span

Related Commands	Command	Description
	monitor session	Enables SPAN and RSPAN monitoring on a port and configures a port as a source or destination port.
	vlan (global configuration)	Changes to config-vlan mode where you can configure VLANs 1 to 1005. Do not enter leading zeros.

rmon collection stats

Use the **rmon collection stats** interface configuration command to collect Ethernet group statistics. The Ethernet group statistics include utilization statistics about broadcast and multicast packets and error statistics about Cyclic Redundancy Check (CRC) alignment errors and collisions. Use the **no** form of this command to return to the default setting.

rmon collection stats index [owner name]

no rmon collection stats index [owner name]

Syntax Description	<i>index</i> Remote Network Monitoring (RMON) collection control index. The range is 1 to 65535. <i>owner name</i> (Optional) Owner of the RMON collection.
---------------------------	--

Defaults The RMON statistics collection is disabled.

Command Modes Interface configuration

Command History	Release	Modification
	12.0(5.2)WC(1)	This command was introduced.

Usage Guidelines The RMON statistics collection command is based on hardware counters.

Examples This example shows how to collect RMON statistics for the owner root on an interface:

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# rmon collection stats 2 owner root
```

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

Related Commands	Command	Description
	show rmon statistics	Displays RMON statistics. For more information on this command, select Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 > Cisco IOS System Management Commands > RMON Commands .

■ rmon collection stats

service-policy

Use the **service-policy** interface configuration command to apply a policy map defined by the **policy-map** command to the input of a particular interface. Use the **no** form of this command to remove the policy map and interface association.

service-policy input *policy-map-name*

no service-policy input *policy-map-name*

This command is available only if your switch is running the enhanced software image (EI).

Syntax Description	<i>policy-map-name</i>	Apply the specified policy map to the input of an interface.
Defaults	No policy maps are attached to the interface.	
Command Modes	Interface configuration	
Command History	Release	Modification
	12.1(6)EA2	This command was introduced.
Usage Guidelines	Only one policy map per ingress interface is supported. Service policy maps cannot be defined on egress interfaces.	 For more information about configuring access control lists (ACLs), refer to the “Configuring Network Security with ACLs” chapter in the <i>Catalyst 2950 Desktop Switch Software Configuration Guide</i> for this release.
Examples	<p>This example shows how to apply <i>plcmpl1</i> to an ingress interface:</p> <pre>Switch(config)# interface gigabitethernet0/1 Switch(config-if)# service-policy input plcmpl1</pre> <p>You can verify your settings by entering the show policy-map privileged EXEC command.</p>	
Related Commands	Command	Description
	policy-map	Creates or modifies a policy map that can be attached to multiple interfaces to specify a service policy.
	show policy-map	Displays quality of service (QoS) policy maps.

set

set

Use the **set** policy-map class configuration command to classify IP traffic by setting a Differentiated Services Code Point (DSCP) value. Use the **no** form of this command to remove traffic classification.

```
set ip dscp new-dscp
```

```
no set ip dscp new-dscp
```

This command is available only if your switch is running the enhanced software image (EI).

Syntax Description	<i>new-dscp</i>	New DSCP value assigned to the classified traffic. The supported DSCP values are 0, 8, 10, 16, 18, 24, 26, 32, 34, 40, 46, 48, and 56.
---------------------------	-----------------	---

Defaults	No traffic classification is defined.
-----------------	---------------------------------------

Command Modes	Policy-map class configuration
----------------------	--------------------------------

Command History	Release	Modification
	12.1(6)EA2	This command was introduced.

Usage Guidelines	The set command can be used in a policy with a match command.
	The set command sets the DSCP value for in-profile packets.



This command does not support IP precedence.

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



For more information about configuring access control lists (ACLs), refer to the “Configuring Network Security with ACLs” chapter in the *Catalyst 2950 Desktop Switch Software Configuration Guide* for this release.

Examples

This example shows how to assign a DSCP value of 10 to all FTP traffic without any policers:

```
Switch(config)# policy-map policy_ftp
Switch(config-pmap)# class ftp_class
Switch(config-pmap-c)# set ip dscp 10
Switch(config-pmap)# exit
```

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

Related Commands

Command	Description
police	Defines a policer for classified traffic.
policy-map	Creates or modifies a policy map that can be attached to multiple interfaces to specify a service policy.
show policy-map	Displays quality of service (QoS) policy maps.

show access-lists

show access-lists

Use the **show access-lists** privileged EXEC command to display access control lists (ACLs) configured on the switch.

show access-lists [name | number] [| {begin | exclude | include} expression]

Syntax Description

<i>name</i>	(Optional) Name of the ACL.
<i>number</i>	(Optional) ACL number. The range is from 1 to 2699.
begin	(Optional) Display begins with the line that matches the <i>expression</i> .
exclude	(Optional) Display excludes lines that match the <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(6)EA2	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter | **exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show access-lists** command:

```
Switch# show access-lists
Standard IP access list testingacl
    permit 10.10.10.2
Standard IP access list wizard_1-1-1-2
    permit 1.1.1.2
Extended IP access list 103
    permit tcp any any eq www
Extended IP access list CMP-NAT-ACL
    Dynamic Cluster-HSRP deny ip any any
    Dynamic Cluster-NAT permit ip any any
        permit ip host 10.123.222.192 any
        permit ip host 10.228.215.0 any
        permit ip host 10.245.137.0 any
        permit ip host 10.245.155.128 any
        permit ip host 10.221.111.64 any
        permit ip host 10.216.25.128 any
        permit ip host 10.186.122.64 any
        permit ip host 10.169.110.128 any
        permit ip host 10.146.106.192 any
```

Related Commands	Command	Description
	access-list (IP extended)	Configures an extended IP ACL on the switch.
	access-list (IP standard)	Configures a standard IP ACL on the switch.
	ip access-list	Configures an IP ACL on the switch.
	mac access-list extended	Creates an ACL based on MAC addresses.
	show ip access-lists	Displays the IP ACLs configured on a switch.

■ show auto qos

show auto qos

Use the **show auto qos** user EXEC command to display the configuration applied and the new defaults in effect by the automatic quality of service (auto-QoS) feature.

```
show auto qos [interface [interface-id]] | [voip [interface [interface-id]] [ | {begin | exclude | include} expression]
```

This command is available only if your switch is running the enhanced software image (EI).

Syntax Description	interface [interface-id]	(Optional) Display auto-QoS information for the specified interface or for all interfaces. Valid interfaces include physical ports.
	voip	(Optional) Display auto-QoS information for voice over IP (VoIP).
	 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	 include	(Optional) Display includes lines that match the specified <i>expression</i> .
	expression	Expression in the output to use as a reference point.

Command Modes	User EXEC
----------------------	-----------

Command History	Release	Modification
	12.1(11)EA1	This command was introduced.

Usage Guidelines	This command displays the auto-QoS defaults; it does not display any user changes to the configuration that might be in effect.
-------------------------	---

To display information about the current QoS configuration that might be affected by auto-QoS, use one of these commands:

- **show mls qos**
- **show mls qos map cos-dscp**
- **show mls qos interface [interface-id] [policers]**



The **show running-config** privileged EXEC command displays only user-entered commands, which can be written to nonvolatile RAM (NVRAM) by using the **copy running-config startup-config** privileged EXEC command. The **show running-config** command does not display the auto-QoS-generated configuration, and this configuration is not written to NVRAM.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show auto qos voip** command when auto-QoS is enabled:

```
Switch# show auto qos voip
AutoQoS is enabled with defaults as follows:
Cos-dscp map:
cos: 0 1 2 3 4 5 6 7
-----
dscp: 0 10 18 26 34 46 48 56
Cos-queue map:
CoS Value : 0 1 2 3 4 5 6 7
Priority Queue : 1 1 1 3 3 4 3 3
WRR Queue : 1 2 3 4
Bandwidth : 20 1 80 0
```

This is an example of output from the **show auto qos voip interface gigabitethernet0/2** command when the **auto qos voip cisco-phone** interface configuration command is enabled:

```
Switch# show auto qos voip interface gigabitethernet0/2
Switch#sh auto qos voip int fa0/1
FastEthernet0/1
Ingress AutoQoS is enabled
trust mode:trust cos
trust device:cisco-phone
Switch#sh auto qos voip int g0/1
GigabitEthernet0/1
Ingress AutoQoS is enabled
trust mode:trust cos
trust device:cisco-phone
Egress AutoQoS is enabled with defaults as follows:
Notify Q depth:
qid-size
1 - 80
2 - 1
3 - 20
4 - 1
Egress expedite queue: ena
wrr bandwidth weights:
qid-weights
1 - 20
2 - 1
3 - 80
4 - 0      when expedite queue is disabled
Cos-queue map:
cos-qid
0 - 1
1 - 1
2 - 1
3 - 3
4 - 3
5 - 4
6 - 3
7 - 3
```

■ show auto qos

This is an example of output from the **show auto qos voip interface fastethernet0/1** command when the **auto qos voip cisco-phone** interface configuration command is entered:

```
Switch# show auto qos voip interface fastethernet0/1
FastEthernet0/1
Ingress AutoQoS is enabled
trust mode: cos
trust device: cisco-phone
Egress AutoQoS is enabled with defaults as follows:
Minimum reserve buffer size:
  170 0 65 26 0 0 0 0
Egress expedite queue: ena
wrr bandwidth weights:
qid-weights
  1 - 20
  2 - 1
  3 - 80
  4 - 0 when expedite queue is disabled
Cos-queue map:
cos-qid
  0 - 1
  1 - 1
  2 - 1
  3 - 3
  4 - 3
  5 - 4
  6 - 3
  7 - 3
```

Related Commands

Command	Description
auto qos voip	Automatically configures QoS for VoIP within a QoS domain.

show boot

Use the **show boot** privileged EXEC command to display the settings of the boot environment variables.

show boot [| {begin | exclude | include} expression]

Syntax Description	<table border="0"> <tr> <td> begin</td><td>(Optional) Display begins with the line that matches the <i>expression</i>.</td></tr> <tr> <td> exclude</td><td>(Optional) Display excludes lines that match the <i>expression</i>.</td></tr> <tr> <td> include</td><td>(Optional) Display includes lines that match the specified <i>expression</i>.</td></tr> <tr> <td><i>expression</i></td><td>Expression in the output to use as a reference point.</td></tr> </table>	begin	(Optional) Display begins with the line that matches the <i>expression</i> .	exclude	(Optional) Display excludes lines that match the <i>expression</i> .	include	(Optional) Display includes lines that match the specified <i>expression</i> .	<i>expression</i>	Expression in the output to use as a reference point.
begin	(Optional) Display begins with the line that matches the <i>expression</i> .								
exclude	(Optional) Display excludes lines that match the <i>expression</i> .								
include	(Optional) Display includes lines that match the specified <i>expression</i> .								
<i>expression</i>	Expression in the output to use as a reference point.								

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

Command History	Release	Modification
	12.1(11)EA1	This command was introduced.

Usage Guidelines	Expressions are case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> do not appear, but the lines that contain <i>Output</i> appear.
-------------------------	--

Examples	This example shows output from the show boot command. Table 2-6 describes each field in the output.
-----------------	--

```
Switch# show boot
BOOT path-list:      flash:boot
Config file:         flash:config.text
Private Config file: flash:private-config.text
Enable Break:        no
Manual Boot:         yes
HELPER path-list:
NVRAM/Config file
    buffer size:   32768
```

show boot**Table 2-6 show boot Field Descriptions**

Field	Description
BOOT path-list	Displays a semicolon-separated list of executable files to load and to execute when automatically booting. If the BOOT environment variable is not set, the system attempts to load and execute the first executable image it can find by using a recursive, depth-first search through the Flash file system. In a depth-first search of a directory, each encountered subdirectory is completely searched before continuing the search in the original directory. If the BOOT variable is set but the specified images cannot be loaded, the system attempts to boot the first bootable file that it can find in the Flash file system.
Config file	Displays the filename that IOS uses to read and write a nonvolatile copy of the system configuration.
Private Config file	Displays the filename that IOS uses to read and write a nonvolatile copy of the private configuration.
Enable Break	Displays whether a break during booting is enabled or disabled. If it is set to <i>yes</i> , <i>on</i> , or <i>1</i> , you can interrupt the automatic boot process by pressing the Break key on the console after the Flash file system is initialized.
Manual Boot	Displays whether the switch automatically or manually boots. If it is set to <i>no</i> or <i>0</i> , the boot loader attempts to automatically boot the system. If it is set to anything else, you must manually boot the switch from the boot loader mode.
Helper path-list	Displays a semicolon-separated list of loadable files to dynamically load during the boot loader initialization. Helper files extend or patch the functionality of the boot loader.
NVRAM/Config file buffer size	Displays the buffer size that IOS uses to hold a copy of the configuration file in memory. The configuration file cannot be larger than the buffer size allocation.

Related Commands

Command	Description
boot private-config-file	Specifies the filename that IOS uses to read and write a nonvolatile copy of the private configuration.

show class-map

Use the **show class-map** user EXEC command to display quality of service (QoS) class maps, which define the match criteria to classify traffic.

show class-map [class-map-name] [| {begin | exclude | include} expression]

This command is available only if your switch is running the enhanced software image (EI).

Syntax Description	<table border="0"> <tr> <td><i>class-map-name</i></td><td>(Optional) Display the contents of the specified class map.</td></tr> <tr> <td> begin</td><td>(Optional) Display begins with the line that matches the <i>expression</i>.</td></tr> <tr> <td> exclude</td><td>(Optional) Display excludes lines that match the <i>expression</i>.</td></tr> <tr> <td> include</td><td>(Optional) Display includes lines that match the specified <i>expression</i>.</td></tr> <tr> <td><i>expression</i></td><td>Expression in the output to use as a reference point.</td></tr> </table>	<i>class-map-name</i>	(Optional) Display the contents of the specified class map.	begin	(Optional) Display begins with the line that matches the <i>expression</i> .	exclude	(Optional) Display excludes lines that match the <i>expression</i> .	include	(Optional) Display includes lines that match the specified <i>expression</i> .	<i>expression</i>	Expression in the output to use as a reference point.
<i>class-map-name</i>	(Optional) Display the contents of the specified class map.										
begin	(Optional) Display begins with the line that matches the <i>expression</i> .										
exclude	(Optional) Display excludes lines that match the <i>expression</i> .										
include	(Optional) Display includes lines that match the specified <i>expression</i> .										
<i>expression</i>	Expression in the output to use as a reference point.										

Command Modes	User EXEC
----------------------	-----------

Command History	Release	Modification
	12.1(6)EA2	This command was introduced.

Usage Guidelines	If you do not specify a <i>class-map-name</i> , all class maps appear. Expressions are case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> do not appear, but the lines that contain <i>Output</i> appear.
-------------------------	--

Examples	This is an example of output from the show class-map test command:
-----------------	---

```
Switch> show class-map test
Class Map match-all test (id 2)
  Match access-group name testingacl
```

This is an example of output from the **show class-map** command:

```
Switch> show class-map
Class Map match-all wizard_1-1-1-2 (id 3)
  Match access-group name videowizard_1-1-1-2

Class Map match-all test (id 2)
  Match access-group name testingacl

Class Map match-any class-default (id 0)
  Match any

Class Map match-all class1 (id 5)
  Match access-group 103

Class Map match-all classtest (id 4)
  Description: This is a test.
  Match access-group name testingacl
```

■ **show class-map**

Related Commands	Command	Description
	class-map	Creates a class map to be used for matching packets to the class whose name you specify.
	match	Defines the match criteria to classify traffic.

show cluster

Use the **show cluster** privileged EXEC command to display the cluster status and a summary of the cluster to which the switch belongs. This command can be entered on command and member switches.

show cluster [| {begin | exclude | include} expression]

Syntax Descriptions	<table border="0"> <tr> <td> begin</td><td>(Optional) Display begins with the line that matches the specified <i>expression</i>.</td></tr> <tr> <td> exclude</td><td>(Optional) Display excludes lines that match the specified <i>expression</i>.</td></tr> <tr> <td> include</td><td>(Optional) Display includes lines that match the specified <i>expression</i>.</td></tr> <tr> <td><i>expression</i></td><td>Expression in the output to use as a reference point.</td></tr> </table>	begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .	exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .	include	(Optional) Display includes lines that match the specified <i>expression</i> .	<i>expression</i>	Expression in the output to use as a reference point.
begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .								
exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .								
include	(Optional) Display includes lines that match the specified <i>expression</i> .								
<i>expression</i>	Expression in the output to use as a reference point.								

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

Command History	Release	Modification
	12.0(5.2)WC(1)	This command was introduced.

Usage Guidelines On a member switch, this command displays the identity of the command switch, the switch member number, and the state of its connectivity with the command switch.

On a command switch, this command displays the cluster name and the total number of members. It also shows the cluster status and time since the status changed. If redundancy is enabled, it displays the primary and secondary command-switch information.

If you enter this command on a switch that is not a cluster member, the error message *Not a management cluster member* appears.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples This is an example of output when this command is entered on the active command switch:

```
Switch# show cluster
Command switch for cluster "Switch1"
Total number of members: 7
Status: 1 members are unreachable
Time since last status change: 0 days, 0 hours, 2 minutes
Redundancy: Enabled
Standby command switch: Member 1
Standby Group: Switch1_standby
Standby Group Number: 110
Heartbeat interval: 8
Heartbeat hold-time: 80
Extended discovery hop count: 3
```

■ show cluster

This is an example of output when this command is entered on a member switch:

```
Switch# show cluster
Member switch for cluster "commander"
  Member number: 3
  Management IP address: 192.192.192.192
  Command switch mac address: 0000.0c07.ac14
  Heartbeat interval: 8
  Heartbeat hold-time: 80
```

This is an example of output when this command is entered on a member switch that is configured as the standby command switch:

```
Switch# show cluster
Member switch for cluster "commander"
  Member number: 3 (Standby command switch)
  Management IP address: 192.192.192.192
  Command switch mac address: 0000.0c07.ac14
  Heartbeat interval: 8
  Heartbeat hold-time: 80
```

This is an example of output when this command is entered on the command switch that has lost connectivity from member 1:

```
Switch# show cluster
Command switch for cluster "Switch1"
  Total number of members: 7
  Status: 1 members are unreachable
  Time since last status change: 0 days, 0 hours, 5 minutes
  Redundancy: Disabled
  Heartbeat interval: 8
  Heartbeat hold-time: 80
  Extended discovery hop count: 3
```

This is an example of output when this command is entered on a member switch that has lost connectivity with the command switch:

```
Switch# show cluster
Member switch for cluster "commander"
  Member number: <UNKNOWN>
  Management IP address: 192.192.192.192
  Command switch mac address: 0000.0c07.ac14
  Heartbeat interval: 8
  Heartbeat hold-time: 80
```

Related Commands

Command	Description
cluster enable	Enables a command-capable switch as the cluster command switch, assigns a cluster name, and optionally assigns a member number to it.
show cluster candidates	Displays a list of candidate switches.
show cluster members	Displays information about the cluster members.

show cluster candidates

Use the **show cluster candidates** privileged EXEC command on the command switch to display a list of candidate switches.

show cluster candidates [detail | mac-address H.H.H.] [| {begin | exclude | include} expression]

Syntax Description

detail	(Optional) Display detailed information for all candidates.
mac-address H.H.H.	(Optional) Hexadecimal MAC address of the cluster candidate.
 begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5.2)WC(1)	This command was introduced.

Usage Guidelines

You should only enter this command on a command switch.

If the switch is not a command switch, the command displays an empty line at the prompt.

The SN in the output means *switch member number*. If *E* is in the SN column, it means that the switch is discovered through extended discovery. If *E* does not appear in the SN column, it means that the *switch member number* is the upstream neighbor of the candidate switch. The hop count is the number of devices the candidate is from the command switch.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show cluster candidates** command:

```
Switch# show cluster candidates
| ---Upstream--- |
MAC Address      Name       Device Type      PortIf    FEC Hops SN PortIf    FEC
00d0.7961.c4c0  c2950-012  WS-C2950-12   Fa0/5     1  0   Fa0/3
00d0.bbf5.e900  ldf-dist-128 WS-C3524-XL   Fa0/7     1  0   Fa0/24
00e0.1e7e.be80  1900_Switch 1900          3         0   1  0   Fa0/11
00e0.1e9f.7a00  c2924XL-24  WS-C2924-XL   Fa0/5     1  0   Fa0/3
00e0.1e9f.8c00  c2912XL-12-2 WS-C2912-XL   Fa0/4     1  0   Fa0/7
00e0.1e9f.8c40  c2912XL-12-1 WS-C2912-XL   Fa0/1     1  0   Fa0/9
0050.2e4a.9fb0  C3508XL-0032 WS-C3508-XL E
0050.354e.7cd0  C2924XL-0034 WS-C2924-XL E
```

■ show cluster candidates

This is an example of output from the **show cluster candidates** command that uses the MAC address of a member switch directly connected to the command switch:

```
Switch# show cluster candidates mac-address 00d0.7961.c4c0
Device 'c2950-12' with mac address number 00d0.7961.c4c0
  Device type: cisco WS-C2950-12
  Upstream MAC address: 00d0.796d.2f00 (Cluster Member 0)
  Local port: Fa0/3 FEC number:
  Upstream port: Fa0/13 FEC Number:
  Hops from cluster edge: 1
  Hops from command device: 1
```

This is an example of output from the **show cluster candidates** command that uses the MAC address of a member switch three hops from the cluster edge:

```
Switch# show cluster candidates mac-address 0010.7bb6.1cc0
Device 'c2950-24' with mac address number 0010.7bb6.1cc0
  Device type: cisco WS-C2950-24
  Upstream MAC address: 0010.7bb6.1cd4
  Local port: Fa2/1 FEC number:
  Upstream port: Fa0/24 FEC Number:
  Hops from cluster edge: 3
  Hops from command device: -
```

This is an example of output from the **show cluster candidates detail** command:

```
Switch# show cluster candidates detail
Device 'c2950-12' with mac address number 00d0.7961.c4c0
  Device type: cisco WS-C2950-12
  Upstream MAC address: 00d0.796d.2f00 (Cluster Member 1)
  Local port: Fa0/3 FEC number:
  Upstream port: Fa0/13 FEC Number:
  Hops from cluster edge: 1
  Hops from command device: 2
Device '1900_Switch' with mac address number 00e0.1e7e.be80
  Device type: cisco 1900
  Upstream MAC address: 00d0.796d.2f00 (Cluster Member 2)
  Local port: 3 FEC number: 0
  Upstream port: Fa0/11 FEC Number:
  Hops from cluster edge: 1
  Hops from command device: 2
Device 'c2924-XL' with mac address number 00e0.1e9f.7a00
  Device type: cisco WS-C2924-XL
  Upstream MAC address: 00d0.796d.2f00 (Cluster Member 3)
  Local port: Fa0/5 FEC number:
  Upstream port: Fa0/3 FEC Number:
  Hops from cluster edge: 1
  Hops from command device: 2
```

Related Commands

Command	Description
show cluster	Displays the cluster status and a summary of the cluster to which the switch belongs.
show cluster members	Displays information about the cluster members.

show cluster members

Use the **show cluster members** privileged EXEC command on the command switch to display information about the cluster members.

show cluster members [n | detail] [| {begin | exclude | include} expression]

Syntax Description

n	(Optional) Number that identifies a cluster member. The range is from 0 to 15.
detail	(Optional) Display detailed information for all cluster members.
 begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5.2)WC(1)	This command was introduced.

Usage Guidelines

You should only enter this command on a command switch.

If the cluster has no members, this command displays an empty line at the prompt.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show cluster members** command. The SN in the display means *switch number*.

```
Switch# show cluster members
|---Upstream---|
SN MAC Address      Name       PortIf FEC Hops      SN PortIf   FEC State
0  0002.4b29.2e00  StLouis1          0                  Up  (Cmdr)
1  0030.946c.d740  tal-switch-1  Fa0/13    1      0  Gi0/1     Up
2  0002.b922.7180  nms-2820     10      0  2      1  Fa0/18    Up
3  0002.4b29.4400  SanJuan2      Gi0/1     2      1  Fa0/11    Up
4  0002.4b28.c480  GenieTest    Gi0/2     2      1  Fa0/9     Up
```

This is an example of output from the **show cluster members 3** command for cluster member 3:

```
Switch# show cluster members 3
Device 'SanJuan2' with member number 3
  Device type:           cisco WS-C3550-12T
  MAC address:          0002.4b29.4400
  Upstream MAC address: 0030.946c.d740 (Cluster member 1)
  Local port:            Gi0/1   FEC number:
  Upstream port:         Fa0/11  FEC Number:
  Hops from command device: 2
```

■ **show cluster members**

This is an example of output from the **show cluster members detail** command:

```
Switch# show cluster members detail
Device 'StLouis1' with member number 0 (Command Switch)
  Device type:           cisco WS-C3550-12T
  MAC address:          0002.4b29.2e00
  Upstream MAC address:
    Local port:           FEC number:
    Upstream port:        FEC Number:
    Hops from command device: 0
Device 'tal-switch-14' with member number 1
  Device type:           cisco WS-C3548-XL
  MAC address:          0030.946c.d740
  Upstream MAC address: 0002.4b29.2e00 (Cluster member 0)
  Local port:            Fa0/13  FEC number:
  Upstream port:         Gi0/1   FEC Number:
  Hops from command device: 1
Device 'nms-2820' with member number 2
  Device type:           cisco 2820
  MAC address:          0002.b922.7180
  Upstream MAC address: 0030.946c.d740 (Cluster member 1)
  Local port:            10     FEC number: 0
  Upstream port:         Fa0/18  FEC Number:
  Hops from command device: 2
Device 'SanJuan2' with member number 3
  Device type:           cisco WS-C3550-12T
  MAC address:          0002.4b29.4400
  Upstream MAC address: 0030.946c.d740 (Cluster member 1)
  Local port:            Gi0/1   FEC number:
  Upstream port:         Fa0/11  FEC Number:
  Hops from command device: 2
Device 'Test' with member number 4
  Device type:           cisco SeaHorse
  MAC address:          0002.4b28.c480
  Upstream MAC address: 0030.946c.d740 (Cluster member 1)
  Local port:            Gi0/2   FEC number:
  Upstream port:         Fa0/9   FEC Number:
  Hops from command device: 2
Device 'Palpatine' with member number 5
  Device type:           cisco WS-C2924M-XL
  MAC address:          00b0.6404.f8c0
  Upstream MAC address: 0002.4b29.2e00 (Cluster member 0)
  Local port:            Gi2/1   FEC number:
  Upstream port:         Gi0/7   FEC Number:
  Hops from command device: 1
```

Related Commands

Command	Description
show cluster	Displays the cluster status and a summary of the cluster to which the switch belongs.
show cluster candidates	Displays a list of candidate switches.

show controllers ethernet-controller

Use the **show controllers ethernet-controller** privileged EXEC command to display the Ethernet link send and receive statistics on a Fast Ethernet or Long-Reach Ethernet (LRE) port.

```
show controllers ethernet-controller [interface-id] [cpe [port port-id] [ | {begin | exclude | include} expression]
```

Syntax Description	
interface-id	(Optional) ID of the Fast Ethernet or LRE port.
cpe	(Optional) Display both LRE and all Fast Ethernet ports on connected devices.
port	(Optional) CPE port keywords display the Ethernet statistics of the designated customer premises equipment (CPE) Ethernet port.
port-id	CPE Ethernet port identifier. Valid values vary from 1 to 4, depending on CPE device.
 begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
expression	Expression in the output to use as a reference point.

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

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.

Usage Guidelines	Using the show controllers ethernet-controller command without specifying a Fast Ethernet or LRE port displays the Ethernet link statistics of all Ethernet ports on the switch. The output shows the internal switch statistics, the statistics collected by the LRE interface on the switch, and if the CPE option is specified, the statistics collected by the LRE interface on the connected customer premises equipment (CPE) devices.
-------------------------	---

The CPE Ethernet link on a switch LRE port is the connection between the Cisco LRE CPE and the remote Ethernet device (such as a PC) connected to it. It is not the link between the switch LRE port and the LRE CPE device.

Examples	This is an example of output from the show controllers ethernet-controller command on Long-Reach Ethernet port 2:
-----------------	--

```
Switch# show controllers ethernet-controller lo0/2

Transmit          Receive
18230744 Bytes   901461 Bytes
      9014 Unicast frames    40 Unicast frames
```

■ show controllers ethernet-controller

```

55624 Multicast frames
 285 Broadcast frames
 0 Discarded frames
 0 Too old frames
 0 Deferred frames
 0 1 collision frames
 0 2 collision frames
 0 3 collision frames
 0 4 collision frames
 0 5 collision frames
 0 6 collision frames
 0 7 collision frames
 0 8 collision frames
 0 9 collision frames
 0 10 collision frames
 0 11 collision frames
 0 12 collision frames
 0 13 collision frames
 0 14 collision frames
 0 15 collision frames
 0 Excessive collisions
 0 Late collisions

1249 Multicast frames
 0 Broadcast frames
 0 No bandwidth frames
 0 No buffers frames
7456 No dest, unicast
 0 No dest, multicast
 0 No dest, broadcast
 0 Alignment errors
 0 FCS errors
 0 Collision fragments

 0 Undersize frames
7473 Minimum size frames
 25 65 to 127 byte frames
 0 128 to 255 byte frames
1247 256 to 511 byte frames
 0 512 to 1023 byte frames
 0 1024 to 1518 byte frames
 0 Oversize frames

```

LRE Enet Stats on Switch:

592145 Bytes	114825 Bytes
7107 Frames	1116 Frames
0 Pause frames	26 Broadcast frames
128 1 collision frames	0 Pause frames
0 Multiple collisions	0 Alignment errors
0 Late collisions	0 Collisions and Runts
0 Excessive collisions	0 Oversize frames
0 Deferred frames	0 FCS errors
0 Carrier sense errors	

This is an example of output from the Ethernet statistics of the LRE chipset and all the LRE Ethernet ports on the CPE device:

Switch# **show controllers ethernet-controller lo0/5 cpe**

Transmit	Receive
LRE Enet Stats on CPE:	
592145 Bytes	114825 Bytes
7108 Frames	1116 Frames
0 Pause frames	0 Broadcast frames
177 1 collision frames	0 Pause frames
0 Multiple collisions	0 Alignment errors
0 Late collisions	2 Collisions and Runts
0 Excessive collisions	0 Oversize frames
0 Deferred frames	0 FCS errors
0 Carrier sense errors	
CPE Fast Ethernet Port: 1	
42308326 Bytes	8264733 Bytes
193 Unicast Frames	8264733 Good Bytes
511408 Multicast Frames	68745 Unicast Frames
1886 Broadcast Frames	11469 Multicast Frames
0 Dropped Frames	0 Broadcast Frames
	0 Dropped Frames

```

0 Pause Frames
0 Collision Frames
0 One Collision Frames
0 Multiple Collisions
0 Late Collisions
0 Excess Collisions
0 Frame Discard
2 Deferred Frames
0 Pause Frames
0 Alignment Errors
0 Fragments
0 Undersize Frames
0 Oversize Frames
0 FCS errors
0 Excess Size Discards
0 Jabbers
1 Source Address Change
0 Symbol Errors

68745 64 Byte Frames
0 65-127 Byte Frames
0 128-255 Byte Frames
11469 256-511 Byte Frames
0 512-1023 Byte Frames
0 1024-1522 Byte Frame

CPE Fast Ethernet Port: 2
42308326 Bytes

193 Unicast Frames
511408 Multicast Frames
1886 Broadcast Frames
0 Dropped Frames
0 Pause Frames
0 Collision Frames
0 One Collision Frames
0 Multiple Collisions
0 Late Collisions
0 Excess Collisions
0 Frame Discard
2 Deferred Frames
8264733 Bytes
8264733 Good Bytes
68745 Unicast Frames
11469 Multicast Frames
0 Broadcast Frames
0 Dropped Frames
0 Pause Frames
0 Alignment Errors
0 Fragments
0 Undersize Frames
0 Oversize Frames
0 FCS errors
0 Excess Size Discards
0 Jabbers
1 Source Address Change
0 Symbol Errors

68745 64 Byte Frames
0 65-127 Byte Frames
0 128-255 Byte Frames
11469 256-511 Byte Frames
0 512-1023 Byte Frames
0 1024-1522 Byte Frame

CPE Fast Ethernet Port: 3
42308326 Bytes

193 Unicast Frames
511408 Multicast Frames
1886 Broadcast Frames
0 Dropped Frames
0 Pause Frames
0 Collision Frames
0 One Collision Frames
0 Multiple Collisions
0 Late Collisions
0 Excess Collisions
0 Frame Discard
2 Deferred Frames
8264733 Bytes
8264733 Good Bytes
68745 Unicast Frames
11469 Multicast Frames
0 Broadcast Frames
0 Dropped Frames
0 Pause Frames
0 Alignment Errors
0 Fragments
0 Undersize Frames
0 Oversize Frames
0 FCS errors
0 Excess Size Discards
0 Jabbers
1 Source Address Change
0 Symbol Errors

68745 64 Byte Frames
0 65-127 Byte Frames
0 128-255 Byte Frames

```

■ show controllers ethernet-controller

```

11469 256-511 Byte Frames
0 512-1023 Byte Frames
0 1024-1522 Byte Frame

CPE Fast Ethernet Port: 4
42308326 Bytes
193 Unicast Frames
511408 Multicast Frames
1886 Broadcast Frames
0 Dropped Frames
0 Pause Frames
0 Collision Frames
0 One Collision Frames
0 Multiple Collisions
0 Late Collisions
0 Excess Collisions
0 Frame Discard
2 Deferred Frames
8264733 Bytes
8264733 Good Bytes
68745 Unicast Frames
11469 Multicast Frames
0 Broadcast Frames
0 Dropped Frames
0 Pause Frames
0 Alignment Errors
0 Fragments
0 Undersize Frames
0 Oversize Frames
0 FCS errors
0 Excess Size Discards
0 Jabbers
1 Source Address Change
0 Symbol Errors

68745 64 Byte Frames
0 65-127 Byte Frames
0 128-255 Byte Frames
11469 256-511 Byte Frames
0 512-1023 Byte Frames
0 1024-1522 Byte Frame

```

This is an example of output of the Ethernet statistics from port 3 on the CPE device:

```
Switch# show controllers ethernet-controller lo0/5 cpe port 3
```

Transmit	Receive
42308326 Bytes	8264733 Bytes
193 Unicast Frames	8264733 Good Bytes
511408 Multicast Frames	68745 Unicast Frames
1886 Broadcast Frames	11469 Multicast Frames
0 Dropped Frames	0 Broadcast Frames
0 Pause Frames	0 Dropped Frames
0 Collision Frames	0 Pause Frames
0 One Collision Frames	0 Alignment Errors
0 Multiple Collisions	0 Fragments
0 Late Collisions	0 Undersize Frames
0 Excess Collisions	0 Oversize Frames
0 Frame Discard	0 FCS errors
2 Deferred Frames	0 Excess Size Discards
	0 Jabbers
	1 Source Address Change
	0 Symbol Errors
	68745 64 Byte Frames
	0 65-127 Byte Frames
	0 128-255 Byte Frames
	11469 256-511 Byte Frames
	0 512-1023 Byte Frames
	0 1024-1522 Byte Frame

Related Commands	Command	Description
	clear controllers ethernet-controller	Deletes the Ethernet link send and receive statistics on a Fast Ethernet or an LRE switch port.

show controllers lre cpe identity

Use the **show controllers lre cpe identity** privileged EXEC command to display the model numbers of the Long-Reach Ethernet (LRE) customer premises equipment (CPE) devices connected to the LRE switch. This command also shows whether or not the connected CPE devices meet the minimum requirements for management by the LRE switch.

show controllers lre cpe identity [interface-id] [| {begin | exclude | include} expression]

Syntax Description	<i>interface-id</i>	(Optional) ID of the switch LRE port.
begin		(Optional) Display begins with the line that matches the specified <i>expression</i> .
exclude		(Optional) Display excludes lines that match the specified <i>expression</i> .
include		(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>		Expression in the output to use as a reference point.

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

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.

Usage Guidelines	This command shows the type of CPE device attached to each LRE interface. For all Cisco supported CPE devices, the status can be <i>certified</i> , <i>non-certified</i> , or <i>NA</i> :
------------------	---

A certified status means that the CPE device meets the minimum requirements (such as having a certain CPE device patch version) for management by the LRE switch.

A non-certified status means that the CPE device did not meet the minimum requirements. If a CPE device shows a status of non-certified, or if the family is not either a Cisco 585 LRE CPE or a Cisco 575 LRE CPE, use the **show controllers lre cpe mfg** command to verify the validity of the CPE manufacturing fields.

A NA status means that there is not a link or there is not any information about that port.

Using the **show controllers lre cpe identity** command without specifying a switch LRE port displays the model numbers and status of all connected CPE devices.

Examples	This is an example of output from the show controllers lre cpe identity command:
----------	---

```
Switch# show controllers lre cpe identity

Port      CPE Model       Status      Family
-----  -----
Lo0/1    CISCO585-LRE   CERTIFIED   CISCO585-LRE
Lo0/2    CISCO585-LRE   CERTIFIED   CISCO585-LRE
Lo0/3    CISCO585-LRE   CERTIFIED   CISCO585-LRE
Lo0/4          NA        NA         NA
```

■ **show controllers lre cpe identity**

Lo0/5	NA	NA	NA
Lo0/6	Cisco575-LRE	CERTIFIED	CISCO575-LRE
Lo0/7	NA	NA	NA
Lo0/8	Cisco575-LRE	CERTIFIED	CISCO575-LRE
Lo0/9	NA	NA	NA
Lo0/10	NA	NA	NA
Lo0/11	CISCO585-LRE	CERTIFIED	CISCO585-LRE
Lo0/12	CISCO585-LRE	CERTIFIED	CISCO585-LRE
Lo0/13	CISCO585-LRE	CERTIFIED	CISCO585-LRE
Lo0/14	NA	NA	NA
Lo0/15	NA	NA	NA
Lo0/16		NON-CERTIFIED	UNSUPPORTED-MAC-MODE
Lo0/17	NA	NA	NA
Lo0/18	NA	NA	NA
Lo0/19	NA	NA	NA
Lo0/20	NA	NA	NA
Lo0/21	NA	NA	NA
Lo0/22	NA	NA	NA
Lo0/23	NA	NA	NA
Lo0/24	NA	NA	NA

Related Commands

Command	Description
show controllers lre version	Displays the version number of the hardware, software, and patch software components of the switch LRE interface and the CPE LRE interface.

show controllers lre cpe mfg

Use the **show controllers lre cpe mfg** privileged EXEC command to display the revision and serial numbers of the connected Cisco Long-Reach Ethernet (LRE) customer premises equipment (CPE) board, assembly, and system.

show controllers lre cpe mfg [interface-id] [| {begin | exclude | include} expression]

Syntax Description	
<i>interface-id</i>	(Optional) ID of the switch LRE port.
begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .
exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

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

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.

Usage Guidelines	This command displays fields specific to each CPE device unit. The IOS software uses the model number field to identify the kind of CPE device attached to a Long-Reach Ethernet interface. The System Serial Number is also unique to each CPE device unit.
-------------------------	--

Examples	This is an example of output that shows the manufacturing information for the CPE device:
-----------------	---

```
Switch# show controllers lre cpe mfg lo0/5
```

CPE Manufacturer Information:

```
Lo0/1
Assembly Revision Number:
Model Number      :CISCO585-LRE
Model Revision Number :A0
Board Assembly Number :
Board Serial Number :
System Serial Number :ACT0613004E
```

```
Lo0/2
Assembly Revision Number:
Model Number      :CISCO585-LRE
Model Revision Number :A0
Board Assembly Number :
Board Serial Number :
System Serial Number :ACT0613005B
```

```
Lo0/3
Assembly Revision Number:
```

■ show controllers lre cpe mfg

```

Model Number          : CISCO585-LRE
Model Revision Number : A0
Board Assembly Number :
Board Serial Number   :
System Serial Number   : ACT06130068

Lo0/4
Assembly Revision Number:
Model Number          :
Model Revision Number   :
Board Assembly Number   :
Board Serial Number   :
System Serial Number   :

Lo0/5
Assembly Revision Number:
Model Number          :
Model Revision Number   :
Board Assembly Number   :
Board Serial Number   :
System Serial Number   :

Lo0/6
Assembly Revision Number:
Model Number          : Cisco575-LRE
Model Revision Number   : A0
Board Assembly Number   :
Board Serial Number   :
System Serial Number   :

Lo0/7
Assembly Revision Number:
Model Number          :
Model Revision Number   :
Board Assembly Number   :
Board Serial Number   :
System Serial Number   :

Lo0/8
Assembly Revision Number:
Model Number          : Cisco575-LRE
Model Revision Number   : A0
Board Assembly Number   :
Board Serial Number   :
System Serial Number   :

Lo0/9
Assembly Revision Number:
Model Number          :
Model Revision Number   :
Board Assembly Number   :
Board Serial Number   :
System Serial Number   :

Lo0/10
Assembly Revision Number:
Model Number          :
Model Revision Number   :
Board Assembly Number   :
Board Serial Number   :
System Serial Number   :

```

```
Lo0/11
Assembly Revision Number:
Model Number      :CISCO585-LRE
Model Revision Number :A0
Board Assembly Number :
```

Related Commands	Command	Description
	show controllers lre cpe identity	Displays the revision and serial numbers of the connected Cisco LRE CPE board, assembly, and system.
	show controllers lre version	Displays the version number of the hardware, software, and patch software components of the switch LRE interface.

■ **show controllers lre cpe protected**

show controllers lre cpe protected

Use the **show controllers lre cpe protected** privileged EXEC command to display and identify Cisco 585 LRE customer premises equipment (CPE) Ethernet ports that are configured as protected.

show controllers lre cpe protected [interface-id] [| {begin | exclude | include} expression]

Syntax Description	<table border="0"> <tr> <td><i>interface-id</i></td><td>(Optional) ID of the switch Long-Reach Ethernet (LRE) port.</td></tr> <tr> <td> begin</td><td>(Optional) Display begins with the line that matches the specified <i>expression</i>.</td></tr> <tr> <td> exclude</td><td>(Optional) Display excludes lines that match the specified <i>expression</i>.</td></tr> <tr> <td> include</td><td>(Optional) Display includes lines that match the specified <i>expression</i>.</td></tr> <tr> <td><i>expression</i></td><td>Expression in the output to use as a reference point.</td></tr> </table>	<i>interface-id</i>	(Optional) ID of the switch Long-Reach Ethernet (LRE) port.	begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .	exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .	include	(Optional) Display includes lines that match the specified <i>expression</i> .	<i>expression</i>	Expression in the output to use as a reference point.
<i>interface-id</i>	(Optional) ID of the switch Long-Reach Ethernet (LRE) port.										
begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .										
exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .										
include	(Optional) Display includes lines that match the specified <i>expression</i> .										
<i>expression</i>	Expression in the output to use as a reference point.										

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.

Usage Guidelines Using the **show controllers lre cpe protected** command without specifying an LRE interface displays the protected port setting for each CPE port. Any Cisco 575 LRE CPE devices display a protected field output of NA.

Examples This is an example of output that shows the CPE protected information for LRE interface lo0/9:

```
Switch# show controllers lre cpe protected lo0/9
Interface    Port    Protected
-----      ---      -----
Lo0/9        1       true
Lo0/9        2       true
Lo0/9        3       true
Lo0/9        4       true
```

This is an example of output that shows the CPE protected information for all switch LRE interfaces:

```
Switch# show controllers lre cpe protected
Interface    Port    Protected
-----      ---      -----
Lo0/1        1       NA
Lo0/2        1       NA
Lo0/3        1       NA
Lo0/4        1       NA
Lo0/5        1       NA
Lo0/6        1       NA
Lo0/7        1       NA
Lo0/8        1       false
Lo0/8        2       false
Lo0/8        3       false
```

Lo0/8	4	false
Lo0/9	1	true
Lo0/9	2	true
Lo0/9	3	true
Lo0/9	4	true
Lo0/10	1	NA
Lo0/11	1	NA
Lo0/12	1	NA
Lo0/13	1	NA
Lo0/14	1	NA
Interface	Port	Protected
-----	---	-----
Lo0/15	1	NA
Lo0/16	1	NA
Lo0/17	1	NA
Lo0/18	1	NA
Lo0/19	1	NA
Lo0/20	1	NA
Lo0/21	1	NA
Lo0/22	1	NA
Lo0/23	1	NA
Lo0/24	1	NA

Related Commands

Command	Description
cpe protected	Restricts data traffic to individual ports on Cisco 585 LRE CPE ports.

 show controllers lre cpe version

show controllers lre cpe version

Use the **show controllers lre cpe version** privileged EXEC command to display the version numbers of the various components (hardware, firmware, patch software, and bootloader firmware and application firmware) of the Long-Reach Ethernet (LRE) customer premises equipment (CPE) interface.

show controllers lre cpe version [interface-id] [| {begin | exclude | include} expression]

Syntax Description	
<i>interface-id</i>	(Optional) ID of the switch LRE port.
begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .
exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

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

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.

Usage Guidelines	Using the show controllers lre cpe version command without specifying a switch LRE port displays the version numbers of all CPE device interfaces.
-------------------------	---

Examples	This is an example of output from the show controllers lre cpe version command:
-----------------	--

```
Switch# show controllers lre cpe version lo0/5

Interface      Hw   Sw   Patch  Boot   App
-----        ---  ---  -----  ---   ---
Lo0/5          52    B4     51    1.02   1.02
```

Related Commands	Command	Description
	show controllers lre cpe identity	Displays the model numbers of the LRE CPE devices connected to the LRE switch and shows whether or not the connected CPE devices meet the minimum requirements for management by the LRE switch.
	show controllers lre cpe mfg	Displays the revision and serial numbers of the connected Cisco Long-Reach Ethernet (LRE) customer premises equipment (CPE) board, assembly, and system.

show controllers lre *interface-id* actual

Use the **show controllers lre *interface-id* actual** privileged EXEC command to display the actual values of the Long-Reach Ethernet (LRE) link on a specific switch LRE port.

```
show controllers lre interface-id actual [dsrserrs | usrserrs | txpower | rxpower | snr | link]
[ | {begin | exclude | include} expression]
```

Syntax Description

<i>interface-id</i>	ID of the switch LRE port.
actual	Display the LRE port current status, which might not be the same as the administratively configured settings.
dsrserrs	Display the downstream Reed-Solomon errors on the LRE port.
usrserrs	Display the upstream Reed-Solomon errors on the LRE port.
txpower	Display the remote transmit power (dBm/Hz) on the LRE port.
rxpower	Display the local receive power (dBm/Hz) on the customer premises equipment (CPE) port.
snr	Display the signal-to-noise ratio (SNR) ratio on the LRE port.
link	Display the LRE link status of the LRE port.
 begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(11)YJ	This command was introduced.

Usage Guidelines

Use the SNR and Reed-Solomon error information to measure the quality of the LRE link. The SNR is the amount of increased received signal-power (in decibels) relative to the noise-power level that the switch can tolerate without disconnecting from the CPE device. The higher the ratio, the more resilient is the link.

The Reed-Solomon errors show the number of errors detected and corrected in the data being received on and sent from the switch LRE ports. Reed-Solomon errors are the result of noise exceeding the noise margin. For short bursts of noise (such as motor power on or power surges), the interleaver prevents the loss of Ethernet data packets. Then the number of Reed-Solomon errors exceeds the number of Ethernet CRC errors.

The remote transmit power-rates from the connected CPE devices might be different from each other, depending on how long the cable is between the switch and the CPE device. A longer cable typically causes the CPE device to send a higher signal to overcome the loss effects of distance.

■ show controllers lre interface-id actual

The local receive-power actually displays the switch's adjustment to the incoming power level. These numbers might be different from LRE port to LRE port, as the length of the cables to the CPE devices might be different.

If the SNR is too low for the environment but the link still establishes, the Reed-Solomon error rate is high, and there might be link instability (as shown by the number of *Fail* events counted). If the network is being used for data only, a high incidence of Ethernet Frame Check Sequence (FCS) errors or micro-interruptions might be tolerable.

For more information about what can affect the LRE link and for the minimum required SNR ratios, refer to the “LRE Links and LRE Profiles” section in the *Catalyst 2950 Desktop Switch Software Configuration Guide*.

Examples

This is an example of output from the **show controllers lre interface-id actual dsrserrs** command on switch LRE port 2:

```
Switch# show controllers lre lo0/2 actual dsrserrs
0
Switch#
```

This is an example of output from the **show controllers lre interface-id actual link** command on switch LRE port 2:

```
Switch# show controllers lre lo0/2 actual link
UP
Switch#
```

This is an example of output from the **show controllers lre interface-id actual rxpower** command on switch LRE port 2:

```
Switch# show controllers lre lo0/2 actual rxpower
26.0
Switch#
```

This is an example of output from the **show controllers lre interface-id actual snr** command on switch LRE port 2:

```
Switch# show controllers lre lo0/2 actual snr
27
Switch#
```

This is an example of output from the **show controllers lre interface-id actual txpower** command on switch LRE port 2:

```
Switch# show controllers lre lo0/2 actual txpower
-89.7
Switch#
```

This is an example of output from the **show controllers lre interface-id actual usrserrs** command on switch LRE port 2:

```
Switch# show controllers lre lo0/2 actual usrserrs
0
Switch#
```

This is an example of output from the **show controllers lre interface-id actual link** command on switch LRE port 1:

```
Switch# show controllers lre lo0/1 actual link
DOWN
Switch#
```

Related Commands

Command	Description
show controllers lre interface-id admin	Displays the administrative settings of the LRE link on a specific switch LRE port.

 show controllers lre interface-id admin

show controllers lre *interface-id* admin

Use the **show controllers lre *interface-id* admin** privileged EXEC command to display the administrative settings of the Long-Reach Ethernet (LRE) link for a specific switch LRE port.

show controllers lre *interface-id* admin [dsrate | usrate] [| {begin | exclude | include} *expression*]

Syntax Description

<i>interface-id</i>	ID of the switch LRE port.
admin	Administrative settings display, which might not be the same as the actual values.
dsrate	Downstream rate (Mbps) display of the LRE link.
usrate	Upstream rate (Mbps) display of the LRE link.
 begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(11)YJ	This command was introduced.

Usage Guidelines

This command displays the profile settings of a switch LRE port, even though they might not be active if a global profile is configured on the switch.

The upstream and downstream rates are defined by the profile on the switch LRE port. To change these rates, assign a different profile to the switch LRE port. For information about the LRE profiles, refer to the *Catalyst 2950 Desktop Switch Software Configuration Guide*.

Examples

This is an example of output from the **show controllers lre *interface-id* admin dsrate** and **show controllers lre *interface-id* admin usrate** commands on switch LRE ports 1 and 2:

```
Switch# show controllers lre lo0/1 admin usrate
18.750
Switch#
Switch# show controllers lre lo0/1 admin dsrate
16.667
Switch#
Switch# show controllers lre lo0/2 admin usrate
12.500
Switch#
```

```
Switch# show controllers lre lo0/2 admin dsrate
12.500
Switch#
```

Related Commands

Command	Description
show controllers lre cpe identity	Displays the actual values of the LRE link on a specific switch LRE port.
lre profile	Assigns a profile to all switch LRE ports.
profile (interface mode)	Assigns a profile to a specific switch LRE port.

 show controllers lre link monitor errors

show controllers lre link monitor errors

Use the **show controllers lre link monitor errors** privileged EXEC command to display and analyze Long-Reach Ethernet (LRE) Reed Solomon errors and Ethernet errors.

show controllers lre monitor errors {local [interface-id] | remote [interface-id]} [| {begin | exclude | include} expression]

Syntax Description	
local	(Optional) Data from the LRE switch controller.
remote	(Optional) Data from the customer premises equipment (CPE) device.
<i>interface-id</i>	(Optional) ID of the switch LRE port.
 begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

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

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.

Usage Guidelines	The link monitor process collects error information at minute intervals for 15 minutes. After 15 minutes, the data is analyzed and stored before starting a new collection sequence. Up to 2 hours of link monitor data can be shown.
-------------------------	---

The Time heading in the output shows the timestamp for the last collection sequence. The Reed Solomon (RS) error count shows the cumulative error count from the last reading. Alignment errors, frame check sequence (FCS) errors, receive errors, and oversize errors are the Ethernet statistics collected either at the switch or at the CPE device.

Using this command without specifying a switch port displays data for all ports.

Examples	This is an example of output that shows how to display LRE Reed Solomon and Ethernet errors for the LRE switch on LRE link 0/1:
-----------------	---

```
Switch# show controllers lre link monitor errors local lo0/1

LongReachEthernet0/1:LRE Link Health Monitor Error counts :
Time      RS Errors   Align Errs FCS Errs   Rcv Errs   Oversz Errs
-----  -----
14:42:28    41216        0        0        0          0
14:30:28    40960        0        0        0          0
14:15:28    40960        0        0        0          0
14:00:29    40704        0        0        0          0
```

```

13:45:28    40704      0      0      0      0
13:30:29    40448      0      0      0      0
13:15:29    40448      0      0      0      0
13:00:28    40448      0      0      0      0
Switch#

```

This example displays Reed Solomon and Ethernet errors for a CPE device connected to LRE 0/1:

```
Switch# show controllers lre link monitor errors remote lo0/1
```

```

LongReachEthernet0/1:LRE Link Health Monitor Error counts :
Time      RS Errors   Align Errs   FCS Errs   Rcv Errs   Oversz Errs
-----
14:42:28    6400        45835       0          0          0
14:30:28    6400        45835       0          0          0
14:15:28    6400        45835       0          0          0
14:00:29    6400        45835       0          0          0
13:45:28    6144        45835       0          0          0
13:30:29    6144        45835       0          0          0
13:15:29    6144        45835       0          0          0
13:00:28    6144        45835       0          0          0
Switch #

```

Related Commands

Command	Description
clear controllers lre link monitor	Deletes LRE link monitor data.
link monitor	Enables the LRE link monitor on a port.
link monitor logging	Enables link monitor event logging per port.
link monitor threshold snr	Sets an signal-to-noise margin for the LRE link monitor.
link monitor threshold rserr	Sets a Reed-Solomon error threshold for the LRE link monitor.
show controllers lre link monitor parameters	Displays the Long-Reach Ethernet (LRE) operating parameter data collected by the link monitor.
show controllers lre link monitor statistics	Displays the Long-Reach Ethernet (LRE) link monitor statistics.

■ **show controllers lre link monitor parameters**

show controllers lre link monitor parameters

Use the **show controllers lre link monitor parameters** privileged EXEC command to display the Long-Reach Ethernet (LRE) operating parameter data collected by the link monitor. Local monitoring collects data from the LRE switch, and the remote monitoring collects data from attached CPE device.

show controllers lre monitor parameters {local [interface-id] | remote [interface-id]}[| {begin | exclude | include} expression]

Syntax Description	local (Optional) Data from the LRE switch controller. remote (Optional) Data from the customer premises equipment (CPE) device. interface-id (Optional) ID of the switch LRE port. begin (Optional) Display begins with the line that matches the specified <i>expression</i> . exclude (Optional) Display excludes lines that match the specified <i>expression</i> . include (Optional) Display includes lines that match the specified <i>expression</i> . expression Expression in the output to use as a reference point.
---------------------------	---

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.

Usage Guidelines The link monitor process collects error information at minute intervals for 15 minutes. After 15 minutes, the data is analyzed and stored before starting a new collection sequence. Up to 2 hours of link monitor data can be shown.

The Time heading in the output shows the timestamp for the last collection sequence. The signal-to-noise (SNR) error counter, shown under the SNR Err heading, increments when the SNR value read from the chipset falls below the theoretical SNR added to the threshold.

Using this command without specifying a switch port, displays data for all ports.

Examples This is an example that shows how to display all LRE link monitor parameters for the attached CPE device:

```
Switch# show controllers lre link monitor parameters remote

LongReachEthernet0/1: LRE Link Health Monitor Parameters :
          SNR           Tx Power      SwAGCGain
          Time   Samples Min Max Err   Min    Max   Min    Max
          ----- -----
          00:32:30    2      0  0  0 - 85.6 - 85.6 - 2.0 - 2.0
          00:30:30   15      0  0  0 - 85.6 - 85.6 - 2.0 - 2.0
          00:15:30   15      0  0  0 - 85.6 - 85.6 - 2.0 - 2.0
```

	Time	Samples	Min	Max	Err	Min	Max	Min	Max
	00:00:30	15	0	0	0	- 85.6	- 85.6	- 2.0	- 2.0
	23:45:30	15	0	0	0	- 85.6	- 85.6	- 2.0	- 2.0
	23:30:30	15	0	0	0	- 85.6	- 85.6	- 2.0	- 2.0
	23:15:30	15	0	0	0	- 85.6	- 85.6	- 2.0	- 2.0

LongReachEthernet0/2: LRE Link Health Monitor Parameters :

	Time	Samples	Min	Max	Err	Min	Max	Min	Max
	00:32:31	2	27	27	0	- 85.9	- 85.9	- 2.0	- 2.0
	00:30:31	15	27	27	0	- 85.9	- 85.9	- 2.0	- 2.0
	00:15:31	15	27	27	0	- 85.9	- 85.9	- 2.0	- 2.0
	00:00:31	15	27	27	0	- 85.9	- 85.9	- 2.0	- 2.0
	23:45:31	15	27	27	0	- 85.9	- 85.9	- 2.0	- 2.0
	23:30:31	15	27	27	0	- 85.9	- 85.9	- 2.0	- 2.0
	23:15:31	15	27	27	0	- 85.9	- 85.9	- 2.0	- 2.0
	23:00:31	15	27	27	0	- 85.9	- 85.9	- 2.0	- 2.0

LongReachEthernet0/3: LRE Link Health Monitor Parameters :

	Time	Samples	Min	Max	Err	Min	Max	Min	Max
	00:33:31	3	0	0	0	- 85.6	- 85.6	- 2.0	- 2.0
	00:30:31	15	0	0	0	- 85.6	- 85.6	- 2.0	- 2.0
	00:15:31	15	0	0	0	- 85.6	- 85.6	- 2.0	- 2.0
	00:00:31	15	0	0	0	- 85.6	- 85.6	- 2.0	- 2.0
	23:45:31	15	0	0	0	- 85.6	- 85.6	- 2.0	- 2.0
	23:30:31	15	0	0	0	- 85.6	- 85.6	- 2.0	- 2.0
	23:15:31	15	0	0	0	- 85.6	- 85.6	- 2.0	- 2.0
	23:00:31	15	0	0	0	- 85.6	- 85.6	- 2.0	- 2.0

LongReachEthernet0/4: LRE Link Health Monitor Parameters :

	Time	Samples	Min	Max	Err	Min	Max	Min	Max
--	------	---------	-----	-----	-----	-----	-----	-----	-----

LongReachEthernet0/5: LRE Link Health Monitor Parameters :

	Time	Samples	Min	Max	Err	Min	Max	Min	Max
--	------	---------	-----	-----	-----	-----	-----	-----	-----

LongReachEthernet0/6: LRE Link Health Monitor Parameters :

	Time	Samples	Min	Max	Err	Min	Max	Min	Max
	00:34:31	4	27	27	0	- 85.9	- 85.9	- 2.0	- 2.0
	00:30:32	15	27	27	0	- 85.9	- 85.9	- 2.0	- 2.0
	00:15:32	15	27	27	0	- 85.9	- 85.9	- 2.0	- 2.0
	00:00:32	15	27	27	0	- 85.9	- 85.9	- 2.0	- 2.0
	23:45:32	15	27	27	0	- 85.9	- 85.9	- 2.0	- 2.0
	23:30:32	15	27	27	0	- 85.9	- 85.9	- 2.0	- 2.0
	23:15:32	15	27	27	0	- 85.9	- 85.9	- 2.0	- 2.0
	23:00:31	15	27	27	0	- 85.9	- 85.9	- 2.0	- 2.0

LongReachEthernet0/7: LRE Link Health Monitor Parameters :

	Time	Samples	Min	Max	Err	Min	Max	Min	Max
	3:00:30	15	0	0	0	- 85.6	- 85.6	- 2.0	- 2.0

■ **show controllers lre link monitor parameters**

Related Commands	Command	Description
	clear controllers lre link monitor	Deletes LRE link monitor data.
	link monitor	Enables the LRE link monitor on a port.
	link monitor logging	Enables link monitor event logging per port.
	link monitor threshold snr	Sets an signal-to-noise margin for the LRE link monitor.
	link monitor threshold snr	Sets a Reed-Solomon error threshold for the LRE link monitor.
	show controllers lre link monitor errors	Displays Reed-Solomon and Ethenet errors captured by the LRE link monitor.
	show controllers lre link monitor statistics	Display the Long-Reach Ethernet (LRE) link monitor statistics.

show controllers lre link monitor statistics

Use the **show controllers lre link monitor statistics** privileged EXEC command to display the Long-Reach Ethernet (LRE) link monitor statistics. Local monitoring collects data from the LRE switch while the remote monitoring collects data from attached CPE device.

```
show controllers lre monitor statistics {local [interface-id] | remote [interface-id]} [ | {begin | exclude | include} expression]
```

Syntax Description	local (Optional) Data from the LRE switch controller.
remote((Optional) Data from the customer premises equipment (CPE) device.
<i>interface-id</i>	(Optional) ID of the switch LRE port.
 begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

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

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.

Usage Guidelines	The link monitor process collects error information at minute intervals for 15 minutes. After 15 minutes, the data is analyzed and stored before starting a new collection sequence. Up to 2 hours of link monitor data can be shown.
-------------------------	---

The Time heading in the output shows the timestamp for the last collection sequence. The Reed Solomon (RS) error count shows the cumulative error count from the last reading. This count is cleared only when the interface is shut down or when the **clear controllers lre link monitor** command is run. The Reed Solomon error alarm shows the number of 1 minute intervals that had Reed Solomon errors above the configured threshold.

Using this command without specifying a switch port displays statistics for all ports.

show controllers lre link monitor statistics
Examples

This is an example that shows how to display all LRE link monitor statistics for the LRE controller:

```
Switch# show controllers lre link monitor statistics local
```

```
LongReachEthernet0/1: LRE Link Health Monitor Stats :
```

Time	Samples	Count	RS Errors	Link Fail	Freeze
			Alarm	Count	Count
06:58:30	13	0	0	2	3
06:45:30	15	0	0	2	3
06:30:30	15	0	0	2	3
06:15:30	15	0	0	2	3
06:00:30	15	0	0	2	3
05:45:30	15	0	0	2	3
05:30:30	15	0	0	2	3
05:15:30	15	0	0	2	3

Related Commands

Command	Description
clear controllers lre link monitor	Deletes LRE link monitor data.
link monitor	Enables the LRE link monitor on a port.
link monitor logging	Enables link monitor event logging per port.
link monitor threshold snr	Sets an signal-to-noise margin for the LRE link monitor.
link monitor threshold rserr	Sets a Reed-Solomon error threshold for the LRE link monitor.
show controllers lre link monitor errors	Displays Reed-Solomon and Ethernet errors captured by the LRE link monitor.
show controllers lre link monitor parameters	Displays the Long-Reach Ethernet (LRE) operating parameter data collected by the link monitor.

show controllers lre log

Use the **show controllers lre log** privileged EXEC command to display the history of link, configuration, and timer events for a specific Long-Reach Ethernet (LRE) port or for all switch LRE ports.

show controllers lre log [interface-id] [| {begin | exclude | include} expression]

Syntax Description	
<i>interface-id</i>	(Optional) ID of the switch LRE port.
begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .
exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

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

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.

Usage Guidelines	Using the show controllers lre log command without specifying a switch LRE port displays the events for all LRE ports on the switch.
-------------------------	---

The time-stamped and sequentially tagged log entries can be helpful in confirming LRE link drops and configuration changes.

Examples	This is an example of output from the show controllers lre log command that displays events on LRE interface lo0/5:
-----------------	--

```
Switch# show controllers lre log lo0/5

LongReachEthernet0/5: Events Log: =====
1d00h: [0]: State RESTART: Got event:Reset

1d00h: [1]: State MODEZERO_APPLIED: Got event:Link Up

1d00h: [2]: State MODEZERO_APPLIED: Got event:Link Down

1d00h: [3]: State PROFILE_APPLIED: Got event:Link Up

1d00h: [4]: State PROFILE_LINKUP: Got event:Link Down

1d00h: [5]: State PROFILE_LINKUP: Got event:Link Up

1d00h: [6]: State PROFILE_LINKUP: Got event:Link Down

1d00h: [7]: State PROFILE_LINKUP: Got event:Link Up
```

■ **show controllers lre log**

Related Commands	Command	Description
	clear controllers lre log	Deletes the history of link, configuration, and timer events for a specific switch LRE port or for all LRE ports on the switch.
	show controllers lre log level	Displays the log level for a specific switch LRE port or for all LRE ports on the switch.

show controllers lre log level

Use the **show controllers lre log level** privileged EXEC command to display information about the Long-Reach Ethernet (LRE) event log level.

show controllers lre log level [interface-id] [| {begin | exclude | include} expression]

Syntax Description

<i>interface-id</i>	(Optional) ID of the switch LRE port.
begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .
exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(11)YJ	This command was introduced.

Usage Guidelines

Using the **show controllers lre log level** command without specifying a switch LRE port lists the log level for each LRE port on the switch.

Examples

This is an example of output from the **show controllers lre log level** command that displays the log level on LRE port lo0/1:

```
Switch> show controllers lre log level lo0/1
Port    Log Level
=====
Lo0/1  Logging disabled
Switch#
```

Related Commands

Command	Description
clear controllers lre log	Deletes the history of link, configuration, and timer events for a specific switch LRE port or for all LRE ports on the switch.
logging lre	Specifies the logging level on the LRE port.

■ **show controllers lre profile names**

show controllers lre profile names

Use the **show controllers lre profile names** privileged EXEC command to display information about the Long-Reach Ethernet (LRE) profiles available on the switch.

show controllers lre profile names [| {begin | exclude | include} expression]

Syntax Description	<ul style="list-style-type: none"> begin (Optional) Display begins with the line that matches the <i>expression</i>. exclude (Optional) Display excludes lines that match the <i>expression</i>. include (Optional) Display includes lines that match the specified <i>expression</i>.
	<i>expression</i> Expression in the output to use as a reference point.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.

Usage Guidelines [Table 2-7, Part 1](#), lists the LRE profiles shipped with the switch, including the upstream and downstream data rates that they support on the LRE link. For more information about LRE profiles and LRE links, refer to the *Catalyst 2950 Desktop Switch Software Configuration Guide*.



Note Use the rates in [Table 2-7, Part 1](#), only as guidelines. Factors such as the type of cable that you use, how it is bundled, and the interference and noise on the LRE link can affect the actual LRE link performance. Contact Cisco Systems for information about limitations and optimization of LRE link performance. The net data rates in the table are slightly less than the gross data rates displayed by the **show controllers lre profile names** privileged EXEC command.

Table 2-7, Part 1 LRE Profiles

Profile Name	LRE Link Downstream Rate (Mbps)	LRE Link Upstream Rate (Mbps)
LRE-998-15-4	16.667	4.688
LRE-997-10-4	12.5	4.688
LRE-2	2.08	2.08
LRE-3	3.13	3.13
LRE-4	4.17	4.17
LRE-4-1	4.167	1.563
LRE-5	5.69	6.25
LRE-7	8.33	8.33
LRE-8	9.38	9.38
LRE-10 (default)	12.5	12.5

Table 2-7, Part 2 LRE Profiles

Profile Name	LRE Link Downstream Rate (Mbps)	LRE Link Upstream Rate (Mbps)
LRE-10-1	12.5	1.56
LRE-10-3	11.38	3.125
LRE-10-5	11.38	6.25
LRE-15	16.667	18.75
LRE-15-1	16.667	1.56
LRE-15-3	16.667	3.125
LRE-15-5	16.667	6.25
LRE-4-1-LL	4.167	1.563
LRE-5LL	5.69	5.69
LRE-10LL	11.38	11.38
LRE-15LL	15.17	17.06

Examples

This is an example of output from the **show controllers lre profile names** command:

```
Switch# show controllers lre profile names
```

Profile Name	Type	Downstream Rate (Mbps)	Upstream Rate (Mbps)
LRE-15	System-Configured	16.667	18.750
LRE-10	System-Configured	12.500	12.500
LRE-5	System-Configured	6.250	6.250
LRE-998-15-4	System-Configured	16.667	4.688
LRE-997-10-4	System-Configured	12.500	4.688
LRE-15LL	System-Configured	16.667	18.750
LRE-10LL	System-Configured	12.500	12.500
LRE-5LL	System-Configured	6.250	6.250
LRE-10-5	System-Configured	12.500	6.250
LRE-10-3	System-Configured	12.500	3.125
LRE-10-1	System-Configured	12.500	1.563
LRE-8	System-Configured	9.375	9.375
LRE-7	System-Configured	8.333	8.333
LRE-15-5	System-Configured	16.667	6.250
LRE-15-3	System-Configured	16.667	3.125
LRE-15-1	System-Configured	16.667	1.563
LRE-4	System-Configured	4.167	4.167
LRE-3	System-Configured	3.125	3.125
LRE-2	System-Configured	2.083	2.083
LRE-4-1LL	System-Configured	4.167	1.563

Related Commands

Command	Description
lre profile	Assigns an LRE profile to all the LRE ports on the switch.
show controllers lre profile details	Displays detailed information about the profiles and sequences running on an LRE switch.

 show controllers lre profile details

show controllers lre profile details

Use the **show controllers lre profile details** privileged EXEC command to display information about the Long-Reach Ethernet (LRE) profiles and sequences available on the switch.

show controllers lre profile names details [| {begin | exclude | include} expression]

Syntax Description	<ul style="list-style-type: none"> begin (Optional) Display begins with the line that matches the <i>expression</i>. exclude (Optional) Display excludes lines that match the <i>expression</i>. include (Optional) Display includes lines that match the specified <i>expression</i>.
	<i>expression</i> Expression in the output to use as a reference point.

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

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.

Usage Guidelines	Use this command to see the profiles and sequences running on each port. This command also shows profiles and sequences set at the global scope.
-------------------------	--

Examples	This is an example of output from the show controllers lre profile details command:
-----------------	--

```
Switch# show controllers lre profile details
```

```
Global Profile:LRE-10-3
```

Interface	Configured Profile	Running Profile	Type
Lo0/1	LRE-10-5	LRE-15	Port Sequence
Lo0/2	LRE-10-3	LRE-10-3	Global Profile
Lo0/3	LRE-10-3	LRE-15	Port Sequence
Lo0/4	LRE-10-3	LRE-10-3	Global Profile
Lo0/5	LRE-10-3	LRE-10-3	Global Profile
Lo0/6	LRE-10-3	LRE-10-3	Global Profile
Lo0/7	LRE-10-3	LRE-15	Global Profile
Lo0/8	LRE-10-3	LRE-10-3	Global Profile
Lo0/9	LRE-10-3	LRE-10-3	Global Profile
Lo0/10	LRE-10-3	LRE-10-3	Global Profile
Lo0/11	LRE-10-3	LRE-10-3	Global Profile
Lo0/12	LRE-10-3	LRE-10-3	Global Profile
Lo0/13	LRE-10-3	LRE-10-3	Global Profile
Lo0/14	LRE-10-3	LRE-10-3	Global Profile
Lo0/15	LRE-10-3	LRE-10-3	Global Profile
Lo0/16	LRE-10-3	LRE-10-3	Global Profile
Lo0/17	LRE-10-3	LRE-10-3	Global Profile
Lo0/18	LRE-10-3	LRE-10-3	Global Profile
Lo0/19	LRE-10-3	LRE-10-3	Global Profile
Lo0/20	LRE-10-3	LRE-10-3	Global Profile
Lo0/21	LRE-10-3	LRE-10-3	Global Profile

```
Lo0/22      LRE-10-3        LRE-10-3        Global Profile
Lo0/23      LRE-10-3        LRE-10-3        Global Profile
Lo0/24      LRE-10-3        LRE-15          Global Profile
```

```
Switch#
```

Related Commands	Command	Description
	lre profile	Assigns an LRE profile to all switch LRE ports.
	show controllers lre profile names	Displays upstream and downstream data rates for profiles running on an LRE switch.

■ **show controllers lre sequence**

show controllers lre sequence

Use the **show controllers lre sequence** privileged EXEC command to display the list of sequences, the profiles that are configured in that sequence, and the downstream and upstream rates of the corresponding profiles.

show controllers lre sequence [| {begin | exclude | include} expression]

Syntax Description	<p> begin (Optional) Display begins with the line that matches the <i>expression</i>.</p> <p> exclude (Optional) Display excludes lines that match the <i>expression</i>.</p> <p> include (Optional) Display includes lines that match the specified <i>expression</i>.</p> <p><i>expression</i> Expression in the output to use as a reference point.</p>
---------------------------	---

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.

Usage Guidelines Use the **show controllers lre sequence** command to display the list of sequences supported in the switch. This command displays the system-defined and user-defined sequences.

Examples This is an example of output from the **show controllers lre sequence** command:

```
Switch# show controllers lre sequence

Global Sequence:LRE-SEQ-COMPLETE-REACH

Sequence:LRE-SEQ-COMPLETE-REACH      Type:System-Configured

      Profile Name    Downstream      Upstream
      Rate(Mbps)     Rate(Mbps)

      -----  -----
      LRE-15          16.667         18.750
      LRE-10          12.500         12.500
      LRE-15-5        16.667         6.250
      LRE-10-5        12.500         6.250
      LRE-8           9.375          9.375
      LRE-7           8.333          8.333
      LRE-15-3        16.667         3.125
      LRE-10-3        12.500         3.125
      LRE-5            6.250          6.250
      LRE-15-1        16.667         1.563
      LRE-10-1        12.500         1.563
      LRE-4            4.167          4.167
      LRE-3            3.125          3.125
      LRE-2            2.083          2.083
      LRE-4-1          4.167          1.563
```

Sequence:LRE-SEQ-DOWNSTREAM

Type:System-Configured

Profile Name	Downstream Rate(Mbps)	Upstream Rate(Mbps)
LRE-15	16.667	18.750
LRE-15-5	16.667	6.250
LRE-15-3	16.667	3.125
LRE-15-1	16.667	1.563
LRE-10	12.500	12.500
LRE-10-5	12.500	6.250
LRE-10-3	12.500	3.125
LRE-10-1	12.500	1.563
LRE-8	9.375	9.375
LRE-7	8.333	8.333
LRE-5	6.250	6.250
LRE-4	4.167	4.167
LRE-4-1	4.167	1.563
LRE-3	3.125	3.125
LRE-2	2.083	2.083

Sequence:LRE-SEQ-SYM

Type:System-Configured

Profile Name	Downstream Rate(Mbps)	Upstream Rate(Mbps)
LRE-15	16.667	18.750
LRE-10	12.500	12.500
LRE-8	9.375	9.375
LRE-7	8.333	8.333
LRE-5	6.250	6.250
LRE-4	4.167	4.167
LRE-3	3.125	3.125
LRE-2	2.083	2.083

Sequence:LRE-SEQ-SYM-LONGREACH

Type:System-Configured

Profile Name	Downstream Rate(Mbps)	Upstream Rate(Mbps)
LRE-5	6.250	6.250
LRE-4	4.167	4.167
LRE-3	3.125	3.125
LRE-2	2.083	2.083
LRE-4-1	4.167	1.563

Sequence:LRE-SEQ-SYMLL

Type:System-Configured

Profile Name	Downstream Rate(Mbps)	Upstream Rate(Mbps)
LRE-15LL	16.667	18.750
LRE-10LL	12.500	12.500
LRE-5LL	6.250	6.250

Sequence:LRE-SEQ-UPSTREAM

Type:System-Configured

Profile Name	Downstream Rate(Mbps)	Upstream Rate(Mbps)
LRE-15	16.667	18.750
LRE-10	12.500	12.500
LRE-8	9.375	9.375

■ show controllers lre sequence

LRE-7	8.333	8.333
LRE-15-5	16.667	6.250
LRE-10-5	12.500	6.250
LRE-5	6.250	6.250
LRE-4	4.167	4.167
LRE-15-3	16.667	3.125
LRE-10-3	12.500	3.125
LRE-3	3.125	3.125
LRE-2	2.083	2.083
LRE-4-1	4.167	1.563

Sequence:LRE-SEQ-VIDEO-TRANSMIT1 Type:System-Configured

Profile Name	Downstream Rate(Mbps)	Upstream Rate(Mbps)
-----	-----	-----
LRE-15	16.667	18.750
LRE-15-5	16.667	6.250
LRE-15-3	16.667	3.125
LRE-15-1	16.667	1.563
LRE-10	12.500	12.500
LRE-10-5	12.500	6.250
LRE-10-3	12.500	3.125
LRE-10-1	12.500	1.563

Sequence:LRE-SEQ-VIDEO-TRANSMIT2 Type:System-Configured

Profile Name	Downstream Rate(Mbps)	Upstream Rate(Mbps)
-----	-----	-----
LRE-15	16.667	18.750
LRE-15-5	16.667	6.250
LRE-10	12.500	12.500
LRE-10-5	12.500	6.250
LRE-15-3	16.667	3.125
LRE-10-3	12.500	3.125
LRE-15-1	16.667	1.563
LRE-10-1	12.500	1.563

Sequence:SEQ3 Type:User-Configured

Profile Name	Downstream Rate(Mbps)	Upstream Rate(Mbps)
-----	-----	-----
LRE-15-5	16.667	6.250
LRE-15-3	16.667	3.125
LRE-15-5	16.667	6.250
LRE-15-3	16.667	3.125
LRE-15LL	16.667	18.750
LRE-15-1	16.667	1.563
LRE-3	3.125	3.125
LRE-10	12.500	12.500

Related Commands

Command	Description
lre rate selection sequence	Assigns a rate selection sequence to the entire switch.
lre sequence	Defines a user-defined sequence.

show controllers lre status

Use the **show controllers lre status** privileged EXEC command to display the Long-Reach Ethernet (LRE) link statistics and profile information on a switch LRE port, including link state, link duration, profile name, and data rates.

```
show controllers lre status {link | profile | psd | sequence [ detail ]} [ interface-id ] [ | {begin | exclude | include} expression]
```

Syntax Description

<i>interface-id</i>	(Optional) ID of the switch LRE port.
link	Various parameters and status associated with the LRE link.
profile	Various administrative parameters and status associated with the LRE link.
psd	Power related status.
sequence	Status of profiles in a sequence. Possible status values are converged; waiting on link; executing; and locked.
<i>detail</i>	(Optional) When added to the sequence keyword, it displays additional information about the sequences, such as margins, locked profiles, and convergence times.
 begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(11)YJ	This command was introduced.

Usage Guidelines

Use this command to display the status of all switch LRE ports.

Use the signal-to-noise ratio (SNR) and Reed-Solomon error information to measure the quality of the LRE link. The SNR represents the amount of increased received signal power (in decibels) relative to the noise power-level that the switch can tolerate without disconnecting from the CPE device. The higher the ratio, the more resilient is the link.

The Reed-Solomon errors show the number of errors detected and corrected in the data being received on and sent from the switch LRE ports. Reed-Solomon errors are the result of noise exceeding the noise margin. For short bursts of noise (such as motor power on or power surges), the interleaver prevents the loss of Ethernet data packets. The number of Reed-Solomon errors then exceeds the number of Ethernet CRC errors.



The Reed-Solomon errors are reset each time the **show controllers lre status link** command is executed.

■ show controllers lre status

The remote transmit power levels from the connected CPE devices might be different from each other, depending on how long the cable is between the switch and the CPE device. A longer cable typically causes the CPE device to send a higher signal to overcome the loss effects of distance.

The local receive-power rates actually displays the switch's adjustment to the incoming power level. These numbers might be different from LRE port to LRE port, as the length of the cables to the CPE devices might be different.

The interleaver columns display the interleaver block size for both directions of data. A higher interleaver setting is less susceptible to certain kinds of impairments but can introduce a very small amount of delay in the data path.

The PMD-S column refers to physical media dependent status and is provided as diagnostic information.

For more information about what can affect the LRE link and for the minimum required SNR ratios, refer to the “LRE Links and LRE Profiles” section in the *Catalyst 2950 Desktop Switch Software Configuration Guide*.

The **sequence** and **sequence detail** parameters display these status codes of profiles and sequences during rate selection:

- Converged—Rate selection has converged on a profile.
- Locked—Rate selection has converged on a profile, and the port is locked to that profile.
- Executing—Rate selection is running on the port.
- Waiting on Link—No link is established.
- N/A—Sequence is not assigned to the port.

You can adjust the noise level during convergence by using the **margin** command.

Examples

This is an example of output that shows how to display link information for LRE interface lo0/2:

```
Switch# show controller lre status link lo0/2
```

Port	Link	SNR	RS Errs	CPE-Tx	Sw-AGC-Gain	Interleaver	PMD-S
		(dB)		(dBm/Hz)	(dB)	Rx-Bsz	Tx-Bsz
Lo0/2	UP	41	4829	- 57.7	- 7.6	16	16 0x04

This is an example of output that shows output from the **show controllers lre status profile** command:

```
Switch# show controllers lre status profile
```

Port	Link	Uptime	Profile	DSRate	USRate	Fail
Lo0/1	UP	2d23h	LRE-10	12.500	12.500	0
Lo0/2	UP	2d23h	LRE-10	4.167	1.563	0
Lo0/3	UP	2d23h	LRE-10	4.167	1.563	0
Lo0/4	UP	2d23h	LRE-10	4.167	1.563	0
Lo0/5	DOWN	00:00:00	LRE-10	0.000	0.000	0
Lo0/6	UP	2d23h	LRE-10	4.167	1.563	0
Lo0/7	UP	2d23h	LRE-10	4.167	1.563	0
Lo0/8	UP	2d23h	LRE-10	4.167	1.563	0
Lo0/9	UP	2d23h	LRE-10	4.167	1.563	0
Lo0/10	DOWN	00:00:00	LRE-10	0.000	0.000	0
Lo0/11	DOWN	00:00:00	LRE-10	0.000	0.000	0
Lo0/12	DOWN	00:00:00	LRE-10	0.000	0.000	0
Lo0/13	UP	2d23h	LRE-10	12.500	12.500	0
Lo0/14	DOWN	00:00:00	LRE-10	0.000	0.000	0
Lo0/15	UP	2d23h	LRE-10	4.167	1.563	0
Lo0/16	DOWN	00:00:00	LRE-10	0.000	0.000	0

Lo0/17	DOWN	00:00:00	LRE-10		0.000	0.000	0
Lo0/18	DOWN	00:00:00	LRE-10		0.000	0.000	0
Lo0/19	DOWN	00:00:00	LRE-10		0.000	0.000	0
Lo0/20	DOWN	00:00:00	LRE-10		0.000	0.000	0
Lo0/21	UP	2d23h	LRE-10		4.167	1.563	0
Lo0/22	DOWN	00:00:00	LRE-10		0.000	0.000	0
Lo0/23	DOWN	00:00:00	LRE-10		0.000	0.000	0
Lo0/24	DOWN	00:00:00	LRE-10		0.000	0.000	0

This is an example of output from the **show controllers lre status psd** command:

```
Switch# show controllers lre status psd
```

----- Switch -----						CPE -----			
Port	Link	SNR	RSErr	TxPwr	AGCgain	SNR	RSErr	TxPwr	AGCgain
Lo0/1	UP	32		0 - 6.13	13.0	43		0 - 85.6	- 2.0
Lo0/2	UP	32		0 - 6.13	15.1	42		0 - 85.9	- 2.0
Lo0/3	UP	32		0 - 6.13	13.5	42		0 - 85.6	- 2.0
Lo0/4	DOWN	10		0 - 5.85	63.9	0		0 0.0	0.0
Lo0/5	DOWN	10		0 - 5.85	58.9	0		0 0.0	0.0
Lo0/6	UP	33		0 - 6.13	15.1	42		0 - 85.9	- 2.0
Lo0/7	DOWN	10		0 - 5.85	54.2	0		0 0.0	0.0
Lo0/8	UP	33		0 - 6.13	14.6	42		0 - 85.9	- 2.5
Lo0/9	DOWN	10		0 - 5.85	52.9	0		0 0.0	0.0
Lo0/10	DOWN	10		0 - 5.85	61.5	0		0 0.0	0.0
Lo0/11	UP	33		0 - 6.13	15.1	42		0 - 85.9	- 1.6
Lo0/12	UP	33		0 - 6.13	15.1	42		0 - 85.9	- 2.5
Lo0/13	UP	33		0 - 6.13	15.1	42		0 - 85.9	- 2.5
Lo0/14	DOWN	10		268305 - 5.85	57.5	0		0 0.0	0.0
Lo0/15	DOWN	10		0 - 5.85	50.7	0		0 0.0	0.0
Lo0/16	UP	35		38 - 5.85	15.1	41	1238	- 85.9	- 6.4
Lo0/17	DOWN	10		767128 - 5.85	61.8	0		0 0.0	0.0
Lo0/18	DOWN	10		0 - 5.85	54.2	0		0 0.0	0.0
Lo0/19	DOWN	10		0 - 5.85	51.5	0		0 0.0	0.0
Lo0/20	DOWN	10		0 - 5.85	54.7	0		0 0.0	0.0
Lo0/21	DOWN	10		0 - 5.85	67.8	0		0 0.0	0.0
Lo0/22	DOWN	10		0 - 5.85	50.7	0		0 0.0	0.0
Lo0/23	DOWN	10		0 - 5.85	66.5	0		0 0.0	0.0
Lo0/24	DOWN	10		0 - 5.85	53.6	0		0 0.0	0.0

This is an example of output from the **show controllers lre status sequence** command:

```
Switch# show controllers lre status sequence
```

Port	Sequence	Status	Profile
Lo0/1	LRE-SEQ-DOWNSTREAM	Converged	LRE-15
Lo0/2	N/A	N/A	N/A
Lo0/3	LRE-SEQ-SYM	Converged	LRE-15

This is an example of output using the **details** keyword to obtain further information about the sequence:

```
Switch# show controllers lre status sequence detail
```

```
Lo0/1 :
Sequence:LRE-SEQ-DOWNSTREAM      Status:Converged      Attempts:1
Profile:LRE-15                    Convergence Time: 00:01:54
Rate-Selection:Enabled            Locking:Not-Configured
Downstream Margin:2              Upstream Margin:0
```

■ **show controllers lre status**

```

Lo0/2 :
Sequence:N/A          Status:N/A           Attempts:0
Profile:N/A           Convergence Time: 00:00:00
Rate-Selection:Disabled Locking:Not-Configured
Downstream Margin:0   Upstream Margin:0

Lo0/3 :
Sequence:LRE-SEQ-SYM    Status:Converged      Attempts:1
Profile:LRE-15          Convergence Time: 00:01:57
Rate-Selection:Enabled   Locking:Not-Configured
Downstream Margin:0     Upstream Margin:0

Lo0/4 :
Sequence:N/A          Status:N/A           Attempts:0
Profile:N/A           Convergence Time: 00:00:00
Rate-Selection:Disabled Locking:Not-Configured

```

Related Commands

Command	Description
margin	Specifies the margin value used to determine link quality during LRE rate selection.
show controllers lre profile details	Displays the sequence running on a specific switch LRE port.
show controllers lre profile names	Displays information about the LRE profiles available on the switch.
show controllers lre cpe identity	Displays the actual values of the LRE link on a specific switch LRE port.
show controllers lre interface-id admin	Displays the administrative settings of the LRE link on a specific switch LRE port.
show controllers lre profile names	Displays information about the LRE profiles available on the switch.

show controllers lre version

Use the **show controllers lre version** privileged EXEC command to display the version numbers of the various components (hardware, firmware, and patch software) that make up the switch Long-Reach Ethernet (LRE) interface.

show controllers lre version [interface-id] [| {begin | exclude | include} expression]

Syntax Description	<i>interface-id</i> (Optional) ID of the switch LRE port. begin (Optional) Display begins with the line that matches the specified <i>expression</i> . exclude (Optional) Display excludes lines that match the specified <i>expression</i> . include (Optional) Display includes lines that match the specified <i>expression</i> . <i>expression</i> Expression in the output to use as a reference point.
--------------------	---

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

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.

Usage Guidelines	Using the show controllers lre version command without specifying a switch LRE port displays the version numbers of all switch LRE interfaces.
-------------------------	---

Examples	This is an example of output that shows the version information for LRE interface lo0/2:
	<pre>Switch# show controllers lre version lo0/2 Interface Hw Sw Patch ----- -- -- Lo0/2 32 B4 50</pre>

Related Commands	Command	Description
	show controllers lre cpe identity	Displays the model numbers of the LRE CPE devices connected to the LRE switch and shows whether or not the connected CPE devices meet the minimum requirements for management by the LRE switch.

 show dot1x

show dot1x

Use the **show dot1x** privileged EXEC command to display the 802.1X statistics, administrative status, and operational status for the switch or for the specified interface.

```
show dot1x [interface interface-id] | [statistics [interface interface-id]] [ | {begin | exclude | include} expression]
```

Syntax Description	
interface <i>interface-id</i>	(Optional) Display the 802.1X status for the specified port.
statistics [interface <i>interface-id</i>]	(Optional) Display 802.1X statistics for the switch or the specified interface.
 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

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

Command History	Release	Modification
	12.1(6)EA2	This command was introduced.

Usage Guidelines If you do not specify an interface, global parameters and a summary appear. If you specify an interface, details for that interface appear.

If you specify the **statistics** keyword without the **interface *interface-id*** option, statistics appear for all interfaces. If you specify the **statistics** keyword with the **interface *interface-id*** option, statistics appear for the specified interface.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples This is an example of output from the **show dot1x** command:

```
Switch# show dot1x
```

```
Global 802.1X Parameters
  reauth-enabled          no
  reauth-period           3600
  quiet-period            60
  tx-period               30
  supp-timeout            30
  server-timeout          30
  reauth-max              2
  max-req                 2
```

```

802.1X Port Summary
Port Name          Status      Mode           Authorized
Gi0/1              disabled   n/a            n/a
Gi0/2              enabled    Auto (negotiate) no

802.1X Port Details
802.1X is disabled on GigabitEthernet0/1

802.1X is enabled on GigabitEthernet0/2
Status             Unauthorized
Port-control      Auto
Supplicant         0060.b0f8.fbfb
Multiple Hosts    Disallowed
Current Identifier 2

Authenticator State Machine
State             AUTHENTICATING
Reauth Count      1

Backend State Machine
State             RESPONSE
Request Count    0
Identifier (Server) 2

Reauthentication State Machine
State             INITIALIZE

```



In the previous example, the supp-timeout, server-timeout, and reauth-max values in the Global 802.1X Parameters section are not configurable. When relaying a request from the Remote Authentication Dial-In User Service (RADIUS) authentication server to the client, the supp-timeout is the amount of time the switch waits for a response before it resends the request. When relaying a response from the client to the RADIUS authentication server, the server-timeout is the amount of time the switch waits for a reply before it resends the response. The reauth-max parameter is the maximum number of times that the switch tries to authenticate the client without receiving any response before the switch resets the port and restarts the authentication process.

In the 802.1X Port Summary section of the example, the Status column shows whether the port is enabled for 802.1X (the **dot1x port-control** interface configuration command is set to **auto** or **force-unauthorized**). The Mode column shows the operational status of the port; for example, if you configure the **dot1x port-control** interface configuration command to **force-unauthorized**, but the port has not transitioned to that state, the Mode column displays *auto*. If you disable 802.1X, the Mode column displays *n/a*.

The Authorized column shows the authorization state of the port. For information about port states, refer to the “Configuring 802.1X Port-Based Authentication” chapter in the *Catalyst 2950 Desktop Switch Software Configuration Guide*.

This is an example of output from the **show dot1x interface gigabitethernet0/2** privileged EXEC command. [Table 2-8](#) describes the fields in the example.

```

Switch# show dot1x interface gigabitethernet0/2

802.1X is enabled on GigabitEthernet0/2
Status             Authorized
Port-control      Auto
Supplicant         0060.b0f8.fbfb
Multiple Hosts    Disallowed
Current Identifier 3

```

■ show dot1x

```

Authenticator State Machine
  State          AUTHENTICATED
  Reauth Count   0

Backend State Machine
  State          IDLE
  Request Count  0
  Identifier (Server) 2

Reauthentication State Machine
  State          INITIALIZE

```

Table 2-8 show dot1x interface Field Description

Field	Description
802.1X is enabled on GigabitEthernet0/2	
Status	Status of the port (authorized or unauthorized). The status of a port appears as authorized if the dot1x port-control interface configuration command is set to auto , and authentication was successful.
Port-control	Setting of the dot1x port-control interface configuration command.
Supplicant	Ethernet MAC address of the client, if one exists. If the switch has not discovered the client, this field displays <i>Not set</i> .
Multiple Hosts	Setting of the dot1x multiple-hosts interface configuration command (allowed or disallowed).
Current Identifier ¹	Each exchange between the switch and the client includes an identifier, which matches requests with responses. This number is incremented with each exchange and can be reset by the authentication server.

1. This field and the remaining fields in the example show internal state information. For a detailed description of these state machines and their settings, refer to the IEEE 802.1X standard.

This is an example of output from the **show dot1x statistics interface gigabitethernet0/1** command. **Table 2-9** describes the fields in the example.

```
Switch# show dot1x statistics interface gigabitethernet0/1
```

```
GigabitEthernet0/1
```

Rx:	EAPOL Start 0	EAPOL Logoff 0	EAPOL Invalid 0	EAPOL Total 21	EAP Resp/Id 0	EAP Resp/Oth 0	EAP LenError 0
Last EAPOLVer 1	Last EAPOLSrc 0002.4b29.2a03						
Tx:	EAPOL Total 622	EAP Req/Id 445	EAP Req/Oth 0				

Table 2-9 show dot1x statistics Field Descriptions

Field	Description
RX EAPOL ¹ Start	Number of valid EAPOL-start frames that have been received
RX EAPOL Logoff	Number of EAPOL-logoff frames that have been received
RX EAPOL Invalid	Number of EAPOL frames that have been received and have an unrecognized frame type
RX EAPOL Total	Number of valid EAPOL frames of any type that have been received
RX EAP ² Resp/ID	Number of EAP-response/identity frames that have been received
RX EAP Resp/Oth	Number of valid EAP-response frames (other than response/identity frames) that have been received
RX EAP LenError	Number of EAPOL frames that have been received in which the packet body length field is invalid
Last EAPOLVer	Protocol version number carried in the most recently received EAPOL frame
LAST EAPOLSrc	Source MAC address carried in the most recently received EAPOL frame
TX EAPOL Total	Number of EAPOL frames of any type that have been sent
TX EAP Req/Id	Number of EAP-request/identity frames that have been sent
TX EAP Req/Oth	Number of EAP-request frames (other than request/identity frames) that have been sent

1. EAPOL = Extensible Authentication Protocol over LAN
2. EAP = Extensible Authentication Protocol

Related Commands

Command	Description
dot1x default	Resets the global 802.1X parameters to their default values.

show env

show env

Use the **show env** user EXEC command to display fan information for the switch.

```
show env {all | fan} [ | {begin | exclude | include} expression]
```

Syntax Description

all	Display both fan and temperature environmental status.
fan	Display the switch fan status (only available in privileged EXEC mode).
 begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.0(5.2)WC(1)	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show env all** command:

```
Switch> show env all
FAN 1 is OK
```

This is an example of output from the **show env fan** command:

```
Switch# show env fan
FAN 1 is FAULTY
```

show errdisable recovery

Use the **show errdisable recovery** user EXEC command to display the error-disable recovery timer information.

show errdisable recovery [| {begin | exclude | include} expression]

Syntax Description

begin	(Optional) Display begins with the line that matches the <i>expression</i> .
exclude	(Optional) Display excludes lines that match the <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(6)EA2	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter | **exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show errdisable recovery** command:

```
Switch> show errdisable recovery
ErrDisable Reason      Timer Status
-----
udld                  Enabled
bpduguard             Enabled
channel-misconfig     Enabled
pagp-flap              Enabled
dtp-flap              Enabled
link-flap              Enabled
psecure-violation     Enabled
gbic-invalid          Enabled

Timer interval:300 seconds

Interfaces that will be enabled at the next timeout:

Interface    Errdisable reason      Time left(sec)
-----
Gi0/4        link-flap            279
```

■ **show errdisable recovery**

Related Commands	Command	Description
	errdisable recovery	Configures the recover mechanism variables.
	show interfaces trunk	Displays interface status or a list of interfaces in error-disabled state.

show etherchannel

Use the **show etherchannel** user EXEC command to display EtherChannel information for a channel.

```
show etherchannel [channel-group-number] {brief | detail | load-balance / port | port-channel | summary} [ | {begin | exclude | include} expression]
```

Syntax Description

<i>channel-group-number</i>	(Optional) Number of the channel group. Valid numbers range from 1 to 6.
brief	Display a summary of EtherChannel information.
detail	Display detailed EtherChannel information.
load-balance	Display the load-balance or frame-distribution scheme among ports in the port channel.
port	Display EtherChannel port information.
port-channel	Display port-channel information.
summary	Display a one-line summary per channel-group.
 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(6)EA2	This command was introduced. It replaced the show port group command.

Usage Guidelines

If you do not specify a *channel-group*, all channel groups appear.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

■ show etherchannel**Examples**

This is an example of output from the **show etherchannel 1 detail** command:

```
Switch> show etherchannel 1 detail
Group state = L2
Ports: 1 Maxports = 8
Port-channels: 1 Max Port-channels = 1
          Ports in the group:
          -----
          Port: Fa0/3
          -----

          Port state      = Down Not-in-Bndl
          Channel group = 1           Mode = Automatic-Sl      Gcchange = 0
          Port-channel   = null        GC    = 0x00000000    Pseudo port-channel = Po1
          Port index     = 0            Load  = 0x00

          Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
                  A - Device is in Auto mode.          P - Device learns on physical port.
                  d - PAgP is down.
          Timers: H - Hello timer is running.        Q - Quit timer is running.
                  S - Switching timer is running.       I - Interface timer is running.

          Local information:
          Hello      Partner    PAgP      Learning   Group
          Port      Flags State   Timers Interval Count Priority Method Ifindex
          Fa0/3     dA    U1/S1      1s        0        200      Any      0

          Age of the port in the current state: 10d:23h:07m:37s
          Port-channels in the group:
          -----

          Port-channel: Po1
          -----

          Age of the Port-channel = 03d:02h:22m:43s
          Logical slot/port = 1/0           Number of ports = 0
          GC                = 0x00000000    HotStandBy port = null
          Port state        = Port-channel Ag-Not-Inuse
```

This is an example of output from the **show etherchannel 1 summary** command:

```
Switch> show etherchannel 1 summary
Flags: D - down      P - in port-channel
      I - stand-alone S - suspended
      R - Layer3     S - Layer2
      u - unsuitable for bundling
      U - port-channel in use
      d - default port
Group Port-channel Ports
-----+-----+
1     Po1(SU)      Fa0/6(Pd) Fa0/15(P)
```

This is an example of output from the **show etherchannel 1 brief** command:

```
Switch> show etherchannel 1 brief
Group state = L2
Ports: 1 Maxports = 8
Port-channels: 1 Max Port-channels = 1
```

This is an example of output from the **show etherchannel 1 port** command:

```
Switch> show etherchannel 1 port
          Ports in the group:
          -----
          Port: Fa0/3
          -----
          Port state      = Down Not-in-Bndl
          Channel group  = 1           Mode = Automatic-Sl    Gcchange = 0
          Port-channel   = null        GC   = 0x00000000  Pseudo port-channel = Po1
          Port index     = 0            Load = 0x00

          Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
                  A - Device is in Auto mode.          P - Device learns on physical port.
                  d - PAgP is down.

          Timers: H - Hello timer is running.        Q - Quit timer is running.
                  S - Switching timer is running.       I - Interface timer is running.

          Local information:
          Hello      Partner    PAgP      Learning   Group
          Port      Flags State   Timers Interval Count Priority Method Ifindex
          Fa0/3     dA      U1/S1      1s        0        200      Any      0

          Age of the port in the current state: 10d:23h:13m:21s
```

Related Commands

Command	Description
channel-group	Assigns an Ethernet interface to an EtherChannel group.
interface port-channel	Accesses or creates the port channel.

show file

show file

Use the **show file** privileged EXEC command to display a list of open file descriptors, file information, and file system information.

show file {descriptors | information {device: }filename / systems} [| {begin | exclude | include} expression]

Syntax Description	descriptors	Display a list of open file descriptors.
	information	Display file information.
	device:	Device containing the file. Valid devices include the switch Flash memory.
	filename	Name of file.
	systems	Display file system information.
	 begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .
	 exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .
	 include	(Optional) Display includes lines that match the specified <i>expression</i> .
	expression	Expression in the output to use as a reference point.

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

Command History	Release	Modification
	12.0(5.2)WC(1)	This command was introduced.
	12.1(6)EA2	The descriptors and information keywords were added.

Usage Guidelines	File descriptors are the internal representations of open files. You can use this command to see if another user has a file open.
-------------------------	---

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples	This is an example of output from the show file descriptors command:
-----------------	---

```
Switch# show file descriptors
File Descriptors:
FD  Position  Open   PID  Path
0   187392    0001    2    tftp://temp/hampton/c2950g.a
1   184320    030A    2    flash:c2950-i-m.a
```

Table 2-10 describes the fields in the **show file descriptors** command output.

Table 2-10 show file descriptors Field Descriptions

Field	Description
FD	File descriptor. The file descriptor is a small integer used to specify the file once it has been opened.
Position	Byte offset from the start of the file.
Open	Flags supplied when opening the file.
PID	Process ID of the process that opened the file.
Path	Location of the file.

This is an example of output from the **show file information nvram:startup-config** command:

```
Switch# show file information nvram:startup-config
nvram:startup-config:
    type is ascii text
```

[Table 2-11](#) lists the possible file types for the previous example.

Table 2-11 Possible File Types

Field	Description
ascii text	Configuration file or other text file.
coff	Runnable image in coff format.
ebcdic	Text generated on an IBM mainframe.
image (a.out)	Runnable image in a.out format.
image (elf)	Runnable image in elf format.
lzw compression	Lzw compressed file.
tar	Text archive file used by the CIP.

This is an example of output from the **show file systems** command:

```
Switch# show file systems
File Systems:

      Size(b)   Free(b)     Type   Flags  Prefixes
*    7741440     433152   flash   rw    flash:
    7741440     433152  unknown   rw    zflash:
      32768     25316   nvram   rw    nvram:
      -          -   network   rw    tftp:
      -          -   opaque   rw    null:
      -          -   opaque   rw    system:
      -          -   opaque   ro    xmodem:
      -          -   opaque   ro    ymodem:
      -          -   network   rw    rcp:
      -          -   network   rw    ftp:
```

show file

For this example, [Table 2-12](#) describes the fields in the **show file systems** command output. [Table 2-13](#) lists the file system types. [Table 2-14](#) lists the file system flags.

Table 2-12 show file systems Field Descriptions

Field	Description
Size(b)	Amount of memory in the file system, in bytes.
Free(b)	Amount of free memory in the file system, in bytes.
Type	Type of file system.
Flags	Permissions for file system.
Prefixes	Alias for file system.

Table 2-13 File System Types

Field	Description
disk	The file system is for a rotating medium.
flash	The file system is for a Flash memory device.
network	The file system is a network file system, such as TFTP, rcp, or FTP.
nvram	The file system is for an NVRAM device.
opaque	The file system is a locally generated <i>pseudo</i> file system (for example, the <i>system</i>) or a download interface, such as brimux.
rom	The file system is for a ROM or EPROM device.
tty	The file system is for a collection of terminal devices.
unknown	The file system is of unknown type.

Table 2-14 File System Flags

Field	Description
ro	The file system is Read Only.
wo	The file system is Write Only
rw	The file system is Read/Write.

show interfaces

Use the **show interfaces** privileged EXEC command to display the administrative and operational status of all interfaces or a specified interface.

```
show interfaces [interface-id | vlan vlan-id] [accounting | [cpe [port port-id]]| description | etherchannel | media | media [interface-id] pruning | stats | status [err-disabled] | switchport | trunk] [ | {begin | exclude | include} expression]
```

Syntax Description		
	interface-id	(Optional) Valid interfaces include physical ports (including type, slot, and port number) and port channels. The valid port-channel range is 1 to 6.
	vlan <i>vlan-id</i>	(Optional) VLAN ID. The valid VLAN range is 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1005 when the standard software image (SI) is installed. Do not enter leading zeros.
	accounting	(Optional) Display interface accounting information.
	cpe	(Optional) Display link status, speed, and duplex of all the customer premises equipment (CPE) Ethernet ports.
	port <i>port-id</i>	(Optional) Display only the designated CPE Ethernet port. Valid values are 1 to 4.
	description	(Optional) Display the administrative status and description set for an interface.
	etherchannel	(Optional) Display interface EtherChannel information.
	media	(Optional) Display the type of media connection.
	media <i>interface-id</i>	(Optional) Display the type of media connection on a specific interface.
	pruning	(Optional) Display interface trunk VTP pruning information.
	stats	(Optional) Display the input and output packets by switching path for the interface.
	status	(Optional) Display the status of the interface.
	err-disabled	(Optional) Display interfaces in error-disabled state.
	switchport	(Optional) Display the administrative and operational status of a switching (nonrouting) port.
	trunk	Display interface trunk information. If you do not specify an interface, only information for active trunking ports appears.
begin		(Optional) Display begins with the line that matches the <i>expression</i> .
exclude		(Optional) Display excludes lines that match the <i>expression</i> .
include		(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>		Expression in the output to use as a reference point.


Note

Though visible in the command-line help strings, the **crb**, **fair-queue**, **irb**, **mac-accounting**, **precedence**, **random-detect**, **rate-limit**, and **shape** options are not supported.

Command Modes

Privileged EXEC

show interfaces

Command History	Release	Modification
	12.0(5.2)WC(1)	This command was introduced.
	12.1(11)YJ	Additional keywords were added to support LRE switches.

Usage Guidelines Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples This is an example of output from the **show interfaces accounting** command:

```
Switch# show interfaces accounting
Vlan1
      Protocol      Pkts In    Chars In      Pkts Out    Chars Out
          IP        17950    2351279        3205     411175
          ARP       8626    552064           62      3720
Interface Vlan5 is disabled

FastEthernet0/1
      Protocol      Pkts In    Chars In      Pkts Out    Chars Out
      Spanning Tree 2956958  179218508      34383    2131700
          CDP        14301    5777240        14307    5722418
          VTP         0        0            1408    145908
          DTP        28592    1572560           0        0
<output truncated>
```

This is an example of output from the **show interfaces gigabitethernet0/1** command:

```
Switch# show interfaces gigabitethernet0/1
FastEthernet0/1 is up, line protocol is down
  Hardware is Fast Ethernet, address is 0005.7428.09c1 (bia 0005.7428.09c1)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, Auto-speed
  input flow-control is off, output flow-control is off
  Last input never, output 4d21h, output hang never
  Last clearing of "show interface" counters never
  Input queue:0/75/0/0 (size/max/drops/flushes); Total output drops:0
  Queueing strategy:fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    1 packets input, 64 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 0 multicast, 0 pause input
    0 input packets with dribble condition detected
    1 packets output, 64 bytes, 0 underruns
    0 output errors, 0 collisions, 2 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier, 0 PAUSE output
    0 output buffer failures, 0 output buffers swapped out
```

This is an example of output from the **show interfaces gigabitethernet0/2 description** command when the interface has been described as *Connects to Marketing* by using the **description** interface configuration command.

```
Switch# show interfaces gigabitethernet0/2 description
Interface Status      Protocol Description
G10/2 up             down     Connects to Marketing
```

This is an example of output from the **show interfaces fastethernet0/1 pruning** command when pruning is enabled in the VTP domain:

```
Switch# show interfaces fastethernet0/1 pruning
Port      Vlans pruned for lack of request by neighbor
Fa0/1    4,196

Port      Vlan traffic requested of neighbor
Fa0/1    1,4
```

This is an example of output from the **show interfaces stats** command:

```
Switch# show interfaces stats
Vlan1
  Switching path      Pkts In   Chars In      Pkts Out   Chars Out
    Processor          3224706  223689126    3277307  280637322
    Route cache        0          0            0          0
    Total              3224706  223689126    3277307  280637322
Interface Vlan5 is disabled

FastEthernet0/1
  Switching path      Pkts In   Chars In      Pkts Out   Chars Out
    Processor          3286423  231672787    179501   17431060
    Route cache        0          0            0          0
    Total              3286423  231672787    179501   17431060
```

This is an example of output from the **show interfaces status** command. It displays the status of all interfaces. The prefix *a* in the Duplex and Speed columns shows the result of autonegotiation for that function.

```
Switch# show interfaces status
```

Port	Name	Status	Vlan	Duplex	Speed	Type
Fa0/1		notconnect	1	auto	auto	10/100BaseTX
Fa0/2		notconnect	1	auto	auto	10/100BaseTX
Fa0/3		disabled	100	auto	auto	10/100BaseTX
Fa0/4		connected	trunk	a-full	a-100	10/100BaseTX
Fa0/5		notconnect	1	auto	auto	10/100BaseTX
Fa0/6		connected	trunk	a-full	a-100	10/100BaseTX
Fa0/7		notconnect	1	auto	auto	10/100BaseTX
Fa0/8		connected	1	a-full	a-100	10/100BaseTX
Fa0/9		disabled	1	auto	auto	10/100BaseTX
Fa0/10		notconnect	5	auto	100	10/100BaseTX
Fa0/11		disabled	1	auto	auto	10/100BaseTX
Fa0/12		disabled	1	auto	auto	10/100BaseTX
Gi0/1		disabled	1	auto	auto	unknown
Gi0/2		notconnect	1	auto	auto	unknown
Po1		notconnect	1	auto	auto	

■ show interfaces

This is an example of output from the **show interfaces status** command for a specific interface:

```
Switch# show interfaces gi0/1 status

Port      Name          Status  Vlan      Duplex  Speed Type
Gi0/1           connected    1       a-full   a-100  10/100/1000BasX
Switch#
```

This example shows output from the **show interfaces status err-disabled** command. It displays the status of interfaces in error-disabled state.

```
switch#show interfaces fa0/15 status err-disabled
```

```
Port      Name          Status      Reason
Fa0/15            err-disabled psecure-violation
```

This is an example of output from the **show interfaces etherchannel** command when port channels are configured on the switch:

```
Switch# show interfaces etherchannel
-----
FastEthernet0/1:
Port state      = Up Mstr In-Bndl
Channel group   = 1          Mode = On/FEC      Gcchange = 0
Port-channel    = Po1          GC   = 0x00010001    Pseudo port-channel = Po1
Port index      = 0          Load = 0x00

Age of the port in the current state:00d:00h:06m:54s
-----
Port-channel:
Age of the Port-channel    = 09d:22h:45m:14s
Logical slot/port   = 1/0          Number of ports = 1
GC                  = 0x00010001    HotStandBy port = null
Port state         = Port-channel Ag-Inuse

Ports in the Port-channel:
Index  Load  Port   EC state
-----+----+----+-----
  0     00    Fa0/1   on

Time since last port bundled: 00d:00h:06m:54s      Fa0/1
```

This is an example of output from the **show interfaces switchport** command for a single interface. [Table 2-15](#) describes the fields in the output.

```
Switch# show interfaces gigabitethernet0/1 switchport
Name:Fa0/1
Switchport:Enabled
Administrative Mode:static access
Operational Mode:down
Administrative Trunking Encapsulation:dot1q
Negotiation of Trunking:Off
Access Mode VLAN:1 (default)
Trunking Native Mode VLAN:1 (default)
Trunking VLANs Enabled:ALL
Pruning VLANs Enabled:2-1001

Protected:false

Voice VLAN:dot1p (Inactive)
Appliance trust:5
```

This is an example of output from the **show interfaces** command for port 5 on an LRE switch:

```
Switch# show interfaces lo0/5
LongReachEthernet0/5 is up, line protocol is up
  Hardware is Ethernet over LRE, address is 0006.2871.5902 (bia 0006.2871.5902)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not set
  Half-duplex, Auto Speed (10), 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:21, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    8272 packets input, 852898 bytes, 0 no buffer
    Received 1182 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 1182 multicast
    0 input packets with dribble condition detected
    61899 packets output, 17981033 bytes, 0 underruns
    0 output errors, 0 collisions, 1 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
```

This is an example of output from the **show interfaces** command for all interfaces on a CPE device:

```
Switch# show interfaces lo0/2 cpe
```

Port	Status	Speed	Duplex
1	notconnected	auto	NA
2	notconnected	auto	NA
3	notconnected	auto	NA
4	notconnected	auto	NA
5	connected	100	half

```
Switch#
```

This is an example of output from the **show interfaces** command for port 5 on a CPE device:

```
Switch# show interfaces lo0/2 cpe port 5
```

Port	Status	Speed	Duplex
5	connected	100	half

```
Switch#
```

This is an example of output from the **show interfaces interface-id media** command:

```
Switch# show interfaces gi0/1 media
```

Port	Media-configured	Active	Attached
Gi0/1	auto-select	rj45	1000BaseSX-10/100/1000BaseTX

```
Switch#
```

■ show interfaces

This is an example of output from the **show interfaces media** command:

```
Switch# show interfaces media

Port    Media-configured   Active      Attached
Gi0/1  auto-select       rj45       1000BaseSX-10/100/1000BaseTX
Gi0/2  prefer-sfp        sfp        1000BaseSX-10/100/1000BaseTX

Switch#
```

Table 2-15 show interfaces switchport Field Descriptions

Field	Description
Name	Displays the port name.
Switchport	Displays the administrative and operational status of the port. In this output, the port is in switchport mode.
Administrative Mode	Displays the administrative and operational mode.
Operational Mode	
Administrative Trunking Encapsulation	Displays the administrative and operational encapsulation method and whether trunking negotiation is enabled.
Operation Trunking Encapsulation	
Negotiation of Trunking	
Access Mode VLAN	Displays the VLAN ID to which the port is configured.
Trunking Native Mode VLAN	Lists the VLAN ID of the trunk that is in native mode. Lists the allowed VLANs on the trunk. Lists the active VLANs on the trunk.
Trunking VLANs Enabled	
Trunking VLANs Active	
Pruning VLANs Enabled	Lists the VLANs that are pruning-eligible.
Protected	Displays whether or not protected port is enabled (True) or disabled (False) on the interface.
Voice VLAN	Displays the VLAN ID on which voice VLAN is enabled.
Appliance trust	Displays the class of service (CoS) setting of the data packets of the IP phone.

This example shows output from the **show interfaces trunk** command:

```
Switch# show interfaces trunk

Port      Mode       Encapsulation  Status      Native vlan
Fa0/4     on         802.1q        trunking    1
Fa0/6     on         802.1q        trunking    1

Port      Vlans allowed on trunk
Fa0/4     1-4094
Fa0/6     1-4094

Port      Vlans allowed and active in management domain
Fa0/4     1-2,51-52
Fa0/6     1-2,51-52

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/4     1
Fa0/6     1-2,51-52
```

This example shows output from the **show interfaces fastethernet0/1 trunk** command. It displays trunking information for the interface.

```
Switch# show interfaces fastethernet0/1 trunk

Port      Mode       Encapsulation  Status      Native vlan
Fa0/1    desirable     802.1q        trunking      1

Port      Vlans allowed on trunk
Fa0/1    1-4094

Port      Vlans allowed and active in management domain
Fa0/1    1,4,196,306

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1    1,306
```

Related Commands

Command	Description
switchport access	Configures a port as a static-access or dynamic-access port.
switchport protected	Isolates Layer 2 unicast, multicast, and broadcast traffic from other protected ports on the same switch.
switchport trunk pruning	Configures the VLAN pruning-eligible list for ports in trunking mode.

■ **show interfaces counters**

show interfaces counters

Use the **show interfaces counters** privileged EXEC command to display various counters for a specific interface or for all interfaces.

```
show interfaces [interface-id | vlan vlan-id] counters [broadcast | errors | multicast | trunk | unicast] [ | {begin | exclude | include} expression]
```

Syntax Description	
<i>interface-id</i>	(Optional) ID of the physical interface, including type and slot and port number.
vlan <i>vlan-id</i>	(Optional) VLAN number of the management VLAN. Valid IDs are from 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1001 when the standard software image (SI) is installed. Do not enter leading zeros.
broadcast	(Optional) Display discarded broadcast traffic.
errors	(Optional) Display error counters.
multicast	(Optional) Display discarded multicast traffic.
trunk	(Optional) Display trunk counters.
unicast	(Optional) Display discarded unicast traffic.
 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(6)EA2	This command was introduced.

Usage Guidelines If you do not enter any keywords, all counters for all interfaces are included.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show interfaces counters** command. It displays all the counters for the switch.

```
Switch# show interfaces counters
Port      InOctets   InUcastPkts   InMcastPkts   InBcastPkts
Gi0/1    23324617     10376        185709        126020
Gi0/2          0           0           0           0

Port      OutOctets  OutUcastPkts  OutMcastPkts  OutBcastPkts
Gi0/1   4990607      28079        21122         10
Gi0/2   1621568      25337         0           0
```

This is an example of output from the **show interfaces counters broadcast** command. It displays the dropped broadcast traffic for all interfaces.

```
Switch# show interfaces counters broadcast
Port      BcastSuppDiscards
Gi0/1            1
Gi0/2            0
```

This is an example of output from the **show interfaces gigabitethernet0/1 counters broadcast** command. It displays the dropped broadcast traffic for an interface.

```
Switch# show interfaces gigabitethernet0/1 counters broadcast
Port      BcastSuppDiscards
Gi0/1            0
```

This is an example of output from the **show interfaces counters errors** command. It displays the interface error counters for all interfaces.

```
Switch# show interfaces counters errors
Port      Align-Err    FCS-Err    Xmit-Err    Rcv-Err  UnderSize
Gi0/1        0          0          0          0          0
Gi0/2        0          0          0          0          0

Port      Single-Col  Multi-Col  Late-Col  Excess-Col  Carri-Sen    Runts    Giants
Gi0/1        0          0          0          0          0          0          0
Gi0/2        0          0          0          0          0          0          0
```

This is an example of output from the **show interfaces counters multicast** command. It displays the dropped multicast traffic for all interfaces.

```
Switch# show interfaces counters multicast
Port      McastSuppDiscards
Gi0/1            0
Gi0/2            0
```

This is an example of output from the **show interfaces counters trunk** command. It displays the trunk counters for all interfaces.

```
Switch# show interfaces counters trunk
Port      TrunkFramesTx  TrunkFramesRx  WrongEncap
Gi0/1        0            0            0
Gi0/2        0            0            0
```

■ show interfaces counters

This is an example of output from the **show interfaces counters unicast** command. It displays the dropped unicast traffic for all interfaces.

```
Switch# show interfaces counters unicast
```

Port	UcastSuppDiscards
Gi0/1	6872
Gi0/2	0

Related Commands

Command	Description
show interfaces	Displays interface characteristics.
speed	Configures broadcast, multicast, and unicast storm control for an interface.

show ip access-lists

Use the **show ip access-lists** privileged EXEC command to display IP access control lists (ACLs) configured on the switch.

show ip access-lists [name | number] [| {begin | exclude | include} expression]

Syntax Description

<i>name</i>	(Optional) ACL name.
<i>number</i>	(Optional) ACL number. The range is from 1 to 199 and from 1300 to 2699.
begin	(Optional) Display begins with the line that matches the <i>expression</i> .
exclude	(Optional) Display excludes lines that match the <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(6)EA2	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter | **exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show ip access-lists** command:

```
Switch# show ip access-lists
Standard IP access list testingacl
    permit 10.10.10.2
Standard IP access list wizard_1-1-1-2
    permit 1.1.1.2
Extended IP access list 103
    permit tcp any any eq www
Extended IP access list CMP-NAT-ACL
    Dynamic Cluster-HSRP deny ip any any
    Dynamic Cluster-NAT permit ip any any
        permit ip host 10.245.155.128 any
        permit ip host 10.245.137.0 any
        permit ip host 10.146.106.192 any
        permit ip host 10.216.25.128 any
        permit ip host 10.228.215.0 any
        permit ip host 10.221.111.64 any
        permit ip host 10.123.222.192 any
        permit ip host 10.169.110.128 any
        permit ip host 10.186.122.64 any
```

■ show ip access-lists

This is an example of output from the **show ip access-lists 103** command:

```
Switch# show ip access-lists 103
Extended IP access list 103
    permit tcp any any eq www
```

Related Commands	Command	Description
	access-list (IP extended)	Configures an extended IP ACL on the switch.
	access-list (IP standard)	Configures a standard IP ACL on the switch.
	ip access-list	Configures an IP ACL on the switch.
	show access-lists	Displays ACLs configured on a switch.

show ip igmp snooping

Use the **show ip igmp snooping** privileged EXEC command to display the Internet Group Management Protocol (IGMP) snooping configuration of the switch or the VLAN.

show ip igmp snooping [vlan *vlan-id*] [| {begin | exclude | include} *expression*]

show ip igmp snooping [vlan *vlan-id*] [| {begin | exclude | include} *expression*]

Syntax Description	vlan <i>vlan-id</i> (Optional) Keyword and variable to specify a VLAN; valid values are 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1001 when the standard software image (SI) is installed. Do not enter leading zeros. begin (Optional) Display begins with the line that matches the specified <i>expression</i> . exclude (Optional) Display excludes lines that match the specified <i>expression</i> . include (Optional) Display includes lines that match the specified <i>expression</i> . <i>expression</i> Expression in the output to use as a reference point.
---------------------------	--

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

Command History	Release	Modification
	12.0(5.2)WC(1)	This command was introduced.

Usage Guidelines	Use this command to display snooping characteristics for the switch or for a specific VLAN. Expressions are case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> do not appear, but the lines that contain <i>Output</i> appear.
-------------------------	---

Examples	This is an example of output from the show ip igmp snooping command:
-----------------	---

```
Switch# show ip igmp snooping

vlan 1
-----
  IGMP snooping is globally enabled
  IGMP snooping is enabled on this Vlan
  IGMP snooping immediate-leave is enabled on this Vlan
  IGMP snooping mrouter learn mode is pim-dvmrp on this Vlan

vlan 2
-----
  IGMP snooping is globally enabled
  IGMP snooping is enabled on this Vlan
  IGMP snooping immediate-leave is enabled on this Vlan
  IGMP snooping mrouter learn mode is cgmp on this Vlan
```

■ show ip igmp snooping

```
vlan 3
-----
IGMP snooping is globally enabled
IGMP snooping is enabled on this Vlan
IGMP snooping immediate-leave is disabled on this Vlan
IGMP snooping mrouter learn mode is cgmp on this Vlan
vlan 4
-----
IGMP snooping is globally enabled
IGMP snooping is enabled on this Vlan
IGMP snooping immediate-leave is disabled on this Vlan
IGMP snooping mrouter learn mode is cgmp on this Vlan
vlan 5
-----
IGMP snooping is globally enabled
IGMP snooping is enabled on this Vlan
IGMP snooping immediate-leave is disabled on this Vlan
IGMP snooping mrouter learn mode is pim-dvmrp on this Vlan
vlan 33
-----
IGMP snooping is globally enabled
IGMP snooping is enabled on this Vlan
IGMP snooping immediate-leave is disabled on this Vlan
IGMP snooping mrouter learn mode is pim-dvmrp on this Vlan
```

This is an example of output from the **show ip igmp snooping vlan 1** command:

```
Switch# show ip igmp snooping vlan 1

vlan 1
-----
IGMP snooping is globally enabled
IGMP snooping is enabled on this Vlan
IGMP snooping immediate-leave is enabled on this Vlan
IGMP snooping mrouter learn mode is pim-dvmrp on this Vlan
```

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping.
ip igmp snooping vlan <i>vlan-id</i>	Enables IGMP snooping on the VLAN interface.
ip igmp snooping vlan <i>vlan</i> immediate-leave	Configures IGMP Immediate-Leave processing.
ip igmp snooping vlan mrouter	Configures a Layer 2 port as a multicast router port.
show mac address-table multicast	Displays the Layer 2 multicast entries for a VLAN.

show ip igmp snooping mrouter

Use the **show ip igmp snooping mrouter** privileged EXEC command to display information on dynamically learned and manually configured multicast router ports.

show ip igmp snooping mrouter [vlan *vlan-id*] [| {begin | exclude | include} *expression*]

Syntax Description	vlan <i>vlan-id</i>	(Optional) Keyword and variable to specify a VLAN; valid values are 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1001 when the standard software image (SI) is installed. Do not enter leading zeros.
begin		(Optional) Display begins with the line that matches the specified <i>expression</i> .
exclude		(Optional) Display excludes lines that match the specified <i>expression</i> .
include		(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>		Expression in the output to use as a reference point.

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

Command History	Release	Modification
	12.0(5.2)WC(1)	This command was introduced.

Usage Guidelines	You can also use the show mac address-table multicast command to display entries in the MAC address table for a VLAN that has Internet Group Management Protocol (IGMP) snooping enabled. Expressions are case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> do not appear, but the lines that contain <i>Output</i> appear.
-------------------------	---

Examples	This is an example of output from the show ip igmp snooping mrouter vlan 1 command:
-----------------	--



In this example, Fa0/3 is a dynamically learned router port, and Fa0/2 is a configured static router port.

```
Switch# show ip igmp snooping mrouter vlan 1
```

Vlan	ports
---	----
1	Fa0/2(static), Fa0/3(dynamic)

■ **show ip igmp snooping mrouter**

Related Commands	Command	Description
	ip igmp snooping	Enables IGMP snooping.
	ip igmp snooping vlan	Enables IGMP snooping on the VLAN interface.
	ip igmp snooping vlan immediate-leave	Configures IGMP Immediate-Leave processing.
	ip igmp snooping vlan mrouter	Configures a Layer 2 port as a multicast router port.
	show mac address-table multicast	Displays the Layer 2 multicast entries for a VLAN.

show lre upgrade binaries

Use the **show lre upgrade binaries** privileged EXEC command to display the Long-Reach Ethernet (LRE) binaries present on the system Flash memory.

show lre upgrade binaries [| {begin | exclude | include} expression]

Syntax Description	<table border="0"> <tr> <td> begin</td><td>(Optional) Display begins with the line that matches the specified <i>expression</i>.</td></tr> <tr> <td> exclude</td><td>(Optional) Display excludes lines that match the specified <i>expression</i>.</td></tr> <tr> <td> include</td><td>(Optional) Display includes lines that match the specified <i>expression</i>.</td></tr> <tr> <td><i>expression</i></td><td>Expression in the output to use as a reference point.</td></tr> </table>	begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .	exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .	include	(Optional) Display includes lines that match the specified <i>expression</i> .	<i>expression</i>	Expression in the output to use as a reference point.
begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .								
exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .								
include	(Optional) Display includes lines that match the specified <i>expression</i> .								
<i>expression</i>	Expression in the output to use as a reference point.								

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

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.

Usage Guidelines	Using the show lre upgrade binaries command displays the LRE binary information for each interface.
-------------------------	--

The output of the command shows the path to the LRE binaries, which are always in the same directory as the IOS image. LRE binary file names consist of:

- The device family. A device family could be an LRE switch or a customer premises equipment (CPE) device.
- The function of the firmware, such as an upgrade for an application, the bootloader, or for the LRE chipset.
- The firmware version.

Files marked with an exclamation point (!) are version description files. A version description file is only for informational purposes and is not a candidate for upgrade. Version description files are used to determine whether or not a CPE device on an LRE link is running a supported LRE binary version.

Examples	This example shows output from the show lre upgrade binaries command:
-----------------	--

```
Switch# show lre upgrade binaries
Path containing LRE binaries is flash:/c2950lre-i612q4-mz.121-0.18.YJ/lre-bin;
zflash:/c2950lre-i612q4-mz.121-0.18.YJ/lre-bin

LRE Binary: CISCO585-LRE_vdlsngl_51.00.00,
Flash file name: CISCO585-LRE_vdlsngl_51.00.00.bin

LRE Binary: CISCO585-LRE_MC8051boot_01.03.00,
Flash file name: CISCO585-LRE_MC8051boot_01.03.00.bin!

LRE Binary: CISCO585-LRE_MC8051boot_01.02.00,
```

■ **show lre upgrade binaries**

```

Flash file name: CISCO585-LRE_MC8051boot_01.02.00.bin!
LRE Binary: CISCO585-LRE_MC8051appl_01.03.00,
Flash file name: CISCO585-LRE_MC8051appl_01.03.00.bin!

LRE Binary: CISCO585-LRE_MC8051appl_01.02.00,
Flash file name: CISCO585-LRE_MC8051appl_01.02.00.bin

LRE Binary: CISCO575-LRE_vdsslsgl_50.00.00,
Flash file name: CISCO575-LRE_vdsslsgl_50.00.00.bin

LRE Binary: CISCO2950-LRE_vdsloctl_02.60.00,
Flash file name: CISCO2950-LRE_vdsloctl_02.60.00.bin

LRE Binary: CISCO2950-LRE_vdsloctl_02.51.00,
Flash file name: CISCO2950-LRE_vdsloctl_02.51.00.bin

LRE Binary: CISCO2950-LRE_vdsloctl_02.50.00,
Flash file name: CISCO2950-LRE_vdsloctl_02.50.00.bin

```

Related Commands

Command	Description
show lre upgrade status	Displays the upgrade status on all ports in the switch.
show lre upgrade version	Displays the versions of binaries on local and remote ends on all ports.

show lre upgrade status

Use the **show lre upgrade status** privileged EXEC command to display the upgrade status on all ports in the switch.

show lre upgrade status [| {begin | exclude | include} expression]

Syntax Description	<table border="0"> <tr> <td> begin</td><td>(Optional) Display begins with the line that matches the specified <i>expression</i>.</td></tr> <tr> <td> exclude</td><td>(Optional) Display excludes lines that match the specified <i>expression</i>.</td></tr> <tr> <td> include</td><td>(Optional) Display includes lines that match the specified <i>expression</i>.</td></tr> <tr> <td><i>expression</i></td><td>Expression in the output to use as a reference point.</td></tr> </table>	begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .	exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .	include	(Optional) Display includes lines that match the specified <i>expression</i> .	<i>expression</i>	Expression in the output to use as a reference point.
begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .								
exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .								
include	(Optional) Display includes lines that match the specified <i>expression</i> .								
<i>expression</i>	Expression in the output to use as a reference point.								

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

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.

Usage Guidelines	Use the show lre upgrade status command during LRE upgrades to display both the local and remote upgrade status levels in progress on an LRE link. Status levels are:
-------------------------	--

None—An upgrade is not in progress.

Pending—An upgrade is initialized, but transfer has not begun.

Active—Data transfer is in progress.

Cmplt—An upgrade is complete.

When an upgrade is running on an LRE switch controller, the status for the controller does not change from *active* to *cmplt* until all hardware elements finish upgrading.

Other information displayed includes the local current (lcl curr) and proposed configuration (cfg) for each LRE interface. File names consist of:

- The device family. A device family could be an LRE switch or a customer premises equipment (CPE) device.
- The function of the firmware, such as an upgrade for an application, for the bootloader, or for the LRE or CPE chipsets.
- The firmware version.

During data transfer but before the upgrade completes, the status also shows the time in hours and minutes that the upgrade has been in progress and the number of attempts that were made.

show lre upgrade status**Examples**

This example shows the status of an upgrade after it starts, but before the data transfer begins:

```
Switch# show lre upgrade status

Lo0/1:
  lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 new:CISCO2950-LRE_vdsloctl_02.60.00
  Status:Pending
  rmt curr:CISCO575-LRE_vdsslsgl_52.00.00 new:CISCO575-LRE_vdsslsgl_52.00.00
  Status:Pending
Lo0/2:
  lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 new:CISCO2950-LRE_vdsloctl_02.60.00
  Status:Pending
  rmt curr:CISCO575-LRE_vdsslsgl_52.00.00 new:CISCO575-LRE_vdsslsgl_52.00.00
  Status:Pending
Lo0/3:
  lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 new:CISCO2950-LRE_vdsloctl_02.60.00
  Status:Pending
  rmt curr:CISCO575-LRE_vdsslsgl_52.00.00 new:CISCO575-LRE_vdsslsgl_52.00.00
  Status:Pending
Lo0/4:
  lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 new:CISCO2950-LRE_vdsloctl_02.60.00
  Status:Pending
  rmt curr:CISCO575-LRE_vdsslsgl_52.00.00 new:CISCO575-LRE_vdsslsgl_52.00.00
  Status:Pending
Lo0/5:
  lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 new:CISCO2950-LRE_vdsloctl_02.60.00
  Status:Pending
  rmt curr:CISCO575-LRE_vdsslsgl_52.00.00 new:CISCO575-LRE_vdsslsgl_52.00.00
  Status:Pending
Lo0/6:
  lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 new:CISCO2950-LRE_vdsloctl_02.60.00
  Status:Pending
  rmt curr:CISCO575-LRE_vdsslsgl_52.00.00 new:CISCO575-LRE_vdsslsgl_52.00.00
  Status:Pending
Lo0/7:
  lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 new:CISCO2950-LRE_vdsloctl_02.60.00
  Status:Pending
  rmt curr:CISCO575-LRE_vdsslsgl_52.00.00 new:CISCO575-LRE_vdsslsgl_52.00.00
  Status:Pending
Lo0/8:
  lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 new:CISCO2950-LRE_vdsloctl_02.60.00
  Status:Pending
  rmt curr:CISCO575-LRE_vdsslsgl_52.00.00 new:CISCO575-LRE_vdsslsgl_52.00.00
  Status:Pending
Lo0/9:
  lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 new:CISCO2950-LRE_vdsloctl_02.60.00
  Status:Pending
  No remote devices on Lo0/9
Lo0/10:
  lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 new:CISCO2950-LRE_vdsloctl_02.60.00
  Status:Pending
  rmt curr:CISCO575-LRE_vdsslsgl_52.00.00 new:CISCO575-LRE_vdsslsgl_52.00.00
  Status:Pending
Lo0/11:
  lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 new:CISCO2950-LRE_vdsloctl_02.60.00
  Status:Pending
  rmt curr:CISCO575-LRE_vdsslsgl_52.00.00 new:CISCO575-LRE_vdsslsgl_52.00.00
  Status:Pending
Lo0/12:
  lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 new:CISCO2950-LRE_vdsloctl_02.60.00
  Status:Pending
  rmt curr:CISCO575-LRE_vdsslsgl_52.00.00 new:CISCO575-LRE_vdsslsgl_52.00.00
  Status:Pending
```

```

Lo0/13:
  lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 new:CISCO2950-LRE_vdsloctl_02.60.00
  Status:Pending
  rmt curr:CISCO575-LRE_vdslsngl_52.00.00 new:CISCO575-LRE_vdslsngl_52.00.00
  Status:Pending
Lo0/14:
  lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 new:CISCO2950-LRE_vdsloctl_02.60.00
  Status:Pending
  rmt curr:CISCO575-LRE_vdslsngl_52.00.00 new:CISCO575-LRE_vdslsngl_52.00.00
  Status:Pending
Lo0/15:
  lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 new:CISCO2950-LRE_vdsloctl_02.60.00
  Status:Pending
  rmt curr:CISCO575-LRE_vdslsngl_52.00.00 new:CISCO575-LRE_vdslsngl_52.00.00
  Status:Pending
Lo0/16:
  lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 new:CISCO2950-LRE_vdsloctl_02.60.00
  Status:Pending
  rmt curr:CISCO575-LRE_vdslsngl_52.00.00 new:CISCO575-LRE_vdslsngl_52.00.00
  Status:Pending
Lo0/17:
  lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 new:CISCO2950-LRE_vdsloctl_02.60.00
  Status:Pending
  rmt curr:CISCO575-LRE_vdslsngl_52.00.00 new:CISCO575-LRE_vdslsngl_52.00.00
  Status:Pending
Lo0/18:
  lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 new:CISCO2950-LRE_vdsloctl_02.60.00
  Status:Pending
  rmt curr:CISCO575-LRE_vdslsngl_52.00.00 new:CISCO575-LRE_vdslsngl_52.00.00
  Status:Pending
Lo0/19:
  lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 new:CISCO2950-LRE_vdsloctl_02.60.00
  Status:Pending
  rmt curr:CISCO585-LRE_vdslsngl_52.00.00 new:CISCO585-LRE_vdslsngl_51.00.00
  Status:Pending
  rmt curr:CISCO585-LRE_MC8051appl_00.30.00 new:CISCO585-LRE_MC8051appl_00.30.00
  Status:None
  rmt curr:CISCO585-LRE_MC8051boot_00.30.00 new:CISCO585-LRE_MC8051boot_00.30.00
  Status:None
Lo0/20:
  lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 new:CISCO2950-LRE_vdsloctl_02.60.00
  Status:Pending
  No remote devices on Lo0/20
Lo0/21:
  lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 new:CISCO2950-LRE_vdsloctl_02.60.00
  Status:Pending
  No remote devices on Lo0/21
Lo0/22:
  lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 new:CISCO2950-LRE_vdsloctl_02.60.00
  Status:Pending
  No remote devices on Lo0/22
Lo0/23:
  lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 new:CISCO2950-LRE_vdsloctl_02.60.00
  Status:Pending
  No remote devices on Lo0/23
Lo0/24:
  lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 new:CISCO2950-LRE_vdsloctl_02.60.00
  Status:Pending
  No remote devices on Lo0/24
Switch#

```

■ show lre upgrade status

This example shows the status of an upgrade after data transfer is in progress.

```
Switch# show lre upgrade status

Lo0/1:
  lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 new:CISCO2950-LRE_vdsloctl_02.60.00
  Status:Pending
  rmt curr:CISCO575-LRE_vdslsngl_52.00.00 new:CISCO575-LRE_vdslsngl_52.00.00
  Status:Active
  10 HHMM:0000, Attempt:001

Lo0/2:
  lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 new:CISCO2950-LRE_vdsloctl_02.60.00
  Status:Pending
  rmt curr:CISCO575-LRE_vdslsngl_52.00.00 new:CISCO575-LRE_vdslsngl_52.00.00
  Status:Active
  09 HHMM:0000, Attempt:001

Lo0/3:
  lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 new:CISCO2950-LRE_vdsloctl_02.60.00
  Status:Pending
  rmt curr:CISCO575-LRE_vdslsngl_52.00.00 new:CISCO575-LRE_vdslsngl_52.00.00
  Status:Active
  22 HHMM:0000, Attempt:001

Lo0/4:
  lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 new:CISCO2950-LRE_vdsloctl_02.60.00
  Status:Pending
  rmt curr:CISCO575-LRE_vdslsngl_52.00.00 new:CISCO575-LRE_vdslsngl_52.00.00
  Status:Active
  10 HHMM:0000, Attempt:001

Lo0/5:
  lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 new:CISCO2950-LRE_vdsloctl_02.60.00
  Status:Pending
  rmt curr:CISCO575-LRE_vdslsngl_52.00.00 new:CISCO575-LRE_vdslsngl_52.00.00
  Status:Active
  10 HHMM:0000, Attempt:001

Lo0/6:
  lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 new:CISCO2950-LRE_vdsloctl_02.60.00
  Status:Pending
  rmt curr:CISCO575-LRE_vdslsngl_52.00.00 new:CISCO575-LRE_vdslsngl_52.00.00
  Status:Active
  10 HHMM:0000, Attempt:001

Lo0/7:
  lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 new:CISCO2950-LRE_vdsloctl_02.60.00
  Status:Pending
  rmt curr:CISCO575-LRE_vdslsngl_52.00.00 new:CISCO575-LRE_vdslsngl_52.00.00
  Status:Active
  09 HHMM:0000, Attempt:001

Lo0/8:
  lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 new:CISCO2950-LRE_vdsloctl_02.60.00
  Status:Pending
  rmt curr:CISCO575-LRE_vdslsngl_52.00.00 new:CISCO575-LRE_vdslsngl_52.00.00
  Status:Active
  09 HHMM:0000, Attempt:001

Lo0/9:
  lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 new:CISCO2950-LRE_vdsloctl_02.60.00
  Status:Pending
  No remote devices on Lo0/9

Lo0/10:
  lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 new:CISCO2950-LRE_vdsloctl_02.60.00
  Status:Pending
  rmt curr:CISCO575-LRE_vdslsngl_52.00.00 new:CISCO575-LRE_vdslsngl_52.00.00
  Status:Active
  08 HHMM:0000, Attempt:001

Lo0/11:
  lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 new:CISCO2950-LRE_vdsloctl_02.60.00
```

```

Status:Pending
rmt curr:CISCO575-LRE_vdslsngl_52.00.00 new:CISCO575-LRE_vdslsngl_52.00.00
Status:Active
07 HHMM:0000, Attempt:001
Lo0/12:
lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 new:CISCO2950-LRE_vdsloctl_02.60.00
Status:Pending
rmt curr:CISCO575-LRE_vdslsngl_52.00.00 new:CISCO575-LRE_vdslsngl_52.00.00
Status:Active
06 HHMM:0000, Attempt:003
Lo0/13:
lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 new:CISCO2950-LRE_vdsloctl_02.60.00
Status:Pending
rmt curr:CISCO575-LRE_vdslsngl_52.00.00 new:CISCO575-LRE_vdslsngl_52.00.00
Status:Active
08 HHMM:0000, Attempt:001
Lo0/14:
lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 new:CISCO2950-LRE_vdsloctl_02.60.00
Status:Pending
rmt curr:CISCO575-LRE_vdslsngl_52.00.00 new:CISCO575-LRE_vdslsngl_52.00.00
Status:Active
08 HHMM:0000, Attempt:001
Lo0/15:
lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 new:CISCO2950-LRE_vdsloctl_02.60.00
Status:Pending
rmt curr:CISCO575-LRE_vdslsngl_52.00.00 new:CISCO575-LRE_vdslsngl_52.00.00
Status:Active
08 HHMM:0000, Attempt:001
Lo0/16:
lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 new:CISCO2950-LRE_vdsloctl_02.60.00
Status:Pending
rmt curr:CISCO575-LRE_vdslsngl_52.00.00 new:CISCO575-LRE_vdslsngl_52.00.00
Status:Active
05 HHMM:0000, Attempt:003
Lo0/17:
lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 new:CISCO2950-LRE_vdsloctl_02.60.00
Status:Pending
rmt curr:CISCO575-LRE_vdslsngl_52.00.00 new:CISCO575-LRE_vdslsngl_52.00.00
Status:Active
07 HHMM:0000, Attempt:001
Lo0/18:
lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 new:CISCO2950-LRE_vdsloctl_02.60.00
Status:Pending
rmt curr:CISCO575-LRE_vdslsngl_52.00.00 new:CISCO575-LRE_vdslsngl_52.00.00
Status:Active
07 HHMM:0000, Attempt:001
Lo0/19:
lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 new:CISCO2950-LRE_vdsloctl_02.60.00
Status:Pending
rmt curr:CISCO585-LRE_vdslsngl_52.00.00 new:CISCO585-LRE_vdslsngl_51.00.00
Status:Active
22 HHMM:0000, Attempt:001
rmt curr:CISCO585-LRE_MC8051appl_00.30.00 new:CISCO585-LRE_MC8051appl_00.30.00
Status:None
rmt curr:CISCO585-LRE_MC8051boot_00.30.00 new:CISCO585-LRE_MC8051boot_00.30.00
Status:None
Lo0/20:
lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 new:CISCO2950-LRE_vdsloctl_02.60.00
Status:Pending
No remote devices on Lo0/20
Lo0/21:
lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 new:CISCO2950-LRE_vdsloctl_02.60.00
Status:Pending
No remote devices on Lo0/21

```

■ **show lre upgrade status**

```

Lo0/22:
  lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 new:CISCO2950-LRE_vdsloctl_02.60.00
  Status:Pending
  No remote devices on Lo0/22
Lo0/23:
  lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 new:CISCO2950-LRE_vdsloctl_02.60.00
  Status:Pending
  No remote devices on Lo0/23
Lo0/24:
  lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 new:CISCO2950-LRE_vdsloctl_02.60.00
  Status:Pending
  No remote devices on Lo0/24

```

Related Commands

Command	Description
show lre upgrade binaries	Displays the LRE binary information present on the system Flash memory.
show lre upgrade version	Displays the versions of binaries on local and remote ends on all ports.

show lre upgrade version

Use the **show lre upgrade version** privileged EXEC command to display the version of binaries on local and remote ends of a Long-Reach Ethernet (LRE) link.

show lre upgrade version [| {begin | exclude | include} expression]

Syntax Description	<table border="0"> <tr> <td> begin</td><td>(Optional) Display begins with the line that matches the specified <i>expression</i>.</td></tr> <tr> <td> exclude</td><td>(Optional) Display excludes lines that match the specified <i>expression</i>.</td></tr> <tr> <td> include</td><td>(Optional) Display includes lines that match the specified <i>expression</i>.</td></tr> <tr> <td><i>expression</i></td><td>Expression in the output to use as a reference point.</td></tr> </table>	begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .	exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .	include	(Optional) Display includes lines that match the specified <i>expression</i> .	<i>expression</i>	Expression in the output to use as a reference point.
begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .								
exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .								
include	(Optional) Display includes lines that match the specified <i>expression</i> .								
<i>expression</i>	Expression in the output to use as a reference point.								

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

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.

Usage Guidelines	The show lre upgrade version command displays the LRE binary version for each interface.
-------------------------	---

The command shows local current (lcl curr) and proposed configuration (cfg) for each LRE interface. File names consist of:

- The device family
- The function of the firmware, such as an upgrade for an application, for the bootloader, or for the LRE chipsets of a CPE device
- The firmware version

Examples	This example shows output from the show lre upgrade version command:
-----------------	---

```
Switch# show lre upgrade version

Lo0/1:
  CPE:Family CISCO575-LRE, Model Cisco575-LRE , Rev A0
    lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 cfg:CISCO2950-LRE_vdsloctl_02.60.00
    rmt curr:CISCO575-LRE_vdslsngl_52.00.00 cfg:CISCO575-LRE_vdslsngl_52.00.00
Lo0/2:
  CPE:Family CISCO575-LRE, Model Cisco575-LRE , Rev A0
    lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 cfg:CISCO2950-LRE_vdsloctl_02.60.00
    rmt curr:CISCO575-LRE_vdslsngl_52.00.00 cfg:CISCO575-LRE_vdslsngl_52.00.00
Lo0/3:
  CPE:Family CISCO575-LRE, Model Cisco575-LRE , Rev A0
    lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 cfg:CISCO2950-LRE_vdsloctl_02.60.00
    rmt curr:CISCO575-LRE_vdslsngl_52.00.00 cfg:CISCO575-LRE_vdslsngl_52.00.00
Lo0/4:
  CPE:Family CISCO575-LRE, Model Cisco575-LRE , Rev A0
```

show lre upgrade version

```

lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 cfg:CISCO2950-LRE_vdsloctl_02.60.00
rmt curr:CISCO575-LRE_vdlsngl_52.00.00 cfg:CISCO575-LRE_vdlsngl_52.00.00
Lo0/5:
CPE:Family CISCO575-LRE, Model Cisco575-LRE , Rev A0
lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 cfg:CISCO2950-LRE_vdsloctl_02.60.00
rmt curr:CISCO575-LRE_vdlsngl_52.00.00 cfg:CISCO575-LRE_vdlsngl_52.00.00
Lo0/6:
CPE:Family CISCO575-LRE, Model Cisco575-LRE , Rev A0
lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 cfg:CISCO2950-LRE_vdsloctl_02.60.00
rmt curr:CISCO575-LRE_vdlsngl_52.00.00 cfg:CISCO575-LRE_vdlsngl_52.00.00
Lo0/7:
CPE:Family CISCO575-LRE, Model Cisco575-LRE , Rev A0
lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 cfg:CISCO2950-LRE_vdsloctl_02.60.00
rmt curr:CISCO575-LRE_vdlsngl_52.00.00 cfg:CISCO575-LRE_vdlsngl_52.00.00
Lo0/8:
CPE:Family CISCO575-LRE, Model Cisco575-LRE , Rev A0
lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 cfg:CISCO2950-LRE_vdsloctl_02.60.00
rmt curr:CISCO575-LRE_vdlsngl_52.00.00 cfg:CISCO575-LRE_vdlsngl_52.00.00
Lo0/9:
CPE:Family NONE, Model NONE, Rev NONE
lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 cfg:CISCO2950-LRE_vdsloctl_02.60.00
Lo0/10:
CPE:Family CISCO575-LRE, Model Cisco575-LRE , Rev A0
lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 cfg:CISCO2950-LRE_vdsloctl_02.60.00
rmt curr:CISCO575-LRE_vdlsngl_52.00.00 cfg:CISCO575-LRE_vdlsngl_52.00.00
Lo0/11:
CPE:Family CISCO575-LRE, Model CISCO575-LRE , Rev A0
lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 cfg:CISCO2950-LRE_vdsloctl_02.60.00
rmt curr:CISCO575-LRE_vdlsngl_52.00.00 cfg:CISCO575-LRE_vdlsngl_52.00.00
Lo0/12:
CPE:Family CISCO575-LRE, Model Cisco575-LRE , Rev A0
lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 cfg:CISCO2950-LRE_vdsloctl_02.60.00
rmt curr:CISCO575-LRE_vdlsngl_52.00.00 cfg:CISCO575-LRE_vdlsngl_52.00.00
Lo0/13:
CPE:Family CISCO575-LRE, Model Cisco575-LRE , Rev A0
lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 cfg:CISCO2950-LRE_vdsloctl_02.60.00
rmt curr:CISCO575-LRE_vdlsngl_52.00.00 cfg:CISCO575-LRE_vdlsngl_52.00.00
Lo0/14:
CPE:Family CISCO575-LRE, Model Cisco575-LRE , Rev A0
lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 cfg:CISCO2950-LRE_vdsloctl_02.60.00
rmt curr:CISCO575-LRE_vdlsngl_52.00.00 cfg:CISCO575-LRE_vdlsngl_52.00.00
Lo0/15:
CPE:Family CISCO575-LRE, Model Cisco575-LRE , Rev A0
lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 cfg:CISCO2950-LRE_vdsloctl_02.60.00
rmt curr:CISCO575-LRE_vdlsngl_52.00.00 cfg:CISCO575-LRE_vdlsngl_52.00.00
Lo0/16:
CPE:Family CISCO575-LRE, Model Cisco575-LRE , Rev A0
lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 cfg:CISCO2950-LRE_vdsloctl_02.60.00
rmt curr:CISCO575-LRE_vdlsngl_52.00.00 cfg:CISCO575-LRE_vdlsngl_52.00.00
Lo0/17:
CPE:Family CISCO575-LRE, Model Cisco575-LRE , Rev A0
lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 cfg:CISCO2950-LRE_vdsloctl_02.60.00
rmt curr:CISCO575-LRE_vdlsngl_52.00.00 cfg:CISCO575-LRE_vdlsngl_52.00.00
Lo0/18:
CPE:Family CISCO575-LRE, Model Cisco575-LRE , Rev A0
lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 cfg:CISCO2950-LRE_vdsloctl_02.60.00
rmt curr:CISCO575-LRE_vdlsngl_52.00.00 cfg:CISCO575-LRE_vdlsngl_52.00.00
Lo0/19:
CPE:Family CISCO585-LRE, Model CISCO585-LRE --, Rev A0
lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 cfg:CISCO2950-LRE_vdsloctl_02.60.00
rmt curr:CISCO585-LRE_vdlsngl_51.00.00 cfg:CISCO585-LRE_vdlsngl_51.00.00
rmt curr:CISCO585-LRE_MC8051appl_00.30.00 cfg:CISCO585-LRE_MC8051appl_00.30.00
rmt curr:CISCO585-LRE_MC8051boot_00.30.00 cfg:CISCO585-LRE_MC8051boot_00.30.00
Lo0/20:
CPE:Family NONE, Model NONE, Rev NONE

```

```

lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 cfg:CISCO2950-LRE_vdsloctl_02.60.00
Lo0/21:
CPE:Family NONE, Model NONE, Rev NONE
lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 cfg:CISCO2950-LRE_vdsloctl_02.60.00
Lo0/22:
CPE:Family NONE, Model NONE, Rev NONE
lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 cfg:CISCO2950-LRE_vdsloctl_02.60.00
Lo0/23:
CPE:Family NONE, Model NONE, Rev NONE
lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 cfg:CISCO2950-LRE_vdsloctl_02.60.00
Lo0/24:
CPE:Family NONE, Model NONE, Rev NONE
lcl curr:CISCO2950-LRE_vdsloctl_02.60.00 cfg:CISCO2950-LRE_vdsloctl_02.60.00
Switch#

```

Related Commands

Command	Description
show lre upgrade binaries	Displays the LRE binary information present on the system Flash memory.
show lre upgrade status	Displays the upgrade status on all ports in the switch.

■ **show mac access-group**

show mac access-group

Use the **show mac access-group** user EXEC command to display the MAC access control lists (ACLs) configured for an interface or a switch.

show mac access-group [interface *interface-id*] [| {begin | exclude | include} *expression*]

This command is available only if your switch is running the enhanced software image (EI).

Syntax Description	interface <i>interface-id</i> (Optional) Display the ACLs configured on a specific interface (only available in privileged EXEC mode).
begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .
exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes	User EXEC
----------------------	-----------

Command History	Release	Modification
	12.1(6)EA2	This command was introduced.

Usage Guidelines	Use the show mac access-group command without keywords to display MAC ACLs for all interfaces. Use this command with the interface keyword to display ACLs for a specific interface. Expressions are case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> do not appear, but the lines that contain <i>Output</i> appear.
-------------------------	---

Examples	This is an example of output from the show mac access-group command:
-----------------	---

```
Switch> show mac access-group
Interface FastEthernet0/1:
    Inbound access-list is not set
Interface FastEthernet0/2:
    Inbound access-list is not set
Interface FastEthernet0/3:
    Inbound access-list is not set
Interface FastEthernet0/4:
    Inbound access-list is not set
...
Interface FastEthernet0/47:
    Inbound access-list is not set
Interface FastEthernet0/48:
    Inbound access-list is not set
Interface GigabitEthernet0/1:
    Inbound access-list is not set
```

```
Interface GigabitEthernet0/2:  
  Inbound access-list is 101
```

This is an example of output from the **show mac access-group interface gigabitethernet 0/2** command:

```
Switch# show mac access-group interface gigabitethernet 0/2  
Interface GigabitEthernet0/2:  
  Inbound access-list is 101
```

Related Commands

Command	Description
mac access-group	Applies a MAC ACL to an interface.

■ show mac address-table

show mac address-table

Use the **show mac address-table** user EXEC command to display the MAC address table.

```
show mac address-table [aging-time | count | dynamic | static] [address hw-addr]
[interface interface-id] [vlan vlan-id] [ | {begin | exclude | include} expression]
```



Note

Beginning with Release 12.1(11)EA1, the **show mac address-table** command replaces the **show mac-address-table** command (with the hyphen). The **show mac-address-table** command (with the hyphen) will become obsolete in a future release.

Syntax Description

aging-time	(Optional) Display aging time for dynamic addresses for all VLANs.
count	(Optional) Display the count for different kinds of MAC addresses (only available in privileged EXEC mode).
dynamic	(Optional) Display only the dynamic addresses.
static	(Optional) Display only the static addresses.
address hw-addr	(Optional) Display information for a specific address (only available in privileged EXEC mode).
interface interface-id	(Optional) Display addresses for a specific interface.
vlan vlan-id	(Optional) Display addresses for a specific VLAN. Valid IDs are from 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1001 when the standard software image (SI) is installed. Do not enter leading zeros.
 begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.0(5.2)WC(1)	This command was introduced.
12.1(6)EA2	The show mac-address table secure command was replaced by the show port-security command. The self keyword is not supported in this release or later.
12.1(11)EA1	The show mac-address-table command was replaced by the show mac address-table command.

Usage Guidelines

This command displays the MAC address table for the switch. Specific views can be defined by using the optional keywords and values. If more than one optional keyword is used, all of the conditions must be true in order for that entry to appear.

Expressions are case sensitive. For example, if you enter | **exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show mac address-table** command:

```
Switch> show mac-address-table

Dynamic Addresses Count: 9
Secure Addresses (User-defined) Count: 0
Static Addresses (User-defined) Count: 0
System Self Addresses Count: 41
Total MAC addresses: 50

Non-static Address Table:
Destination Address Address Type VLAN Destination Port
-----  -----
0010.0de0.e289 Dynamic 1 FastEthernet0/1
0010.7b00.1540 Dynamic 2 FastEthernet0/5
0010.7b00.1545 Dynamic 2 FastEthernet0/5
0060.5cf4.0076 Dynamic 1 FastEthernet0/1
0060.5cf4.0077 Dynamic 1 FastEthernet0/1
0060.5cf4.1315 Dynamic 1 FastEthernet0/1
0060.70cb.f301 Dynamic 1 FastEthernet0/1
00e0.1e42.9978 Dynamic 1 FastEthernet0/1
00e0.1e9f.3900 Dynamic 1 FastEthernet0/1
```

This is an example of output from the **show mac address-table static interface fastethernet0/2 vlan 1** command:

```
Switch> show mac address-table static interface fastethernet0/2 vlan 1
vlan   mac address      type      ports
-----+-----+-----+
    1 abcd.2345.0099  static   Fa0/2
    1 abcd.0070.0070  static   Fa0/2
    1 abcd.2345.0099  static   Fa0/2
    1 abcd.2345.0099  static   Fa0/2
    1 00d0.d333.7f34  static   Fa0/2
    1 abcd.2345.0099  static   Fa0/2
    1 0005.6667.0007  static   Fa0/2
```

This is an example of output from the **show mac address-table count vlan 1** command:

```
Switch# show mac address-table count vlan 1
MAC Entries for Vlan 1 :
Dynamic Address Count: 1
Static Address (User-defined) Count: 41
Total MAC Addresses In Use:42
Remaining MAC addresses: 8150
```

This is an example of output from the **show mac address-table aging-time** command:

```
Switch> show mac address-table aging-time
Vlan Aging Time
----- -----
 1    450
 2    300
 3    600
300  450
301  450
```

■ **show mac address-table**

This is an example of output from the **show mac address-table aging-time vlan 1** command:

```
Switch> show mac address-table aging-time vlan 1
Vlan Aging Time
-----
1    450
```

Related Commands

Command	Description
clear mac address-table dynamic	Deletes from the MAC address table a specific dynamic address, all dynamic addresses on a particular interface, or all dynamic addresses on a particular VLAN.

show mac address-table multicast

Use the **show mac address-table multicast** user EXEC command to display the Layer 2 multicast entries for the switch or for the VLAN.

show mac address-table multicast [vlan *vlan-id*] [count] [igmp-snooping | user] [| {begin | exclude | include} *expression*]


Note

Beginning with Release 12.1(11)EA1, the **show mac address-table multicast** command replaces the **show mac-address-table multicast** command (with the hyphen). The **show mac-address-table multicast** command (with the hyphen) will become obsolete in a future release.

Syntax Description

vlan <i>vlan-id</i>	(Optional) Specify a VLAN; valid values are 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1005 when the standard software image (SI) is installed. Do not enter leading zeros. (This keyword is only available in privileged EXEC mode.)
count	(Optional) Display total number of entries for the specified criteria instead of the actual entries (only available in privileged EXEC mode).
igmp-snooping	(Optional) Display only entries learned through Internet Group Management Protocol (IGMP) snooping (only available in privileged EXEC mode).
user	(Optional) Display only the user-configured multicast entries (only available in privileged EXEC mode).
 begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Defaults

This command has no default setting.

Command Modes

User EXEC

Command History

Release	Modification
12.0(5.2)WC(1)	This command was introduced.
12.1(11)EA1	The show mac-address-table multicast command was replaced by the show mac address-table multicast command.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

■ **show mac address-table multicast**

Examples

This is an example of output from the **show mac address-table multicast vlan 1** command:

```
Switch# show mac address-table multicast vlan 1

Vlan      Mac Address      Type      Ports
----      -----          ----      -----
  1      0100.5e00.0128    IGMP      Fa0/11
  1      0100.5e01.1111    USER      Fa0/5, Fa0/6, Fa0/7, Fa0/11
```

This is an example of output from the **show mac address-table multicast count** command:

```
Switch# show mac address-table multicast count
Multicast Mac Entries for all vlans: 10
```

This is an example of output from the **show mac address-table multicast vlan 1 count** command:

```
Switch# show mac address-table multicast vlan 1 count
Multicast Mac Entries for vlan 1: 2
```

This is an example of output from the **show mac address-table multicast vlan 1 user** command:

```
Switch# show mac address-table multicast vlan 1 user
vlan      mac address      type      ports
----      -----          ----      -----
  1      0100.5e02.0203    user      Fa0/1,Fa0/2,Fa0/4
```

This is an example of output from the **show mac address-table multicast vlan 1 igmp-snooping count** command:

```
Switch# show mac address-table multicast vlan 1 igmp-snooping count
Number of igmp-snooping programmed entries : 1
```

show mac address-table notification

Use the **show mac address-table notification** user EXEC command to display parameters for the MAC notification feature.

show mac address-table notification [interface *interface-id*] [| {begin | exclude | include} *expression*]


Note

Beginning with Release 12.1(11)EA1, the **show mac address-table notification** command replaces the **show mac-address-table notification** command (with the hyphen). The **show mac-address-table notification** command (with the hyphen) will become obsolete in a future release.

Syntax Description

interface <i>interface-id</i>	(Optional) Specify an interface.
 begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Defaults

This command has no default setting.

Command Modes

User EXEC

Command History

Release	Modification
12.1(6)EA2	This command was introduced.
12.1(11)EA1	The show mac-address-table notification command was replaced by the show mac address-table notification command.

Usage Guidelines

Use the **show mac address-table notification** command without keywords to display parameters for all interfaces.

Use this command with the **interface** keyword to display parameters for a specific interface.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show mac address-table notification** command:

```
Switch> show mac address-table notification
MAC Notification Feature is Disabled on the switch
```

■ **show mac address-table notification**

Related Commands	Command	Description
	clear mac address-table notification	Clears the MAC address notification global counters.
	mac address-table notification	Enables the MAC notification feature.
	snmp trap mac-notification	Enables MAC-notification traps on a port.

show mls masks

Use the **show mls masks** user EXEC command to display the details of the Access Control Parameters (ACPs) used for quality of service (QoS) and security access control lists (ACLs).

show mls masks [qos | security] [| {begin | exclude | include} expression]

This command is available only if your switch is running the enhanced software image (EI).

Syntax Description

qos	(Optional) Display ACPs used for QoS ACLs.
security	(Optional) Display ACPs used for security ACLs.
 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
expression	Expression in the output to use as a reference point.



ACPs are called masks in the command-line interface (CLI) commands and output.

Command Modes

User EXEC

Command History

Release	Modification
12.1(6)EA2	This command was introduced.

Usage Guidelines

Use the **show mls mask** command without keywords to display all ACPs configured on the switch.

Use this command with the **qos** keyword to display the ACPs used for QoS ACLs.

Use this command with the **security** keyword to display the ACPs used for security ACLs.



You can configure up to four ACPs (QoS and security) on a switch.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

show mls masks**Examples**

This is an example of output from the **show mls masks** command:

```
Switch> show mls masks

Mask1
    Type : qos
    Fields : ip-sa(0.0.0.255), ip-da(host), dest-port, ip-dscp
    Policymap: pmap1
        Interfaces: Fa0/9, Gi0/1
    Policymap: pmap2
        Interfaces: Fa0/1, Fa0/5, Fa0/13

Mask2
    Type : security
    Fields : mac-sa (host), ethertype, ip-dscp
    Access-group: 3
        Interfaces: Fa0/2, Fa0/6
    Access-group: macag1
        Interfaces: Fa0/16
```

In this example, *Mask 1* is a QoS ACP consisting an IP source address (with wildcard bits 0.0.0.255), an IP destination address, and Layer 4 destination port fields. This ACP is used by the QoS policy maps *pmap1* and *pmap2*.

Mask 2 is a security ACP consisting of a MAC source address and ethertype fields. This ACP is used by the MAC security access groups *3* and *macag1*.

Related Commands

Command	Description
ip access-group	Applies an IP ACL to an interface.
mac access-group	Applies a named extended MAC ACL to an interface.
policy-map	Creates or modifies a policy map that can be attached to multiple interfaces and enters policy-map configuration mode.

show mls qos interface

Use the **show mls qos interface** user EXEC command to display quality of service (QoS) information at the interface level.

show mls qos interface [interface-id] [policers] [| {begin | exclude | include} expression]

Syntax Description

<i>interface-id</i>	(Optional) Display QoS information for the specified interface.
policers	(Optional) Display all the policers configured on the interface, their settings, and the number of policers unassigned (available only when the switch is running the enhanced software image (EI)).
 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.



Though visible in the command-line help strings, the **vlan *vlan-id*** option is not supported.

Command Modes

User EXEC

Command History

Release	Modification
12.1(6)EA2	This command was introduced.

Usage Guidelines

Though visible in the command-line help string, the **policers** keyword is available only when your switch is running the EI.

Use the **show mls qos interface** command without keywords to display parameters for all interfaces.

Use the **show mls qos interface *interface-id*** command to display the parameters for a specific interface.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show mls qos interface** command when the Cisco IP Phone is a trusted device:

```
Switch> show mls qos interface fastethernet0/1
FastEthernet0/1
trust state:trust cos
trust mode:trust cos
COS override:dis
default COS:0
pass-through:none
trust device:cisco-phone
```

■ **show mls qos interface**

This is an example of output from the **show mls qos interface** command when pass-through mode is configured on an interface:

```
Switch> show mls qos interface fastethernet0/2
FastEthernet0/2
trust state:not trusted
trust mode:not trusted
COS override:dis
default COS:0
pass-through:dscp
```

Related Commands

Command	Description
mls qos cos	Defines the default class of service (CoS) value of a port or assigns the default CoS to all incoming packets on the port.
mls qos map	Defines the class of service (CoS)-to-Differentiated Services Code Point (DSCP) map and DSCP-to-CoS map.
mls qos trust	Configures the port trust state. Ingress traffic can be trusted and classification is performed by examining the CoS or DSCP value.

show mls qos maps

Use the **show mls qos maps** user EXEC command to display quality of service (QoS) mapping information. Maps are used to generate an internal Differentiated Services Code Point (DSCP) value, which represents the priority of the traffic.

show mls qos maps [cos-dscp | dscp-cos] [| {begin | exclude | include} expression]

This command is available only if your switch is running the enhanced software image (EI).

Syntax Description	cos-dscp (Optional) Display class of service (CoS)-to-DSCP map.
dscp-cos	(Optional) Display DSCP-to-CoS map.
 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
expression	Expression in the output to use as a reference point.

Command Modes	User EXEC
----------------------	-----------

Command History	Release	Modification
	12.1(6)EA2	This command was introduced.

Usage Guidelines	<p>Use the show mls qos maps command without keywords to display all maps.</p> <p>Use this command with the cos-dscp keyword to display the CoS-to-DSCP map.</p> <p>Use this command with the dscp-cos keyword to display the DSCP-to-CoS map.</p> <p>Expressions are case sensitive. For example, if you enter exclude output, the lines that contain <i>output</i> do not appear, but the lines that contain <i>Output</i> appear.</p>
-------------------------	--

Examples	This is an example of output from the show mls qos maps cos-dscp command:
-----------------	--

```
Switch> show mls qos maps cos-dscp

Cos-dscp map:
  cos:  0  1  2  3  4  5  6  7
  -----
  dscp:  8  8  8  8 24 32 56 56
```

■ **show mls qos maps**

This is an example of output from the **show mls qos maps dscp-cos** command:

```
Switch> show mls qos maps dscp-cos

Dscp-cos map:
dscp: 0 8 10 16 18 24 26 32 34 40 46 48 56
-----
cos: 0 1 1 1 2 2 3 3 4 4 5 6 7
```

This is an example of output from the **show mls qos maps** command:

```
Switch> show mls qos maps

Dscp-cos map:
dscp: 0 8 10 16 18 24 26 32 34 40 46 48 56
-----
cos: 0 1 1 2 2 3 7 4 4 5 5 7 7

Cos-dscp map:
cos: 0 1 2 3 4 5 6 7
-----
dscp: 0 8 16 24 32 40 48 56
```

Related Commands	Command	Description
	mls qos map	Defines the CoS-to-DSCP map and DSCP-to-CoS map.

show monitor

Use the **show monitor** user EXEC command to display Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) session information.

show monitor [session {session_number | all | local | remote}] [| {begin | exclude | include} expression]

Syntax Description	<table border="0"> <tr> <td>session session_number</td><td>(Optional) Specify the session number identified with this SPAN or RSPAN session.</td></tr> <tr> <td>all</td><td>Specify all sessions.</td></tr> <tr> <td>local</td><td>Specify local sessions.</td></tr> <tr> <td>remote</td><td>Specify remote sessions.</td></tr> <tr> <td> begin</td><td>(Optional) Display begins with the line that matches the <i>expression</i>.</td></tr> <tr> <td> exclude</td><td>(Optional) Display excludes lines that match the <i>expression</i>.</td></tr> <tr> <td> include</td><td>(Optional) Display includes lines that match the specified <i>expression</i>.</td></tr> <tr> <td>expression</td><td>Expression in the output to use as a reference point.</td></tr> </table>	session session_number	(Optional) Specify the session number identified with this SPAN or RSPAN session.	all	Specify all sessions.	local	Specify local sessions.	remote	Specify remote sessions.	 begin	(Optional) Display begins with the line that matches the <i>expression</i> .	 exclude	(Optional) Display excludes lines that match the <i>expression</i> .	 include	(Optional) Display includes lines that match the specified <i>expression</i> .	expression	Expression in the output to use as a reference point.
session session_number	(Optional) Specify the session number identified with this SPAN or RSPAN session.																
all	Specify all sessions.																
local	Specify local sessions.																
remote	Specify remote sessions.																
 begin	(Optional) Display begins with the line that matches the <i>expression</i> .																
 exclude	(Optional) Display excludes lines that match the <i>expression</i> .																
 include	(Optional) Display includes lines that match the specified <i>expression</i> .																
expression	Expression in the output to use as a reference point.																

Command Modes	User EXEC
----------------------	-----------

Command History	Release	Modification
	12.1(6)EA1	This command was introduced.
	12.1(11)EA1	The all , local , and remote keywords were added.

Usage Guidelines	Expressions are case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> are not displayed, but the lines that contain <i>Output</i> are displayed.
-------------------------	---

■ show monitor**Examples**

This is an example of output for the **show monitor** privileged EXEC command for RSPAN source session 1:

```
Switch# show monitor session 1
Session 1
-----
Type: Remote Source Session
Source Ports:
    RX Only:      Fa0/3
    TX Only:      None
    Both:        None
Source VLANs:
    RX Only:      None
    TX Only:      None
    Both:        None
Source RSPAN VLAN: None
Destination Ports: None
    Encapsulation: Native
Reflector Port: Fa0/4
Filter VLANs:      None
Dest RSPAN VLAN: 901
```

Related Commands

Command	Description
monitor session	Enables SPAN and RSPAN monitoring on a port and configures a port as a source or destination port.

show mvr

Use the **show mvr** privileged EXEC command without keywords to display the Multicast VLAN Registration (MVR) global parameter values, including whether or not MVR is enabled, the MVR multicast VLAN, the maximum query response time, the number of multicast groups, and the MVR mode (dynamic or compatible).

show mvr [| {begin | exclude | include} expression]

Syntax Description	<table border="0"> <tr> <td> begin</td><td>(Optional) Display begins with the line that matches the <i>expression</i>.</td></tr> <tr> <td> exclude</td><td>(Optional) Display excludes lines that match the <i>expression</i>.</td></tr> <tr> <td> include</td><td>(Optional) Display includes lines that match the specified <i>expression</i>.</td></tr> <tr> <td><i>expression</i></td><td>Expression in the output to use as a reference point.</td></tr> </table>	begin	(Optional) Display begins with the line that matches the <i>expression</i> .	exclude	(Optional) Display excludes lines that match the <i>expression</i> .	include	(Optional) Display includes lines that match the specified <i>expression</i> .	<i>expression</i>	Expression in the output to use as a reference point.
begin	(Optional) Display begins with the line that matches the <i>expression</i> .								
exclude	(Optional) Display excludes lines that match the <i>expression</i> .								
include	(Optional) Display includes lines that match the specified <i>expression</i> .								
<i>expression</i>	Expression in the output to use as a reference point.								

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

Command History	Release	Modification
	12.1(6)EA2	This command was introduced.

Usage Guidelines	Expressions are case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> do not appear, but the lines that contain <i>Output</i> appear.
-------------------------	--

Examples	This is an example of output from the show mvr command:
	<pre>Switch# show mvr MVR Running: TRUE MVR multicast vlan: 1 MVR Max Multicast Groups: 256 MVR Current multicast groups: 256 MVR Global query response time: 5 (tenths of sec) MVR Mode: compatible</pre>

In the previous example, the maximum number of multicast groups is 256. The MVR mode is either compatible (for interoperability with Catalyst 2900 XL and Catalyst 3500 XL switches) or dynamic (where operation is consistent with Internet Group Management Protocol [IGMP] snooping operation, and dynamic MVR membership on source ports is supported).

■ **show mvr**

Related Commands	Command	Description
	mvr	Enables and configures multicast VLAN registration on the switch.
	mvr type	Configures an MVR port as a receiver or a source port.
	show mvr interface	Displays the configured MVR interfaces, status of the specified interface, or all multicast groups to which the interface belongs.
	show mvr members	Displays all ports that are members of an MVR multicast group.

show mvr interface

Use the **show mvr interface** privileged EXEC command without keywords to display the Multicast VLAN Registration (MVR) receiver and source ports. Use the command with keywords to display MVR parameters for a specific receiver port.

```
show mvr interface [interface-id [members [vlan vlan-id]]] [ | {begin | exclude | include} expression]
```

Syntax Description	<table border="0"> <tr> <td><i>interface-id</i></td><td>(Optional) Display MVR type, status, and Immediate-Leave setting for the interface.</td></tr> <tr> <td>members</td><td>(Optional) Display all MVR groups to which the specified interface belongs.</td></tr> <tr> <td>vlan <i>vlan-id</i></td><td>(Optional) Display the VLAN to which the receiver port belongs.</td></tr> <tr> <td> begin</td><td>(Optional) Display begins with the line that matches the <i>expression</i>.</td></tr> <tr> <td> exclude</td><td>(Optional) Display excludes lines that match the <i>expression</i>.</td></tr> <tr> <td> include</td><td>(Optional) Display includes lines that match the specified <i>expression</i>.</td></tr> <tr> <td><i>expression</i></td><td>Expression in the output to use as a reference point.</td></tr> </table>	<i>interface-id</i>	(Optional) Display MVR type, status, and Immediate-Leave setting for the interface.	members	(Optional) Display all MVR groups to which the specified interface belongs.	vlan <i>vlan-id</i>	(Optional) Display the VLAN to which the receiver port belongs.	 begin	(Optional) Display begins with the line that matches the <i>expression</i> .	 exclude	(Optional) Display excludes lines that match the <i>expression</i> .	 include	(Optional) Display includes lines that match the specified <i>expression</i> .	<i>expression</i>	Expression in the output to use as a reference point.
<i>interface-id</i>	(Optional) Display MVR type, status, and Immediate-Leave setting for the interface.														
members	(Optional) Display all MVR groups to which the specified interface belongs.														
vlan <i>vlan-id</i>	(Optional) Display the VLAN to which the receiver port belongs.														
 begin	(Optional) Display begins with the line that matches the <i>expression</i> .														
 exclude	(Optional) Display excludes lines that match the <i>expression</i> .														
 include	(Optional) Display includes lines that match the specified <i>expression</i> .														
<i>expression</i>	Expression in the output to use as a reference point.														

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

Command History	Release	Modification
	12.1(6)EA2	This command was introduced.

Usage Guidelines	If the entered port identification is a non-MVR port or a source port, the command returns an error message. For receiver ports, it displays the port type, per port status, and Immediate-Leave setting. Expressions are case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> do not appear, but the lines that contain <i>Output</i> appear.
-------------------------	--

Examples	This is an example of output from the show mvr interface command:
-----------------	--

```
Switch# show mvr interface
Port      Type          Status        Immediate Leave
----      ----          -----        -----
Gi0/1    SOURCE        ACTIVE/UP     DISABLED
Gi0/2    RECEIVER      ACTIVE/DOWN  DISABLED
```

In the previous example, Status is defined as:

- Active means the port is part of a VLAN.
- Up/Down means that the port is forwarding/nonforwarding.
- Inactive means that the port is not part of any VLAN.

■ show mvr interface

This is an example of output from the **show mvr interface gigabitethernet0/2** command:

```
Switch# show mvr interface gigabitethernet0/2
Type: RECEIVER Status: ACTIVE Immediate Leave: DISABLED
```

This is an example of output from the **show mvr interface fastethernet0/6 member** command:

```
Switch# show mvr interface fastethernet0/6 member
239.255.0.0    DYNAMIC ACTIVE
239.255.0.1    DYNAMIC ACTIVE
239.255.0.2    DYNAMIC ACTIVE
239.255.0.3    DYNAMIC ACTIVE
239.255.0.4    DYNAMIC ACTIVE
239.255.0.5    DYNAMIC ACTIVE
239.255.0.6    DYNAMIC ACTIVE
239.255.0.7    DYNAMIC ACTIVE
239.255.0.8    DYNAMIC ACTIVE
239.255.0.9    DYNAMIC ACTIVE
```

Related Commands	Command	Description
	mvr	Enables and configures multicast VLAN registration on the switch.
	mvr type	Configures an MVR port as a receiver or a source port.
	show mvr	Displays the global MVR configuration on the switch.
	show mvr members	Displays all receiver ports that are members of an MVR multicast group.

show mvr members

Use the **show mvr members** privileged EXEC command to display all receiver ports that are members of an IP multicast group.

show mvr members [ip-address] [| {begin | exclude | include} expression]

Syntax Description	<i>ip-address</i>	(Optional) The IP multicast address. If the address is entered, all receiver ports that are members of the multicast group appear. If no address is entered, all members of all Multicast VLAN Registration (MVR) groups are listed. If a group has no members, the group is listed as <i>Inactive</i> .
	begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	include	(Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.

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

Command History	Release	Modification
	12.1(6)EA2	This command was introduced.

Usage Guidelines	The show mvr members command only applies to receiver ports. All source ports are members of all multicast groups.
-------------------------	---

Expressions are case sensitive. For example, if you enter | **exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples	This is an example of output from the show mvr members command:
-----------------	--

```
Switch# show mvr members
MVR Group IP      Status        Members
-----
239.255.0.1      ACTIVE        Gi0/1(d), Gi0/2(s)
239.255.0.2      INACTIVE     None
239.255.0.3      INACTIVE     None
239.255.0.4      INACTIVE     None
239.255.0.5      INACTIVE     None
239.255.0.6      INACTIVE     None
239.255.0.7      INACTIVE     None
239.255.0.8      INACTIVE     None
239.255.0.9      INACTIVE     None
239.255.0.10     INACTIVE     None
<output truncated>
239.255.0.255    INACTIVE     None
239.255.1.0      INACTIVE     None
```

■ show mvr members

This is an example of output from the **show mvr members 239.255.0.2** command. It shows how to view the members of the IP multicast group 239.255.0.2.

```
Switch# show mvr member 239.255.0.2
239.255.0.2      ACTIVE          Gi0/1(d), Gi0/2(d)
```

Related Commands	Command	Description
	mvr	Enables and configures multicast VLAN registration on the switch.
	mvr type	Configures an MVR port as a receiver or a source port.
	show mvr	Displays the global MVR configuration on the switch.
	show mvr interface	Displays the configured MVR interfaces, status of the specified interface, or all multicast groups to which the interface belongs.

show pagp

Use the **show pagp** user EXEC command to display Port Aggregation Protocol (PAgP) channel-group information.

```
show pagp [channel-group-number] {counters | internal | neighbor} [ | {begin | exclude | include} expression]
```

Syntax Description	
channel-group-number	(Optional) Number of the channel group. Valid numbers range from 1 to 6.
counters	Display traffic information.
internal	Display internal information.
neighbor	Display neighbor information.
 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
expression	Expression in the output to use as a reference point.

Command Modes	User EXEC
----------------------	-----------

Command History	Release	Modification
	12.1(6)EA2	This command was introduced.

Usage Guidelines	You can enter any show pagp command to display the active port channel information. To display the nonactive information, enter the show pagp command with a group number. Expressions are case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> do not appear, but the lines that contain <i>Output</i> appear.
-------------------------	--

Examples	This is an example of output from the show pagp 1 counters command:
	<pre>Switch> show pagp 1 counters Information Flush Port Sent Recv Sent Recv ----- Channel group: 1 Gi0/1 45 42 0 0 Gi0/2 45 41 0 0</pre>

■ show pagp

This is an example of output from the **show pagp 1 internal** command:

```
Switch> show pagp 1 internal
Flags: S - Device is sending Slow hello. C - Device is in Consistent state.
      A - Device is in Auto mode.
Timers: H - Hello timer is running.          Q - Quit timer is running.
        S - Switching timer is running.       I - Interface timer is running.

Channel group 1
               Hello    Partner   PAgP     Learning   Group
Port   Flags State Timers Interval Count Priority Method Ifindex
Gi0/1  SC    U6/S7  H       30s      1        128      Any     16
Gi0/2  SC    U6/S7  H       30s      1        128      Any     16
```

This is an example of output from the **show pagp 1 neighbor** command:

```
Switch> show pagp 1 neighbor
Flags: S - Device is sending Slow hello. C - Device is in Consistent state.
      A - Device is in Auto mode.          P - Device learns on physical port.

Channel group 1 neighbors
      Partner           Partner           Partner           Partner Group
  Port   Name            Device ID        Port      Age  Flags Cap.
  Gi0/1  device-p2      0002.4b29.4600  Gi0/1    9s  SC   10001
  Gi0/2  device-p2      0002.4b29.4600  Gi0/2    24s SC   10001
```

Related Commands

Command	Description
clear pagp	Clears PAgP channel-group information.
pagp learn-method	Sets the source-address learning method of incoming packets received from an EtherChannel port.

show policy-map

Use the **show policy-map** user EXEC command to display quality of service (QoS) policy maps, which define classification criteria for incoming traffic. Policy maps can include policers that specify the bandwidth limitations and the action to take if the limits are exceeded.

show policy-map [policy-map-name [class class-name]] [| {begin | exclude | include} expression]

This command is available only if your switch is running the enhanced software image (EI).

Syntax Description

<i>policy-map-name</i>	(Optional) Display the specified policy-map name.
class <i>class-name</i>	(Optional) Display QoS policy actions for a individual class.
 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

	Release	Modification
	12.1(6)EA2	This command was introduced.

Usage Guidelines

Use the **show policy-map** command without keywords to display all policy maps configured on the switch.



In a policy map, the class named *class-default* is not supported. The switch does not filter traffic based on the policy map defined by the **class class-default** policy-map configuration command.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show policy-map** command:

```
Switch> show policy-map
Policy Map bumbum
    Description: this is a description.

Policy Map wizard_policy3
    class wizard_1-1-1-2
        set ip dscp 34
```

■ show policy-map

```

Policy Map test

Policy Map policytest
  class classtest
    set ip dscp 20
    police 10000000 8192 exceed-action drop

```

This is an example of output from the **show policy-map policytest** command:

```

Switch> show policy-map policytest
Policy Map policytest
  class classtest
    set ip dscp 20
    police 10000000 8192 exceed-action drop

```

This is an example of output from the **show policy-map policytest class classtest** command:

```

Switch> show policy-map policytest class classtest
  set ip dscp 20
  police 10000000 8192 exceed-action drop

```

Related Commands

Command	Description
policy-map	Creates or modifies a policy map that can be attached to multiple interfaces to specify a service policy.

show port-security

Use the **show port-security** privileged EXEC command to display the port security settings defined for an interface or for the switch.

show port-security [interface *interface-id*] [address] [| {begin | exclude | include} *expression*]

Syntax Description	interface <i>interface-id</i> (Optional) Display the port security settings for the specified interface.
address	(Optional) Display all the secure addresses on all ports.
 begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(6)EA2	This command was introduced. It replaced the show port security and show mac-address-table secure commands.

Usage Guidelines If you enter this command without keywords, the output includes the administrative and the operational status of all secure ports on the switch.

If you enter an *interface-id*, the **show port-security** command displays port security settings for the interface.

If you enter the **address** keyword, the **show port-security address** command displays the secure MAC addresses for all interfaces and the aging information for each secure address.

If you enter an *interface-id* and the **address** keyword, the **show port-security interface *interface-id* address** command displays all the MAC addresses for the interface with aging information for each secure address. You can also use this command to display all the MAC addresses for an interface even if you have not enabled port security on it.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

■ show port-security**Examples**

This is an example of output from the **show port-security** command:

```
Switch# show port-security
Secure Port      MaxSecureAddr  CurrentAddr  SecurityViolation  Security
Action
          (Count)        (Count)        (Count)
-----
---  

Fa0/1           11             11            0               Shutdown  

Fa0/5           15             5              0               Restrict  

Fa0/11          5              4              0               Protect  

-----  

---  

Total Addresses in System :21  

Max Addresses limit in System :1024
```

This is an example of output from the **show port-security interface fastethernet0/2** command:

```
Switch# show port-security interface fastethernet0/2
Port Security :Enabled
Port status :SecureUp
Violation mode :Shutdown
Maximum MAC Addresses :11
Total MAC Addresses :11
Configured MAC Addresses :3
Aging time :20 mins
Aging type :Inactivity
SecureStatic address aging :Enabled
Security Violation count :0
```

This is an example of output from the **show port-security address** command:

```
Switch# show port-security address

Secure Mac Address Table
-----
Vlan   Mac Address     Type          Ports      Remaining Age
                                         (mins)
-----  

1      0001.0001.0001  SecureDynamic  Fa0/1      15 (I)  

1      0001.0001.0002  SecureDynamic  Fa0/1      15 (I)  

1      0001.0001.1111  SecureConfigured  Fa0/1      16 (I)  

1      0001.0001.1112  SecureConfigured  Fa0/1      -  

1      0001.0001.1113  SecureConfigured  Fa0/1      -  

1      0005.0005.0001  SecureConfigured  Fa0/5      23  

1      0005.0005.0002  SecureConfigured  Fa0/5      23  

1      0005.0005.0003  SecureConfigured  Fa0/5      23  

1      0011.0011.0001  SecureConfigured  Fa0/11     25 (I)  

1      0011.0011.0002  SecureConfigured  Fa0/11     25 (I)  

-----  

Total Addresses in System :10
Max Addresses limit in System :1024
```

This is an example of output from the **show port-security interface fastethernet0/5 address** command:

```
Switch# show port-security interface fastethernet0/5 address
Secure Mac Address Table
-----
Vlan    Mac Address      Type          Ports      Remaining Age
                                         (mins)
-----
1      0005.0005.0001    SecureConfigured  Fa0/5     19 (I)
1      0005.0005.0002    SecureConfigured  Fa0/5     19 (I)
1      0005.0005.0003    SecureConfigured  Fa0/5     19 (I)
-----
Total Addresses:3
```

Related Commands

Command	Description
switchport port-security	Enables port security on a port, restricts the use of the port to a user-defined group of stations, and configures secure MAC addresses.

show remote lre

show remote lre

Use the **show remote lre** privileged exec command to display the switch registers on a customer premises equipment (CPE) device connected on an Long-Reach Ethernet (LRE) link.

```
show remote lre interface-id switch address length value [ | {begin | exclude | include} expression]
```

Syntax Description	
<i>interface-id</i>	ID of the LRE port.
<i>address</i>	Register address. Valid values are between 0 and 65535.
<i>value</i>	The number of bytes being read.
 begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Defaults A default is not defined.

Command Modes Privileged Exec

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.

Usage Guidelines


Caution

Use this command only under the direction of a technical support representative. Setting a CPE device switch address while the switch is functioning in a network can disrupt network operation. Only technical personnel who have access to source code and detailed memory maps can interpret the data displayed by this command.

This command is supported when the interface is connected to a Cisco 585 LRE CPE. This operation can fail if the LRE link is not stable.

Examples

No examples are provided because this command needs to be run with information from technical support personnel who have access to source code and detailed memory maps.

Related Commands	Command	Description
	show access-lists	Configures a switch register on a CPE device connected through an LRE link.

show rps

show rps

Use the **show rps** privileged EXEC command to display the status of the Cisco Redundant Power System (RPS).

show rps [| {begin | exclude | include} expression]

Syntax Description	<table border="0"> <tr> <td> begin</td><td>(Optional) Display begins with the line that matches the specified <i>expression</i>.</td></tr> <tr> <td> exclude</td><td>(Optional) Display excludes lines that match the specified <i>expression</i>.</td></tr> <tr> <td> include</td><td>(Optional) Display includes lines that match the specified <i>expression</i>.</td></tr> <tr> <td><i>expression</i></td><td>Expression in the output to use as a reference point.</td></tr> </table>	begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .	exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .	include	(Optional) Display includes lines that match the specified <i>expression</i> .	<i>expression</i>	Expression in the output to use as a reference point.
begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .								
exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .								
include	(Optional) Display includes lines that match the specified <i>expression</i> .								
<i>expression</i>	Expression in the output to use as a reference point.								

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

Command History	Release	Modification
	12.0(5.2)WC(1)	This command was introduced.

Usage Guidelines	Expressions are case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> do not appear, but the lines that contain <i>Output</i> appear.
-------------------------	--

Examples	This is an example of output from the show rps command. Table 2-16 describes the possible output.
-----------------	--

```
Switch# show rps
GREEN
```

Table 2-16 show rps Output Description

Display	Description
BLACK	The RPS is off or not properly connected.
GREEN	The RPS is connected and ready to provide back-up power, if required.
ALT_GREEN_BLACK	The RPS is connected but is unavailable because it is providing power to another device (redundancy has been allocated to a neighboring device).

Table 2-16 show rps Output Description (continued)

Display	Description
ALT_AMBER_BLACK	The internal power supply in the switch has failed, and the RPS is providing power to the switch (redundancy has been allocated to this device).
AMBER	<p>The RPS is in standby mode, or the RPS has detected a failure.</p> <p>Press the Standby/Active button on the RPS to put the RPS in active mode. If the RPS LED on the switch remains amber, the RPS has detected a failure.</p> <p>If the failure is minor, the RPS might be in any of the previously described modes. If the failure is critical, the RPS will be down.</p> <p>RPS failures include these modes:</p> <ul style="list-style-type: none"> • The RPS +12V or -48V voltages exceed the specified thresholds. • The RPS has a fan failure. • The RPS detects excessive temperature. • The RPS has a faulty connection to the switch.

 show running-config vlan

show running-config vlan

Use the **show running-config vlan** privileged EXEC command to display all or a range of VLAN-related configurations on the switch.

show running-config vlan [vlan-ids] [| {begin | exclude | include} expression]

Syntax Description	<i>vlan-ids</i> (Optional) Display configuration information for a single VLAN identified by VLAN ID number or a range of VLANs separated by a hyphen. For <i>vlan-id</i> , the range is 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1005 when the standard software image (SI) is installed. Do not enter leading zeros. <i> begin</i> (Optional) Display begins with the line that matches the <i>expression</i> . <i> exclude</i> (Optional) Display excludes lines that match the <i>expression</i> . <i> include</i> (Optional) Display includes lines that match the specified <i>expression</i> . <i>expression</i> Expression in the output to use as a reference point.
--------------------	---

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

Command History	Release	Modification
	12.1(9)EA1	This command was introduced.

Usage Guidelines	Expressions are case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> are not displayed, but the lines that contain <i>Output</i> are displayed.
------------------	---

Examples	This is an example of output from the show running-config vlan command:
----------	--

```

Switch# show running-config vlan 900-2005
Building configuration...

Current configuration:
!
vlan 907
!
vlan 920
!
vlan 1025
!
vlan 2000
!
vlan 2001
end
  
```

Related Commands	Command	Description
	show running-config vlan	Displays the running configuration on the switch. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 > Cisco IOS File Management Commands > Configuration File Commands .
	vlan (global configuration)	Enters config-vlan mode for creating and editing VLANs. When VLAN Trunking Protocol (VTP) mode is transparent, you can use this mode to create extended-range VLANs (VLAN IDs greater than 1005).
	vlan database	Enters VLAN configuration mode for creating and editing normal-range VLANs.

■ **show spanning-tree**

show spanning-tree

Use the **show spanning-tree** user EXEC command to display spanning-tree state information.

```
show spanning-tree [active [detail] | backbonefast | blockedports | bridge | detail [active] |
    inconsistentports | interface interface-id | mst | pathcost method | root | summary [totals] |
    uplinkfast | vlan vlan-id] [ | {begin | exclude | include} expression]

show spanning-tree vlan vlan-id [active [detail] | blockedports | bridge | detail [active] |
    inconsistentports | interface interface-id | root | summary] [ | {begin | exclude | include} expression]

show spanning-tree {vlan vlan-id} bridge [address | detail | forward-time | hello-time | id |
    max-age | priority [system-id] | protocol] [ | {begin | exclude | include} expression]

show spanning-tree {vlan vlan-id} root [address | cost | detail | forward-time | hello-time | id |
    max-age | port | priority [system-id] [ | {begin | exclude | include} expression]

show spanning-tree interface interface-id [active [detail] | cost | detail [active] | inconsistency |
    portfast | priority | rootcost | state] [ | {begin | exclude | include} expression]

show spanning-tree mst [configuration | instance-id] [detail | interface interface-id [detail]] |
    [ | {begin | exclude | include} expression]
```

Syntax Description	
active [detail]	(Optional) Display spanning-tree information only on active interfaces (only available in privileged EXEC mode).
backbonefast	(Optional) Display spanning-tree BackboneFast status (only available in privileged EXEC mode).
blockedports	(Optional) Display blocked port information (only available in privileged EXEC mode).
bridge [address detail forward-time hello-time id max-age priority [system-id] protocol]	(Optional) Display status and configuration of this switch (only available in privileged EXEC mode).
detail [active]	(Optional) Display a detailed summary of interface information (only available in privileged EXEC mode).
inconsistentports	(Optional) Display inconsistent port information (only available in privileged EXEC mode).
interface <i>interface-id</i> [active [detail] cost detail [active] inconsistency portfast priority rootcost state]	(Optional) Display spanning-tree information for the specified interface (all options only available in privileged EXEC mode). Enter each interface separated by a space. Ranges are not supported. Valid interfaces include physical ports, VLANs, and port channels. The valid VLAN range is 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1005 when the standard software image (SI) is installed. Do not enter leading zeros. The valid port-channel range is 1 to 6.

mst [configuration instance-id] [detail interface interface-id [detail]]	These keywords and options are available only if your switch is running the EI. (Optional) Display the multiple spanning-tree (MST) region configuration and status (all options only available in privileged EXEC mode). Valid interfaces include physical ports, VLANs, and port channels. The valid VLAN range is 1 to 4094; do not enter leading zeros. The valid port-channel range is 1 to 6.
pathcost method	(Optional) Display the default path cost method (only available in privileged EXEC mode).
root [address cost detail forward-time hello-time id max-age port priority [system-id]]	(Optional) Display root switch status and configuration (all options only available in privileged EXEC mode).
summary [totals]	(Optional) Display a summary of port states or the total lines of the spanning-tree state section (only available in privileged EXEC mode).
uplinkfast	(Optional) Display spanning-tree UplinkFast status (only available in privileged EXEC mode).
vlan vlan-id [active detail] backbonefast blockedports bridge [address detail forward-time hello-time id max-age priority [system-id] protocol]	(Optional) Display spanning-tree information for the specified VLAN (only available in privileged EXEC mode). The range is 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1005 when the standard software image (SI) is installed. Do not enter leading zeros.
 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC; indicated keywords available only in privileged EXEC mode

Command History

Release	Modification
12.0(5.2)WC(1)	This command was introduced.
12.1(6)EA2	The active , backbonefast , blockedports , bridge , inconsistentports , pathcost method , root , total , and uplinkfast keywords were added.
12.1(9)EA1	The mst keyword and options were added. The brief keyword was removed, and the detail keyword was added.

Usage Guidelines

If the *vlan-id* variable is omitted, the command applies to the spanning-tree instance for all VLANs. Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

■ **show spanning-tree**

Examples

This is an example of output from the **show spanning-tree active** command:

```
Switch# show spanning-tree active
VLAN0001
  Spanning tree enabled protocol ieee
    Root ID      Priority    32768
                  Address     0001.4297.e000
                  Cost        57
                  Port        1 (GigabitEthernet0/1)
                  Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

    Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
                  Address     0002.4b29.7a00
                  Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
                  Aging Time   300

    Interface    Port ID      Designated
    Name          Prio.Nbr    Cost  Bridge ID
                  -----  -----
    Gi0/1         128.1       19    FWD      38 32768 0030.9441.62c1 128.25
    Gi0/2         128.2       19    FWD      57 32769 0002.4b29.7a00 128.2
    Po1           128.65      19    FWD      57 32769 0002.4b29.7a00 128.65
```

This is an example of output from the **show spanning-tree detail** command:

```
Switch> show spanning-tree detail
VLAN0001 is executing the ieee compatible Spanning Tree protocol
Bridge Identifier has priority 32768, sysid 1, address 0002.4b29.7a00
Configured hello time 2, max age 20, forward delay 15
Current root has priority 32768, address 0001.4297.e000
Root port is 1 (GigabitEthernet0/1), cost of root path is 57
Topology change flag not set, detected flag not set
Number of topology changes 2 last change occurred 2d18h ago
  from Port-channel1
Times: hold 1, topology change 35, notification 2
  hello 2, max age 20, forward delay 15
Timers: hello 0, topology change 0, notification 0, aging 300

Port 1 (GigabitEthernet0/1) of VLAN0001 is forwarding
  Port path cost 19, Port priority 128, Port Identifier 128.1.
  Designated root has priority 32768, address 0001.4297.e000
  Designated bridge has priority 32768, address 0030.9441.62c1
  Designated port id is 128.25, designated path cost 38
  Timers: message age 4, forward delay 0, hold 0
  Number of transitions to forwarding state: 1
  BPDU: sent 2, received 120638

<output truncated>
```

This is an example of output from the **show spanning-tree interface fastethernet 0/1** command:

```
Switch> show spanning-tree interface fastethernet0/1
```

Vlan	Port ID	Designated	Port ID	
Name	Prio.Nbr	Cost Sts	Cost Bridge ID	Prio.Nbr
VLAN0001	128.1	19 FWD	38 32768 0030.9441.62c1	128.25

This is an example of output from the **show spanning-tree summary** command:

```
Switch> show spanning-tree summary
Root bridge for: none.
Extended system ID is enabled
PortFast BPDU Guard is disabled
EtherChannel misconfiguration guard is enabled
UplinkFast is disabled
BackboneFast is disabled
Default pathcost method used is short

Name          Blocking Listening Learning Forwarding STP Active
-----
VLAN1         13      0        0      1      14
VLAN2         1       0        0      1      2
VLAN3         1       0        0      1      2

<output truncated>
```

This is an example of output from the **show spanning-tree mst configuration** command:

```
Switch# show spanning-tree mst configuration
Name      [region1]
Revision  1
Instance  Vlans Mapped
-----
0        1-9,21-4094
1        10-20
-----
```

This is an example of output from the **show spanning-tree mst interface fastethernet0/1** command:

```
Switch# show spanning-tree mst interface fastethernet0/1

FastEthernet0/1 of MST00 is root forwarding
Edge port: no           (default)      port guard : none      (default)
Link type: point-to-point (auto)      bpdu filter: disable  (default)
Boundary : boundary      (STP)        bpdu guard : disable  (default)
Bpdus sent 5, received 74

Instance role state cost      prio vlans mapped
-----
0      root FWD   200000    128  1,12,14-4094
```

This is an example of output from the **show spanning-tree mst 0** command:

```
Switch# show spanning-tree mst 0
#####
MST00      vlans mapped: 1-9,21-4094
Bridge     address 0002.4b29.7a00 priority 32768 (32768 sysid 0)
Root      address 0001.4297.e000 priority 32768 (32768 sysid 0)
          port Gi0/1      path cost 200038
IST master *this switch
Operational hello time 2, forward delay 15, max age 20, max hops 20
Configured hello time 2, forward delay 15, max age 20, max hops 20

Interface      role state cost      prio type
-----
GigabitEthernet0/1  root FWD   200000    128  P2P bound(STP)
GigabitEthernet0/2  desg FWD   200000    128  P2P bound(STP)
Port-channel1     desg FWD   200000    128  P2P bound(STP)
```

■ **show spanning-tree**

Related Commands	Command	Description
	spanning-tree backbonefast	Enables the BackboneFast feature.
	spanning-tree bpdufilter	Prevents a port from sending or receiving bridge protocol data units (BPDUs).
	spanning-tree bpduguard	Puts a port in the error-disabled state when it receives a BPDU.
	spanning-tree cost	Sets the path cost for spanning-tree calculations.
	spanning-tree extend system-id	Enables the extended system ID feature.
	spanning-tree guard	Enables the root guard or the loop guard feature for all the VLANs associated with the selected interface.
	spanning-tree link-type	Overrides the default link-type setting for rapid spanning-tree transitions to the forwarding state.
	spanning-tree loopguard default	Prevents alternate or root ports from becoming the designated port because of a failure that leads to a unidirectional link.
	spanning-tree mst configuration	Enters multiple spanning-tree (MST) configuration mode through which the MST region configuration occurs.
	spanning-tree mst cost	Sets the path cost for MST calculations.
	spanning-tree mst forward-time	Sets the forward-delay time for all MST instances.
	spanning-tree mst hello-time	Sets the interval between hello BPDUs sent by root switch configuration messages.
	spanning-tree mst max-age	Sets the interval between messages that the spanning tree receives from the root switch.
	spanning-tree mst max-hops	Sets the number of hops in an MST region before the BPDU is discarded and the information held for a port is aged.
	spanning-tree mst port-priority	Configures an interface priority.
	spanning-tree mst priority	Configures the switch priority for the specified spanning-tree instance.
	spanning-tree mst root	Configures the MST root switch priority and timers based on the network diameter.
	spanning-tree port-priority	Configures an interface priority.
	spanning-tree portfast (global configuration)	Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled ports or enables the Port Fast feature on all nontrunking ports.
	spanning-tree portfast (interface configuration)	Enables the Port Fast feature on an interface and all its associated VLANs.
	spanning-tree uplinkfast	Accelerates the choice of a new root port when a link or switch fails or when the spanning tree reconfigures itself.
	spanning-tree vlan	Configures spanning tree on a per-VLAN basis.

show storm-control

Use the **show storm-control** user EXEC command to display the packet-storm control information. This command also displays the action that the switch takes when the thresholds are reached.

```
show storm-control [interface-id] [{broadcast | history | multicast | unicast }] [| {begin | exclude | include} expression]
```

Syntax Description

<i>interface-id</i>	(Optional) Port for which information is to be displayed.
broadcast	(Optional) Display broadcast storm information.
history	(Optional) Display storm history on a per-port basis.
multicast	(Optional) Display multicast storm information.
unicast	(Optional) Display unicast storm information.
 begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(6)EA2	This command was introduced. It replaced the show port storm-control command.

Usage Guidelines

If the variable *interface-id* is omitted, the **show storm-control** command displays storm-control settings for all ports on the switch.

You can display broadcast, multicast, or unicast packet-storm information by using the corresponding keyword. When no option is specified, the default is to display broadcast storm-control information.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

■ **show storm-control**

Examples

This is an example of output from the **show storm-control broadcast** command:

```
Switch> show storm-control broadcast
```

Interface	Filter State	Trap State	Upper	Lower	Current	Traps Sent
Fa0/1	<inactive>	<inactive>	100.00%	100.00%	0.00%	0
Fa0/2	<inactive>	<inactive>	100.00%	100.00%	0.00%	0
Fa0/3	<inactive>	<inactive>	100.00%	100.00%	0.00%	0
Fa0/4	Forwarding	Below rising	30.00%	20.00%	20.32%	17
...						

Table 2-17 lists the **show storm-control** field descriptions.

Table 2-17 show storm-control Field Descriptions

Field	Description
Interface	Displays the ID of the interface.
Filter State	Displays the status of the filter: <ul style="list-style-type: none"> Blocking—Storm control is enabled, action is filter, and a storm has occurred. Forwarding—Storm control is enabled, and a storm has not occurred. Inactive—Storm control is disabled. Shutdown—Storm control is enabled, the action is to shut down, and a storm has occurred. Note If an interface is disabled by a broadcast, multicast, or unicast storm, the filter state for all traffic types is <i>shutdown</i> .
Trap State	Displays the status of the SNMP trap: <ul style="list-style-type: none"> Above rising—Storm control is enabled, and a storm has occurred. Below rising—Storm control is enabled, and a storm has not occurred. Inactive—The trap option is not enabled.
Upper	Displays the rising suppression level as a percentage of total available bandwidth.
Lower	Displays the falling suppression level as a percentage of total available bandwidth.
Current	Displays the bandwidth utilization of a specific traffic type as a percentage of total available bandwidth. This field is valid only when storm control is enabled.
Traps Sent	Displays the number traps sent on an interface for a specific traffic type.

This is an example of output from the **show storm-control fastethernet0/4 history** command, which displays the ten most recent storm events for an interface.

```
Switch> show storm-control fastethernet0/4 history
```

Interface Fa0/4 Storm Event History

Event Type	Event Start Time	Duration (seconds)
Unicast	04:58:18	206
Broadcast	05:01:54	n/a
Multicast	05:01:54	n/a
Unicast	05:01:54	108
Broadcast	05:05:00	n/a
Multicast	05:05:00	n/a
Unicast	05:06:00	n/a
Broadcast	05:09:39	n/a
Multicast	05:09:39	n/a
Broadcast	05:11:32	172



Note The duration field could be *n/a* when a storm is still present or when a new storm of a different type occurs before the current storm ends.

Related Commands

Command	Description
speed	Enables broadcast, multicast, or unicast storm control on a port.

 show system mtu

show system mtu

Use the **show system mtu** privileged EXEC command to display the global maximum packet size or maximum transmission unit (MTU) set for the switch.

show system mtu [| {begin | exclude | include} expression]

Syntax Description	<table border="1"> <tr> <td> begin</td><td>(Optional) Display begins with the line that matches the <i>expression</i>.</td></tr> <tr> <td> exclude</td><td>(Optional) Display excludes lines that match the <i>expression</i>.</td></tr> <tr> <td> include</td><td>(Optional) Display includes lines that match the specified <i>expression</i>.</td></tr> <tr> <td><i>expression</i></td><td>Expression in the output to use as a reference point.</td></tr> </table>	begin	(Optional) Display begins with the line that matches the <i>expression</i> .	exclude	(Optional) Display excludes lines that match the <i>expression</i> .	include	(Optional) Display includes lines that match the specified <i>expression</i> .	<i>expression</i>	Expression in the output to use as a reference point.
begin	(Optional) Display begins with the line that matches the <i>expression</i> .								
exclude	(Optional) Display excludes lines that match the <i>expression</i> .								
include	(Optional) Display includes lines that match the specified <i>expression</i> .								
<i>expression</i>	Expression in the output to use as a reference point.								

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

Command History	Release	Modification
	12.1(6)EA2	This command was introduced.

Usage Guidelines	Expressions are case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> do not appear, but the lines that contain <i>Output</i> appear.
-------------------------	--

Examples	This is an example of output from the show system mtu command:
	<pre>Switch# show system mtu System MTU size is 1500 bytes</pre>

Related Commands	Command	Description
	system mtu	Sets the MTU size for the switch.

show udld

Use the **show udld** user EXEC command to display UniDirectional Link Detection (UDLD) status for all ports or the specified port.

show udld [interface-id] [| {begin | exclude | include} expression]

Syntax Description	<table border="0"> <tr> <td><i>interface-id</i></td><td>(Optional) ID of the interface and port number. Valid interfaces include physical ports and VLANs. The VLAN range is 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1001 when the standard software image (SI) is installed. Do not enter leading zeros.</td></tr> <tr> <td> begin</td><td>(Optional) Display begins with the line that matches the specified <i>expression</i>.</td></tr> <tr> <td> exclude</td><td>(Optional) Display excludes lines that match the specified <i>expression</i>.</td></tr> <tr> <td> include</td><td>(Optional) Display includes lines that match the specified <i>expression</i>.</td></tr> <tr> <td><i>expression</i></td><td>Expression in the output to use as a reference point.</td></tr> </table>	<i>interface-id</i>	(Optional) ID of the interface and port number. Valid interfaces include physical ports and VLANs. The VLAN range is 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1001 when the standard software image (SI) is installed. Do not enter leading zeros.	begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .	exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .	include	(Optional) Display includes lines that match the specified <i>expression</i> .	<i>expression</i>	Expression in the output to use as a reference point.
<i>interface-id</i>	(Optional) ID of the interface and port number. Valid interfaces include physical ports and VLANs. The VLAN range is 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1001 when the standard software image (SI) is installed. Do not enter leading zeros.										
begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .										
exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .										
include	(Optional) Display includes lines that match the specified <i>expression</i> .										
<i>expression</i>	Expression in the output to use as a reference point.										

Command Modes	User EXEC
----------------------	-----------

Command History	Release	Modification
	12.0(5.2)WC(1)	This command was introduced.

Usage Guidelines	If you do not enter an <i>interface-id</i> , the administrative and the operational UDLD status for all interfaces appear. Expressions are case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> do not appear, but the lines that contain <i>Output</i> appear.
-------------------------	--

Examples	This is an example of output from the show udld gigabitethernet0/1 command. In this example, UDLD is enabled on both ends of the link, and UDLD detects that the link is bidirectional. Table 2-18 describes the fields in this example.
-----------------	---

```
Switch> show udld gigabitethernet0/1
Interface gi0/1
---
Port enable administrative configuration setting: Follows device default
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single Neighbor detected
Message interval: 60
Time out interval: 5
Entry 1
Expiration time: 146
Device ID: 1
Current neighbor state: Bidirectional
Device name: 0050e2826000
Port ID: Gi0/2
```

■ show udld

```

Neighbor echo 1 device: SAD03160954
Neighbor echo 1 port: Gi0/1
Message interval: 5
CDP Device name: 066527791

```

Table 2-18 show udld Field Descriptions

Field	Description
Interface	The interface on the local device configured for UDLD.
Port enable administrative configuration setting	How UDLD is configured on the port. If UDLD is enabled or disabled, the port enable configuration setting is the same as the operational enable state. Otherwise, the enable operational setting depends on the global enable setting.
Port enable operational state	Operational state that shows whether UDLD is actually running on this port.
Current bidirectional state	The bidirectional state of the link. An unknown state appears if the link is down or if it is connected to an UDLD-incapable device. A bidirectional state appears if the link is a normal two-way connection to a UDLD-capable device. All other values mean miswiring.
Current operational state	The phase of the UDLD state machine. For a normal bidirectional link, the state machine is usually in the Advertisement phase.
Message interval	How often advertisement messages are sent from the local device. Measured in seconds.
Time out interval	The time period, in seconds, that UDLD waits for echoes from a neighbor device during the detection window.
Entry 1	Information from the first cache entry, which contains a copy of echo information received from the neighbor.
Expiration time	The amount of time in seconds remaining before this cache entry is aged out.
Device ID	The neighbor device identification.
Current neighbor state	The neighbor's state. If both the local and neighbor devices are running UDLD, the neighbor state and the local state is bidirectional. If the link is down or the neighbor is not UDLD-capable, no cache entries appear.
Device name	The neighbor MAC address.
Port ID	The neighbor port ID enabled for UDLD.
Neighbor echo 1 device	The MAC address of the neighbors' neighbor from which the echo originated.
Neighbor echo 1 port	The port number ID of the neighbor from which the echo originated.
Message interval	The rate, in seconds, at which the neighbor is sending advertisement messages.
CDP ¹ device name	CDP name of the device.

1. CDP = Cisco Discovery Protocol

This is an example of output from the **show udld** interface configuration command when the aggressive mode is configured:

```
Switch# show udld gi0/1
Interface Gi0/1
---
Port enable administrative configuration setting:Enabled / in aggressive mode
Port enable operational state:Enabled / in aggressive mode
Current bidirectional state:Unknown
Current operational state:Link down
Message interval:7
Time out interval:5
No neighbor cache information stored
```

Related Commands	Command	Description
	udld (global configuration)	Enables UDLD on all ports on the switch.
	udld (interface configuration)	Enables UDLD on a port.
	udld reset	Resets any interface that was shut down by UDLD.

show version

show version

Use the **show version** user EXEC command to display version information for the hardware and firmware.

show version [| {begin | exclude | include} expression]

Syntax Description	<table border="0"> <tr> <td> begin</td><td>(Optional) Display begins with the line that matches the specified <i>expression</i>.</td></tr> <tr> <td> exclude</td><td>(Optional) Display excludes lines that match the specified <i>expression</i>.</td></tr> <tr> <td> include</td><td>(Optional) Display includes lines that match the specified <i>expression</i>.</td></tr> <tr> <td><i>expression</i></td><td>Expression in the output to use as a reference point.</td></tr> </table>	begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .	exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .	include	(Optional) Display includes lines that match the specified <i>expression</i> .	<i>expression</i>	Expression in the output to use as a reference point.
begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .								
exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .								
include	(Optional) Display includes lines that match the specified <i>expression</i> .								
<i>expression</i>	Expression in the output to use as a reference point.								

Command Modes	User EXEC
----------------------	-----------

Command History	Release	Modification
	12.0(5.2)WC(1)	This command was introduced.

Usage Guidelines	Expressions are case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> do not appear, but the lines that contain <i>Output</i> appear.
-------------------------	--

Examples	This is an example of output from the show version command:
-----------------	--

```
Switch> show version

Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(9)EA1
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Wed 27-Feb-02 06:51 by antonino
Image text-base:0x80010000, data-base:0x804E2000

ROM:Bootstrap program is C2950 boot loader

Switch uptime is 1 hour, 54 minutes
System returned to ROM by power-on
System image file is "flash:c2950-i6q4l2-mz.121-0.0.9.EA1.bin"

cisco WS-C2950G-12-EI (RC32300) processor with 20830K bytes of memory.
Last reset from system-reset
Running Enhanced Image
12 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)

32K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address:00:05:74:28:09:C0
Configuration register is 0xF
```

show vlan

Use the **show vlan** user EXEC command to display the parameters for all configured VLANs or one VLAN (if the VLAN ID or name is specified) on the switch.

```
show vlan [brief | id vlan-id | name vlan-name | remote-span | summary] [ | {begin | exclude | include} expression]
```

Syntax Description	brief	(Optional) Display one line for each VLAN with the VLAN name, status, and its ports.
	id <i>vlan-id</i>	(Optional) Display information about a single VLAN identified by VLAN ID number. For <i>vlan-id</i> , the range is 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1005 when the standard software image (SI) is installed. Do not enter leading zeros.
	name <i>vlan-name</i>	(Optional) Display information about a single VLAN identified by VLAN name. The VLAN name is an ASCII string from 1 to 32 characters.
	remote-span	(Optional) Display information about Remote SPAN (RSPAN) VLANs.
	summary	(Optional) Display VLAN summary information. This keyword is available only if your switch is running the EI.
	 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	 include	(Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.



Though visible in the command-line help string when the EI is installed, the **internal usage**, **ifindex**, and **private-vlan** keywords are not supported.

Command Modes	User EXEC
----------------------	-----------

Command History	Release	Modification
	12.0(5.2)WC(1)	This command was introduced.
	12.1(9)EA1	The summary keyword was added.
	12.1(11)EA1	The remote-span keyword was added.

Usage Guidelines	Expressions are case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> are not displayed, but the lines that contain <i>Output</i> are displayed.
-------------------------	---

■ show vlan**Examples**

This is an example of output from the **show vlan** command. Table 2-19 describes each field in the display.

```
Switch> show vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/5, Fa0/7 Fa0/8, Fa0/9, Fa0/11, Fa0/12 Gi0/1, Gi0/2
2	VLAN0002	active	
51	VLAN0051	active	
52	VLAN0052	active	
100	VLAN0100	suspended	Fa0/3
400	VLAN0400	suspended	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fdnet-default	active	
1005	trnet-default	active	
<hr/>			
VLAN	Type	SAID	MTU
			Parent
			RingNo
			BridgeNo
			Stp
			BrdgMode
			Transl
			Trans2
1	enet	100001	1500
2	enet	100002	1500
51	enet	100051	1500
52	enet	100052	1500
100	enet	100100	1500
400	enet	100400	1500
1002	fddi	101002	1500
1003	tr	101003	1500
1004	fdnet	101004	1500
1005	trnet	101005	1500
<hr/>			
Remote SPAN VLANs			
<hr/>			
Primary	Secondary	Type	Ports

Table 2-19 show vlan Command Output Fields

Field	Description
VLAN	VLAN number.
Name	Name, if configured, of the VLAN.
Status	Status of the VLAN (active or suspend).
Ports	Ports that belong to the VLAN.
Type	Media type of the VLAN.
SAID	Security association ID value for the VLAN.
MTU	Maximum transmission unit size for the VLAN.
Parent	Parent VLAN, if one exists.
RingNo	Ring number for the VLAN, if applicable.

Table 2-19 show vlan Command Output Fields (continued)

Field	Description
BrdgNo	Bridge number for the VLAN, if applicable.
Stp	Spanning Tree Protocol type used on the VLAN.
BrdgMode	Bridging mode for this VLAN—possible values are source-route bridging (SRB) and source-route transparent (SRT); the default is SRB.
Trans1	Translation bridge 1.
Trans2	Translation bridge 2.
AREHops	Maximum number of hops for All-Routes Explorer frames—possible values are 1 through 13; the default is 7.
STEHops	Maximum number of hops for Spanning-Tree Explorer frames—possible values are 1 through 13; the default is 7.
Backup CRF	Status of whether or not the Token Ring concentrator relay function (TrCRF) is a backup path for traffic.

This is an example of output from the **show vlan brief** command:

```
Switch> show vlan brief
```

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

This is an example of output from the **show vlan id** command. The specified VLAN is in the extended VLAN range.

```
Switch# show vlan id 2005
```

VLAN Name	Status	Ports							
2005 VLAN2005	active	Fa0/2							
VLAN Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
2005 enet	102005	1500	-	-	-	-	-	0	0

This is an example of output from the **show vlan summary** command:

```
Switch> show vlan summary
Number of existing VLANs : 7
Number of existing VTP VLANs : 7
Number of existing extended VLANs : 0
```

■ **show vlan**

Related Commands	Command	Description
	switchport mode	Configures the VLAN membership mode of a port.
	vlan (global configuration)	Enables config-vlan mode where you can configure VLANs 1 to 4094 when the EI is installed and 1 to 1005 when the standard software image (SI) is installed. Do not enter leading zeros.
	vlan (VLAN configuration)	Configures VLAN characteristics in the VLAN database. Only available for normal-range VLANs (VLAN IDs 1 to 1005). Do not enter leading zeros.

show vmmps

Use the **show vmmps** user EXEC command without keywords to display the VLAN Query Protocol (VQP) version, reconfirmation interval, retry count, VLAN Membership Policy Server (VMPS) IP addresses, and the current and primary servers, or use the **statistics** keyword to display client-side statistics.

show vmmps [statistics] [| {begin | exclude | include} expression]

Syntax Description	statistics (Optional) Display VQP client-side statistics and counters. begin (Optional) Display begins with the line that matches the <i>expression</i> . exclude (Optional) Display excludes lines that match the <i>expression</i> . include (Optional) Display includes lines that match the specified <i>expression</i> . expression Expression in the output to use as a reference point.
---------------------------	---

Command Modes	User EXEC
----------------------	-----------

Command History	Release	Modification
	12.1(6)EA2	This command was introduced.

Usage Guidelines	Expressions are case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> do not appear, but the lines that contain <i>Output</i> appear.
-------------------------	--

Examples	This is an example of output from the show vmmps command:
-----------------	--

```
Switch> show vmmps
VQP Client Status:
-----
VMPS VQP Version:    1
Reconfirm Interval: 60 min
Server Retry Count:  3
VMPS domain server:

Reconfirmation status
-----
VMPS Action:          other
```

This is an example of output from the **show vmmps statistics** command. [Table 2-20](#) describes each field in the example.

```
Switch> show vmmps statistics
VMPS Client Statistics
-----
VQP  Queries:          0
VQP  Responses:         0
VMPS Changes:          0
VQP  Shutdowns:         0
VQP  Denied:            0
VQP  Wrong Domain:      0
```

show vmps

```
VQP Wrong Version: 0
VQP Insufficient Resource: 0
```

Table 2-20 show vmps statistics Field Descriptions

Field	Description
VQP Queries	Number of queries sent by the client to the VMPS.
VQP Responses	Number of responses sent to the client from the VMPS.
VMPS Changes	Number of times that the VMPS changed from one server to another.
VQP Shutdowns	Number of times the VMPS sent a response to shut down the port. The client disables the port and removes all dynamic addresses on this port from the address table. You must administratively re-enable the port to restore connectivity.
VQP Denied	Number of times the VMPS denied the client request for security reasons. When the VMPS response denies an address, no frame is forwarded to or from the workstation with that address. (Broadcast or multicast frames are delivered to the workstation if the port on the switch has been assigned to a VLAN.) The client keeps the denied address in the address table as a blocked address to prevent further queries from being sent to the VMPS for each new packet received from this workstation. The client ages the address if no new packets are received from this workstation on this port within the aging time period.
VQP Wrong Domain	Number of times the management domain in the request does not match the one for the VMPS. Any previous VLAN assignments of the port are not changed. This response means that the server and the client have not been configured with the same VTP management domain.
VQP Wrong Version	Number of times the version field in the query packet contains a value that is higher than the version supported by the VMPS. The previous VLAN assignment of the port is not changed. The switches send only VMPS version 1 requests.
VQP Insufficient Resource	Number of times the VMPS is unable to answer the request because of a resource availability problem. If the retry limit has not yet been reached, the client repeats the request with the same server or with the next alternate server, depending on whether the per-server retry count has been reached.

Related Commands

Command	Description
clear vmps statistics	Clears the statistics maintained by the VQP client.
vmps reconfirm (global configuration)	Sends VQP queries to reconfirm all dynamic VLAN assignments with the VMPS.
vmps retry	Configures the per-server retry count for the VQP client.
vmps server	Configures the primary VMPS and up to three secondary servers.

show vtp

Use the **show vtp** user EXEC command to display general information about the VLAN Trunking Protocol (VTP) management domain, status, and counters.

```
show vtp {counters | status} [ | {begin | exclude | include} expression] 
```

Syntax Description	counters	Display the VTP statistics for the switch.
	status	Display general information about the VTP management domain status.
	 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	 include	(Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

Command History	Release	Modification
	12.0(5.2)WC(1)	This command was introduced.

Usage Guidelines Expressions are case sensitive. For example, if you enter | **exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples This is an example of output from the **show vtp counters** command. Table 2-21 describes each field in the display.

Switch> show vtp counters

```
VTP statistics:  
Summary advertisements received      : 38  
Subset advertisements received       : 0  
Request advertisements received     : 0  
Summary advertisements transmitted  : 13  
Subset advertisements transmitted   : 3  
Request advertisements transmitted : 0  
Number of config revision errors   : 0  
Number of config digest errors    : 0  
Number of V1 summary errors        : 0
```

VTP pruning statistics:

Trunk	Join Transmitted	Join Received	Summary advts received from non-pruning-capable device
Fa0/9	827	824	0
Fa0/10	827	823	0
Fa0/11	827	823	0

show vtp

Table 2-21 show vtp counters Field Descriptions

Field	Description
Summary advertisements received	Number of summary advertisements received by this switch on its trunk ports. Summary advertisements contain the management domain name, the configuration revision number, the update timestamp and identity, the authentication checksum, and the number of subset advertisements to follow.
Subset advertisements received	Number of subset advertisements received by this switch on its trunk ports. Subset advertisements contain all the information for one or more VLANs.
Request advertisements received	Number of advertisement requests received by this switch on its trunk ports. Advertisement requests normally request information on all VLANs. They can also request information on a subset of VLANs.
Summary advertisements transmitted	Number of summary advertisements sent by this switch on its trunk ports. Summary advertisements contain the management domain name, the configuration revision number, the update timestamp and identity, the authentication checksum, and the number of subset advertisements to follow.
Subset advertisements transmitted	Number of subset advertisements sent by this switch on its trunk ports. Subset advertisements contain all the information for one or more VLANs.
Request advertisements transmitted	Number of advertisement requests sent by this switch on its trunk ports. Advertisement requests normally request information on all VLANs. They can also request information on a subset of VLANs.
Number of configuration revision errors	<p>Number of revision errors.</p> <p>Whenever you define a new VLAN, delete an existing one, suspend or resume an existing VLAN, or modify the parameters on an existing VLAN, the configuration revision number of the switch increments.</p> <p>Revision errors increment whenever the switch receives an advertisement whose revision number matches the revision number of the switch, but the MD5 digest values do not match. This error means that the VTP password in the two switches is different or that the switches have different configurations.</p> <p>These errors mean that the switch is filtering incoming advertisements, which causes the VTP database to become unsynchronized across the network.</p>

Table 2-21 show vtp counters Field Descriptions (continued)

Field	Description
Number of configuration digest errors	Number of MD5 digest errors. Digest errors increment whenever the MD5 digest in the summary packet and the MD5 digest of the received advertisement calculated by the switch do not match. This error usually means that the VTP password in the two switches is different. To solve this problem, make sure the VTP password on all switches is the same. These errors mean that the switch is filtering incoming advertisements, which causes the VTP database to become unsynchronized across the network.
Number of V1 summary errors	Number of version 1 errors. Version 1 summary errors increment whenever a switch in VTP V2 mode receives a VTP version 1 frame. These errors mean that at least one neighboring switch is either running VTP version 1 or VTP version 2 with V2-mode disabled. To solve this problem, change the configuration of the switches in VTP V2-mode to disabled.
Join Transmitted	Number of VTP pruning messages sent on the trunk.
Join Received	Number of VTP pruning messages received on the trunk.
Summary Advts Received from non-pruning-capable device	Number of VTP summary messages received on the trunk from devices that do not support pruning.

This is an example of output from the **show vtp status** command. [Table 2-22](#) describes each field in the display.

Switch> **show vtp status**

```
VTP Version : 2
Configuration Revision : 0
Maximum VLANs supported locally : 250
Number of existing VLANs : 5
VTP Operating Mode : Server
VTP Domain Name :
VTP Pruning Mode : Disabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0xBF 0x86 0x94 0x45 0xFC 0xDF 0xB5 0x70
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 172.20.135.196 on interface V11 (lowest numbered VLAN interface found)
```

Table 2-22 show vtp status Field Descriptions

Field	Description
VTP Version	Displays the VTP version operating on the switch. By default, the switch implements version 1 but can be set to version 2.
Configuration Revision	Current configuration revision number on this switch.
Maximum VLANs Supported Locally	Maximum number of VLANs supported locally.
Number of Existing VLANs	Number of existing VLANs.

show vtp

Table 2-22 show vtp status Field Descriptions (continued)

Field	Description
VTP Operating Mode	<p>Displays the VTP operating mode, which can be server, client, or transparent.</p> <p>Server: a switch in VTP server mode is enabled for VTP and sends advertisements. You can configure VLANs on it. The switch guarantees that it can recover all the VLAN information in the current VTP database from nonvolatile RAM (NVRAM) after reboot. By default, every switch is a VTP server.</p> <p>Note The switch automatically changes from VTP server mode to VTP client mode if it detects a failure while writing the configuration to NVRAM and cannot return to server mode until the NVRAM is functioning.</p> <p>Client: a switch in VTP client mode is enabled for VTP, can send advertisements, but does not have enough nonvolatile storage to store VLAN configurations. You cannot configure VLANs on it. When a VTP client starts up, it does not send VTP advertisements until it receives advertisements to initialize its VLAN database.</p> <p>Transparent: a switch in VTP transparent mode is disabled for VTP, does not send or learn from advertisements sent by other devices, and cannot affect VLAN configurations on other devices in the network. The switch receives VTP advertisements and forwards them on all trunk ports except the one on which the advertisement was received.</p>
VTP Domain Name	Name that identifies the administrative domain for the switch.
VTP Pruning Mode	Displays whether pruning is enabled or disabled. Enabling pruning on a VTP server enables pruning for the entire management domain. Pruning restricts flooded traffic to those trunk links that the traffic must use to access the appropriate network devices.
VTP V2 Mode	Displays if VTP version 2 mode is enabled. All VTP version 2 switches operate in version 1 mode by default. Each VTP switch automatically detects the capabilities of all the other VTP devices. A network of VTP devices should be configured to version 2 only if all VTP switches in the network can operate in version 2 mode.
VTP Traps Generation	Displays whether VTP traps are sent to a network management station.
MD5 Digest	A 16-byte checksum of the VTP configuration.
Configuration Last Modified	Displays the date and time of the last configuration modification. Displays the IP address of the switch that caused the configuration change to the database.

Related Commands	Command	Description
	clear vtp counters	Clears the VTP and pruning counters.
	vtp (global configuration)	Configures the VTP filename, interface name, domain name, and mode. You can save configuration resulting from this command in the switch configuration file.
	vtp (privileged EXEC)	Configures the VTP password, pruning, and version.
	vtp (VLAN configuration)	Configures the VTP domain name, password, pruning, and mode.

■ **show wrr-queue bandwidth**

show wrr-queue bandwidth

Use the **show wrr-queue bandwidth** user EXEC command to display the weighted round-robin (WRR) bandwidth allocation for the four class of service (CoS) priority queues.

show wrr-queue bandwidth [| {begin | exclude | include} expression]

Syntax Description	<table border="0"> <tr> <td> begin</td><td>(Optional) Display begins with the line that matches the specified <i>expression</i>.</td></tr> <tr> <td> exclude</td><td>(Optional) Display excludes lines that match the specified <i>expression</i>.</td></tr> <tr> <td> include</td><td>(Optional) Display includes lines that match the specified <i>expression</i>.</td></tr> <tr> <td><i>expression</i></td><td>Expression in the output to use as a reference point.</td></tr> </table>	begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .	exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .	include	(Optional) Display includes lines that match the specified <i>expression</i> .	<i>expression</i>	Expression in the output to use as a reference point.
begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .								
exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .								
include	(Optional) Display includes lines that match the specified <i>expression</i> .								
<i>expression</i>	Expression in the output to use as a reference point.								

Command Modes User EXEC

Command History	Release	Modification
	12.0(5.2)WC(1)	This command was introduced.

Usage Guidelines Expressions are case sensitive. For example, if you enter | **exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples This is an example of output from the **show wrr-queue bandwidth** command:

Switch> **show wrr-queue bandwidth**

```
WRR Queue : 1 2 3 4
Bandwidth : 10 20 30 40
```

Related Commands	Command	Description
	show wrr-queue cos-map	Displays the mapping of the CoS to the priority queues.
	wrr-queue cos-map	Assigns WRR weights to the four CoS priority queues.
	wrr-queue cos-map	Assigns CoS values to the CoS priority queues.

show wrr-queue cos-map

Use the **show wrr-queue cos-map** user EXEC command to display the mapping of the class of service (CoS) priority queues.

show wrr-queue cos-map [| {begin | exclude | include} expression]

Syntax Description	<table border="0"> <tr> <td> begin</td><td>(Optional) Display begins with the line that matches the specified <i>expression</i>.</td></tr> <tr> <td> exclude</td><td>(Optional) Display excludes lines that match the specified <i>expression</i>.</td></tr> <tr> <td> include</td><td>(Optional) Display includes lines that match the specified <i>expression</i>.</td></tr> <tr> <td><i>expression</i></td><td>Expression in the output to use as a reference point.</td></tr> </table>	begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .	exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .	include	(Optional) Display includes lines that match the specified <i>expression</i> .	<i>expression</i>	Expression in the output to use as a reference point.
begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .								
exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .								
include	(Optional) Display includes lines that match the specified <i>expression</i> .								
<i>expression</i>	Expression in the output to use as a reference point.								

Command Modes	User EXEC
----------------------	-----------

Command History	Release	Modification
	12.0(5.2)WC(1)	This command was introduced.

Usage Guidelines	Expressions are case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> do not appear, but the lines that contain <i>Output</i> appear.
-------------------------	--

Examples	This is an example of output from the show wrr-queue cos-map command:
<pre>Switch> show wrr-queue cos-map CoS Value : 0 1 2 3 4 5 6 7 Priority Queue : 1 1 2 2 3 3 4 4</pre>	

Related Commands	Command	Description
	show wrr-queue bandwidth	Displays the WRR bandwidth allocation for the four CoS priority queues.
	wrr-queue bandwidth	Assigns weighted round-robin (WRR) weights to the four CoS priority queues.
	wrr-queue cos-map	Assigns CoS values to the CoS priority queues.

shutdown

shutdown

Use the **shutdown** interface configuration command to disable a port and to shut down the management VLAN. On an LRE model, this command disables the LRE interface by deactivating the MAC interface and the LRE chipset transmitter. Use the **no** form of this command to enable a disabled port or to activate the management VLAN.

shutdown

no shutdown

Syntax Description This command has no arguments or keywords.

Command Modes Interface configuration

Command History	Release	Modification
	12.0(5.2)WC(1)	This command was introduced.

Usage Guidelines The **shutdown** command for a port causes it to stop forwarding. You can enable the port with the **no shutdown** command.

The **no shutdown** command has no effect if the port is a static-access port assigned to a VLAN that has been deleted, suspended, or shut down. The port must first be a member of an active VLAN before it can be re-enabled.

Only one management VLAN interface can be active at a time. The remaining VLANs are shut down. In the **show running-config** command output, the active management VLAN interface is the one without the **shutdown** command displayed.

On LRE switches, this command disables the LRE transmitter of an LRE interface. Under some circumstances, the power emitted by switch LRE ports can affect other switch LRE ports. We recommend that ports that are not connected to CPE devices be shut down by using this command. Also use this command to disable access to the switch from a particular port.

Examples This example shows how to disable fixed Fast Ethernet port 0/8 and how to re-enable it:

```
Switch(config)# interface fastethernet0/8
Switch(config-if)# shutdown
Switch(config-if)# no shutdown
```

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

shutdown vlan

Use the **shutdown vlan** global configuration command to shut down (suspend) local traffic on the specified VLAN. Use the **no** form of this command to restart local traffic on the VLAN.

shutdown vlan *vlan-id*

no shutdown vlan *vlan-id*

Syntax Description	<i>vlan-id</i>	ID of the VLAN to be locally shut down. Valid IDs are from 2 to 1001. VLANs defined as default VLANs under the VLAN Trunking Protocol (VTP), as well as extended-range VLANs (greater than 1005) cannot be shut down. The default VLANs are 1 and 1002 to 1005. Do not enter leading zeros.
---------------------------	----------------	---

Defaults	No default is defined.
-----------------	------------------------

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

Command History	Release	Modification
	12.0(5.2)WC(1)	This command was introduced.

Usage Guidelines	The shutdown vlan command does not change the VLAN information in the VTP database. It shuts down traffic locally, but the switch still advertises VTP information.
-------------------------	--

Examples	This example shows how to shutdown traffic on VLAN 2:
-----------------	---

```
Switch(config)# shutdown vlan 2
```

You can verify your setting by entering the **show vlan** privileged EXEC command.

Related Commands	Command	Description
	shutdown	Shuts down local traffic on the VLAN when in config-VLAN mode (accessed by the (config-vlan mode) vlan <i>vlan-id</i> global configuration command).
	vlan (VLAN configuration)	Enables config-vlan mode.
	vlan database	Enters VLAN configuration mode.

■ **snmp-server enable traps**

snmp-server enable traps

Use the **snmp-server enable traps** global configuration command to enable the switch to send Simple Network Management Protocol (SNMP) notification for various trap types to the network management system (NMS). Use the **no** form of this command to return to the default setting.

snmp-server enable traps [c2900 | cluster | config | entity | hsrp | mac-notification | rtr | snmp | syslog | vlan-membership | vtp]

no snmp-server enable traps [c2900 | cluster | config | entity | hsrp | mac-notification | rtr | snmp | syslog | vlan-membership | vtp]



Note Though visible in the command-line help strings, the **snmp-server enable informs** command has no functionality. To enable sending SNMP inform notifications, use the **snmp-server enable traps** command combined with the **snmp-server host host-addr informs** command.

Syntax Description

c2900	(Optional) Enable SNMP configuration traps.
cluster	(Optional) Enable cluster traps.
config	(Optional) Enable SNMP configuration traps.
entity	(Optional) Enable SNMP entity traps.
hsrp	(Optional) Enable Hot Standby Router Protocol (HSRP) traps.
mac-notification	(Optional) Enable MAC address notification traps.
rtr	(Optional) Enable SNMP Response Time Reporter traps.
snmp	(Optional) Enable SNMP traps.
syslog	(Optional) Enable SNMP syslog traps.
vlan-membership	(Optional) Enable SNMP VLAN membership traps.
vtp	(Optional) Enable VLAN Trunking Protocol (VTP) traps.

Defaults

The sending of SNMP traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(6)EA2	This command was introduced.
12.1(9)EA1	The vlan-membership keyword was added.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Use the **snmp-server enable traps** command to enable sending of traps or informs, when supported.

**Note**

Informs are not supported in SNMPv1.

To enable more than one type of trap, you must issue a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to send VTP traps to the NMS:

```
Switch(config)# snmp-server enable traps vtp
```

You can verify your setting by entering the **show vtp status** privileged EXEC or the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show running-config	Displays the running configuration on the switch. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 > Cisco IOS File Management Commands > Configuration File Commands .
snmp-server host	Specifies the host that receives SNMP traps.

snmp-server host

Use the **snmp-server host** global configuration command to specify the recipient (host) of a Simple Network Management Protocol (SNMP) notification operation. Use the **no** form of this command to remove the specified host.

```
snmp-server host host-addr [informs | traps] [version {1 | 2c | 3 [auth | noauth | priv]}]
  community-string [c2900 | cluster | config | entity | hsrp | mac-notification | rtr | snmp | tty |
  udp-port | vlan-membership | vtp]

no snmp-server host host-addr [informs | traps] [version {1 | 2c | 3 [auth | noauth | priv]}]
  community-string [c2900 | cluster | config | entity | hsrp | mac-notification | rtr | snmp | tty |
  udp-port | vlan-membership | vtp]
```

Syntax Description

<i>host-addr</i>	Name or Internet address of the host (the targeted recipient).
informs traps	(Optional) Send SNMP traps or informs to this host.
version 1 2c 3	(Optional) Version of SNMP used to send the traps. These keywords are supported: 1 —SNMPv1. This option is not available with informs. 2c —SNMPv2C. 3 —SNMPv3. These three optional keywords can follow the version 3 keyword: <ul style="list-style-type: none">• auth (Optional). Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication.• noauth (Default). The noAuthNoPriv security level. This is the default if the [auth noauth priv] keyword choice is not specified.• priv (Optional). Enables Data Encryption Standard (DES) packet encryption (also called <i>privacy</i>).
Note	The priv keyword is available only when the enhanced crypto (encrypted) software image is installed.
<i>community-string</i>	Password-like community string sent with the notification operation. Though you can set this string by using the snmp-server host command, we recommend that you define this string by using the snmp-server community global configuration command before using the snmp-server host command.
c2900	(Optional) Send SNMP switch traps.
cluster	(Optional) Send cluster member status traps.
config	(Optional) Send SNMP configuration traps.
entity	(Optional) Send SNMP entity traps.
hsrp	(Optional) Send Hot Standby Router Protocol (HSRP) traps.
mac-notification	(Optional) Send MAC notification traps.
rtr	(Optional) Send SNMP Response Time Reporter traps.
snmp	(Optional) Send SNMP-type traps.
tty	(Optional) Send Transmission Control Protocol (TCP) connection traps.

udp-port	(Optional) Send notification host's User Datagram Protocol (UDP) port number.
vlan-membership	(Optional) Send SNMP VLAN membership traps.
ftp	(Optional) Send VLAN Trunking Protocol (VTP) traps.

Defaults

This command is disabled by default. No notifications are sent.

If you enter this command with no keywords, the default is to send all trap types to the host. No informs are sent to this host.

If no **version** keyword is present, the default is version 1.

If version 3 is selected and no authentication keyword is entered, the default is the **noauth** (noAuthNoPriv) security level.



If the *community-string* is not defined by using the **snmp-server community** global configuration command before using this command, the default form of the **snmp-server community** command is automatically inserted into the configuration. The password (*community-string*) used for this automatic configuration of the **snmp-server community** will be the same as that specified in the **snmp-server host** command.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5.2)WC(1)	This command was introduced.
12.1(6)EA2	The cluster , mac-notification , and rtr keywords were added.
12.1(9)EA1	The vlan-membership keyword was added.
12.1(11)EA1	The version 3 option was added, with the auth and noauth keywords.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response PDU. If the sender never receives the response, the inform request can be sent again. Thus, informs are more likely to reach their intended destinations.

However, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Traps are also sent only once, but an inform might be retried several times. The retries increase traffic and contribute to a higher overhead on the network.

If you do not enter an **snmp-server host** command, no notifications are sent. To configure the switch to send SNMP notifications, you must enter at least one **snmp-server host** command. If you enter the command with no keywords, all trap types are enabled for the host. To enable multiple hosts, you must enter a separate **snmp-server host** command for each host. You can specify multiple notification types in the command for each host.

■ snmp-server host

When multiple **snmp-server host** commands are given for the same host and kind of notification (trap or inform), each succeeding command overwrites the previous command. Only the last **snmp-server host** command is in effect. For example, if you enter an **snmp-server host inform** command for a host and then enter another **snmp-server host inform** command for the same host, the second command replaces the first.

The **snmp-server host** command is used with the **snmp-server enable traps** global configuration command. Use the **snmp-server enable traps** command to specify which SNMP notifications are sent globally. For a host to receive most notifications, at least one **snmp-server enable traps** command and the **snmp-server host** command for that host must be enabled. Some notification types cannot be controlled with the **snmp-server enable traps** command. For example, some notification types are always enabled. Other notification types are enabled by a different command.

The **no snmp-server host** command with no keywords disables traps, but not informs, to the host. To disable informs, use the **no snmp-server host informs** command.

Examples

This example shows how to configure a unique SNMP community string named *comaccess* for traps and prevent SNMP polling access with this string through access-list 10:

```
Switch(config)# snmp-server community comaccess ro 10
Switch(config)# snmp-server host 172.20.2.160 comaccess
Switch(config)# access-list 10 deny any
```

This example shows how to send the SNMP traps to the host specified by the name *myhost.cisco.com*. The community string is defined as *comaccess*:

```
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server host myhost.cisco.com comaccess snmp
```

This example shows how to enable the switch to send all traps to the host *myhost.cisco.com* using the community string *public*:

```
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server host myhost.cisco.com public
```

Related Commands

Command	Description
show running-config	Displays the running configuration on the switch. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 > Cisco IOS File Management Commands > Configuration File Commands .
snmp-server enable traps	Enables SNMP notification for various trap types.

snmp trap mac-notification

Use the **snmp trap mac-notification** interface configuration command to enable the MAC notification traps on a port. Use the **no** form of this command to disable the traps and to return the port to default settings.

snmp trap mac-notification [added | removed]

no snmp trap mac-notification [added | removed]

Syntax Description	added (Optional) Enable MAC notification traps when a MAC address is added to a port. removed (Optional) Enable MAC notification traps when a MAC address is removed from a port.
---------------------------	--

Defaults	The Simple Network Management Protocol (SNMP) address-addition and address-removal traps are disabled.
-----------------	--

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

Command History	Release	Modification
	12.1(6)EA2	This command was introduced.

Usage Guidelines	Even though you enable the notification trap for a specific interface by using the snmp trap mac-notification command, the trap is generated only when you enter the snmp-server enable traps mac-notification and the mac address-table notification global configuration commands.
-------------------------	---

Examples	This example shows how to enable an address-addition trap on a port:
-----------------	--

```
Switch(config-if)# snmp trap mac-notification added
```

This example shows how to enable an address-removal trap on a port:

```
Switch(config-if)# snmp trap mac-notification removed
```

You can verify your settings by entering the **show mac address-table notification** privileged EXEC command.

Related Commands	Command	Description
	clear mac address-table notification	Clears the MAC address notification global counters.
	mac address-table notification	Enables the MAC notification feature on a switch.

■ snmp trap mac-notification

Command	Description
show mac address-table notification	Displays MAC notification parameters.
snmp-server enable traps	Enables SNMP notification for various trap types.

spanning-tree backbonefast

Use the **spanning-tree backbonefast** global configuration command to enable the BackboneFast feature. Use the **no** form of this command to return to the default setting.

spanning-tree backbonefast

no spanning-tree backbonefast

Syntax Description This command has no arguments or keywords.

Defaults BackboneFast is disabled.

Command Modes Global configuration

Command History	Release	Modification
	12.1(6)EA2	This command was introduced.

Usage Guidelines The BackboneFast feature is supported only when the switch is running per-VLAN spanning-tree (PVST).

BackboneFast is started when a root port or blocked port on a switch receives inferior bridge protocol data units (BPDUs) from its designated bridge. An inferior BPDU identifies one switch as both the root bridge and the designated bridge. When a switch receives an inferior BPDU, it means that a link to which the switch is not directly connected (an *indirect* link) has failed (that is, the designated bridge has lost its connection to the root switch). If there are alternate paths to the root switch, BackboneFast causes the maximum aging time on the ports on which it received the inferior BPDU to expire and allows a blocked port to move immediately to the listening state. BackboneFast then transitions the interface to the forwarding state. For more information, refer to the software configuration guide for this release.

Enable BackboneFast on all supported switches to allow the detection of indirect link failures and to start the spanning-tree reconfiguration sooner.

Examples This example shows how to enable BackboneFast on the switch:

```
Switch(config)# spanning-tree backbonefast
```

You can verify your setting by entering the **show spanning-tree summary** privileged EXEC command.

Related Commands	Command	Description
	show spanning-tree summary	Displays a summary of the spanning-tree port states.

■ **spanning-tree bpdufilter**

spanning-tree bpdufilter

Use the **spanning-tree bpdufilter** interface configuration command to prevent a port from sending or receiving bridge protocol data units (BPDUs). Use the **no** form of this command to return to the default setting.

```
spanning-tree bpdufilter {disable | enable}
```

```
no spanning-tree bpdufilter
```

Syntax Description	disable Disable BPDU filtering on the specified interface. enable Enable BPDU filtering on the specified interface.
---------------------------	--

Defaults	BPDU filtering is disabled.
-----------------	-----------------------------

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

Command History	Release	Modification
	12.1(9)EA1	This command was introduced.

Usage Guidelines	You can enable the BPDU filtering feature when the switch is operating in the per-VLAN spanning-tree (PVST) or the multiple spanning-tree (MST) mode. The MST mode is available only if you have the enhanced software image (EI) installed on your switch.
-------------------------	---


Caution

Enabling BPDU filtering on an interface is the same as disabling spanning tree on it and can result in spanning-tree loops.

You can globally enable BPDU filtering on all Port Fast-enabled ports by using the **spanning-tree portfast bpdufilter default** global configuration command.

You can use the **spanning-tree bpdufilter** interface configuration command to override the setting of the **spanning-tree portfast bpdufilter default** global configuration command.

Examples

This example shows how to enable the BPDU filtering feature on a port:

```
Switch(config)# interface fastethernet0/1  
Switch(config-if)# spanning-tree bpdufilter enable
```

You can verify your setting by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show running-config	Displays the current operating configuration. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 > Cisco IOS File Management Commands > Configuration File Commands .
spanning-tree portfast (global configuration)	Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled ports or enables the Port Fast feature on all nontrunking ports.
spanning-tree portfast (interface configuration)	Enables the Port Fast feature on an interface and all its associated VLANs.

■ **spanning-tree bpduguard**

spanning-tree bpduguard

Use the **spanning-tree bpduguard** interface configuration command to put a port in the error-disabled state when it receives a bridge protocol data unit (BPDU). Use the **no** form of this command to return to the default setting.

spanning-tree bpduguard {disable | enable}

no spanning-tree bpduguard

Syntax Description	disable Disable BPDU guard on the specified interface. enable Enable BPDU guard on the specified interface.
---------------------------	--

Defaults BPDU guard is disabled.

Command Modes Interface configuration

Command History	Release	Modification
	12.1(9)EA1	This command was introduced.

Usage Guidelines The BPDU guard feature provides a secure response to invalid configurations because you must manually put the port back in service. Use the BPDU guard feature in a service-provider network to prevent a port from being included in the spanning-tree topology.

You can enable the BPDU guard feature when the switch is operating in the per-VLAN spanning-tree (PVST) or the multiple spanning-tree (MST) mode. The MST mode is available only if you have the enhanced software image (EI) installed on your switch.

You can globally enable BPDU guard on all Port Fast-enabled ports by using the **spanning-tree portfast bpduguard default** global configuration command.

You can use the **spanning-tree bpduguard** interface configuration command to override the setting of the **spanning-tree portfast bpduguard default** global configuration command.

Examples This example shows how to enable the BPDU guard feature on a port:

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# spanning-tree bpduguard enable
```

You can verify your setting by entering the **show running-config** privileged EXEC command.

Related Commands	Command	Description
	show running-config	Displays the current operating configuration. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 > Cisco IOS File Management Commands > Configuration File Commands .
	spanning-tree portfast (global configuration)	Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled ports or enables the Port Fast feature on all nontrunking ports.
	spanning-tree portfast (interface configuration)	Enables the Port Fast feature on an interface and all its associated VLANs.

spanning-tree cost

spanning-tree cost

Use the **spanning-tree cost** interface configuration command to set the path cost for spanning-tree calculations. If a loop occurs, spanning tree considers the path cost when selecting an interface to place in the forwarding state. Use the **no** form of this command to return to the default setting.

spanning-tree [vlan *vlan-id*] cost *cost*

no spanning-tree [vlan *vlan-id*] cost

Syntax Description	vlan <i>vlan-id</i> (Optional) VLAN ID associated with a spanning-tree instance. The range is 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1005 when the standard software image (SI) is installed. Do not enter leading zeros. cost Path cost can range from 1 to 200000000, with higher values meaning higher costs.
---------------------------	--

Defaults The default path cost is computed from the interface bandwidth setting. These are the IEEE default path cost values:

- 10 Mbps—100
- 100 Mbps—19
- 155 Mbps—14
- 1000 Mbps—4
- 1 Gbps—4
- 10 Gbps—2
- Speeds greater than 10 Gbps—1

Command Modes Interface configuration

Command History	Release	Modification
	12.0(5.2)WC(1)	This command was introduced.
	12.1(9)EA1	The range for the <i>cost</i> variable increased.

Usage Guidelines When you configure the cost, higher values represent higher costs.

You can set a cost on a VLAN that does not exist. The setting takes effect when the VLAN exists.

Examples This example shows how to set a path cost of 250 on an interface (an access port):

```
Switch(config)# interface fastethernet0/4
Switch(config-if)# spanning-tree cost 250
```

This example shows how to set a path cost of 300 for VLAN 10 on an interface that is a trunk port:

```
Switch(config-if)# spanning-tree vlan 10 cost 300
```

You can verify your settings by entering the **show spanning-tree interface *interface-id*** privileged EXEC command.

Related Commands

Command	Description
show spanning-tree interface <i>interface-id</i>	Displays spanning-tree information for the specified interface.
spanning-tree port-priority	Configures an interface priority.
spanning-tree vlan priority	Sets the switch priority for the specified spanning-tree instance.

■ **spanning-tree extend system-id**

spanning-tree extend system-id

Use the **spanning-tree extend system-id** global configuration command to enable the extended system ID feature.

spanning-tree extend system-id



Note

Though visible in the command-line help strings, the **no** version of this command is not supported. You cannot disable the extended system ID feature.

Syntax Description This command has no arguments or keywords.

Defaults The extended system ID is enabled.

Command Modes Global configuration

Command History	Release	Modification
	12.1(9)EA1	This command was introduced.

Usage Guidelines In Release 12.1(9)EA1 and later, the switches support the 802.1T spanning-tree extensions, and some of the bits previously used for the switch priority are now used for the extended system ID (VLAN identifier for the per-VLAN spanning-tree [PVST] or an instance identifier for the multiple spanning tree [MST]). In earlier releases, the switch priority is a 16-bit value.

The spanning tree uses the extended system ID, the switch priority, and the allocated spanning-tree MAC address to make the bridge ID unique for each VLAN or multiple spanning-tree instance. With earlier releases, spanning tree used one MAC address per VLAN to make the bridge ID unique for each VLAN.

Support for the extended system ID affects how you manually configure the root switch, the secondary root switch, and the switch priority of a VLAN. For more information, see the “[spanning-tree mst root](#)” and the “[spanning-tree vlan](#)” sections.

If your network consists of switches that do not support the extended system ID and switches that do support it, it is unlikely that the switch with the extended system ID support will become the root switch. The extended system ID increases the switch priority value every time the VLAN number is greater than the priority of the connected switches running older software.

Related Commands	Command	Description
	show spanning-tree summary	Displays a summary of spanning-tree port states.
	spanning-tree mst root	Configures the multiple spanning-tree (MST) root switch priority and timers based on the network diameter.
	spanning-tree vlan priority	Sets the switch priority for the specified spanning-tree instance.

spanning-tree guard

Use the **spanning-tree guard** interface configuration command to enable root guard or loop guard on all the VLANs associated with the selected interface. Root guard restricts which interface is allowed to be the spanning-tree root port or the path-to-the root for the switch. Loop guard prevents alternate or root ports from becoming designated ports when a failure creates a unidirectional link. Use the **no** form of this command to return to the default setting.

spanning-tree guard {loop | none | root}

no spanning-tree guard

Syntax Description	loop	Enable loop guard.
	none	Disable root guard or loop guard.
	root	Enable root guard.

Defaults

Root guard is disabled.

Loop guard is configured according to the **spanning-tree loopguard default** global configuration command (globally disabled).

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

Command History	Release	Modification
	12.1(6)EA2	This command was introduced. It replaced the spanning-tree rootguard command.
	12.1(9)EA1	The loop keyword was added.

Usage Guidelines

You can enable root guard or loop guard when the switch is operating in the per-VLAN spanning-tree (PVST) or the multiple spanning-tree (MST) mode. However, you cannot enable both features at the same time. The MST mode is available only if you have the enhanced software image (EI) installed on your switch.

When root guard is enabled, if spanning-tree calculations cause a port to be selected as the root port, the port transitions to the root-inconsistent (blocked) state to prevent the customer's switch from becoming the root switch or being in the path to the root. The root port provides the best path from the switch to the root switch.

When the **no spanning-tree guard** or the **no spanning-tree guard none** command is entered, root guard is disabled for all VLANs on the selected interface. If this interface is in the root-inconsistent (blocked) state, it automatically transitions to the listening state.

Do not enable root guard on interfaces that will be used by the UplinkFast feature. With UplinkFast, the backup interfaces (in the blocked state) replace the root port in the case of a failure. However, if root guard is also enabled, all the backup interfaces used by the UplinkFast feature are placed in the root-inconsistent state (blocked) and prevented from reaching the forwarding state. The UplinkFast feature is not available when the switch is operating in MST mode.

Loop guard is most effective when it is configured on the entire switched network. When the switch is operating in PVST mode, loop guard prevents alternate and root ports from becoming designated ports, and spanning tree does not send bridge protocol data units (BPDUs) on root or alternate ports. When the switch is operating in MST mode, BPDUs are not sent on nonboundary ports only if the port is blocked by loop guard in all MST instances. On a boundary port, loop guard blocks the port in all MST instances.

To disable root guard or loop guard, use the **spanning-tree guard none** interface configuration command. You cannot enable both root guard and loop guard at the same time.

You can override the setting of the **spanning-tree loopguard default** global configuration command by using the **spanning-tree guard loop** interface configuration command.

Examples

This example shows how to enable root guard on all the VLANs associated with the specified interface:

```
Switch(config)# interface fastethernet0/3
Switch(config-if)# spanning-tree guard root
```

This example shows how to enable loop guard on all the VLANs associated with the specified interface:

```
Switch(config)# interface fastethernet0/3
Switch(config-if)# spanning-tree guard loop
```

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

Related Commands

Command	Description
show running-config	Displays the current operating configuration. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 > Cisco IOS File Management Commands > Configuration File Commands .
spanning-tree cost	Sets the path cost for spanning-tree calculations.
spanning-tree loopguard default	Prevents alternate or root ports from becoming designated ports because of a failure that leads to a unidirectional link.
spanning-tree mst cost	Configures the path cost for MST calculations.
spanning-tree mst port-priority	Configures an interface priority.
spanning-tree mst root	Configures the MST root switch priority and timers based on the network diameter.
spanning-tree port-priority	Configures an interface priority.
spanning-tree vlan priority	Sets the switch priority for the specified spanning-tree instance.

spanning-tree link-type

spanning-tree link-type

Use the **spanning-tree link-type** interface configuration command to override the default link-type setting, which is determined by the duplex mode of the port, and to enable Rapid Spanning-Tree Protocol (RSTP) transitions to the forwarding state. Use the **no** form of this command to return to the default setting.

spanning-tree link-type {point-to-point | shared}

no spanning-tree link-type

Syntax Description

point-to-point	Specify that the link type of a port is point-to-point.
shared	Specify that the link type of a port is shared.

Defaults

The switch derives the link type of a port from the duplex mode. A full-duplex port is considered a point-to-point link, and a half-duplex port is considered a shared link.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(9)EA1	This command was introduced.

Usage Guidelines

You can override the default setting of the link type by using the **spanning-tree link-type** command; for example, a half-duplex link can be physically connected point-to-point to a single port on a remote switch running RSTP and be enabled for rapid transitions.

Examples

This example shows how to specify the link type as shared (regardless of the duplex setting) and to prevent RSTP rapid transitions to the forwarding state:

```
Switch(config-if)# spanning-tree link-type shared
```

You can verify your settings by entering the **show spanning-tree mst interface *interface-id*** privileged EXEC command.

Related Commands

Command	Description
show spanning-tree mst interface <i>interface-id</i>	Displays multiple spanning-tree (MST) information for the specified interface.

spanning-tree loopguard default

Use the **spanning-tree loopguard default** global configuration command to prevent alternate or root ports from becoming designated ports because of a failure that leads to a unidirectional link. Use the **no** form of this command to return to the default setting.

spanning-tree loopguard default

no spanning-tree loopguard default

Syntax Description This command has no arguments or keywords.

Defaults Loop guard is disabled.

Command Modes Global configuration

Command History	Release	Modification
	12.1(9)EA1	This command was introduced.

Usage Guidelines You can enable the loop guard feature when the switch is operating in the per-VLAN spanning-tree (PVST) or the multiple spanning-tree (MST) mode. The MST mode is available only if you have the enhanced software image (EI) installed on your switch.

Loop guard is most effective when it is configured on the entire switched network. When the switch is operating in PVST mode, loop guard prevents alternate and root ports from becoming designated ports, and spanning tree does not send bridge protocol data units (BPDUs) on root or alternate ports. When the switch is operating in MST mode, BPDUs are not sent on nonboundary ports only if the port is blocked by loop guard in all MST instances. On a boundary port, loop guard blocks the port in all MST instances.

Loop guard operates only on ports that are considered point-to-point by the spanning tree.

You can override the setting of the **spanning-tree loopguard default** global configuration command by using the **spanning-tree guard loop** interface configuration command.

Examples This example shows how to globally enable loop guard:

```
Switch(config)# spanning-tree loopguard default
```

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

■ **spanning-tree loopguard default**

Related Commands	Command	Description
	show running-config	Displays the current operating configuration. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 > Cisco IOS File Management Commands > Configuration File Commands .
	spanning-tree guard loop	Enables the loop guard feature on all the VLANs associated with the specified interface.

spanning-tree mode

Use the **spanning-tree mode** global configuration command to enable either per-VLAN spanning-tree (PVST) or multiple spanning tree (MST) on your switch. Use the **no** form of this command to return to the default setting.

spanning-tree mode {mst | pvst}

no spanning-tree mode

Syntax Description	mst Enable MST. This keyword is available only if your switch is running the enhanced software image (EI). pvst Enable PVST.
---------------------------	---

Defaults	The default mode is PVST.
-----------------	---------------------------

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

Command History	Release	Modification
	12.1(9)EA1	This command was introduced.

Usage Guidelines	You cannot run both PVST and MST at the same time.
-------------------------	--



Caution Changing spanning-tree modes can disrupt traffic because all spanning-tree instances are stopped for the previous mode and restarted in the new mode.

Examples	This example shows to enable MST on the switch:
-----------------	---

```
Switch(config)# spanning-tree mode mst
```

You can verify your setting by entering the **show running-config** privileged EXEC command.

Related Commands	Command	Description
	show running-config	Displays the current operating configuration. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 > Cisco IOS File Management Commands > Configuration File Commands .

■ **spanning-tree mst configuration**

spanning-tree mst configuration

Use the **spanning-tree mst configuration** global configuration command to enter multiple spanning-tree (MST) configuration mode through which you configure the MST region. Use the **no** form of this command to return to the default settings.

spanning-tree mst configuration

no spanning-tree mst configuration

This command is available only if your switch is running the enhanced software image (EI).

Syntax Description This command has no arguments or keywords.

Defaults The default mapping is that all VLANs are mapped to the common and internal spanning tree (CIST) instance (instance 0).

The default name is an empty string.

The revision number is 0.

Command Modes Global configuration

Command History	Release	Modification
	12.1(9)EA1	This command was introduced.

Usage Guidelines Entering the **spanning-tree mst configuration** command enables the MST configuration mode. These configuration commands are available:

- **abort**: exits the MST region configuration mode without applying configuration changes.
- **exit**: exits the MST region configuration mode and applies all configuration changes.
- **instance *instance-id* *vlan* *vlan-range***: maps VLANs to an MST instance. The range for the *instance-id* is 1 to 15; the range for *vlan-range* is 1 to 4094. Do not enter leading zeros.
- **name *name***: sets the configuration name. The *name* string has a maximum length of 32 characters and is case sensitive.
- **no**: negates the **instance**, **name**, and **revision** commands or sets them to their defaults.
- **private-vlan**: Though visible in the command-line help strings, this command is not supported.
- **revision *version***: sets the configuration revision number. The range is 0 to 65535.
- **show [current | pending]**: displays the current or pending MST region configuration.

When you map VLANs to an MST instance, the mapping is incremental, and the range of VLANs specified is added or removed to the existing ones. To specify a range, use a hyphen; for example, **instance 1 vlan 1-63** maps VLANs 1 to 63 to MST instance 1. To specify a series, use a comma; for example, **instance 1 vlan 10, 20, 30** maps VLANs 10, 20, and 30 to MST instance 1.

All VLANs that are not explicitly mapped to an MST instance are mapped to the common and internal spanning tree (CIST) instance (instance 0) and cannot be unmapped from the CIST by using the **no** form of the command.

For two or more switches to be in the same MST region, they must have the same VLAN mapping, the same configuration revision number, and the same name.

Examples

This example shows how to enter MST configuration mode, map VLAN 10 to 20 to MST instance 1, name the region *region1*, set the configuration revision to 1, display the pending configuration, apply the changes, and return to global configuration mode:

```
Switch# spanning-tree mst configuration
Switch(config-mst)# instance 1 vlan 10-20
Switch(config-mst)# name region1
Switch(config-mst)# revision 1
Switch(config-mst)# show pending
Pending MST configuration
Name      [region1]
Revision  1
Instance  Vlans Mapped
-----
0        1-9,21-4094
1        10-20
-----
Switch(config-mst)# exit
Switch(config)#
```

This example shows how to add VLANs 1 to 100 to the ones already mapped (if any) to instance 2, to move VLANs 40 to 60 that were previously mapped to instance 2 to the CIST instance, to add VLAN 10 to instance 10, and to remove all the VLANs mapped to instance 2 and map them to the CIST instance:

```
Switch(config-mst)# instance 2 vlan 1-100
Switch(config-mst)# no instance 2 vlan 40-60
Switch(config-mst)# instance 10 vlan 10
Switch(config-mst)# no instance 2
```

You can verify your settings by entering the **show pending** MST configuration command.

Related Commands

Command	Description
show spanning-tree mst configuration	Displays the MST region configuration.

■ **spanning-tree mst cost**

spanning-tree mst cost

Use the **spanning-tree mst cost** interface configuration command to set the path cost for multiple spanning-tree (MST) calculations. If a loop occurs, spanning tree considers the path cost when selecting an interface to put in the forwarding state. Use the **no** form of this command to return to the default setting.

spanning-tree mst *instance-id* cost *cost*

no spanning-tree mst *instance-id* cost

This command is available only if your switch is running the enhanced software image (EI).

Syntax Description

<i>instance-id</i>	ID associated with a spanning-tree instance. The range is 0 to 15.
<i>cost</i>	Path cost is 1 to 200000000, with higher values meaning higher costs.

Defaults

The default path cost is computed from the interface bandwidth setting. These are the IEEE default path cost values:

- 1000 Mbps—20000
- 100 Mbps—200000
- 10 Mbps—2000000

Command Modes

Interface configuration

Command History

Release	Modification
12.1(9)EA1	This command was introduced.

Usage Guidelines

When you configure the cost, higher values represent higher costs.

Examples

This example shows how to set a path cost of 250 on an interface associated with instance 2:

```
Switch(config)# interface fastethernet0/4
Switch(config-if)# spanning-tree mst 2 cost 250
```

You can verify your settings by entering the **show spanning-tree mst interface *interface-id*** privileged EXEC command.

Related Commands	Command	Description
	show spanning-tree mst interface <i>interface-id</i>	Displays MST information for the specified interface.
	spanning-tree mst port-priority	Configures an interface priority.
	spanning-tree mst priority	Configures the switch priority for the specified spanning-tree instance.

■ **spanning-tree mst forward-time**

spanning-tree mst forward-time

Use the **spanning-tree mst forward-time** global configuration command to set the forward-delay time for all multiple spanning-tree (MST) instances. The forwarding time determines how long each of the listening and learning states last before the interface begins forwarding. Use the **no** form of this command to return to the default setting.

spanning-tree mst forward-time *seconds*

no spanning-tree mst forward-time

This command is available only if your switch is running the enhanced software image (EI).

Syntax Description	<i>seconds</i>	Length of the listening and learning states. The range is 4 to 30 seconds.
Defaults	The default is 15 seconds.	
Command Modes	Global configuration	
Command History	Release	Modification
	12.1(9)EA1	This command was introduced.
Usage Guidelines	Changing the spanning-tree mst forward-time command affects all spanning-tree instances.	
Examples	<p>This example shows how to set the spanning-tree forwarding time to 18 seconds for all MST instances:</p> <pre>Switch(config)# spanning-tree mst forward-time 18</pre> <p>You can verify your settings by entering the show spanning-tree mst privileged EXEC command.</p>	
Related Commands	Command	Description
	show spanning-tree mst	Displays MST information.
	spanning-tree mst hello-time	Sets the interval between hello bridge protocol data units (BPDUs) sent by root switch configuration messages.
	spanning-tree mst max-age	Sets the interval between messages that the spanning tree receives from the root switch.
	spanning-tree mst max-hops	Sets the number of hops in a region before the BPDU is discarded.

spanning-tree mst hello-time

Use the **spanning-tree mst hello-time** global configuration command to set the interval between hello bridge protocol data units (BPDUs) sent by root switch configuration messages. Use the **no** form of this command to return to the default setting.

spanning-tree mst hello-time *seconds*

no spanning-tree mst hello-time

This command is available only if your switch is running the enhanced software image (EI).

Syntax Description	<i>seconds</i>	Interval between hello BPDUs sent by root switch configuration messages. The range is 1 to 10 seconds.
---------------------------	----------------	--

Defaults	The default is 2 seconds.
-----------------	---------------------------

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

Command History	Release	Modification
	12.1(9)EA1	This command was introduced.

Usage Guidelines	After you set the spanning-tree mst max-age <i>seconds</i> global configuration command, if a switch does not receive BPDUs from the root switch within the specified interval, the switch recomputes the spanning-tree topology. The max-age setting must be greater than the hello-time setting. Changing the spanning-tree mst hello-time command affects all spanning-tree instances.
-------------------------	--

Examples	This example shows how to set the spanning-tree hello time to 3 seconds for all MST instances: Switch(config)# spanning-tree mst hello-time 3
	You can verify your settings by entering the show spanning-tree mst privileged EXEC command.

■ **spanning-tree mst hello-time**

Related Commands	Command	Description
	show spanning-tree mst	Displays multiple spanning-tree (MST) information.
	spanning-tree mst forward-time	Sets the forward-delay time for all MST instances.
	spanning-tree mst max-age	Sets the interval between messages that the spanning tree receives from the root switch.
	spanning-tree mst max-hops	Sets the number of hops in a region before the BPDU is discarded.

spanning-tree mst max-age

Use the **spanning-tree mst max-age** global configuration command to set the interval between messages that the spanning tree receives from the root switch. If a switch does not receive a bridge protocol data unit (BPDU) message from the root switch within this interval, it recomputes the spanning-tree topology. Use the **no** form of this command to return to the default setting.

spanning-tree mst max-age *seconds*

no spanning-tree mst max-age

This command is available only if your switch is running the enhanced software image (EI).

Syntax Description	<i>seconds</i> Interval between messages the spanning tree receives from the root switch. If a switch does not receive a BPDU message from the root switch within this interval, it recomputes the spanning-tree topology. The range is 6 to 40 seconds.
---------------------------	--

Defaults	The default is 20 seconds.
-----------------	----------------------------

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

Command History	Release	Modification
	12.1(9)EA1	This command was introduced.

Usage Guidelines	After you set the spanning-tree mst max-age global configuration command, if a switch does not receive BPDUs from the root switch within the specified interval, the switch recomputes the spanning-tree topology. The max-age setting must be greater than the hello-time setting. Changing the spanning-tree mst max-age command affects all spanning-tree instances.
-------------------------	--

Examples	This example shows how to set the spanning-tree max-age to 30 seconds for all MST instances: <pre>Switch(config)# spanning-tree mst max-age 30</pre> You can verify your settings by entering the show spanning-tree mst privileged EXEC command.
-----------------	---

■ **spanning-tree mst max-age**

Related Commands	Command	Description
	show spanning-tree mst	Displays multiple spanning-tree (MST) information.
	spanning-tree mst forward-time	Sets the forward-delay time for all MST instances.
	spanning-tree mst hello-time	Sets the interval between hello BPDUs sent by root switch configuration messages.
	spanning-tree mst max-hops	Sets the number of hops in a region before the BPDU is discarded.

spanning-tree mst max-hops

Use the **spanning-tree mst max-hops** global configuration command to set the number of hops in a region before the bridge protocol data unit (BPDU) is discarded and the information held for a port is aged. Use the **no** form of this command to return to the default setting.

spanning-tree mst max-hops *hop-count*

no spanning-tree mst max-hops

This command is available only if your switch is running the enhanced software image (EI).

Syntax Description	<i>hop-count</i> Number of hops in a region before the BPDU is discarded. The range is 1 to 40 hops.
---------------------------	--

Defaults	The default is 20 hops.
-----------------	-------------------------

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

Command History	Release	Modification
	12.1(9)EA1	This command was introduced.

Usage Guidelines	The root switch of the instance always sends a BPDU (or M-record) with a cost of 0 and the hop count set to the maximum value. When a switch receives this BPDU, it decrements the received remaining hop count by one and propagates the decremented count as the remaining hop count in the generated M-records. A switch discards the BPDU and ages the information held for the port when the count reaches 0.
-------------------------	--

Changing the **spanning-tree mst max-hops** command affects all spanning-tree instances.

Examples	This example shows how to set the spanning-tree max-hops to 10 for all MST instances:
	Switch(config)# spanning-tree mst max-hops 10

You can verify your settings by entering the **show spanning-tree mst** privileged EXEC command.

spanning-tree mst max-hops

Related Commands	Command	Description
	show spanning-tree mst	Displays multiple spanning-tree (MST) information.
	spanning-tree mst forward-time	Sets the forward-delay time for all MST instances.
	spanning-tree mst hello-time	Sets the interval between hello BPDUs sent by root switch configuration messages.
	spanning-tree mst max-age	Sets the interval between messages that the spanning tree receives from the root switch.

spanning-tree mst port-priority

Use the **spanning-tree mst port-priority** interface configuration command to configure an interface priority. If a loop occurs, the Multiple Spanning Tree Protocol (MSTP) can determine which interface to put in the forwarding state. Use the **no** form of this command to return to the default setting.

spanning-tree mst *instance-id* port-priority *priority*

no spanning-tree mst *instance-id* port-priority

This command is available only if your switch is running the enhanced software image (EI).

Syntax Description	<i>instance-id</i> ID associated with a spanning-tree instance. The range is 0 to 15. <i>priority</i> Number from 0 to 255. The lower the number, the higher the priority.
---------------------------	---

Defaults	The default is 128.
-----------------	---------------------

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

Command History	Release	Modification
	12.1(9)EA1	This command was introduced.

Usage Guidelines	You can assign higher priority values (lower numerical values) to interfaces that you want selected first and lower priority values (higher numerical values) that you want selected last. If all interfaces have the same priority value, the MST puts the interface with the lowest interface number in the forwarding state and blocks other interfaces.
-------------------------	---

Examples	This example shows how to increase the likelihood that the interface associated with spanning-tree instance 20 is placed into the forwarding state if a loop occurs:
-----------------	--

```
Switch(config)# interface fastethernet0/2
Switch(config-if)# spanning-tree mst 20 port-priority 0
```

You can verify your settings by entering the **show spanning-tree mst interface *interface-id*** privileged EXEC command.

■ **spanning-tree mst port-priority**

Related Commands	Command	Description
	show spanning-tree mst interface <i>interface-id</i>	Displays MST information for the specified interface.
	spanning-tree mst cost	Sets the path cost for MST calculations.
	spanning-tree mst priority	Sets the switch priority for the specified spanning-tree instance.

spanning-tree mst priority

Use the **spanning-tree mst priority** global configuration command to set the switch priority for the specified spanning-tree instance. Use the **no** form of this command to return to the default setting.

spanning-tree mst *instance-id* priority *priority*

no spanning-tree mst *instance-id* priority

This command is available only if your switch is running the enhanced software image (EI).

Syntax Description	<p><i>instance-id</i> ID associated with a spanning-tree instance. The range is 0 to 15.</p> <p><i>priority</i> Set the switch priority for the specified spanning-tree instance. This setting affects the likelihood that the switch is selected as the root switch. A lower value increases the probability that the switch is selected as the root switch.</p> <p>The range is 0 to 61440 in increments of 4096. Valid priority values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected.</p>
---------------------------	--

Defaults	The default is 32768.
-----------------	-----------------------

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

Command History	Release	Modification
	12.1(9)EA1	This command was introduced.

Examples	This example shows how to set the spanning-tree priority to 8192 for multiple spanning-tree (MST) instance 20:
	<pre>Switch(config)# spanning-tree mst 20 priority 8192</pre>

You can verify your settings by entering the **show spanning-tree mst *instance-id*** privileged EXEC command.

Related Commands	Command	Description
	show spanning-tree mst <i>instance-id</i>	Displays MST information for the specified interface.
	spanning-tree mst cost	Sets the path cost for MST calculations.
	spanning-tree mst port-priority	Configures an interface priority.

 spanning-tree mst root

spanning-tree mst root

Use the **spanning-tree mst root** global configuration command to configure the multiple spanning-tree (MST) root switch priority and timers based on the network diameter. Use the **no** form of this command to return to the default setting.

spanning-tree mst *instance-id* root {primary | secondary} [diameter *net-diameter* [hello-time *seconds*]]]

no spanning-tree mst *instance-id* root

This command is available only if your switch is running the enhanced software image (EI).

Syntax Description

<i>instance-id</i>	ID associated with a MST instance. The range is 0 to 15.
root primary	Force this switch to be the root switch.
root secondary	Set this switch to be the root switch should the primary root switch fail.
diameter <i>net-diameter</i>	Set the maximum number of switches between any two end stations. The range is 2 to 7. This keyword is available only for MST instance 0.
hello-time <i>seconds</i>	Set the interval between hello bridge protocol data units (BPDUs) sent by the root switch configuration messages. The range is 1 to 10 seconds. This keyword is available only for MST instance 0.

Defaults

The primary root switch priority is 24576.

The secondary root switch priority is 28672.

The hello time is 2 seconds.

Command Modes

Global configuration

Command History

	Release	Modification
	12.1(9)EA1	This command was introduced.

Usage Guidelines

Use the **spanning-tree mst *instance-id* root** command used only on backbone switches.

When you enter the **spanning-tree mst *instance-id* root** command, the software tries to set a high enough priority to make this switch the root of the spanning-tree instance. Because of the extended system ID support, the switch sets the switch priority for the instance to 24576 if this value will cause this switch to become the root for the specified instance. If any root switch for the specified instance has a switch priority lower than 24576, the switch sets its own priority to 4096 less than the lowest switch priority. (4096 is the value of the least-significant bit of a 4-bit switch priority value.)

When you enter the **spanning-tree mst *instance-id* root secondary** command, because of support for the extended system ID, the software changes the switch priority from the default value (32768) to 28672. If the root switch fails, this switch becomes the next root switch (if the other switches in the network use the default switch priority of 32768 and are therefore unlikely to become the root switch).

Examples

This example shows how to configure the switch as the root switch for instance 10 with a network diameter of 4:

```
Switch(config)# spanning-tree mst 10 root primary diameter 4
```

This example shows how to configure the switch as the secondary root switch for instance 10 with a network diameter of 4:

```
Switch(config)# spanning-tree mst 10 root secondary diameter 4
```

You can verify your settings by entering the **show spanning-tree mst *instance-id*** privileged EXEC command.

Related Commands

Command	Description
show spanning-tree mst <i>instance-id</i>	Displays MST information for the specified instance.
spanning-tree mst forward-time	Sets the forward-delay time for all MST instances.
spanning-tree mst hello-time	Sets the interval between hello BPDUs sent by root switch configuration messages.
spanning-tree mst max-age	Sets the interval between messages that the spanning tree receives from the root switch.
spanning-tree mst max-hops	Sets the number of hops in a region before the BPDU is discarded.

spanning-tree port-priority

spanning-tree port-priority

Use the **spanning-tree port-priority** interface configuration command to configure an interface priority. If a loop occurs, spanning tree can determine which interface to put in the forwarding state. Use the **no** form of this command to return to the default setting.

spanning-tree [vlan *vlan-id*] port-priority *priority*

no spanning-tree [vlan *vlan-id*] port-priority

Syntax Description	vlan <i>vlan-id</i> (Optional) VLAN ID associated with a spanning-tree instance. The range is 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1005 when the standard software image (SI) is installed. Do not enter leading zeros. priority Number from 0 to 255. The lower the number, the higher the priority.
---------------------------	---

Defaults	The default is 128.
-----------------	---------------------

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

Command History	Release	Modification
	12.0(5.2)WC(1)	This command was introduced.

Usage Guidelines	If the variable <i>vlan-id</i> is omitted, the command applies to the spanning-tree instance associated with VLAN 1.
-------------------------	--

You can set the priority on a VLAN that has no interfaces assigned to it. The setting takes effect when you assign the interface to the VLAN.

Examples	This example shows how to increase the likelihood that the Fast Ethernet interface 0/2 will be put in the forwarding state if a loop occurs:
-----------------	--

```
Switch(config)# interface fastethernet0/2
Switch(config-if)# spanning-tree vlan 20 port-priority 0
```

You can verify your settings by entering the **show spanning-tree interface *interface-id*** privileged EXEC command.

Related Commands	Command	Description
	show spanning-tree interface <i>interface-id</i>	Displays spanning-tree information for the specified interface.
	spanning-tree cost	Sets the path cost for spanning-tree calculations.
	spanning-tree vlan priority	Sets the switch priority for the specified spanning-tree instance.

■ **spanning-tree portfast (global configuration)**

spanning-tree portfast (global configuration)

Use the **spanning-tree portfast** global configuration command to globally enable bridge protocol data unit (BPDU) filtering on Port Fast-enabled ports, the BPDU guard feature on Port Fast-enabled ports, or the Port Fast feature on all nontrunking ports. The BPDU filtering feature prevents the switch port from sending or receiving BPDUs. The BPDU guard feature puts Port Fast-enabled ports that receive BPDU in an error-disabled state. Use the **no** form of this command to return to the default setting.

```
spanning-tree portfast {bpdufilter default | bpduguard default | default}
```

```
no spanning-tree portfast {bpdufilter default | bpduguard default | default}
```

Syntax Description	bpdufilter default Globally enable BPDU filtering on Port Fast-enabled ports and prevent the switch port connected to end stations from sending or receiving BPDU. bpduguard default Globally enable the BPDU guard feature on Port Fast-enabled ports and place the ports that receive BPDU in an error-disabled state. default Globally enable the Port Fast feature on all nontrunking ports. When the Port Fast feature is enabled, the port changes directly from a blocking state to a forwarding state without making the intermediate spanning-tree state changes.
---------------------------	---

Defaults	The BPDU filtering, the BPDU guard, and the Port Fast features are disabled on all ports unless they are individually configured.
-----------------	---

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

Command History	Release	Modification
	12.1(6)EA2	This command was introduced.
	12.1(9)EA1	The bpdufilter default and default keywords were added.

Usage Guidelines	You can enable these features when the switch is operating in the per-VLAN spanning-tree (PVST) or the multiple spanning-tree (MST) mode. The MST mode is available only if you have the enhanced software image (EI) installed on your switch.
-------------------------	---

Use the **spanning-tree portfast bpdufilter default** global configuration command to globally enable BPDU filtering on ports that are Port Fast-enabled (the ports are in a Port Fast-operational state). The ports still send a few BPDU at link-up before the switch begins to filter outbound BPDU. You should globally enable BPDU filtering on a switch so that hosts connected to switch ports do not receive BPDU. If a BPDU is received on a Port Fast-enabled port, the port loses its Port Fast-operational status and BPDU filtering is disabled.

You can override the **spanning-tree portfast bpdufilter default** global configuration command by using the **spanning-tree bpdufilter** interface configuration command.

**Caution**

Enabling BPDU filtering on an interface is the same as disabling spanning tree on it and can result in spanning-tree loops.

Use the **spanning-tree portfast bpduguard default** global configuration command to globally enable BPDU guard on ports that are in a Port Fast-operational state. In a valid configuration, Port Fast-enabled ports do not receive BPDUs. Receiving a BPDU on a Port Fast-enabled port signals an invalid configuration, such as the connection of an unauthorized device, and the BPDU guard feature puts the port in the error-disabled state. The BPDU guard feature provides a secure response to invalid configurations because you must manually put the port back in service. Use the BPDU guard feature in a service-provider network to prevent an access port from participating in the spanning tree.

You can override the **spanning-tree portfast bpduguard default** global configuration command by using the **spanning-tree bpduguard** interface configuration command.

Use the **spanning-tree portfast default** global configuration command to globally enable the Port Fast feature on all nontrunking ports. Configure Port Fast only on ports that connect to end stations; otherwise, an accidental topology loop could cause a data packet loop and disrupt switch and network operation. A Port Fast-enabled port moves directly to the spanning-tree forwarding state when linkup occurs without waiting for the standard forward-delay time.

You can override the **spanning-tree portfast default** global configuration command by using the **spanning-tree portfast** interface configuration command. You can use the **no spanning-tree portfast default** global configuration command to disable Port Fast on all ports unless they are individually configured with the **spanning-tree portfast** interface configuration command.

Examples

This example shows how to globally enable the BPDU filtering feature:

```
Switch(config)# spanning-tree portfast bpdufilter default
```

This example shows how to globally enable the BPDU guard feature:

```
Switch(config)# spanning-tree portfast bpduguard default
```

This example shows how to globally enable the Port Fast feature on all nontrunking ports:

```
Switch(config)# spanning-tree portfast default
```

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

Related Commands

Command	Description
show running-config	Displays the current operating configuration. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 > Cisco IOS File Management Commands > Configuration File Commands .
spanning-tree bpdufilter	Prevents a port from sending or receiving BPDUs.
spanning-tree bpduguard	Puts a port in the error-disabled state when it receives a BPDU.
spanning-tree portfast (interface configuration)	Enables the Port Fast feature on an interface in all its associated VLANs.

spanning-tree portfast (interface configuration)

spanning-tree portfast (interface configuration)

Use the **spanning-tree portfast** interface configuration command to enable the Port Fast feature on an interface in all its associated VLANs. When the Port Fast feature is enabled, the interface changes directly from a blocking state to a forwarding state without making the intermediate spanning-tree state changes. Use the **no** form of this command to return to the default setting.

spanning-tree portfast [disable | trunk]

no spanning-tree portfast

Syntax Description	disable (Optional) Disable the Port Fast feature on the specified interface. trunk (Optional) Enable the Port Fast feature on a trunking interface.
---------------------------	--

Defaults	The Port Fast feature is disabled on all interfaces; however, it is automatically enabled on dynamic-access ports.
-----------------	--

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

Command History	Release	Modification
	12.0(5.2)WC(1)	This command was introduced.
	12.1(9)EA1	The disable and trunk keywords were added.

Usage Guidelines	Use this feature only on interfaces that connect to end stations; otherwise, an accidental topology loop could cause a data packet loop and disrupt switch and network operation. You can enable this feature when the switch is operating in the per-VLAN spanning-tree (PVST) or the multiple spanning-tree (MST) mode. This feature affects all VLANs on the interface. A port with the Port Fast feature enabled is moved directly to the spanning-tree forwarding state without waiting the standard forward-time delay. You can use the spanning-tree portfast default global configuration command to globally enable the Port Fast feature on all nontrunking interfaces. However, the spanning-tree portfast interface configuration command can override the global setting. If you configure the spanning-tree portfast default global configuration command, you can enable Port Fast on a port that is not a trunk port by using the no spanning-tree portfast interface configuration command. The no spanning-tree portfast interface configuration command is the same as the spanning-tree portfast disable interface configuration command.
-------------------------	---

Examples

This example shows how to enable the Port Fast feature on an interface:

```
Switch(config)# interface fastethernet0/2
Switch(config-if)# spanning-tree portfast
```

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

Related Commands

Command	Description
show running-config	Displays the current operating configuration. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 > Cisco IOS File Management Commands > Configuration File Commands .
spanning-tree bpdufilter	Prevents a port from sending or receiving bridge protocol data units (BPDUs).
spanning-tree bpduguard	Puts a port in the error-disabled state when it receives a BPDU.
spanning-tree portfast (global configuration)	Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled ports or enables the Port Fast feature on all nontrunking ports.

spanning-tree stack-port

spanning-tree stack-port

Use the **spanning-tree stack-port** interface configuration command to enable cross-stack UplinkFast (CSUF) on an interface and to accelerate the choice of a new root port when a link or switch fails or when spanning tree reconfigures itself. Use the **no** form of this command to return to the default setting.

spanning-tree stack-port

no spanning-tree stack-port

Syntax Description This command has no arguments or keywords.

Defaults CSUF is disabled on all interfaces.

Command Modes Interface configuration

Command History	Release	Modification
	12.1(6)EA2	This command was introduced.

Usage Guidelines This command is effective only if you enable the UplinkFast feature by using the **spanning-tree uplinkfast** global configuration command.

Use this command only on access switches.

The CSUF feature is supported only when the switch is running per-VLAN spanning-tree (PVST).

You can enable CSUF only on one stack-port Gigabit Interface Converter (GBIC) interface. The stack port connects to the GigaStack GBIC multidrop backbone. If you try to enable CSUF on a Fast Ethernet or a copper-based Gigabit Ethernet port, you receive an error message.

If CSUF is already enabled on an interface and you try to enable it on another interface, you receive an error message. You must disable CSUF on the first interface before enabling it on a new interface.

Examples This example shows how to enable CSUF on the GBIC interface:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# spanning-tree stack-port
```

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

Related Commands	Command	Description
	show running-config	Displays the current operating configuration. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 > Cisco IOS File Management Commands > Configuration File Commands .
	spanning-tree uplinkfast	Accelerates the choice of a new root port when a link or switch fails or when spanning tree reconfigures itself.

spanning-tree uplinkfast

spanning-tree uplinkfast

Use the **spanning-tree uplinkfast** global configuration command to accelerate the choice of a new root port when a link or switch fails or when the spanning tree reconfigures itself. Use the **no** form of this command to return to the default setting.

spanning-tree uplinkfast [max-update-rate *pkts-per-second*]

no spanning-tree uplinkfast [max-update-rate]

Syntax Description	max-update-rate <i>pkts-per-second</i>	(Optional) The number of packets per second at which update packets are sent. The range is 0 to 65535.
---------------------------	---	--

Defaults	UplinkFast is disabled. The update rate is 150 packets per second.
-----------------	---

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

Command History	Release	Modification
	12.0(5.2)WC(1)	This command was introduced.
	12.1(6)EA2	The <i>pkts-per-second</i> range was changed to 0 to 65535.

Usage Guidelines	Use this command only on access switches. The UplinkFast feature is supported only when the switch is running per-VLAN spanning-tree (PVST). When you enable UplinkFast, it is enabled for the entire switch and cannot be enabled for individual VLANs. When UplinkFast is enabled, the switch priority of all VLANs is set to 49152. If you change the path cost to a value less than 3000 and you enable UplinkFast or UplinkFast is already enabled, the path cost of all interfaces and VLAN trunks is increased by 3000 (if you change the path cost to 3000 or above, the path cost is not altered). The changes to the switch priority and the path cost reduces the chance that the switch will become the root switch. When UplinkFast is disabled, the switch priorities of all VLANs and path costs of all interfaces are set to default values if you did not modify them from their defaults. When spanning tree detects that the root port has failed, UplinkFast immediately switches over to an alternate root port, changing the new root port directly to FORWARDING state. During this time, a topology change notification is sent. Do not enable the root guard on interfaces that will be used by the UplinkFast feature. With UplinkFast, the backup interfaces (in the blocked state) replace the root port in the case of a failure. However, if root guard is also enabled, all the backup interfaces used by the UplinkFast feature are placed in the root-inconsistent state (blocked) and prevented from reaching the forwarding state.
-------------------------	--

If you set the max-update-rate to 0, station-learning frames are not generated, so the spanning-tree topology converges more slowly after a loss of connectivity.

Examples

This example shows how to enable UplinkFast:

```
Switch(config)# spanning-tree uplinkfast
```

You can verify your setting by entering the **show spanning-tree summary** privileged EXEC command.

Related Commands

Command	Description
show spanning-tree summary	Displays a summary of the spanning-tree port states.
spanning-tree stack-port	Enables cross-stack UplinkFast (CSUF) on an interface and accelerates the choice of a new root port when a link or switch fails or when spanning tree reconfigures itself.
spanning-tree vlan root primary	Forces this switch to be the root switch.

spanning-tree vlan

spanning-tree vlan

Use the **spanning-tree vlan** global configuration command to configure spanning tree on a per-VLAN basis. Use the **no** form of this command to return to the default setting.

```
spanning-tree vlan vlan-id {forward-time seconds | hello-time seconds | max-age seconds |
priority priority | {root {primary | secondary} [diameter net-diameter |
hello-time seconds]}}}
```

```
no spanning-tree vlan vlan-id [forward-time | hello-time | max-age | priority | root]
```

Syntax Description	
vlan-id	VLAN ID associated with a spanning-tree instance. The range is 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1005 when the standard software image (SI) is installed. Do not enter leading zeros.
forward-time <i>seconds</i>	Set the forward-delay time for the specified spanning-tree instance. The forwarding time determines how long each of the listening and learning states last before the interface begins forwarding. The range is 4 to 30 seconds.
hello-time <i>seconds</i>	Set the interval between hello bridge protocol data units (BPDUs) sent by the root switch configuration messages. The range is 1 to 10 seconds.
max-age <i>seconds</i>	Set the interval between messages the spanning tree receives from the root switch. If a switch does not receive a BPDU message from the root switch within this interval, it recomputes the spanning-tree topology. The range is 6 to 40 seconds.
priority <i>priority</i>	Set the switch priority for the specified spanning-tree instance. This setting affects the likelihood that the switch is selected as the root switch. A lower value increases the probability that the switch is selected as the root switch. The range is 0 to 61440 in increments of 4096. Valid priority values are 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected.
root primary	Force this switch to be the root switch.
root secondary	Set this switch to be the root switch should the primary root switch fail.
diameter <i>net-diameter</i>	Set the maximum number of switches between any two end stations. The range is 2 to 7.

Defaults

Spanning tree is enabled on all VLANs.

The forward-delay time is 15 seconds.

The hello time is 2 seconds.

The max-age is 20 seconds.

The primary root switch priority is 24576.

The secondary root switch priority is 28672.

Command Modes

Global configuration

Command History	Release	Modification
	12.0(5.2)WC(1)	This command was introduced.
	12.1(9)EA1	The priority <i>priority</i> range changed from 1 to 65535 to 1 to 61440 (in increments of 4096).

Usage Guidelines

Disabling the STP causes the VLAN to stop participating in the spanning-tree topology. Interfaces that are administratively down remain down. Received BPDUs are forwarded like other multicast frames. The VLAN does not detect and prevent loops when STP is disabled.

You can disable the STP on a VLAN that is not currently active and verify the change by using the **show running-config** or the **show spanning-tree vlan** *vlan-id* privileged EXEC command. The setting takes effect when the VLAN is activated.

When disabling or re-enabling the STP, you must use a single command line to specify each VLAN that you want to disable or enable.

When a VLAN is disabled and then enabled, all assigned VLANs continue to be its members. However, all spanning-tree bridge parameters are returned to their previous settings (the last setting before the VLAN was disabled).

You can enable spanning-tree options on a VLAN that has no interfaces assigned to it. The setting takes effect when you assign interfaces to it.

When setting the **max-age** *seconds*, if a switch does not receive BPDUs from the root switch within the specified interval, it recomputes the spanning-tree topology. The **max-age** setting must be greater than the **hello-time** setting.

The **spanning-tree vlan** *vlan-id* **root** command should be used only on backbone switches.

When you enter the **spanning-tree vlan** *vlan-id* **root** command, the software checks the switch priority of the current root switch for each VLAN. Because of the extended system ID support, the switch sets the switch priority for the specified VLAN to 24576 if this value will cause this switch to become the root for the specified VLAN. If any root switch for the specified VLAN has a switch priority lower than 24576, the switch sets its own priority for the specified VLAN to 4096 less than the lowest switch priority. (4096 is the value of the least-significant bit of a 4-bit switch priority value.)

When you enter the **spanning-tree vlan** *vlan-id* **root secondary** command, because of support for the extended system ID, the software changes the switch priority from the default value (32768) to 28672. If the root switch should fail, this switch becomes the next root switch (if the other switches in the network use the default switch priority of 32768, and therefore, are unlikely to become the root switch).

Examples

This example shows how to disable the STP on VLAN 5:

```
Switch(config)# no spanning-tree vlan 5
```

You can verify your setting by entering the **show spanning-tree** privileged EXEC command. In this instance, VLAN 5 does not appear in the list.

This example shows how to set the spanning-tree forwarding time to 18 seconds for VLAN 20:

```
Switch(config)# spanning-tree vlan 20 forward-time 18
```

This example shows how to set the spanning-tree hello-delay time to 3 seconds for VLAN 20:

```
Switch(config)# spanning-tree vlan 20 hello-time 3
```

spanning-tree vlan

This example shows how to set spanning-tree max-age to 30 seconds for VLAN 20:

```
Switch(config)# spanning-tree vlan 20 max-age 30
```

This example shows how to reset the **max-age** parameter to the default value for spanning-tree instance 100:

```
Switch(config)# no spanning-tree vlan 100 max-age
```

This example shows how to set the spanning-tree priority to 8192 for VLAN 20:

```
Switch(config)# spanning-tree vlan 20 priority 8192
```

This example shows how to configure the switch as the root switch for VLAN 10 with a network diameter of 4:

```
Switch(config)# spanning-tree vlan 10 root primary diameter 4
```

This example shows how to configure the switch as the secondary root switch for VLAN 10 with a network diameter of 4:

```
Switch(config)# spanning-tree vlan 10 root secondary diameter 4
```

You can verify your settings by entering the **show spanning-tree vlan *vlan-id*** privileged EXEC command.

Related Commands

Command	Description
show spanning-tree vlan	Displays spanning-tree information.
spanning-tree cost	Sets the path cost for spanning-tree calculations.
spanning-tree guard	Enables the root guard or the loop guard feature for all the VLANs associated with the selected interface.
spanning-tree port-priority	Sets an interface priority.
spanning-tree portfast (global configuration)	Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled ports or enables the Port Fast feature on all nontrunking ports.
spanning-tree portfast (interface configuration)	Enables the Port Fast feature on an interface in all its associated VLANs.
spanning-tree uplinkfast	Enables the UplinkFast feature, which accelerates the choice of a new root port.

speed

Use the **speed** interface configuration command to specify the speed of a port. Use the **no** form of this command to return the port to its default value.

speed {10 | 100 | 1000 | auto | nonegotiate}

no speed



Note

You cannot configure the speed or duplex modes on Gigabit Interface Converter (GBIC) ports. However, for certain types of GBICs, you can configure speed to not negotiate (nonegotiate) if they are connected to a device that does not support autonegotiation.

Syntax Description

10	Port runs at 10 Mbps on Fast Ethernet, 10BASE-FX, or 10 100 1000 connections.
100	Port runs at 100 Mbps on Fast Ethernet, 10BASE-FX, or 10 100 1000 connections.
1000	Port runs at 1000 Mbps on Fast Ethernet, 10 100 1000, GBIC, or small form-factor pluggable (SFP) connections.
auto	Port automatically detects the appropriate setting. <ul style="list-style-type: none"> • Fast Ethernet, either 10 or 100 Mbps • 10 100 1000 at 10, 100, or 1000 Mbps • SFP at 1000 Mbps
nonegotiate	Autonegotiation is disabled, and the port runs at 1000 Mbps. This option is valid and visible only on 1000BASE-X, -LX, and -ZX GBIC ports. Gigastack GBICs and 1000BASE-T GBICs do not support the disabling of autonegotiation. Nonegotiate does not apply to LRE Gigabit ports.

Defaults

For Fast Ethernet and 10|100|1000 ports, the default is **auto**.

For 100BASE-FX ports, the default is 100 Mbps.

For GBIC-module ports, the default is 1000 Mbps.

For SFP ports, the default is **auto**.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5.2)WC(1)	This command was introduced.
12.1(11)EA1	The nonegotiate keyword was added.
12.1(11)YJ	Support for SFP connections was added.

speed**Usage Guidelines**

Applicability of this command is hardware-dependent.

Non-LRE Switches:

Except for 100BASE-FX ports, Fast Ethernet ports can be configured at 10 or 100 Mbps. The 10/100/1000 ports can be configured at 10, 100, or 1000 Mbps and operate only in the full-duplex mode.

You cannot configure the speed on GBIC interfaces, but you can configure the speed to not negotiate (**nonegotiate**) for the 1000BASE-SX, -LX, or -ZX GBICs if they are connected to devices that do not support autonegotiation. GBIC-module ports support only 1000 Mbps. The 10-Mbps and 100-Mbps speeds are not supported.

If the speed is set to **auto**, the switch negotiates with the device at the other end of the link for the speed setting and then forces the speed setting to the negotiated value. The duplex setting remains as configured on each end of the link, which could result in a duplex setting mismatch. If both the speed and duplex are set to specific values, autonegotiation is disabled.

**Note**

The 100BASE-FX ports on Catalyst 2950C-24 switches do not support the **speed** command. These ports operate only at 100 Mbps and in full-duplex mode.

LRE Switches:

In the default configurations, Long-Reach Ethernet (LRE) Gigabit ports are set to **auto**. A copper connection (10|100|1000) autonegotiates with the device at the other end of the link for the speed setting and then forces the speed setting to the negotiated value. A fiber connection (SFP) also autonegotiates with the device at the other end of the link but only accepts a connection at 1000 Mbps.

You can use the command line interface (CLI) to configure or force SFP Gigabit ports to values other than 1000 Mbps, but the port still continues to run at 1000 Mbps. A copper connection can be force-configured to 10, 100, or 1000 Mbps.

The speed setting for a Gigabit Ethernet port has a close relationship to the setting for duplex. Fiber is always forced to 1000 Mbps and to full duplex. Copper can run at either full duplex or half duplex for 10|100 Mbps but is forced to full-duplex for 1000Mbps. When you force-configure speed and duplex settings, autonegotiation is disabled, and speed and duplex settings can cause a mismatch.

The speed command is not available for LRE interfaces. Use the **cpe speed** command to set the speed of individual CPE ports.

**Note**

For guidelines on setting the switch speed and duplex parameters, refer to “Configuring the Switch Ports” chapter in the *Catalyst 2950 Desktop Switch Software Configuration Guide*.

Examples

This example shows how to set FastEthernet port 1 to 100 Mbps on a non-LRE switch:

```
Switch(config)# interface fastethernet 0/1
Switch(config-if)# speed 100
Switch(config-if)#
```

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

This example shows how to set port 1 to auto on an LRE switch:

```
Switch(config)# interface gigabitEthernet 0/1
Switch(config-if)# speed auto
Switch(config-if)#
```

You can verify the previous commands by entering the **show running-config** command in privileged EXEC mode.

Related Commands

Command	Description
cpe speed	Sets the speed of a CPE port.
duplex	Specifies the duplex mode of operation for switch ports.
show controllers lre status	Display the status for rate selection. Use the sequence keyword to display the status of a sequence for an LRE interface.
show interfaces	Displays the administrative and operational status of all interfaces or a specified interface.
show running config	Displays the current operating configuration for non-LRE switches. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 > Cisco IOS File Management Commands > Configuration File Commands .

storm-control

Use the **storm-control** interface configuration command to enable broadcast, multicast, or unicast storm control on a port and to specify the action taken when a storm occurs on a port. Use the **no** form of this command to disable storm control for broadcast, multicast, or unicast traffic and disable the specified storm-control action.

```
storm-control {{broadcast | multicast | unicast} level level [lower level]} | action {shutdown | trap}}
```

```
no storm-control {{broadcast | multicast | unicast} level} | action}
```

Syntax Description

{broadcast multicast unicast}	Determines the type of packet-storm suppression.
	<ul style="list-style-type: none"> • broadcast—Enable broadcast storm control on the port. • multicast—Enable multicast storm control on the port. • unicast—Enable unicast storm control on the port.
level level [lower level]	Defines the rising and falling suppression levels.
	<ul style="list-style-type: none"> • <i>level</i>—Rising suppression level as a percent of total bandwidth, up to two decimal places; valid values are from 0 to 100 percent. Block the flooding of storm packets when the value specified for <i>level</i> is reached. • <i>lower level</i>—(Optional) Falling suppression level as a percent of total bandwidth, up to two decimal places; valid values are from 0 to 100. This value must be less than the rising suppression value.
action	Action taken when a storm occurs on a port. The default action is to filter traffic and not send an Simple Network Management Protocol (SNMP) trap.
shutdown	Disables the port during a storm.
trap	Sends an SNMP trap when a storm occurs.

Defaults

Broadcast, multicast, and unicast storm control are disabled.

The default action is to filter traffic and to not send an SNMP trap.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(6)EA2	This command was introduced. It replaced port storm-control command.

Usage Guidelines

Use the **storm-control** command to enable or disable broadcast, multicast, or unicast storm control on a port. After a port is disabled during a storm, use the **no shutdown** interface configuration command to enable the port.

The suppression levels are entered as a percentage of total bandwidth. A suppression value of 100 percent means that no limit is placed on the specified traffic type. This feature is enabled only when the rising suppression level is less than 100 percent. If no other storm-control configuration is specified, the default action is to filter the traffic causing the storm and to send no SNMP trap.

When a storm occurs and the action is to filter traffic, if the falling suppression level is not specified, the switch blocks all traffic until the traffic rate drops below the rising suppression level. If the falling suppression level is specified, the switch blocks traffic until the traffic rate drops below this level.

When a multicast or unicast storm occurs and the action is to filter traffic, the switch blocks all traffic (broadcast, multicast, and unicast traffic) and sends only Spanning Tree Protocol (STP) packets.

When a broadcast storm occurs and the action is to filter traffic, the switch blocks only broadcast traffic.

The **trap** and **shutdown** options are independent of each other.

Examples

This example shows how to enable broadcast storm control on a port with a 75.67 percent rising suppression level:

```
Switch(config-if)# storm-control broadcast level 75.67
```

This example shows how to enable multicast storm control on a port with a 87 percent rising suppression level and a 65 percent falling suppression level:

```
Switch(config-if)# storm-control multicast level 87 65
```

This example shows how to enable the **shutdown** action on a port:

```
Switch(config-if)# storm-control action shutdown
```

This example shows how to enable the **trap** action on a port:

```
Switch(config-if)# storm-control action trap
```

This example shows how to disable the **shutdown** action on a port:

```
Switch(config-if)# no storm-control action shutdown
```

You can verify your settings by entering the **show storm-control** privileged EXEC command.

Related Commands

Command	Description
show storm-control	Displays the packet-storm control information.

switchport access

switchport access

Use the **switchport access** interface configuration command to configure a port as a static-access or dynamic-access port. If the mode is set to access, the port operates as a member of the configured VLAN. If set to dynamic, the port starts discovery of its VLAN assignment based on the incoming packets it receives. Use the **no** form of this command to reset the access mode to the default VLAN for the switch.

switchport access vlan {vlan-id | dynamic}

no switchport access

Syntax Description

access vlan	Configure the interface as a static-access port; valid values are from 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1005 when the standard software image (SI) is installed. Do not enter leading zeros.
access vlan dynamic	Specify that the access mode VLAN is dependent on the VLAN Membership Policy Server (VMPS) protocol. The port is assigned to a VLAN based on the source MAC address of a host (or hosts) connected to the port. The switch sends every new MAC address received to the VMPS server to obtain the VLAN name to which the dynamic-access port should be assigned. If the port already has a VLAN assigned and the source has already been approved by the VMPS, the switch forwards the packet to the VLAN.

Defaults

All ports are in static-access mode in VLAN 1 if the port is not connected to a device running Dynamic Trunking Protocol (DTP). The default access VLAN for an access port is VLAN 1.

All ports are dynamic trunk ports.

A dynamic-access port is initially a member of no VLAN and receives its assignment based on the packet it receives.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5.2)WC(1)	This command was introduced.
12.1(6)EA2	The dynamic keyword was added.

Usage Guidelines

The **no switchport access** command resets the access mode VLAN to the appropriate default VLAN for the device.

The port must be in access mode before the **switchport access vlan** command can take effect. For more information, see the **switchport mode** command.

An access port can be assigned to only one VLAN.

The VMPS server (such as a Catalyst 6000 series switch) must be configured before a port is configured as dynamic.

These restrictions apply to dynamic-access ports:

- The software implements the VLAN Query Protocol (VQP) client, which can query a VMPS such as a Catalyst 6000 series switch. The Catalyst 3550 switches are not VMPS servers. The VMPS server must be configured before a port is configured as dynamic.
- Use dynamic-access ports only to connect end stations. Connecting them to switches or routers that use bridging protocols can cause a loss of connectivity.
- Configure the network so that Spanning Tree Protocol (STP) does not put the dynamic-access port in an STP blocking state. The Port Fast feature is automatically enabled on dynamic-access ports.
- Dynamic-access ports can only be in one VLAN and do not use VLAN tagging.
- Dynamic-access ports cannot be configured as:
 - Members of an EtherChannel port group (dynamic-access ports cannot be grouped with any other port, including other dynamic ports).
 - Source or destination ports in a static address entry.
 - Monitor ports.

Examples

This example shows how to assign a port already in access mode to VLAN 2 (instead of the default VLAN 1):

```
Switch(config-if)# switchport access vlan 2
```

You can verify your settings by entering the **show interfaces interface-id switchport** privileged EXEC command and examining information in the Administrative Mode and Operational Mode rows.

Related Commands

Command	Description
show interfaces	Displays the administrative and operational status of a switching port, including port blocking and port protection settings.
switchport mode	Configures the VLAN membership mode of a port.

switchport mode

switchport mode

Use the **switchport mode** interface configuration command to configure the VLAN membership mode of a port. Use the **no** form of this command to reset the mode to the appropriate default for the device.

switchport mode {access | dynamic {auto | desirable} | trunk}

no switchport mode

Syntax Description	access Set the port to access mode (either static-access or dynamic-access depending on the setting of the switchport access vlan interface configuration command). The port is set to access unconditionally and operates as a nontrunking, single VLAN interface that transmits and receives nonencapsulated (non-tagged) frames. An access port can be assigned to only one VLAN. dynamic auto Set the interface trunking mode dynamic parameter to auto to specify that the interface convert the link to a trunk link. dynamic desirable Set the interface trunking mode dynamic parameter to desirable to specify that the interface actively attempt to convert the link to a trunk link. trunk Set the port to trunk unconditionally. The port is a trunking VLAN Layer 2 interface. The port transmits and receives encapsulated (tagged) frames that identify the VLAN of origination. A trunk is a point-to-point link between two switches or between a switch and a router.
---------------------------	--

Defaults

The default mode is **dynamic desirable**.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5.2)WC(1)	This command was introduced.
12.1(6)EA2	The dynamic auto and dynamic desirable keywords were added.

Usage Guidelines

Configuration by using the **access** or **trunk** keywords takes affect only when you configure the port in the appropriate mode by using the **switchport mode** command. The static-access and trunk configurations are saved, but only one configuration is active at a time.

If you enter **access** mode, the interface changes into permanent nontrunking mode and negotiates to convert the link into a nontrunk link even if the neighboring interface does not agree to the change.

If you enter **dynamic auto** mode, the interface converts the link to a trunk link if the neighboring interface is set to **trunk** or **desirable** mode.

If you enter **dynamic desirable** mode, the interface becomes a trunk interface if the neighboring interface is set to **trunk**, **desirable**, or **auto** mode.

If you enter **trunk** mode, the interface changes into permanent trunking mode and negotiates to convert the link into a trunk link even if the interface connecting to it does not agree to the change.

The **no switchport mode** form resets the mode to **dynamic desirable**.

Trunk ports cannot coexist on the same switch.

To autonegotiate trunking, the interfaces must be in the same VTP domain. Trunk negotiation is managed by the Dynamic Trunking Protocol (DTP), which is a point-to-point protocol. However, some internetworking devices might forward DTP frames improperly, which could cause misconfigurations. To avoid this, you should configure interfaces connected to devices that do not support DTP to not forward DTP frames, which turns off DTP.

- If you do not intend to trunk across those links, use the **switchport mode access** interface configuration command to disable trunking.
- To enable trunking to a device that does not support DTP, use the **switchport mode trunk** and **switchport nonegotiate** interface configuration commands to cause the interface to become a trunk but to not generate DTP frames.

Examples

This example shows how to configure a port for access mode:

```
Switch(config-if)# switchport mode access
```

This example shows how set the interface to dynamic desirable mode:

```
Switch(config-if)# switchport mode dynamic desirable
```

This example shows how to configure a port for trunk mode:

```
Switch(config-if)# switchport mode trunk
```

You can verify your settings by entering the **show interfaces interface-id switchport** privileged EXEC command and examining information in the Administrative Mode and Operational Mode rows.

Related Commands

Command	Description
show interfaces	Displays the administrative and operational status of a switching
switchport	(nonrouting) port, including port blocking and port protection settings.
switchport access	Configures a port as a static-access port.

switchport nonegotiate

switchport nonegotiate

Use the **switchport nonegotiate** interface configuration command to specify that Dynamic Trunking Protocol (DTP) negotiation packets are not sent on the Layer 2 interface. The switch does not engage in DTP negotiation on this interface. Use the **no** form of this command to return to the default setting.

switchport nonegotiate

no switchport nonegotiate

Syntax Description This command has no arguments or keywords.

Defaults The default is to use DTP negotiation to determine trunking status.

Command Modes Interface configuration

Command History	Release	Modification
	12.1(6)EA2	This command was introduced.

Usage Guidelines The **no** form of the **switchport nonegotiate** command removes **nonegotiate** status.

This command is valid only when the interface switchport mode is access or trunk (configured by using the **switchport mode access** or the **switchport mode trunk** interface configuration command). This command returns an error if you attempt to execute it in **dynamic (auto or desirable)** mode.

Internetworking devices that do not support DTP might forward DTP frames improperly and cause misconfigurations. To avoid this, you should turn off DTP by using the **switchport no negotiate** command to configure the interfaces connected to devices that do not support DTP to not forward DTP frames.

When you enter the **switchport nonegotiate** command, DTP negotiation packets are not sent on the interface. The device does or does not trunk according to the **mode** parameter given: **access** or **trunk**.

- If you do not intend to trunk across those links, use the **switchport mode access** interface configuration command to disable trunking.
- To enable trunking on a device that does not support DTP, use the **switchport mode trunk** and **switchport nonegotiate** interface configuration commands to cause the interface to become a trunk but to not generate DTP frames.



Note On GigaStack GBICs, dynamic trunking is only supported when one port of a GigaStack GBIC is being used. If trunking is required on a GigaStack GBIC where both ports are in use, use the **switchport mode trunk** and **switchport nonegotiate** interface configuration commands on both GBIC interfaces to cause the interfaces to become trunks.

Examples

This example shows how to cause an interface to refrain from negotiating trunking mode and to act as a trunk or access port (depending on the **mode** set):

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

You can verify your setting by entering the **show interfaces interface-id switchport** privileged EXEC command.

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.
switchport mode	Configures the VLAN membership mode of a port.

switchport port-security

switchport port-security

Use the **switchport port-security** interface configuration command without keywords to enable port security on an interface. Use the keywords to configure secure MAC addresses, a maximum number of secure MAC addresses, or the violation mode. Use the **no** form of this command to disable port security or to set the parameters to their default states.

```
switchport port-security [mac-address mac-address] | [mac-address sticky [mac-address]] |
[maximum value] | [violation {protect | restrict | shutdown}]

no switchport port-security [mac-address mac-address] | [mac-address sticky [mac-address]] |
[maximum value] | [violation {protect | restrict | shutdown}]
```

Syntax Description	
mac-address <i>mac-address</i>	(Optional) Specify a secure MAC address for the port by entering a 48-bit MAC address. You can add additional secure MAC addresses up to the maximum value configured.
mac-address sticky <i>[mac-address]</i>	(Optional) Enable the interface for <i>sticky learning</i> by entering only the mac-address sticky keywords. When sticky learning is enabled, the interface adds all secure MAC addresses that are dynamically learned to the running configuration and converts these addresses to sticky secure MAC addresses. Specify a sticky secure MAC address by entering the mac-address sticky <i>mac-address</i> keywords.
Note	Although you can specify a sticky secure MAC address by entering the mac-address sticky <i>mac-address</i> keywords, we recommend using the mac-address <i>mac-address</i> interface configuration command to enter secure MAC addresses.
maximum <i>value</i>	(Optional) Set the maximum number of secure MAC addresses for the interface. The range is from 1 to 132. The default is 1.
violation	(Optional) Set the security violation mode or the action to be taken if port security is violated. The default is shutdown .
protect	Set the security violation protect mode. When port secure MAC addresses reach the limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses to drop below the maximum value. Users are not notified that a security violation has occurred.

restrict	Set the security violation restrict mode. When port secure MAC addresses reach the limit allowed on the port, packets with unknown source addresses are dropped until a sufficient number of secure MAC addresses is removed to drop below the maximum value. In this mode, users are notified that a security violation has occurred. Specifically, a port security violation causes a trap notification to be sent to the network management station, a syslog message is logged, and the violation counter increments.
shutdown	Set the security violation shutdown mode. In this mode, a port security violation causes the interface to immediately become error-disabled, and turns off the port LED. It also sends an SNMP trap notification, logs a syslog message, and increments the violation counter. When a secure port is in the error-disabled state, you can bring it out of this state by entering the errdisable recovery cause psecure-violation global configuration command, or you can manually re-enable it by entering the shutdown and no shut down interface configuration commands.

Defaults

Port security is disabled.

When port security is enabled, if no keywords are entered, the default maximum number of secure MAC addresses is 1.

Sticky learning is disabled.

The default violation mode is **shutdown**.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(6)EA2	This command was introduced. It replaced the port security and mac-address-table secure commands.
12.1(11)EA1	The mac-address sticky [mac-address] option was added.

Usage Guidelines

A secure port can have from 1 to 132 associated secure addresses. The total number of available secure addresses on the switch is 1024.

After you set the maximum number of secure MAC addresses allowed on a port, you can add secure addresses to the address table by manually configuring all of them, by allowing the port to dynamically configure all of them, or by configuring a number of MAC addresses and allowing the rest to be dynamically configured.

You can delete dynamic secure MAC addresses from the address table by entering the **clear port-security dynamic** privileged EXEC command.

switchport port-security

You can enable sticky learning on an interface by using the **switchport port-security mac-address sticky** interface configuration command. When you enter this command, the interface converts all the dynamic secure MAC addresses, including those that were dynamically learned before sticky learning was enabled, to sticky secure MAC addresses. It adds all the sticky secure MAC addresses to the running configuration.

You can delete a sticky secure MAC addresses from the address table by using the **clear port-security sticky mac-addr** privileged EXEC command. To delete all the sticky addresses on an interface, use the **clear port-security sticky interface-id** privileged EXEC command.

If you disable sticky learning, the sticky secure MAC addresses are converted to dynamic secure addresses and are removed from the running configuration.

If you save the sticky secure MAC addresses in the configuration file, when the switch restarts or the interface shuts down, the interface does not need to relearn these addresses. If you do not save the sticky secure addresses, they are lost.

If you specify **restrict** or **shutdown**, use the **snmp-server host** global configuration command to configure the Simple Network Management Protocol (SNMP) to send traps to the host.

It is a security violation when one of these situations occurs:

- The maximum number of secure MAC addresses have been added to the address table, and a station whose MAC address is not in the address table attempts to access the interface.
- An address learned or configured on one secure interface is seen on another secure interface in the same VLAN.

When a secure port is in the error-disabled state, you can bring it out of this state by entering the **errdisable recovery cause psecure-violation** global configuration command, or you can manually re-enable it by entering the **shutdown** and **no shut down** interface configuration commands.

A secure port has these limitations:

- Port security can only be configured on static access ports.
- A secure port cannot be a dynamic port, a dynamic access port or a trunk port.
- A secure port cannot be a destination port for Switched Port Analyzer (SPAN).
- A secure port cannot belong to a Fast EtherChannel or Gigabit EtherChannel port group.
- You cannot configure static secure MAC addresses in the voice VLAN.
- When you enable port security on a voice VLAN port, you must set the maximum allowed secure addresses on the port to at least two. When the port is connected to a Cisco IP Phone, the IP phone requires two MAC addresses: one for the access VLAN and the other for the voice VLAN. Connecting a PC to the IP phone requires additional MAC addresses.
- You cannot configure an 802.1X port as a secure port. If you try to enable port security on an 802.1X port, an error message appears, and port security is not enabled.
- The switch does not support port security aging of sticky secure MAC addresses.

Examples

This example shows how to enable port security:

```
Switch(config-if)# switchport port-security
```

This example shows how to set the action that the port takes when an address violation occurs:

```
Switch(config-if)# switchport port-security violation shutdown
```

This example shows how to set the maximum number of addresses that a port can learn to 20.

```
Switch(config-if)# switchport port-security maximum 20
```

This example shows how to enable sticky learning and to enter two sticky secure MAC addresses:

```
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.4141
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.000f
```

You can verify your settings by entering the **show port-security** privileged EXEC command.

Related Commands	Command	Description
	clear port-security dynamic	Deletes from the MAC address table a specific dynamic secure address or all the dynamic secure addresses on an interface.
	show port-security	Displays the port security settings defined for the port.

switchport port-security aging

switchport port-security aging

Use the **switchport port-security aging** interface configuration command to set the aging time and type for secure address entries or to change the aging behavior for statically configured secure addresses on a particular port. Use the **no** form of this command to disable port security aging or to set the parameters to their default states.

```
switchport port-security aging {static | time time | type {absolute | inactivity}}
no switchport port-security aging {static | time | type}
```

Syntax Description	
static	Enable aging for statically configured secure addresses on this port.
time time	Specify the aging time for this port. The valid range is from 0 to 1440 minutes. If the time is 0, aging is disabled for this port.
type absolute	Set the aging type as absolute aging. All the secure addresses on this port age out exactly after the time (minutes) specified and are removed from the secure address list.
type inactivity	Set the aging type as inactivity aging. The secure addresses on this port age out only if there is no data traffic from the secure source address for the specified time period.

Defaults

The port security aging feature is disabled. The default time is 0 minutes.

The default aging type is absolute.

The default static aging behavior is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(9)EA1	This command was introduced.

Usage Guidelines

To enable secure address aging for a particular port, set the port aging time to a value other than 0.

To allow limited-time access to particular secure addresses, set the aging type as **absolute**. When the aging time lapses, the secure addresses are deleted.

To allow continuous access to a limited number of secure addresses, set the aging type as **inactivity**. This removes the secure address when it becomes inactive, and other addresses can become secure.

To allow unlimited access to a secure address, configure it as a secure address, and disable aging for the statically configured secure address by using the **no switchport port-security aging static** interface configuration command.

Examples

This example sets the aging time as 2 hours for absolute aging for all the secure addresses on Fast Ethernet interface 0/1.

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport port-security aging time 120
```

This example sets the aging time as 2 minutes for inactivity aging type for configured secure addresses on Fast Ethernet interface 0/2.

```
Switch(config)# interface fastethernet0/2
Switch(config-if)# switchport port-security aging time 2
Switch(config-if)# switchport port-security aging type inactivity
Switch(config-if)# switchport port-security aging static
```

This example shows how to disable aging for configured secure addresses.

```
Switch(config-if)# no switchport port-security aging static
```

Related Commands

Command	Description
show port-security	Displays the port security settings defined for the port.
switchport port-security	Enables port security on a port, restricts the use of the port to a user-defined group of stations, and configures secure MAC addresses.

switchport priority extend

switchport priority extend

Use the **switchport priority extend** interface configuration command to set a port priority for the incoming untagged frames or the priority of frames received by the IP phone connected to the specified port. Use the **no** form of this command to return to the default setting.

switchport priority extend {cos value | none | trust}

no switchport priority extend

Syntax Description	cos value Set the IP phone port to override the priority received from PC or the attached device. The class of service (CoS) value is a number from 0 to 7. Seven is the highest priority. The default is 0. none The IP phone is not instructed what to do with the priority. trust Set the IP phone port to trust the priority received from PC or the attached device.						
Defaults	The port priority is not set, and the default value for untagged frames received on the port is 0. The IP phone connected to the port is not instructed (none) what to do with the priority.						
Command Modes	Interface configuration						
Command History	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>12.1(9)EA1</td><td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification	12.1(9)EA1	This command was introduced.		
Release	Modification						
12.1(9)EA1	This command was introduced.						
Examples	<p>This example shows how to configure the IP phone connected to the specified port to trust the received 802.1P priority:</p> <pre>Switch(config-if)# switchport priority extend trust</pre> <p>You can verify your settings by entering the show interfaces interface-id switchport privileged EXEC command.</p>						
Related Commands	<table border="1"> <thead> <tr> <th>Command</th><th>Description</th></tr> </thead> <tbody> <tr> <td>show interfaces</td><td>Displays the administrative and operational status of a switching (nonrouting) port.</td></tr> <tr> <td>switchport voice vlan</td><td>Configures the voice VLAN on the port.</td></tr> </tbody> </table>	Command	Description	show interfaces	Displays the administrative and operational status of a switching (nonrouting) port.	switchport voice vlan	Configures the voice VLAN on the port.
Command	Description						
show interfaces	Displays the administrative and operational status of a switching (nonrouting) port.						
switchport voice vlan	Configures the voice VLAN on the port.						

switchport protected

Use the **switchport protected** interface configuration command to isolate unicast, multicast, and broadcast traffic at Layer 2 from other protected ports on the same switch. Use the **no** form of this command to return to the default setting.

switchport protected

no switchport protected

Syntax Description This command has no keywords or arguments.

Defaults No protected port is defined. All ports are nonprotected.

Command Modes Interface configuration

Command History	Release	Modification
	12.1(6)EA2	This command was introduced. It replaced the port protected command.

Usage Guidelines The switchport protection feature is local to the switch; communication between protected ports on the same switch is possible only through a Layer 3 device. To prevent communication between protected ports on different switches, you must configure the protected ports for unique VLANs on each switch and configure a trunk link between the switches. A protected port is different from a secure port.

A protected port does not forward any unicast, multicast, or broadcast traffic to any other protected port. A protected port continues to forward unicast, multicast, and broadcast traffic to unprotected ports and vice versa.

Port monitoring does not work if both the monitor and monitored ports are protected ports.

Examples This example shows how to enable a protected port on Fast Ethernet interface 0/3:

```
Switch(config)# interface fastethernet0/3
Switch(config-if)# switchport protected
```

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

Related Commands	Command	Description
	show interfaces switchport	Displays the administrative and operational status of a switching port.

switchport trunk

switchport trunk

Use the **switchport trunk** interface configuration command to set the trunk characteristics when the interface is in trunking mode. Use the **no** form of this command to reset all of the trunking characteristics to the defaults. Use the **no** form with keywords to reset those characteristics to the defaults.

```
switchport trunk { {allowed vlan vlan-list} | {native vlan vlan-id} | {pruning vlan vlan-list} }
no switchport trunk { {allowed vlan vlan-list} | {native vlan vlan-id} | {pruning vlan vlan-list} }
```

Syntax Description	allowed vlan <i>vlan-list</i>	Set the list of allowed VLANs that can receive and send traffic on this interface in tagged format when in trunking mode. See the following <i>vlan-list</i> format. The none keyword is not valid. The default is all .
	native vlan <i>vlan-id</i>	Set the native VLAN for sending and receiving untagged traffic when the interface is in 802.1Q trunking mode. Valid IDs are from 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1001 when the standard software image (SI) is installed. Do not enter leading zeros.
	pruning vlan <i>vlan-list</i>	Set the list of VLANs that are enabled for VTP pruning when in trunking mode. The all keyword is not valid.

The *vlan-list* format is **all** | **none** | [**add** | **remove** | **except**] *vlan-atom* where:

- **all** specifies all VLANs from 1 to 4094 when the EI is installed and 1 to 1005 when the SI is installed. Do not enter leading zeros. This keyword is not allowed on commands that do not permit all VLANs in the list to be set at the same time.
- **none** means an empty list. This keyword is not allowed on commands that require certain VLANs to be set or at least one VLAN to be set.
- **add** adds the defined list of VLANs to those currently set instead of replacing the list. Valid IDs are from 2 to 1001; extended-range VLAN IDs are valid in some cases.



Note You can add extended-range VLANs to the allowed VLAN list, but not to the pruning-eligible VLAN list.

Separate nonconsecutive VLAN IDs with a comma; do not enter a space after the comma. Use a hyphen to designate a range of IDs; do not enter a space before or after the hyphen. Do not enter leading zeros.

- **remove** removes the defined list of VLANs from those currently set instead of replacing the list. Valid IDs are from 2 to 1001; extended-range VLAN IDs are valid in some cases.



Note You cannot remove VLAN 1 or VLANs 1002 to 1005 from the list. You can remove extended-range VLANs (VLAN IDs greater than 1005) from the allowed VLAN list, but you cannot remove them from the pruning-eligible list.

Separate nonconsecutive VLAN IDs with a comma; do not enter a space after the comma. Use a hyphen to designate a range of IDs; do not enter a space before or after the hyphen. Do not enter leading zeros.

- **except** lists the VLANs that should be calculated by inverting the defined list of VLANs. (VLANs are added except the ones specified.) Valid IDs are from 2 to 1001. Separate nonconsecutive VLAN IDs with a comma; do not enter a space after the comma. Use a hyphen to designate a range of IDs; do not enter a space before or after the hyphen. Do not enter leading zeros.
- **vlan-atom** is either a single VLAN number from 1 to 4094 when the EI is installed and 1 to 1005 when the SI is installed, a list of nonconsecutive VLANs, or a continuous range of VLANs described by two VLAN numbers, the lower one first, separated by a hyphen.

For a list of nonconsecutive VLAN IDs, separate the VLAN IDs with a comma. Do not enter a space after the comma. Do not enter leading zeroes.

For a continuous range of VLAN IDs, use a hyphen to designate the range. Do not enter a space before or after the hyphen. Do not enter leading zeroes.

These are examples showing how to specify one or more VLANs:

- Single VLAN—101
- List of nonconsecutive VLANs—10,12,14,16,18
- Continuous range of VLANs—10-15
- List of VLAN continuous ranges—10-15,20-24
- List of nonconsecutive VLANs and VLAN continuous ranges—8,11,20-24,44

Defaults

VLAN 1 is the default native VLAN ID on the port.

The default for all VLAN lists is to include all VLANs.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(6)EA2	This command was introduced.

Usage Guidelines

A trunk port cannot be a secure port or a monitor port. However, a static-access port can monitor a VLAN on a trunk port. The VLAN monitored is the one associated with the static-access port.

Allowed VLAN:

- The **no** form of the **allowed vlan** command resets the list to the default list, which allows all VLANs.
- You cannot remove VLAN 1 or VLANs 1002 to 1005 from the allowed VLAN list.

Native VLANs:

- All untagged traffic received on an 802.1Q trunk port is forwarded with the native VLAN configured for the port.
- If a packet has a VLAN ID that is the same as the sending port native VLAN ID, the packet is sent without a tag; otherwise, the switch sends the packet with a tag.
- The **no** form of the **native vlan** command resets the native mode VLAN to the appropriate default VLAN for the device.

switchport trunk

Trunk Pruning:

- The pruning-eligible list applies only to trunk ports.
- Each trunk port has its own eligibility list.
- If you do not want a VLAN to be pruned, remove it from the pruning-eligible list. VLANs that are pruning-ineligible receive flooded traffic.
- VLAN 1, VLANs 1002 to 1005, and extended-range VLANs (VLANs 1006 to 4094) cannot be pruned.

**Note**

The switch does not support Inter-Switch Link (ISL) trunking.

Examples

This example shows how to configure VLAN 3 as the default port to send all untagged traffic:

```
Switch(config-if)# switchport trunk native vlan 3
```

This example shows how to add VLANs 1, 2, 5, and 6 to the allowed list:

```
Switch(config-if)# switchport trunk allowed vlan add 1,2,5,6
```

This example shows how to remove VLANs 3 and 10 to 15 from the pruning-eligible list:

```
Switch(config-if)# switchport trunk pruning vlan remove 3,10-15
```

You can verify your settings by entering the **show interfaces interface-id switchport** privileged EXEC command.

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.
switchport mode	Configures the VLAN membership mode of a port.

switchport voice vlan

Use the **switchport voice vlan** interface configuration command to configure voice VLAN on the port. Use the **no** form of this command to return to the default setting.

switchport voice vlan {vlan-id | dot1p | none | untagged}

no switchport voice vlan

Syntax Description	<table border="0"> <tr> <td>vlan-id</td><td>VLAN used for voice traffic. Valid IDs are from 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1001 when the standard software image (SI) is installed. Do not enter leading zeros.</td></tr> <tr> <td>dot1p</td><td>The telephone uses priority tagging and uses VLAN 0 (the native VLAN). By default, the Cisco IP Phone forwards the voice traffic with an 802.1P priority of 5.</td></tr> <tr> <td>none</td><td>The telephone is not instructed through the CLI about the voice VLAN. The telephone uses the configuration from the telephone key pad.</td></tr> <tr> <td>untagged</td><td>The telephone does not tag frames and uses VLAN 4095. The default for the telephone is untagged.</td></tr> </table>	vlan-id	VLAN used for voice traffic. Valid IDs are from 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1001 when the standard software image (SI) is installed. Do not enter leading zeros.	dot1p	The telephone uses priority tagging and uses VLAN 0 (the native VLAN). By default, the Cisco IP Phone forwards the voice traffic with an 802.1P priority of 5.	none	The telephone is not instructed through the CLI about the voice VLAN. The telephone uses the configuration from the telephone key pad.	untagged	The telephone does not tag frames and uses VLAN 4095. The default for the telephone is untagged.
vlan-id	VLAN used for voice traffic. Valid IDs are from 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1001 when the standard software image (SI) is installed. Do not enter leading zeros.								
dot1p	The telephone uses priority tagging and uses VLAN 0 (the native VLAN). By default, the Cisco IP Phone forwards the voice traffic with an 802.1P priority of 5.								
none	The telephone is not instructed through the CLI about the voice VLAN. The telephone uses the configuration from the telephone key pad.								
untagged	The telephone does not tag frames and uses VLAN 4095. The default for the telephone is untagged.								

Defaults

The switch default is not to automatically configure the telephone (**none**).

The telephone default is not to tag frames.

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

Command History	Release	Modification
	12.1(9)EA1	This command was introduced.

Usage Guidelines

You should configure voice VLAN on access ports.

If you enable port security on a voice VLAN port and if there is a PC connected to the IP phone, you should set the maximum allowed secure addresses on the port to more than 1.

You cannot configure static secure MAC addresses in the voice VLAN.

The Port Fast feature is automatically enabled when voice VLAN is configured. When you disable voice VLAN, the Port Fast feature is not automatically disabled.

switchport voice vlan**Examples**

This example shows how to configure VLAN 2 as the voice VLAN:

```
Switch(config-if)# switchport voice vlan 2
```

You can verify your settings by entering the **show interfaces *interface-id* switchport** privileged EXEC command.

Related Commands

Command	Description
show interfaces <i>interface-id</i> switchport	Displays the administrative and operational status of a switching (nonrouting) port.
switchport priority extend	Determines how the device connected to the specified port handles priority traffic received on its incoming port.

system mtu

Use the **system mtu** global configuration command to set the maximum packet size or maximum transmission unit (MTU) size for the switch. Use the **no** form of this command to restore the global MTU value to its original default value.

system mtu bytes

no system mtu

Syntax Description	<i>bytes</i>	Packet size in bytes. For valid values, see the “Usage Guidelines” section.
---------------------------	--------------	---

Defaults	The default MTU size is 1500 bytes.
-----------------	-------------------------------------

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

Command History	Release	Modification
	12.1(6)EA2	This command was introduced.

Usage Guidelines	This table lists the valid system MTU values for the switches:
-------------------------	--

Switch	MTU size
Catalyst 2950G-12-EI	1500 to 1530 bytes
Catalyst 2950G-24-EI	
Catalyst 2950G-24-EI-DC	
Catalyst 2950G-48-EI	
Other Catalyst 2950 switches	1500 bytes

The size of frames that can be received by the switch CPU is limited to 1500 bytes, no matter what value was entered with the **system mtu** command. Although frames that are forwarded or routed typically are not received by the CPU, in some cases packets are sent to the CPU, such as traffic sent to control traffic, Simple Network Management Protocol (SNMP), Telnet, or routing protocols.

If you enter a value that is outside of the range for the switch, the value is not accepted.



Note You cannot set the MTU on a per-interface basis.

system mtu**Examples**

This example shows how to set the maximum packet size to 1528 bytes:

```
Switch(config)# system mtu 1528
Switch(config)# exit
```

This example shows the response when you try to set a switch to an out-of-range number:

```
Switch(config)# system mtu 2000
^
% Invalid input detected at '^' marker.
```

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

Related Commands

Command	Description
show system mtu	Displays the maximum packet size set for the switch.

udld (global configuration)

Use the **udld** global configuration command to enable aggressive or normal mode in the UniDirectional Link Detection (UDLD) and to set the configurable message timer. Use the **no** form of this command to disable aggressive or normal mode UDLD on all fiber-optic ports.

udld {aggressive | enable | message time *message-timer-interval*}

no udld {aggressive | enable | message time}

Syntax Description	aggressive Enable UDLD in aggressive mode on all fiber-optic interfaces. enable Enable UDLD in normal mode on all fiber-optic interfaces. message time Configure the period of time between UDLD probe messages on ports that are in the advertisement phase and are determined to be bidirectional. The range is from 7 to 90 seconds. <i>message-timer-interval</i>
--------------------	---

Defaults UDLD is disabled on all fiber-optic interfaces.

The message timer is set at 60 seconds.

Command Modes Global configuration

Command History	Release	Modification
	12.0(5.2)WC(1)	This command was introduced.
	12.1(6)EA2	The udld enable global configuration command was changed to udld (global configuration) .

Usage Guidelines Use the **udld** global configuration command to enable UDLD only on fiber-optic ports.

In normal mode, if UDLD is in the advertisement or in the detection phase and all the neighbor cache entries are aged out, UDLD restarts the link-up sequence to resynchronize with any potentially out-of-sync neighbors.

If you enable aggressive mode, when all the neighbors of a port have aged out either in the advertisement or in the detection phase, UDLD restarts the link-up sequence to resynchronize with any potentially out-of-sync neighbor. UDLD shuts down the port if, after the fast train of messages, the link state is still undetermined. Use aggressive mode on point-to-point links where no failure between two neighbors is allowed. In this situation, UDLD probe packets can be considered as a heart beat whose presence guarantees the health of the link. Conversely, the loss of the heart beat means that the link must be shut down if it is not possible to re-establish a bidirectional link.

If you change the message time between probe packets, you are making a trade-off between the detection speed and the CPU load. By decreasing the time, you can make the detection-response faster but increase the load on the CPU.

This command affects fiber-optic interfaces only. Use the **udld** interface configuration command to enable UDLD on other interface types.

■ udld (global configuration)**Examples**

This example shows how to enable UDLD on all fiber-optic interfaces:

```
Switch(config)# udld enable
```

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

Related Commands

Command	Description
show running-config	Displays the running configuration on the switch. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 > Cisco IOS File Management Commands > Configuration File Commands .
show udld	Displays the UDLD status for all ports or the specified port.
udld (interface configuration)	Enables UDLD on an individual interface or prevents a fiber-optic interface from being enabled by the udld global configuration command.
udld reset	Resets any interface shut down by UDLD and permits traffic to again pass through.

udld (interface configuration)

Use the **udld** interface configuration command to enable UniDirectional Link Detection (UDLD) on an individual interface or to prevent a fiber-optic interface from being enabled by the **udld** global configuration command. Use the **no** form of this command to return to the **udld** global configuration command setting or disable UDLD if entered on a nonfiber-optic port.

udld {aggressive | enable | disable}

no udld {aggressive | enable | disable}

Syntax Description	
aggressive	Enable UDLD in aggressive mode on the specified interface.
disable	Disable UDLD on the specified interface. This keyword applies only to fiber-optic interfaces.
enable	Enable UDLD in normal mode on the specified interface.

Defaults

On fiber-optic interfaces, UDLD is not enabled, in aggressive mode, or disabled. For this reason, fiber-optic interfaces enable UDLD according to the state of the **udld enable** or **udld aggressive** global configuration command.

On nonfiber-optic interfaces, UDLD is disabled.

Command Modes

Interface configuration

Command History	Release	Modification
	12.0(5.2)WC(1)	This command was introduced.
	12.1(6)EA2	The aggressive keyword was added.

Usage Guidelines

UDLD is supported on fiber- and copper-based Ethernet ports.

A UDLD-capable port cannot detect a unidirectional link if it is connected to a UDLD-incapable port of another switch.

This setting overrides the global UDLD configuration on the switch.

In normal mode, if UDLD is in the advertisement or in the detection phase and all the neighbor cache entries are aged out, UDLD restarts the link-up sequence to resynchronize with any potentially out-of-sync neighbors.

If you enable aggressive mode, when all the neighbors of a port have aged out either in the advertisement or in the detection phase, UDLD restarts the link-up sequence to resynchronize with any potentially out-of-sync neighbor. UDLD shuts down the port if, after the fast train of messages, the link state is still undetermined. Use aggressive mode on point-to-point links where no failure between two neighbors is allowed. In this situation, UDLD probe packets can be considered as a heart beat whose presence guarantees the health of the link. Conversely, the loss of the heart beat means that the link must be shut down if it is not possible to re-establish a bidirectional link.

■ udld (interface configuration)

Use the **no udld enable** command on fiber-optic ports to return control of UDLD to the **udld enable** global configuration command or to disable UDLD on nonfiber-optic ports.

Use the **udld aggressive** command on fiber-optic ports to override the settings of the **udld enable** or **udld aggressive** global configuration command. Use the **no** form on fiber-optic ports to remove this setting and to return control of UDLD enabling to the **udld** global configuration command or to disable UDLD on nonfiber-optic ports.

The **disable** keyword is supported on fiber-optic ports only. Use the **no** form of this command to remove this setting and to return control of UDLD to the **udld** global configuration command.

If the switch software detects a GBIC module change and the interface changes from fiber optic to nonfiber optic or from nonfiber optic to fiber optic, all configurations are maintained.

Examples

This example shows how to enable UDLD on an interface:

```
Switch(config)# interface fastethernet0/2
Switch(config-if)# udld enable
```

This example shows how to disable UDLD on a fiber-optic interface despite the setting of the **udld** global configuration command:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# udld disable
```

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

Related Commands

Command	Description
show running-config	Displays the running configuration on the switch. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 > Cisco IOS File Management Commands > Configuration File Commands .
show udld	Displays UDLD status for all ports or the specified port.
udld (global configuration)	Enables UDLD on all fiber-optic ports on the switch.
udld reset	Resets all interfaces shut down by UDLD and permits traffic to again pass through.

udld reset

Use the **udld reset** privileged EXEC command to reset all interfaces shut down by UniDirectional Link Detection (UDLD) and to permit traffic to again pass through. Other features, such as spanning tree, Port Aggregation Protocol (PAgP), and Dynamic Trunking Protocol (DTP), still have their normal effects, if enabled.

udld reset

Syntax Description This command has no keywords or arguments.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.0(5.2)WC(1)	This command was introduced.

Usage Guidelines If the interface configuration is still enabled for UDLD, these ports begin to run UDLD again and might shut down for the same reason if the problem has not been corrected.

Examples This example shows how to reset all interfaces that have been shut down by UDLD:

```
Switch# udld reset
1 ports shutdown by UDLD were reset.
```

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

Related Commands	Command	Description
	show running-config	Displays the running configuration on the switch. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 > Cisco IOS File Management Commands > Configuration File Commands .
	show udld	Displays UDLD status for all ports or the specified port.
	udld (interface configuration)	Enables UDLD on an individual interface or prevents a fiber-optic interface from being enabled by the udld global configuration command.
	udld (global configuration)	Enables UDLD on all fiber-optic ports on the switch.

upgrade binary

upgrade binary

Use the **upgrade binary** controller configuration command to configure the behavior of a Long-Reach Ethernet (LRE) controller upgrade.

upgrade binary LRE binary [remote lre-interface]

no upgrade binary LRE binary [remote lre-interface]

Syntax Description	LRE binary	The LRE binary file name being applied.
	remote lre-interface	(Optional) The LRE interface. If you do not specify the remote parameter for the customer premises equipment (CPE) end of the LRE link, the local or controller end of the LRE link is implied.

Command Modes	Controller configuration
----------------------	--------------------------

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.

Usage Guidelines	This configuration command is normally not needed. The default behavior for an upgrade is for the system to select the binary version. Use this command when you need to specify a particular upgrade binary file for a local controller in an LRE switch or for a remote CPE device connected to the controller. If you use the command without parameters, the LRE binary is applied to the local controller when it is upgraded. If you specify the remote keyword and interface, the LRE binary is applied to the CPE device at the end of the remote LRE link at upgrade time.
-------------------------	---

Upgrade configurations given in the controller configuration mode take precedence over upgrade configurations given in the global configuration mode.

Examples	This example shows how to configures a Cisco 585 LRE CPE on LRE link 0/1 to use version 51.00.00.bin the next time LRE update runs.
-----------------	---

```
Switch# configure t
Switch(config)# controller Lo 0
Switch(config-controller)# upgrade binary CISCO585-LRE_vdlsngl_51.00.00.bin remote lo 0/1
Switch(config-controller)#

```

Related Commands	Command	Description
	upgrade preserve	Prevents an upgrade of the local CPE controller and all remote CPE devices connected to it.

upgrade preserve

Use the **upgrade preserve** controller configuration command to prevent an upgrade from taking place on a controller in a Long-Reach Ethernet (LRE) switch and on all the devices that remotely connect to it. This command does not affect other controllers in the switch and their connected devices. Use the **no** form of the command to allow upgrades on the devices.

upgrade preserve

no upgrade preserve

Syntax Description This command has no keywords or arguments.

Command Modes Controller configuration mode

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.

Usage Guidelines Use the **upgrade preserve** command to cause LRE upgrade to not upgrade a controller and all the devices connected to it.

Examples This example shows how to prevent the controller 0, and the CPE devices attached to it, from being upgraded.

```
Switch# configure t
Switch(config)# controller Lo 0
Switch(config-controller)# upgrade preserve
Switch(config-controller)#
```

Related Commands	Command	Description
	controller LongReachEthernet	Entry for controller configuration mode.
	upgrade binary	Configures upgrades on either end of an LRE link.

vlan (global configuration)

vlan (global configuration)

Use the **vlan** global configuration command to add a VLAN and enter the config-vlan mode. Use the **no** form of this command to delete the VLAN. Configuration information for normal-range VLANs (VLAN IDs 1 to 1005) is always saved in the VLAN database. When VLAN Trunking Protocol (VTP) mode is transparent, you can create extended-range VLANs (VLAN IDs greater than 1005), and the VTP mode and domain name and the VLAN configuration are saved in the switch running configuration file. You can save configurations in the switch startup configuration file by entering the **copy running-config startup-config** privileged EXEC command.

vlan *vlan-id*

no vlan *vlan-id*

Syntax Description	<i>vlan-id</i>	ID of the VLAN to be added and configured. For <i>vlan-id</i> , the range is 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1005 when the standard software image (SI) is installed; do not enter leading zeros. You can enter a single VLAN ID, a series of VLAN IDs separated by commas, or a range of VLAN IDs separated by hyphens.
---------------------------	----------------	--

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

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

Command History	Release	Modification
	12.1(9)EA1	This command was introduced.
	12.1(11)EA1	The remote-span configuration command was added.

Usage Guidelines	You must use the vlan <i>vlan-id</i> global configuration command to add extended-range VLANs (VLAN IDs 1006 to 4094). Before configuring VLANs in the extended range, you must use the vtp transparent global configuration or VLAN configuration command to put the switch in VTP transparent mode. Extended-range VLANs are not learned by VTP and are not added to the VLAN database, but when VTP mode is transparent, VTP mode and domain name and all VLAN configurations are saved in the running configuration, and you can save them in the switch startup configuration file.
-------------------------	--

When you save the VLAN and VTP configurations in the startup configuration file and reboot the switch, the configuration is determined in these ways:

- If both the VLAN database and the configuration file show the VTP mode as transparent and the VTP domain names match, the VLAN database is ignored. The VTP and VLAN configurations in the startup configuration file are used. The VLAN database revision number remains unchanged in the VLAN database.
- If the VTP mode is server, or if the startup VTP mode or domain names do not match the VLAN database, the VTP mode and the VLAN configuration for the first 1005 VLANs use the VLAN database information.

- If the image on the switch or the configuration file is earlier than IOS release 12.1(9)EA1, the switch reboots with information in the VLAN database.

If you try to create an extended-range VLAN when the switch is not in VTP transparent mode, the VLAN is rejected, and you receive an error message.

If you enter an invalid VLAN ID, you receive an error message and do not enter config-vlan mode.

Entering the **vlan** command with a VLAN ID enables config-vlan mode. When you enter the VLAN ID of an existing VLAN, you do not create a new VLAN, but you can modify VLAN parameters for that VLAN. The specified VLANs are added or modified when you exit the config-vlan mode. Only the **shutdown** command (for VLANs 1 to 1005) takes effect immediately.

These configuration commands are available in config-vlan mode. The **no** form of each command returns the characteristic to its default state.


Note

Although all commands are visible, the only config-vlan command supported on extended-range VLANs is **mtu mtu-size**. For extended-range VLANs, all other characteristics must remain at the default state.

- **are are-number**: defines the maximum number of all-routes explorer (ARE) hops for this VLAN. This keyword applies only to TrCRF VLANs. Valid values are from 0 to 13. The default is 7. If no value is entered, 0 is assumed to be the maximum.
- **backuperf**: specifies the backup CRF mode. This keyword applies only to TrCRF VLANs.
 - **enable** backup CRF mode for this VLAN.
 - **disable** backup CRF mode for this VLAN (the default).
- **bridge {bridge-number/ type}**: specifies the logical distributed source-routing bridge, the bridge that interconnects all logical rings having this VLAN as a parent VLAN in FDDI-NET, Token Ring-NET, and TrBRF VLANs. Valid bridge numbers are from 0 to 15. The default bridge number is 0 (no source-routing bridge) for FDDI-NET, TrBRF, and Token Ring-NET VLANs. The **type** keyword applies only to TrCRF VLANs and is one of these:
 - **srp** (source-route bridging)
 - **srt** (source-route transparent) bridging VLAN
- **exit**: applies changes, increments the VLAN database revision number (VLANs 1 to 1005 only), and exits config-vlan mode.
- **media**: defines the VLAN media type. See [Table 2-23](#) for valid commands and syntax for different media types.


Note

The switch supports only Ethernet ports. You configure only FDDI and Token Ring media-specific characteristics for VLAN Trunking Protocol (VTP) global advertisements to other switches. These VLANs are locally suspended.

- **ethernet** is Ethernet media type (the default).
- **fddi** is FDDI media type.
- **fd-net** is FDDI network entity title (NET) media type.
- **tokenring** is Token Ring media type if the VTP v2 mode is disabled, or TrCRF if the VTP version 2 (v) mode is enabled.
- **tr-net** is Token Ring network entity title (NET) media type if the VTP v2 mode is disabled or TrBRF media type if the VTP v2 mode is enabled.

vlan (global configuration)

- **mtu *mtu-size***: specifies the maximum transmission unit (MTU) (packet size in bytes). Valid values are from 1500 to 18190. The default is 1500 bytes.
- **name *vlan-name***: names the VLAN with an ASCII string from 1 to 32 characters that must be unique within the administrative domain. The default is *VLANxxxx* where *xxxx* represents four numeric digits (including leading zeros) equal to the VLAN ID number.
- **no**: negates a command or returns it to the default setting.
- **parent *parent-vlan-id***: specifies the parent VLAN of an existing FDDI, Token Ring, or TrCRF VLAN. This parameter identifies the TrBRF to which a TrCRF belongs and is required when defining a TrCRF. Valid values are from 0 to 1005. The default parent VLAN ID is 0 (no parent VLAN) for FDDI and Token Ring VLANs. For both Token Ring and TrCRF VLANs, the parent VLAN ID must already exist in the database and be associated with a Token Ring-NET or TrBRF VLAN.
- **remote-span**: adds the Remote SPAN (RSPAN) trait to the VLAN. When the RSPAN trait is added to an existing VLAN, the VLAN is first removed and then recreated with the RSPAN trait. Any access ports are deactivated until the RSPAN trait is removed. The new RSPAN VLAN is propagated via VTP for VLAN-IDs less than 1005. This command is available only if your switch is running the EI.
- **ring *ring-number***: defines the logical ring for an FDDI, Token Ring, or TrCRF VLAN. Valid values are from 1 to 4095. The default for Token Ring VLANs is 0. For FDDI VLANs, there is no default.
- **said *said-value***: specifies the security association identifier (SAID) as documented in IEEE 802.10. The value is an integer from 1 to 4294967294 that must be unique within the administrative domain. The default value is 100000 plus the VLAN ID number.
- **shutdown**: shuts down VLAN switching on the VLAN. This command takes effect immediately. Other commands take effect when you exit config-vlan mode.
- **state**: specifies the VLAN state:
 - **active** means the VLAN is operational (the default).
 - **suspend** means the VLAN is suspended. Suspended VLANs do not pass packets.
- **ste *ste-number***: defines the maximum number of spanning-tree explorer (STE) hops. This keyword applies only to TrCRF VLANs. Valid values are from 0 to 13. The default is 7.
- **stp type**: defines the spanning-tree type for FDDI-NET, Token Ring-NET, or TrBRF VLANs. For FDDI-NET VLANs, the default STP type is **ieee**. For Token Ring-NET VLANs, the default STP type is **ibm**. For FDDI and Token Ring VLANs, the default is no type specified.
 - **ieee** for IEEE Ethernet STP running source-route transparent (SRT) bridging.
 - **ibm** for IBM STP running source-route bridging (SRB).
 - **auto** for STP running a combination of source-route transparent bridging (IEEE) and source-route bridging (IBM).
- **tb-vlan1 *tb-vlan1-id* and tb-vlan2 *tb-vlan2-id***: specifies the first and second VLAN to which this VLAN is translationally bridged. Translational VLANs translate FDDI or Token Ring to Ethernet, for example. Valid values are from 0 to 1005. If no value is specified, 0 (no transitional bridging) is assumed.

Table 2-23 Valid Commands and Syntax for Different Media Types

Media Type	Valid Syntax
Ethernet	name vlan-name, media ethernet, state {suspend active}, said said-value, mtu mtu-size, remote-span, tb-vlan1 tb-vlan1-id, tb-vlan2 tb-vlan2-id
FDDI	name vlan-name, media fddi, state {suspend active}, said said-value, mtu mtu-size, ring ring-number, parent parent-vlan-id, tb-vlan1 tb-vlan1-id, tb-vlan2 tb-vlan2-id
FDDI-NET	name vlan-name, media fd-net, state {suspend active}, said said-value, mtu mtu-size, bridge bridge-number, stp type {ieee ibm auto}, tb-vlan1 tb-vlan1-id, tb-vlan2 tb-vlan2-id If VTP v2 mode is disabled, do not set the stp type to auto .
Token Ring	VTP v1 mode is enabled. name vlan-name, media tokenring, state {suspend active}, said said-value, mtu mtu-size, ring ring-number, parent parent-vlan-id, tb-vlan1 tb-vlan1-id, tb-vlan2 tb-vlan2-id
Token Ring concentrator relay function (TrCRF)	VTP v2 mode is enabled. name vlan-name, media tokenring, state {suspend active}, said said-value, mtu mtu-size, ring ring-number, parent parent-vlan-id, bridge type {srp / srt}, are are-number, ste ste-number, backupcrf {enable disable}, tb-vlan1 tb-vlan1-id, tb-vlan2 tb-vlan2-id
Token Ring-NET	VTP v1 mode is enabled. name vlan-name, media tr-net, state {suspend active}, said said-value, mtu mtu-size, bridge bridge-number, stp type {ieee ibm}, tb-vlan1 tb-vlan1-id, tb-vlan2 tb-vlan2-id
Token Ring bridge relay function (TrBRF)	VTP v2 mode is enabled. name vlan-name, media tr-net, state {suspend active}, said said-value, mtu mtu-size, bridge bridge-number, stp type {ieee ibm auto}, tb-vlan1 tb-vlan1-id, tb-vlan2 tb-vlan2-id

Table 2-24 describes the rules for configuring VLANs.

Table 2-24 VLAN Configuration Rules

Configuration	Rule
VTP v2 mode is enabled, and you are configuring a TrCRF VLAN media type.	Specify a parent VLAN ID of a TrBRF that already exists in the database. Specify a ring number. Do not leave this field blank. Specify unique ring numbers when TrCRF VLANs have the same parent VLAN ID. Only one backup concentrator relay function (CRF) can be enabled.
VTP v2 mode is enabled, and you are configuring VLANs other than TrCRF media type.	Do not specify a backup CRF.

Table 2-24 VLAN Configuration Rules (continued)

Configuration	Rule
VTP v2 mode is enabled, and you are configuring a TrBRF VLAN media type.	Specify a bridge number. Do not leave this field blank.
VTP v1 mode is enabled.	No VLAN can have an STP type set to auto. This rule applies to Ethernet, FDDI, FDDI-NET, Token Ring, and Token Ring-NET VLANs.
Add a VLAN that requires translational bridging (values are not set to zero).	The translational bridging VLAN IDs that are used must already exist in the database. The translational bridging VLAN IDs that a configuration points to must also contain a pointer to the original VLAN in one of the translational bridging parameters (for example, Ethernet points to FDDI, and FDDI points to Ethernet). The translational bridging VLAN IDs that a configuration points to must be different media types than the original VLAN (for example, Ethernet can point to Token Ring). If both translational bridging VLAN IDs are configured, these VLANs must be different media types (for example, Ethernet can point to FDDI and Token Ring).

Examples

This example shows how to add an Ethernet VLAN with default media characteristics. The default includes a *vlan-name* of *VLANxxxx*, where *xxxx* represents four numeric digits (including leading zeros) equal to the VLAN ID number. The default **media** option is **ethernet**; the **state** option is **active**. The default *said-value* variable is 100000 plus the VLAN ID; the *mtu-size* variable is 1500; the **stp-type** option is **ieee**. When you enter the **exit** config-vlan configuration command, the VLAN is added if it did not already exist; otherwise, this command does nothing.

This example shows how to create a new VLAN with all default characteristics and enter config-vlan mode:

```
Switch(config)# vlan 200
Switch(config-vlan)# exit
Switch(config)#
```

This example shows how to create a new extended-range VLAN (when the EI is installed) with all the default characteristics, to enter config-vlan mode, and to save the new VLAN in the switch startup configuration file:

```
Switch(config)# vtp mode transparent
Switch(config)# vlan 2000
Switch(config-vlan)# end
Switch# copy running-config startup config
```

You can verify your setting by entering the **show vlan** privileged EXEC command.

Related Commands	Command	Description
	show running-config vlan	Displays all or a range of VLAN-related configurations on the switch.
	show vlan	Displays the parameters for all configured VLANs or one VLAN (if the VLAN ID or name is specified) in the administrative domain.
	vlan (VLAN configuration)	Configures normal-range VLANs in the VLAN database.

vlan (VLAN configuration)

Use the **vlan** VLAN configuration command to configure VLAN characteristics for a normal-range VLAN (VLAN IDs 1 to 1005) in the VLAN database. You access VLAN configuration mode by entering the **vlan database** privileged EXEC command. Use the **no** form of this command without additional parameters to delete a VLAN. Use the **no** form with parameters to change its configured characteristics.

```
vlan vlan-id [are are-number] [backupcrf {enable | disable}] [bridge bridge-number /
type {srp | srt}] [media {ethernet | fddi | fdi-net | tokenring | tr-net}] [mtu mtu-size]
[name vlan-name] [parent parent-vlan-id] [ring ring-number] [said said-value]
[state {suspend | active}] [ste ste-number] [stp type {ieee | ibm | auto}]
[tb-vlan1 tb-vlan1-id] [tb-vlan2 tb-vlan2-id]
```

```
no vlan vlan-id [are are-number] [backupcrf {enable | disable}] [bridge bridge-number /
type {srp | srt}] [media {ethernet | fddi | fdi-net | tokenring | tr-net}] [mtu mtu-size]
[name vlan-name] [parent parent-vlan-id] [ring ring-number] [said said-value]
[state {suspend | active}] [ste ste-number] [stp type {ieee | ibm | auto}]
[tb-vlan1 tb-vlan1-id] [tb-vlan2 tb-vlan2-id]
```

Extended-range VLANs (with VLAN IDs from 1006 to 4094) cannot be added or modified by using these commands. To add extended-range VLANs, use the **vlan (global configuration)** command to enter config-vlan mode.


Note

The switch supports only Ethernet ports. You configure only FDDI and Token Ring media-specific characteristics for VLAN Trunking Protocol (VTP) global advertisements to other switches. These VLANs are locally suspended.

Syntax Description

vlan-id	ID of the configured VLAN. Valid IDs are from 1 to 1005 and must be unique within the administrative domain. Do not enter leading zeros.
are are-number	(Optional) Specify the maximum number of all-routes explorer (ARE) hops for this VLAN. This keyword applies only to TrCRF VLANs. Valid values are from 0 to 13. If no value is entered, 0 is assumed to be the maximum.
backupcrf {enable disable}	(Optional) Specify the backup CRF mode. This keyword applies only to TrCRF VLANs. <ul style="list-style-type: none"> • enable backup CRF mode for this VLAN. • disable backup CRF mode for this VLAN.
bridge bridge-number/ type {srp srt}	(Optional) Specify the logical distributed source-routing bridge, the bridge that interconnects all logical rings having this VLAN as a parent VLAN in FDDI-NET, Token Ring-NET, and TrBRF VLANs. Valid bridge numbers are from 0 to 15. The type keyword applies only to TrCRF VLANs and is one of these: <ul style="list-style-type: none"> • srp (source-route bridging) • srt (source-route transparent) bridging VLAN

media {ethernet fddi fd-net tokenring tr-net}	(Optional) Specify the VLAN media type. Table 2-25 lists the valid syntax for each media type. <ul style="list-style-type: none"> • ethernet is Ethernet media type (the default). • fddi is FDDI media type. • fd-net is FDDI network entity title (NET) media type. • tokenring is Token Ring media type if the VTP v2 mode is disabled, or TrCRF if the VTP v2 mode is enabled. • tr-net is Token Ring network entity title (NET) media type if the VTP v2 mode is disabled or TrBRF media type if the VTP v2 mode is enabled.
mtu mtu-size	(Optional) Specify the maximum transmission unit (MTU) (packet size in bytes). Valid values are from 1500 to 18190.
name vlan-name	(Optional) Specify the VLAN name, an ASCII string from 1 to 32 characters that must be unique within the administrative domain.
parent parent-vlan-id	(Optional) Specify the parent VLAN of an existing FDDI, Token Ring, or TrCRF VLAN. This parameter identifies the TrBRF to which a TrCRF belongs and is required when defining a TrCRF. Valid values are from 0 to 1005.
ring ring-number	(Optional) Specify the logical ring for an FDDI, Token Ring, or TrCRF VLAN. Valid values are from 1 to 4095.
said said-value	(Optional) Enter the security association identifier (SAID) as documented in IEEE 802.10. The value is an integer from 1 to 4294967294 that must be unique within the administrative domain.
state {suspend active}	(Optional) Specify the VLAN state: <ul style="list-style-type: none"> • If active, the VLAN is operational. • If suspend, the VLAN is suspended. Suspended VLANs do not pass packets.
ste ste-number	(Optional) Specify the maximum number of spanning-tree explorer (STE) hops. This keyword applies only to TrCRF VLANs. Valid values are from 0 to 13.
stp type {ieee ibm auto}	(Optional) Specify the spanning-tree type for FDDI-NET, Token Ring-NET, or TrBRF VLAN. <ul style="list-style-type: none"> • ieee for IEEE Ethernet STP running source-route transparent (SRT) bridging. • ibm for IBM STP running source-route bridging (SRB). • auto for STP running a combination of source-route transparent bridging (IEEE) and source-route bridging (IBM).
tb-vlan1 tb-vlan1-id and tb-vlan2 tb-vlan2-id	(Optional) Specify the first and second VLAN to which this VLAN is translationally bridged. Translational VLANs translate FDDI or Token Ring to Ethernet, for example. Valid values are from 0 to 1005. Zero is assumed if no value is specified.

[Table 2-25](#) shows the valid syntax options for different media types.

vlan (VLAN configuration)**Table 2-25 Valid Syntax for Different Media Types**

Media Type	Valid Syntax
Ethernet	vlan vlan-id [name vlan-name] media ethernet [state {suspend active}] [said said-value] [mtu mtu-size] [tb-vlan1 tb-vlan1-id] [tb-vlan2 tb-vlan2-id]
FDDI	vlan vlan-id [name vlan-name] media fddi [state {suspend active}] [said said-value] [mtu mtu-size] [ring ring-number] [parent parent-vlan-id] [tb-vlan1 tb-vlan1-id] [tb-vlan2 tb-vlan2-id]
FDDI-NET	vlan vlan-id [name vlan-name] media fd-net [state {suspend active}] [said said-value] [mtu mtu-size] [bridge bridge-number] [stp type {ieee ibm auto}] [tb-vlan1 tb-vlan1-id] [tb-vlan2 tb-vlan2-id] If VTP v2 mode is disabled, do not set the stp type to auto .
Token Ring	VTP v1 mode is enabled. vlan vlan-id [name vlan-name] media tokenring [state {suspend active}] [said said-value] [mtu mtu-size] [ring ring-number] [parent parent-vlan-id] [tb-vlan1 tb-vlan1-id] [tb-vlan2 tb-vlan2-id]
Token Ring concentrator relay function (TrCRF)	VTP v2 mode is enabled. vlan vlan-id [name vlan-name] media tokenring [state {suspend active}] [said said-value] [mtu mtu-size] [ring ring-number] [parent parent-vlan-id] [bridge type {srp / srt}] [are are-number] [ste ste-number] [backuperf {enable disable}] [tb-vlan1 tb-vlan1-id] [tb-vlan2 tb-vlan2-id]
Token Ring-NET	VTP v1 mode is enabled. vlan vlan-id [name vlan-name] media tr-net [state {suspend active}] [said said-value] [mtu mtu-size] [bridge bridge-number] [stp type {ieee ibm}] [tb-vlan1 tb-vlan1-id] [tb-vlan2 tb-vlan2-id]
Token Ring bridge relay function (TrBRF)	VTP v2 mode is enabled. vlan vlan-id [name vlan-name] media tr-net [state {suspend active}] [said said-value] [mtu mtu-size] [bridge bridge-number] [stp type {ieee ibm auto}] [tb-vlan1 tb-vlan1-id] [tb-vlan2 tb-vlan2-id]

Table 2-26 describes the rules for configuring VLANs.

Table 2-26 VLAN Configuration Rules

Configuration	Rule
VTP v2 mode is enabled, and you are configuring a TrCRF VLAN media type.	Specify a parent VLAN ID of a TrBRF that already exists in the database. Specify a ring number. Do not leave this field blank. Specify unique ring numbers when TrCRF VLANs have the same parent VLAN ID. Only one backup concentrator relay function (CRF) can be enabled.
VTP v2 mode is enabled, and you are configuring VLANs other than TrCRF media type.	Do not specify a backup CRF.

Table 2-26 VLAN Configuration Rules (continued)

Configuration	Rule
VTP v2 mode is enabled, and you are configuring a TrBRF VLAN media type.	Specify a bridge number. Do not leave this field blank.
VTP v1 mode is enabled.	No VLAN can have an STP type set to auto. This rule applies to Ethernet, FDDI, FDDI-NET, Token Ring, and Token Ring-NET VLANs.
Add a VLAN that requires translational bridging (values are not set to zero).	The translational bridging VLAN IDs that are used must already exist in the database. The translational bridging VLAN IDs that a configuration points to must also contain a pointer to the original VLAN in one of the translational bridging parameters (for example, Ethernet points to FDDI, and FDDI points to Ethernet). The translational bridging VLAN IDs that a configuration points to must be different media types than the original VLAN (for example, Ethernet can point to Token Ring). If both translational bridging VLAN IDs are configured, these VLANs must be different media types (for example, Ethernet can point to FDDI and Token Ring).

Defaults

The ARE value is 7.

Backup CRF is disabled.

The bridge number is 0 (no source-routing bridge) for FDDI-NET, TrBRF, and Token Ring-NET VLANs.

The **media** type is **ethernet**.

The default *mtu size* is 1500 bytes.

The *vlan-name* variable is *VLANxxxx*, where *xxxx* represents four numeric digits (including leading zeros) equal to the VLAN ID number.

The parent VLAN ID is 0 (no parent VLAN) for FDDI and Token Ring VLANs. For TrCRF VLANs, you must specify a parent VLAN ID. For both Token Ring and TrCRF VLANs, the parent VLAN ID must already exist in the database and be associated with a Token Ring-NET or TrBRF VLAN.

The *ring number* for Token Ring VLANs is 0. For FDDI VLANs, there is no default.

The *said value* is 100000 plus the VLAN ID.

The state is **active**.

The STE value is 7.

The STP type is **ieee** for FDDI-NET and **ibm** for Token Ring-NET VLANs. For FDDI and Token Ring VLANs, the default is no type specified.

The *tb-vlan1-id* and *tb-vlan2-id* variables are zero (no translational bridging).

vlan (VLAN configuration)**Command Modes** VLAN configuration

Command History	Release	Modification
	12.0(5.2)WC(1)	This command was introduced.

Usage Guidelines You can only use this command mode for configuring normal-range VLANs, that is, VLAN IDs 1 to 1005.

To configure extended-range VLANs (VLAN IDs 1006 to 4094), use the **vlan** global configuration command.

VLAN configuration is always saved in the VLAN database. If VTP mode is transparent, it is also saved in the switch running configuration, along with the VTP mode and domain name. You can then save it in the switch startup configuration file by using the **copy running-config startup-config** privileged EXEC command.

When you save VLAN and VTP configuration in the startup configuration file and reboot the switch, the configuration is determined in these ways:

- If both the VLAN database and the configuration file show the VTP mode as transparent and the VTP domain names match, the VLAN database is ignored. The VTP and VLAN configurations in the startup configuration file are used. The VLAN database revision number remains unchanged in the VLAN database.
- If the VTP mode is server, or if the startup VTP mode or domain names do not match the VLAN database, the VTP mode and the VLAN configuration for the first 1005 VLANs use VLAN database information.
- If the image on the switch or the configuration file is earlier than IOS release 12.1(9)EA1, the switch reboots with information in the VLAN database.

The following are the results of using the **no vlan** commands:

- When the **no vlan *vlan-id*** form is used, the VLAN is deleted. Deleting VLANs automatically resets to zero any other parent VLANs and translational bridging parameters that refer to the deleted VLAN.
- When the **no vlan *vlan-id* bridge** form is used, the VLAN source-routing bridge number returns to the default (0). The **vlan *vlan-id* bridge** command is used only for FDDI-NET and Token Ring-NET VLANs and is ignored in other VLAN types.
- When the **no vlan *vlan-id* media** form is used, the media type returns to the default (**ethernet**). Changing the VLAN media type (including the **no** form) resets the VLAN MTU to the default MTU for the type (unless the **mtu** keyword is also present in the command). It also resets the VLAN parent and translational bridging VLAN to the default (unless the **parent**, **tb-vlan1**, or **tb-vlan2** are also present in the command).
- When the **no vlan *vlan-id* mtu** form is used, the VLAN MTU returns to the default for the applicable VLAN media type. You can also modify the MTU using the **media** keyword.
- When the **no vlan *vlan-id* name *vlan-name*** form is used, the VLAN name returns to the default name (*VLANxxxx*, where *xxxx* represent four numeric digits [including leading zeros] equal to the VLAN ID number).

- When the **no vlan *vlan-id* parent** form is used, the parent VLAN returns to the default (0). The parent VLAN resets to the default if the parent VLAN is deleted or if the **media** keyword changes the VLAN type or the VLAN type of the parent VLAN.
- When the **no vlan *vlan-id* ring** form is used, the VLAN logical ring number returns to the default (0).
- When the **no vlan *vlan-id* said** form is used, the VLAN SAID returns to the default (100,000 plus the VLAN ID).
- When the **no vlan *vlan-id* state** form is used, the VLAN state returns to the default (**active**).
- When the **no vlan *vlan-id* stp type** form is used, the VLAN spanning-tree type returns to the default (**ieee**).
- When the **no vlan *vlan-id* tb-vlan1** or **no vlan *vlan-id* tb-vlan2** form is used, the VLAN translational bridge VLAN (or VLANs, if applicable) returns to the default (0). Translational bridge VLANs must be a different VLAN type than the affected VLAN, and if two are specified, the two must be different VLAN types from each other. A translational bridge VLAN resets to the default if the translational bridge VLAN is deleted, if the **media** keyword changes the VLAN type, or if the **media** keyword changes the VLAN type of the corresponding translation bridge VLAN.

Examples

This example shows how to add an Ethernet VLAN with default media characteristics. The default includes a *vlan-name* of *VLANxxx*, where *xxxx* represents four numeric digits (including leading zeros) equal to the VLAN ID number. The default **media** option is **ethernet**; the **state** option is **active**. The default *said-value* variable is 100000 plus the VLAN ID; the *mtu-size* variable is 1500; the **stp-type** option is **ieee**. When you enter the **exit** or **apply** vlan configuration command, the VLAN is added if it did not already exist; otherwise, this command does nothing.

```
Switch(vlan)# vlan 2
VLAN 2 added:
  Name: VLAN0002
Switch(vlan)# exit
APPLY completed.
Exiting....
```

This example shows how to modify an existing VLAN by changing its name and MTU size:

```
Switch(vlan)# no vlan name engineering mtu 1200
```

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

Related Commands

Command	Description
show vlan	Displays the parameters for all configured VLANs or one VLAN (if the VLAN ID or name is specified) in the administrative domain.
vlan (global configuration)	Enters config-vlan mode for configuring normal-range and extended-range VLANs.

vlan database

Use the **vlan database** privileged EXEC command to enter VLAN configuration mode. From this mode, you can add, delete, and modify VLAN configurations for normal-range VLANs and globally propagate these changes by using the VLAN Trunking Protocol (VTP). Configuration information is saved in the VLAN database.

vlan database


Note

VLAN configuration mode is only valid for VLAN IDs 1 to 1005.

Syntax Description This command has no arguments or keywords.

Defaults No default is defined.

Command Modes Privileged EXEC

Command History

Release	Modification
12.0(5.2)WC(1)	This command was introduced.

Usage Guidelines

You can use the VLAN database configuration commands to configure VLANs 1 to 1005. To configure extended-range VLANs (VLAN IDs 1006 to 4094) (when the enhanced software image (EI) is installed), use the **vlan (global configuration)** command to enter config-vlan mode. You can also configure VLAN IDs 1 to 1005 by using the **vlan** global configuration command.

To return to the privileged EXEC mode from the VLAN configuration mode, enter the **exit** command.


Note

This command mode is different from other modes because it is session-oriented. When you add, delete, or modify VLAN parameters, the changes are not applied until you exit the session by entering the **apply** or **exit** command. When the changes are applied, the VTP configuration version is incremented. You can also *not* apply the changes to the VTP database by entering **abort**.

Once you are in VLAN configuration mode, you can access the VLAN database and make changes by using these commands:

- **vlan**: accesses subcommands to add, delete, or modify values associated with a single VLAN. For more information, see the **vlan (VLAN configuration)** command.
- **vtp**: accesses subcommands to perform VTP administrative functions. For more information, see the **vtp (VLAN configuration)** command.

When you have modified VLAN or VTP parameters, you can use these editing buffer manipulation commands:

- **abort**: exits the mode without applying the changes. The VLAN configuration that was running before you entered VLAN configuration mode continues to be used.
- **apply**: applies current changes to the VLAN database, increments the database configuration revision number, propagates it throughout the administrative domain, and remains in VLAN configuration mode.



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

- **exit**: applies all configuration changes to the VLAN database, increments the database configuration number, propagates it throughout the administrative domain, and returns to privileged EXEC mode.
- **no**: negates a command or set its defaults; valid values are **vlan** and **vtp**.
- **reset**: abandons proposed changes to the VLAN database, resets the proposed database to the implemented VLAN database on the switch, and remains in VLAN configuration mode.
- **show**: displays VLAN database information.
- **show changes [vlan-id]**: displays the differences between the VLAN database on the switch and the proposed VLAN database for all normal-range VLAN IDs (1 to 1005) or the specified VLAN ID (1 to 1005).
- **show current [vlan-id]**: displays the VLAN database on the switch or on a selected VLAN (1 to 1005).
- **show proposed [vlan-id]**: displays the proposed VLAN database or a selected VLAN (1 to 1005) from the proposed database. The proposed VLAN database is not the running configuration until you use the **exit** or **apply** VLAN configuration command.

You can verify that VLAN database changes have been made or aborted by using the **show vlan** privileged EXEC command. This output is different from the **show VLAN** database configuration command output.

Examples

This example shows how to enter the VLAN configuration mode from the privileged EXEC mode and to display VLAN database information:

```

Switch# vlan database
Switch(vlan)# show
Name: default
  Media Type: Ethernet
  VLAN 802.10 Id: 100001
  State: Operational
  MTU: 1500
  Translational Bridged VLAN: 1002
  Translational Bridged VLAN: 1003

Name: VLAN0002
  Media Type: Ethernet
  VLAN 802.10 Id: 100002
  State: Operational
  MTU: 1500

Name: fddi-default
  Media Type: FDDI
  VLAN 802.10 Id: 101002
  State: Operational

```

vlan database

```

MTU: 1500
Bridge Type: SRB
Ring Number: 0
Translational Bridged VLAN: 1
Translational Bridged VLAN: 1003

<output truncated>

```

This is an example of output from the **show changes** command:

```
Switch(vlan)# show changes
```

```

DELETED:
Name: VLAN0004
    Media Type: Ethernet
    VLAN 802.10 Id: 100004
    State: Operational
    MTU: 1500

DELETED:
Name: VLAN0006
    Media Type: Ethernet
    VLAN 802.10 Id: 100006
    State: Operational
    MTU: 1500

MODIFIED:
Current State: Operational
    Modified State: Suspended

```

This example shows how to display the differences between VLAN 7 in the current database and the proposed database.

```
Switch(vlan)# show changes 7
```

```

MODIFIED:
Current State: Operational
    Modified State: Suspended

```

This is an example of output from the **show current 20** command. It displays only VLAN 20 of the current database.

```
Switch(vlan)# show current 20
Name: VLAN0020
    Media Type: Ethernet
    VLAN 802.10 Id: 100020
    State: Operational
    MTU: 1500
```

Related Commands

Command	Description
show vlan	Displays the parameters for all configured VLANs in the administrative domain.
shutdown vlan	Shuts down (suspects) local traffic on the specified VLAN.
vlan (global configuration)	Enters config-vlan mode for configuring normal-range and extended-range VLANs.

vmpls reconfirm (global configuration)

Use the **vmpls reconfirm** global configuration command to change the reconfirmation interval for the VLAN Query Protocol (VQP) client.

vmpls reconfirm *interval*

Syntax Description	<i>interval</i> Reconfirmation interval for VQP client queries to the VLAN Membership Policy Server (VMPS) to reconfirm dynamic VLAN assignments. The interval range is from 1 to 120 minutes.
---------------------------	--

Defaults The default reconfirmation interval is 60 minutes.

Command Modes Global configuration

Command History	Release	Modification
	12.1(6)EA2	This command was introduced.

Examples This example shows how to set the VQP client to reconfirm dynamic VLAN entries every 20 minutes:

```
Switch(config)# vmpls reconfirm 20
```

You can verify your settings by entering the **show vmpls** privileged EXEC command and examining information in the Reconfirm Interval row.

Related Commands	Command	Description
	show vmpls	Displays VQP and VMPS information.
	vmpls reconfirm (privileged EXEC)	Sends VQP queries to reconfirm all dynamic VLAN assignments with the VMPS.

■ vmps reconfirm (privileged EXEC)

vmps reconfirm (privileged EXEC)

Use the **vmps reconfirm** privileged EXEC command to immediately send VLAN Query Protocol (VQP) queries to reconfirm all dynamic VLAN assignments with the VLAN Membership Policy Server (VMPS).

vmps reconfirm

Syntax Description This command has no arguments or keywords.

Defaults No default is defined.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(6)EA2	This command was introduced.

Examples This example shows how to send VQP queries to the VMPS:

```
Switch# vmps reconfirm
```

You can verify your settings by entering the **show vmps** privileged EXEC command and examining the VMPS Action row of the Reconfirmation Status section. The **show vmps** command shows the result of the last time the assignments were reconfirmed either as a result of the reconfirmation timer expired or because the **vmps reconfirm** command was entered.

Related Commands	Command	Description
	show vmps	Displays VQP and VMPS information.
	vmps reconfirm (global configuration)	Changes the reconfirmation interval for the VLAN Query Protocol (VQP) client.

vmpls retry

Use the **vmpls retry** global configuration command to configure the per-server retry count for the VLAN Query Protocol (VQP) client.

vmpls retry *count*

Syntax Description	<i>count</i> Number of attempts to contact the VLAN Membership Policy Server (VMPS) by the client before querying the next server in the list. The retry range is from 1 to 10.
---------------------------	---

Defaults	The default retry count is 3.
-----------------	-------------------------------

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

Command History	Release	Modification
	12.1(6)EA2	This command was introduced.

Examples	This example shows how to set the retry count to 7:
	Switch(config)# vmpls retry 7

You can verify your settings by entering the **show vmpls** privileged EXEC command and examining information in the Server Retry Count row.

Related Commands	Command	Description
	show vmpls	Displays VQP and VMPS information.

vmpls server

Use the **vmpls server** global configuration command to configure the primary VLAN Membership Policy Server (VMPS) and up to three secondary servers. Use the **no** form of this command to remove a VMPS server.

vmpls server *ipaddress* [primary]

no vmpls server [*ipaddress*]

Syntax Description	<p><i>ipaddress</i> IP address or host name of the primary or secondary VMPS servers. If you specify a host name, the Domain Name System (DNS) server must be configured.</p> <p>primary (Optional) Determines whether primary or secondary VMPS servers are being configured.</p>
---------------------------	--

Defaults	No primary or secondary VMPS servers are defined.
-----------------	---

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

Command History	Release	Modification
	12.1(6)EA2	This command was introduced.

Usage Guidelines	<p>The first server entered is automatically selected as the primary server whether or not the primary keyword is entered. The first server address can be overridden by using primary in a subsequent command.</p> <p>If a member switch in a cluster configuration does not have an IP address, the cluster does not use the VMPS server configured for that member switch. Instead, the cluster uses the VMPS server on the command switch, and the command switch proxies the VMPS requests. The VMPS server treats the cluster as a single switch and uses the IP address of the command switch to respond to requests.</p> <p>When using the no form without specifying the <i>ipaddress</i>, all configured servers are deleted. If you delete all servers when dynamic-access ports are present, the switch cannot forward packets from new sources on these ports because it cannot query the VMPS.</p>
-------------------------	---

Examples	<p>This example shows how to configure the server with IP address 191.10.49.20 as the primary VMPS server. The servers with IP addresses 191.10.49.21 and 191.10.49.22 are configured as secondary servers.</p>
-----------------	---

```
Switch(config)# vmpls server 191.10.49.20 primary
Switch(config)# vmpls server 191.10.49.21
Switch(config)# vmpls server 191.10.49.22
```

This example shows how to delete the server with IP address 191.10.49.21:

```
Switch(config)# no vmpls server 191.10.49.21
```

You can verify your settings by entering the **show vmpls** privileged EXEC command and examining information in the VMPS Domain Server row.

Related Commands	Command	Description
	show vmpls	Displays VQP and VMPS information.

vtp (global configuration)

vtp (global configuration)

Use the **vtp** global configuration command to set or modify the VLAN Trunking Protocol (VTP) configuration characteristics. Use the **no** form of this command to remove the settings or to return to the default settings.

```
vtp {domain domain-name | file filename | interface name | mode {client | server | transparent} | password password | pruning | version number}  
no vtp {file | interface | mode | password | pruning | version}
```

Syntax Description		
domain domain-name	Specify the VTP domain name, an ASCII string from 1 to 32 characters that identifies the VTP administrative domain for the switch. The domain name is case sensitive.	
file filename	Specify the IOS file system file where the VTP VLAN configuration is stored.	
interface name	Specify the name of the interface providing the VTP ID updated for this device.	
mode	Specify the VTP device mode as client, server, or transparent.	
client	Place the switch in VTP client mode. A switch in VTP client mode is enabled for VTP, and can send advertisements, but does not have enough nonvolatile storage to store VLAN configurations. You cannot configure VLANs on the switch. When a VTP client starts up, it does not send VTP advertisements until it receives advertisements to initialize its VLAN database.	
server	Place the switch in VTP server mode. A switch in VTP server mode is enabled for VTP and sends advertisements. You can configure VLANs on the switch. The switch can recover all the VLAN information in the current VTP database from nonvolatile storage after reboot.	
transparent	Place the switch in VTP transparent mode. A switch in VTP transparent mode is disabled for VTP, does not send advertisements or learn from advertisements sent by other devices, and cannot affect VLAN configurations on other devices in the network. The switch receives VTP advertisements and forwards them on all trunk ports except the one on which the advertisement was received. When VTP mode is transparent, the mode and domain name are saved in the switch running configuration file, and you can save them in the switch startup configuration file by entering the copy running-config startup config privileged EXEC command.	
password password	Set the administrative domain password for the generation of the 16-byte secret value used in MD5 digest calculation to be sent in VTP advertisements and to validate received VTP advertisements. The password can be an ASCII string from 1 to 32 characters. The password is case sensitive.	
pruning	Enable VTP pruning on the switch.	
version number	Set VTP version to version 1 or version 2.	

Defaults The default filename is *flash:vlan.dat*.

The default mode is server mode.

No domain name or password is defined.

No password is configured.

Pruning is disabled.

The default version is version 1.

Command Modes Global configuration

Command History	Release	Modification
	12.0(5.2)WC(1)	This command was introduced.
	12.1(6)EA2	The if-id keyword was added.
	12.1(9)EA1	The domain and mode keywords were added. The if-id keyword was replaced by the interface keyword.
	12.1(11)EA1	The password , pruning , and version keywords were added.

Usage Guidelines When you save VTP mode and domain name and VLAN configurations in the switch startup configuration file and reboot the switch, the VTP and VLAN configurations are determined by these conditions:

- If both the VLAN database and the configuration file show the VTP mode as transparent and the VTP domain names match, the VLAN database is ignored. The VTP and VLAN configurations in the startup configuration file are used. The VLAN database revision number remains unchanged in the VLAN database.
- If the startup VTP mode is server mode, or the startup VTP mode or domain names do not match the VLAN database, VTP mode and VLAN configuration for the first 1005 VLANs are determined by VLAN database information, and VLANs greater than 1005 are configured from the switch configuration file.
- If the image on the switch or the configuration file is earlier than IOS Release 12.1(9)EA1, the switch reboots using the information in the VLAN database.

The **vtp file** *filename* cannot be used to load a new database; it renames only the file in which the existing database is stored.

Follow these guidelines when configuring a VTP domain name:

- The switch is in the no-management-domain state until you configure a domain name. While in the no-management-domain state, the switch does not send any VTP advertisements even if changes occur to the local VLAN configuration. The switch leaves the no-management-domain state after it receives the first VTP summary packet on any port that is trunking or after you configure a domain name by using the **vtp domain** command. If the switch receives its domain from a summary packet, it resets its configuration revision number to 0. After the switch leaves the no-management-domain state, it can not be configured to re-enter it until you clear the nonvolatile RAM (NVRAM) and reload the software.
- Domain names are case-sensitive.

vtp (global configuration)

- After you configure a domain name, it cannot be removed. You can only reassign it to a different domain.

Follow these guidelines when setting VTP mode:

- The **no vtp mode** command returns the switch to VTP server mode.
- The **vtp mode server** command is the same as **no vtp mode** except that it does not return an error if the switch is not in client or transparent mode.
- If the receiving switch is in client mode, the client switch changes its configuration to duplicate the configuration of the server. If you have switches in client mode, be sure to make all VTP or VLAN configuration changes on a switch in server mode. If the receiving switch is in server mode or transparent mode, the switch configuration is not changed.
- Switches in transparent mode do not participate in VTP. If you make VTP or VLAN configuration changes on a switch in transparent mode, the changes are not propagated to other switches in the network.
- If you change the VTP or VLAN configuration on a switch that is in server mode, that change is propagated to all the switches in the same VTP domain.
- The **vtp mode transparent** command disables VTP from the domain but does not remove the domain from the switch.
- The VTP mode must be transparent for you to add extended-range VLANs or for VTP and VLAN information to be saved in the running configuration file.
- If extended-range VLANs are configured on the switch and you attempt to set the VTP mode to server or client, you receive an error message, and the configuration is not allowed.
- VTP can be set to either server or client mode only when dynamic VLAN creation is disabled.

Follow these guidelines when setting a VTP password:

- Passwords are case sensitive. Passwords should match on all switches in the same domain.
- When you use the **no vtp password** form of the command, the switch returns to the no-password state.

Follow these guidelines when setting VTP pruning:

- VTP pruning removes information about each pruning-eligible VLAN from VTP updates if there are no stations belonging to that VLAN.
- If you enable pruning on the VTP server, it is enabled for the entire management domain for VLAN IDs 1 to 1005.
- Only VLANs in the pruning-eligible list can be pruned.
- Pruning is supported with VTP version 1 and version 2.

Follow these guidelines when setting the VTP version:

- Toggling the version 2 (v2) mode state modifies parameters of certain default VLANs.
- Each VTP switch automatically detects the capabilities of all the other VTP devices. To use version 2, all VTP switches in the network must support version 2; otherwise, you must configure them to operate in VTP version 1 mode.
- If all switches in a domain are VTP version 2-capable, you need only to configure version 2 on one switch; the version number is then propagated to the other version-2 capable switches in the VTP domain.
- If you are using VTP in a Token Ring environment, VTP version 2 must be enabled.

- If you are configuring a Token Ring bridge relay function (TrBRF) or Token Ring concentrator relay function (TrCRF) VLAN media type, you must use version 2.
 - If you are configuring a Token Ring or Token Ring-NET VLAN media type, you must use version 1.
- You cannot save password, pruning, and version configurations in the switch configuration file.

Examples

This example shows how to rename the filename for VTP configuration storage to *vtpfilename*:

```
Switch(config)# vtp file vtpfilename
```

This example shows how to clear the device storage filename:

```
Switch(config)# no vtp file vtpconfig
Clearing device storage filename.
```

This example shows how to specify the name of the interface providing the VTP updater ID for this device:

```
Switch(config)# vtp interface fastethernet
```

This example shows how to set the administrative domain for the switch:

```
Switch(config)# vtp domain OurDomainName
```

This example shows how to place the switch in VTP transparent mode:

```
Switch(config)# vtp mode transparent
```

This example shows how to configure the VTP domain password:

```
Switch(config)# vtp password ThisIsOurDomain'sPassword
```

This example shows how to enable pruning in the VLAN database:

```
Switch(config)# vtp pruning
Pruning switched ON
```

This example shows how to enable version 2 mode in the VLAN database:

```
Switch(config)# vtp version 2
```

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

Related Commands

Command	Description
show vtp status	Displays the VTP statistics for the switch and general information about the VTP management domain status.
vtp (VLAN configuration)	Configures most VTP characteristics.

vtp (privileged EXEC)

vtp (privileged EXEC)

Use the **vtp** privileged EXEC command to configure the VLAN Trunking Protocol (VTP) password, pruning, and version. Use the **no** form of this command to return to the default settings.

vtp {password *password* | pruning | version *number*}

no vtp {password | pruning | version}

**Note**

Beginning with release 12.1(11)EA1, these keywords are available in the **vtp** global configuration command. This command will become obsolete in a future release.

Syntax Description

password <i>password</i>	Set the administrative domain password for the generation of the 16-byte secret value used in MD5 digest calculation to be sent in VTP advertisements and to validate received VTP advertisements. The password can be an ASCII string from 1 to 32 characters. The password is case sensitive.
pruning	Enable VTP pruning on the switch.
version <i>number</i>	Set VTP version to version 1 or version 2.

Defaults

No password is configured.

Pruning is disabled.

The default version is version 1.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(9)EA1	This command was introduced.

Usage Guidelines

Passwords are case sensitive. Passwords should match on all switches in the same domain.

When you use the **no vtp password** form of the command, the switch returns to the no-password state.

VTP pruning removes information about each pruning-eligible VLAN from VTP updates if there are no stations belonging to that VLAN.

If you enable pruning on the VTP server, it is enabled for the entire management domain for VLAN IDs 1 to 1005.

Only VLANs in the pruning-eligible list can be pruned.

Pruning is supported with VTP version 1 and version 2.

Toggling the version 2 (v2) mode state modifies parameters of certain default VLANs.

Each VTP switch automatically detects the capabilities of all the other VTP devices. To use version 2, all VTP switches in the network must support version 2; otherwise, you must configure them to operate in VTP version 1 mode.

If all switches in a domain are VTP version 2-capable, you need only to configure version 2 on one switch; the version number is then propagated to the other version-2 capable switches in the VTP domain.

If you are using VTP in a Token Ring environment, VTP version 2 must be enabled.

If you are configuring a Token Ring bridge relay function (TrBRF) or Token Ring concentrator relay function (TrCRF) VLAN media type, you must use version 2.

If you are configuring a Token Ring or Token Ring-NET VLAN media type, you must use version 1.

You cannot save password, pruning, and version configuration in the switch configuration file.

Examples

This example shows how to configure the VTP domain password:

```
Switch# vtp password ThisIsOurDomain'sPassword
```

This example shows how to enable pruning in the VLAN database:

```
Switch# vtp pruning
Pruning switched ON
```

This example shows how to enable version 2 mode in the VLAN database:

```
Switch# vtp version 2
```

You can verify your setting by entering the **show vtp status** privileged EXEC command.

Related Commands

Command	Description
show vtp status	Displays the VTP statistics for the switch and general information about the VTP management domain status.
switchport trunk pruning	Configures the VLAN pruning-eligible list for ports in trunking mode.
vtp (global configuration)	Configures the VTP filename, interface, domain-name, and mode, which can be saved in the switch configuration file.
vtp (VLAN configuration)	Configures all VTP characteristics but cannot be saved to the switch configuration file.

vtp (VLAN configuration)

vtp (VLAN configuration)

Use the **vtp** VLAN configuration command to configure VLAN Trunking Protocol (VTP) characteristics. You access VLAN configuration mode by entering the **vlan database** privileged EXEC command. Use the **no** form of this command to return to the default settings, disable the characteristic, or remove the password.

```
vtp {domain domain-name | password password | pruning | v2-mode | {server | client | transparent}}
```

```
no vtp {client | password | pruning | transparent | v2-mode}
```

**Note**

VTP configuration in VLAN configuration mode is saved in the VLAN database when applied.

Syntax Description

domain <i>domain-name</i>	Set the VTP domain name by entering an ASCII string from 1 to 32 characters that identifies the VTP administrative domain for the switch. The domain name is case sensitive.
password <i>password</i>	Set the administrative domain password for the generation of the 16-byte secret value used in MD5 digest calculation to be sent in VTP advertisements and to validate received VTP advertisements. The password can be an ASCII string from 1 to 32 characters. The password is case sensitive.
pruning	Enable pruning in the VTP administrative domain. VTP pruning causes information about each pruning-eligible VLAN to be removed from VTP updates if there are no stations belonging to that VLAN.
v2-mode	Enable VLAN Trunking Protocol (VTP) version 2 in the administrative domains.
client	Place the switch in VTP client mode. A switch in VTP client mode is enabled for VTP, can send advertisements, but does not have enough nonvolatile storage to store VLAN configurations. You cannot configure VLANs on it. When a VTP client starts up, it does not send VTP advertisements until it receives advertisements to initialize its VLAN database.
server	Place the switch in VTP server mode. A switch in VTP server mode is enabled for VTP and sends advertisements. You can configure VLANs on it. The switch can recover all the VLAN information in the current VTP database from nonvolatile storage after reboot.
transparent	Place the switch in VTP transparent mode. A switch in VTP transparent mode is disabled for VTP, does not send advertisements or learn from advertisements sent by other devices, and cannot affect VLAN configurations on other devices in the network. The switch receives VTP advertisements and forwards them on all trunk ports except the one on which the advertisement was received.

Defaults

The default mode is server mode.

No domain name is defined.

No password is configured.

Pruning is disabled.

VTP version 2 (v2 mode) is disabled.

Command Modes	VLAN configuration
----------------------	--------------------

Command History	Release	Modification
	12.0(5.2)WC(1)	This command was introduced.

Usage Guidelines	If VTP mode is transparent, the mode and domain name are saved in the switch running configuration file, and you can save the configuration in the switch startup configuration file by using the copy running-config startup-config privileged EXEC command.
-------------------------	--

Follow these guidelines when setting VTP mode:

- The **no vtp client** and **no vtp transparent** forms of the command return the switch to VTP server mode.
- The **vtp server** command is the same as **no vtp client** or **no vtp transparent** except that it does not return an error if the switch is not in client or transparent mode.
- If the receiving switch is in client mode, the client switch changes its configuration to duplicate the configuration of the server. If you have switches in client mode, make sure to make all VTP or VLAN configuration changes on a switch in server mode. If the receiving switch is in server mode or transparent mode, the switch configuration is not changed.
- Switches in transparent mode do not participate in VTP. If you make VTP or VLAN configuration changes on a switch in transparent mode, the changes are not propagated to other switches in the network.
- If you make a change to the VTP or VLAN configuration on a switch in server mode, that change is propagated to all the switches in the same VTP domain.
- The **vtp transparent** command disables VTP from the domain but does not remove the domain from the switch.
- The VTP mode must be transparent for you to add extended-range VLANs or for the VTP and the VLAN configurations to be saved in the running configuration file.
- If extended-range VLANs are configured on the switch and you attempt to set the VTP mode to server or client, you receive an error message and the configuration is not allowed.
- VTP can be set to either server or client mode only when dynamic VLAN creation is disabled.

Follow these guidelines when configuring a VTP domain name:

- The switch is in the no-management-domain state until you configure a domain name. While in the no-management-domain state, the switch does not send any VTP advertisements even if changes occur to the local VLAN configuration. The switch leaves the no-management-domain state after receiving the first VTP summary packet on any port that is currently trunking or after configuring a domain name using the **vtp domain** command. If the switch receives its domain from a summary packet, it resets its configuration revision number to zero. After the switch leaves the no-management-domain state, it can never be configured to reenter it until you clear the nonvolatile RAM (NVRAM) and reload the software.

vtp (VLAN configuration)

- Domain names are case sensitive.
- After you configure a domain name, it cannot be removed. You can reassign it only to a different domain.

Follow these guidelines when configuring a VTP password:

- Passwords are case sensitive. Passwords should match on all switches in the same domain.
- When the **no vtp password** form of the command is used, the switch returns to the no-password state.

Follow these guidelines when enabling VTP pruning:

- If you enable pruning on the VTP server, it is enabled for the entire management domain.
- Only VLANs included in the pruning-eligible list can be pruned.
- Pruning is supported with VTP version 1 and version 2.

Follow these guidelines when enabling VTP version 2 (v2-mode):

- Toggling the version (v2-mode) state modifies certain parameters of certain default VLANs.
- Each VTP switch automatically detects the capabilities of all the other VTP devices. To use VTP version 2, all VTP switches in the network must support version 2; otherwise, you must configure them to operate in VTP version 1 (**no vtp v2-mode**).
- If all switches in a domain are VTP version 2-capable, you need only to enable VTP version 2 on one switch; the version number is then propagated to the other version-2 capable switches in the VTP domain.
- If you are using VTP in a Token Ring environment or configuring a Token Ring bridge relay function (TrBRF) or Token Ring concentrator relay function (TrCRF) VLAN media type, VTP version 2 (**v2-mode**) must be enabled.
- If you are configuring a Token Ring or Token Ring-NET VLAN media type, you must use VTP version 1.

Examples

This example shows how to place the switch in VTP transparent mode:

```
Switch(vlan)# vtp transparent
Setting device to VTP TRANSPARENT mode.
```

This example shows how to set the administrative domain for the switch:

```
Switch(vlan)# vtp domain OurDomainName
Changing VTP domain name from cisco to OurDomainName
```

This example shows how to configure the VTP domain password:

```
Switch(vlan)# vtp password private
Setting device VLAN database password to private.
```

This example shows how to enable pruning in the proposed new VLAN database:

```
Switch(vlan)# vtp pruning
Pruning switched ON
```

This example shows how to enable V2 mode in the proposed new VLAN database:

```
Switch(vlan)# vtp v2-mode
V2 mode enabled.
```

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

Related Commands	Command	Description
	show vtp status	Displays the VTP statistics for the switch and general information about the VTP management domain status.
	switchport trunk pruning	Configures the VLAN pruning-eligible list for ports in trunking mode.
	vtp (global configuration)	Configures the VTP filename, interface, domain-name, and mode.

wrr-queue bandwidth

wrr-queue bandwidth

Use the **wrr-queue bandwidth** global configuration command to assign weighted round-robin (WRR) weights to the four class of service (CoS) priority queues. Use the **no** form of this command to disable the WRR scheduler and enable the strict priority scheduler.

wrr-queue bandwidth *weight1...weight4*

no wrr-queue bandwidth

Syntax Description	<i>weight1...weight4</i>	The ratio of weight1, weight2, weight3, and weight4 determines the weights of the WRR scheduler. Ranges are 1 to 255.
---------------------------	--------------------------	---

Defaults	WRR is disabled. The strict priority is the default scheduler.
-----------------	--

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

Command History	Release	Modification
	12.0(5.2)WC(1)	This command was introduced.

Usage Guidelines	WRR allows bandwidth sharing at the egress port. This command defines the bandwidths for egress WRR through scheduling weights.
-------------------------	---

Examples	This example shows how to assign WRR weights of 10, 20, 30, and 40 to the CoS priority queues 1, 2, 3, and 4:
-----------------	---

```
Switch(config)# wrr-queue bandwidth 10 20 30 40
```

This example shows how to disable the WRR scheduler and enable the strict priority scheduler:

```
Switch(config)# no wrr-queue bandwidth
```

You can verify your settings by entering the **show wrr-queue bandwidth** privileged EXEC command.

Related Commands	Command	Description
	wrr-queue cos-map	Assigns CoS values to the CoS priority queues.
	show wrr-queue bandwidth	Displays the WRR bandwidth allocation for the four CoS priority queues.
	show wrr-queue cos-map	Displays the mapping of the CoS to the CoS priority queues.

wrr-queue cos-map

Use the **wrr-queue cos-map** global configuration command to assign class of service (CoS) values to the CoS priority queues. Use the **no** form of this command to set the CoS map to default setting.

wrr-queue cos-map *quid cos1...cosn*

no wrr-queue cos-map

Syntax Description	<i>quid</i>	The queue id of the CoS priority queue. Ranges are 1 to 4 where 1 is the lowest CoS priority queue.
	<i>cos1...cosn</i>	The CoS values that are mapped to the queue id.

Defaults

These are the default CoS values:

CoS Value	CoS Priority Queues
0, 1	1
2, 3	2
4, 5	3
6, 7	4

Command Modes

Global configuration

Command History

Release	Modification
12.0(5.2)WC(1)	This command was introduced.

Usage Guidelines

CoS assigned at the ingress port is used to select a CoS priority at the egress port.

Examples

This example shows how to map CoS values 0, 1, and 2 to CoS priority queue 1, value 3 to CoS priority queue 2, values 4 and 5 to CoS priority 3, and values 6 and 7 to CoS priority queue 4:

```
Switch(config)# wrr-queue cos-map 1 0 1 2
Switch(config)# wrr-queue cos-map 2 3
Switch(config)# wrr-queue cos-map 3 4 5
Switch(config)# wrr-queue cos-map 4 6 7
```

This example shows how to map CoS values 0, 1, 2, and 3 to CoS priority queue 2:

```
Switch(config)# wrr-queue cos-map 2 0 1 2 3
```

wrr-queue cos-map

After entering the **wrr-queue cos-map 2 0 1 2 3** command, if all other priority queues use their default setting, this is the new mapping:

CoS Value	CoS Priority Queue
Not applied	1
0, 1, 2, 3	2
4, 5	3
6, 7	4

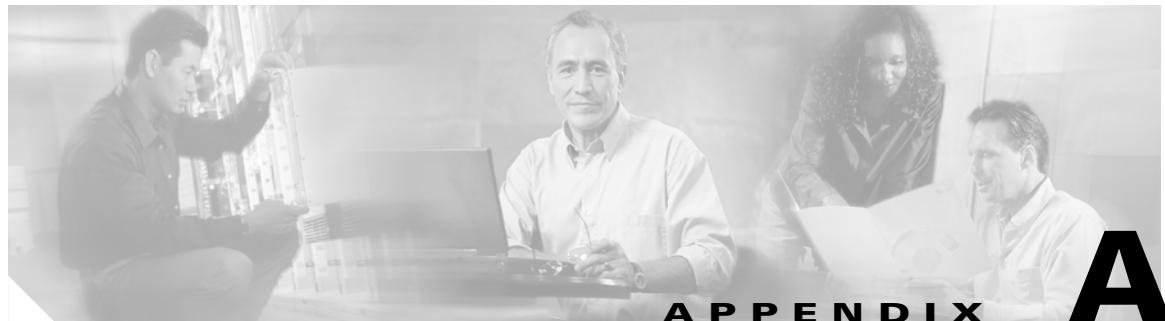
In the previous example, CoS priority queue 1 is no longer used because no CoS value is assigned to the queue.

You can set the CoS values to the default values by entering the **no wrr-queue cos-map** global configuration command.

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

Related Commands

Command	Description
wrr-queue bandwidth	Assigns weighted round-robin (WRR) weights to the four CoS priority queues.
show wrr-queue bandwidth	Displays the WRR bandwidth allocation for the four CoS priority queues.
show wrr-queue cos-map	Displays the mapping of the CoS to the priority queues.



Debug Commands

This appendix describes the Catalyst 2950-specific **debug** privileged EXEC commands. These commands are helpful in diagnosing and resolving internetworking problems and should be used only with the guidance of Cisco technical support staff.



Caution

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use the **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. It is best to use the **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

debug dot1x

debug dot1x

Use the **debug dot1x** privileged EXEC command to enable debugging of the 802.1X feature. Use the **no** form of this command to disable debugging output.

debug dot1x {all | authsm | backend | besm | core | reauthsm}

no debug dot1x {all | authsm | backend | besm | core | reauthsm}

Syntax Description	all Enable debugging of all conditions. authsm Enable debugging of the authenticator state machine, which is responsible for controlling access to the network through 802.1X-enabled ports. backend Enable debugging of the interaction between the 802.1X process and the switch (Remote Authentication Dial-In User Service [RADIUS] client). besm Enable debugging of the backend state machine, which is responsible for relaying authentication request between the client and the authentication server. core Enable debugging of the 802.1X process, which includes 802.1X initialization, configuration, and the interaction with the port manager module. reauthsm Enable debugging of the re-authentication state machine, which manages periodic re-authentication of the client.						
Defaults	Debugging is disabled.						
Command Modes	Privileged EXEC						
Command History	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>12.1(6)EA2</td><td>This command was first introduced.</td></tr> </tbody> </table>	Release	Modification	12.1(6)EA2	This command was first introduced.		
Release	Modification						
12.1(6)EA2	This command was first introduced.						
Usage Guidelines	The undebbug dot1x command is the same as the no debug dot1x command.						
Related Commands	<table border="1"> <thead> <tr> <th>Command</th><th>Description</th></tr> </thead> <tbody> <tr> <td>show debugging</td><td>Displays information about the types of debugging that are enabled. For syntax information, refer to Cisco IOS Configuration Fundamentals Command Reference For IOS Release 12.1 > Cisco IOS System Management Commands > Troubleshooting Commands.</td></tr> <tr> <td>show controllers lre version</td><td>Displays 802.1X statistics, administrative status, and operational status for the switch or for the specified interface.</td></tr> </tbody> </table>	Command	Description	show debugging	Displays information about the types of debugging that are enabled. For syntax information, refer to Cisco IOS Configuration Fundamentals Command Reference For IOS Release 12.1 > Cisco IOS System Management Commands > Troubleshooting Commands .	show controllers lre version	Displays 802.1X statistics, administrative status, and operational status for the switch or for the specified interface.
Command	Description						
show debugging	Displays information about the types of debugging that are enabled. For syntax information, refer to Cisco IOS Configuration Fundamentals Command Reference For IOS Release 12.1 > Cisco IOS System Management Commands > Troubleshooting Commands .						
show controllers lre version	Displays 802.1X statistics, administrative status, and operational status for the switch or for the specified interface.						

debug etherchannel

Use the **debug etherchannel** privileged EXEC command for EtherChannel/Port Aggregation Protocol (PAgP) shim debugging. This shim is the software module that is the interface between the PAgP software module and the port manager software module. Use the **no** form of this command to disable debugging output.

debug etherchannel [all | detail | error | event | idb | linecard]

no debug etherchannel [all | detail | error | event | idb | linecard]

Syntax Description	all (Optional) Display all EtherChannel debug messages. detail (Optional) Display detailed EtherChannel debug messages. error (Optional) Display EtherChannel error debug messages. event (Optional) Debug major EtherChannel event messages. idb (Optional) Debug PAgP interface descriptor block messages. linecard (Optional) Keyword to debug Switch-Module Configuration Protocol messages to the line card.
--------------------	--

Defaults	Debugging is disabled.
Command Modes	Privileged EXEC

Command History	Release	Modification
	12.1(6)EA2	This command was first introduced.

Usage Guidelines	If you do not specify a keyword, all debug messages appear. The undebug etherchannel command is the same as the no debug etherchannel command.
------------------	---

Related Commands	Command	Description
	show debugging	Displays information about the types of debugging that are enabled. For syntax information, refer to Cisco IOS Configuration Fundamentals Command Reference For IOS Release 12.1 > Cisco IOS System Management Commands > Troubleshooting Commands .
	show etherchannel	Displays EtherChannel information for the channel.

debug lre

debug lre

Use the **debug lre** privileged EXEC command for debugging Long-Reach Ethernet (LRE) switches and links. Use the **no** form of this command to disable debugging output.

debug lre [controller | discovery | errors | profile | state | timing | upgrade] [interface-id]

no debug lre [controller | discovery | errors | profile | state | timing | upgrade] [interface-id]

Syntax Description

controller	Enables debugging of the switch.
discovery	Enables customer premises equipment (CPE) discovery debugging.
errors	Enables error debugging.
profile	Enables profile debugging.
state	Enables finite state machine (FSM) debugging.
timing	Enables timing debugging.
upgrade	Enables upgrade debugging.
<i>interface-id</i>	(Optional) ID of the switch port.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(11)YJ	This command was first introduced.

Usage Guidelines

This command can be entered only from the switch console.

The **undebg lre** command is the same as the **no debug lre** command.

Related Commands

Command	Description
show controllers lre status	Displays the LRE link statistics and profile information on a switch LRE port, including link state, link duration, data rates, signal-to-noise ratio, and Reed Solomon errors.

debug pagp

Use the **debug pagp** privileged EXEC command to debug Port Aggregation Protocol (PAgP) activity. Use the **no** form of this command to disable debugging output.

debug pagp [all | event | fsm | misc | packet]

no debug pagp [all | event | fsm | misc | packet]

Syntax Description	all (Optional) Enable all PAgP debugging. event (Optional) Enable debugging of PAgP events. fsm (Optional) Enable debugging of the PAgP finite state machine. misc (Optional) Enable miscellaneous PAgP debugging. packet (Optional) Enable PAgP packet debugging.
--------------------	---

Defaults Debugging is disabled.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(6)EA2	This command was first introduced.

Usage Guidelines This command can be entered only from the switch console.

The **undebug pagp** command is the same as **no debug pagp** command.

Related Commands	Command	Description
	show debugging	Displays information about the types of debugging that are enabled. For syntax information, refer to Cisco IOS Configuration Fundamentals Command Reference For IOS Release 12.1 > Cisco IOS System Management Commands > Troubleshooting Commands .
	show pagp	Displays PAgP channel-group information.

debug pm

debug pm

Use the **debug pm** privileged EXEC command to debug port manager (PM) activity. The port manager is a state machine that controls all the logical and physical interfaces. All features, such as VLANs and UniDirectional Link Detection (UDLD), work with the port manager to provide switch functions. Use the **no** form of this command to disable debugging output.

```
debug pm {all | assert | card | cookies | etherchnl | messages | port | registry | sm | span | split | vlan | vp}
```

```
no debug pm {all | assert | card | cookies | etherchnl | messages | port | registry | sm | span | split | vlan | vp}
```

Syntax Description

all	Display all PM debugging messages.
assert	Debug assert messages.
card	Debug line-card related events.
cookies	Enable internal PM cookie validation.
etherchnl	Debug EtherChannel-related events.
messages	Debug PM messages.
port	Debug port-related events.
registry	Debug PM registry invocations.
sm	Debug state-machine related events.
span	Debug spanning-tree related events.
split	Debug split-processor.
vlan	Debug VLAN-related events.
vp	Debug virtual-port related events.



Though visible in the command-line help strings, the **scp** and **pvlan** keywords are not supported.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(6)EA2	This command was first introduced.

Usage Guidelines

The **undebug pm** command is the same as the **no debug pm** command.

Related Commands	Command	Description
	show debugging	Displays information about the types of debugging that are enabled. For syntax information, refer to Cisco IOS Configuration Fundamentals Command Reference For IOS Release 12.1 > Cisco IOS System Management Commands > Troubleshooting Commands .

■ **debug spanning-tree**

debug spanning-tree

Use the **debug spanning-tree** privileged EXEC command to debug spanning-tree activities. Use the **no** form of this command to disable debugging output.

```
debug spanning-tree {all | backbonefast | bpdu | bpdu-opt | config | csuf | etherchannel | events | exceptions | general | mstp | pvst+ | root | snmp | switch | uplinkfast}
```

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

Syntax Description	
all	Display all spanning-tree debugging messages.
backbonefast	Debug Backbonefast events.
bpdu	Debug spanning-tree bridge protocol data units (BPDUs).
bpdu-opt	Debug optimized BPDU handling.
config	Debug spanning-tree configuration changes.
csuf	Debug cross-stack UplinkFast activity.
etherchannel	Debug EtherChannel support.
events	Debug spanning-tree topology events.
exceptions	Debug spanning-tree exceptions.
general	Debug general spanning-tree activity.
mstp	Debug Multiple Spanning Tree Protocol events.
pvst+	Debug Per-VLAN Spanning Tree Plus (PVST+) events.
root	Debug spanning-tree root events.
snmp	Debug spanning-tree Simple Network Management Protocol (SNMP) handling.
switch	Debug switch shim commands. This shim is the software module that is the interface between the generic Spanning Tree Protocol (STP) code and the platform-specific code of various switch platforms.
uplinkfast	Debug UplinkFast events.

Defaults	Debugging is disabled.
----------	------------------------

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

Command History	Release	Modification
	12.1(6)EA2	This command was first introduced.
	12.1(9)EA1	The mstp and csuf keywords were added.

Usage Guidelines	The undebug spanning-tree command is the same as the no debug spanning-tree command.
------------------	--

Related Commands	Command	Description
	show debugging	Displays information about the types of debugging that are enabled. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference For IOS Release 12.1 > Cisco IOS System Management Commands > Troubleshooting Commands.
	show spanning-tree	Displays spanning-tree state information.

 debug spanning-tree backbonefast

debug spanning-tree backbonefast

Use the **debug spanning-tree backbonefast** privileged EXEC command to enable debugging of spanning-tree BackboneFast events. Use the **no** form of this command to disable debugging output.

debug spanning-tree backbonefast [detail | exceptions]

no debug spanning-tree backbonefast [detail | exceptions]

Syntax Description	detail (Optional) Display detailed BackboneFast debugging messages. exceptions (Optional) Enable debugging of spanning-tree BackboneFast exceptions.						
Defaults	Debugging is disabled.						
Command Modes	Privileged EXEC						
Command History	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>12.1(6)EA2</td><td>This command was first introduced.</td></tr> </tbody> </table>	Release	Modification	12.1(6)EA2	This command was first introduced.		
Release	Modification						
12.1(6)EA2	This command was first introduced.						
Usage Guidelines	<p>This command can be entered only from the switch console.</p> <p>The undebbug spanning-tree backbonefast command is the same as the no debug spanning-tree backbonefast command.</p>						
Related Commands	<table border="1"> <thead> <tr> <th>Command</th><th>Description</th></tr> </thead> <tbody> <tr> <td>show debugging</td><td>Displays information about the types of debugging that are enabled. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference For IOS Release 12.1 > Cisco IOS System Management Commands > Troubleshooting Commands.</td></tr> <tr> <td>show spanning-tree</td><td>Displays spanning-tree state information.</td></tr> </tbody> </table>	Command	Description	show debugging	Displays information about the types of debugging that are enabled. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference For IOS Release 12.1 > Cisco IOS System Management Commands > Troubleshooting Commands .	show spanning-tree	Displays spanning-tree state information.
Command	Description						
show debugging	Displays information about the types of debugging that are enabled. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference For IOS Release 12.1 > Cisco IOS System Management Commands > Troubleshooting Commands .						
show spanning-tree	Displays spanning-tree state information.						

debug spanning-tree bpdu

Use the **debug spanning-tree bpdu** privileged EXEC command to enable debugging of received and transmitted spanning-tree bridge protocol data units (BPDUs). Use the **no** form of this command to disable debugging output.

debug spanning-tree bpdu [receive | transmit]

no debug spanning-tree bpdu [receive | transmit]

Syntax Description	receive (Optional) Enable receive BPDU debugging. transmit (Optional) Enable transmit BPDU debugging.
---------------------------	--

Defaults	Debugging is disabled.
-----------------	------------------------

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

Command History	Release	Modification
	12.1(6)EA2	This command was first introduced.

Usage Guidelines	This command can be entered only from the switch console.
-------------------------	---

The **undebug spanning-tree bpdu** command is the same as the **no debug spanning-tree bpdu** command.

Related Commands	Command	Description
	show debugging	Displays information about the types of debugging that are enabled. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference For IOS Release 12.1 > Cisco IOS System Management Commands > Troubleshooting Commands .
	show spanning-tree	Displays spanning-tree state information.

■ **debug spanning-tree bpdu-opt**

debug spanning-tree bpdu-opt

Use the **debug spanning-tree bpdu-opt** privileged EXEC command to enable debugging of optimized spanning-tree bridge protocol data units (BPDUs) handling. Use the **no** form of this command to disable debugging output.

debug spanning-tree bpdu-opt [detail | packet]

no debug spanning-tree bpdu-opt [detail | packet]

Syntax Description	detail (Optional) Debug detailed optimized BPDU handling. packet (Optional) Debug packet-level optimized BPDU handling.
---------------------------	--

Defaults	Debugging is disabled.
-----------------	------------------------

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

Command History	Release	Modification
	12.1(6)EA2	This command was first introduced.

Usage Guidelines	This command can be entered only from the switch console. The undebug spanning-tree bpdu-opt command is the same as the no debug spanning-tree bpdu-opt command.
-------------------------	---

Related Commands	Command	Description
	show debugging	Displays information about the types of debugging that are enabled. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference For IOS Release 12.1 > Cisco IOS System Management Commands > Troubleshooting Commands .
	show spanning-tree	Displays spanning-tree state information.

debug spanning-tree mstp

Use the **debug spanning-tree mstp** privileged EXEC command to enable debugging of the Multiple Spanning Tree Protocol (MSTP) software. Use the **no** form of this command to disable debugging output.

```
debug spanning-tree mstp {all | boundary | bpdu-rx | bpdu-tx | errors | flush | init | migration | pm | proposals | region | roles | sanity_check | sync | tc | timers}
```

```
no debug spanning-tree mstp {all | boundary | bpdu-rx | bpdu-tx | errors | flush | init | migration | pm | proposals | region | roles | sanity_check | sync | tc | timers}
```

Syntax Description

all	Enable all the debugging messages.
boundary	Debug flag changes at these boundaries: <ul style="list-style-type: none"> An MST region and a single spanning-tree region running RSTP An MST region and a single spanning-tree region running 802.1d An MST region and another MST region with a different configuration
bpdu-rx	Debug the received MST bridge protocol data units (BPDUs)
bpdu-tx	Debug the transmitted MST BPDUs.
errors	Debug MSTP errors.
flush	Debug the port flushing mechanism.
init	Debug the initialization of the MSTP data structures.
migration	Debug the protocol migration state machine.
pm	Debug MSTP port manager events.
proposals	Debug handshake messages between the designated and root switch.
region	Debug the region synchronization between the switch processor (SP) and the route processor (RP).
roles	Debug MSTP roles.
sanity_check	Debug the received BPDU sanity check messages.
sync	Debug the port synchronization events.
tc	Debug topology change notification events.
timers	Debug the MSTP timers for start, stop, and expire events.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(9)EA1	This command was first introduced.

■ **debug spanning-tree mstp**

Usage Guidelines

This command can be entered only from the switch console.

The **undebug spanning-tree mstp** command is the same as the **no debug spanning-tree mstp** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference For IOS Release 12.1 > Cisco IOS System Management Commands > Troubleshooting Commands .
show spanning-tree	Displays spanning-tree state information.

debug spanning-tree switch

Use the **debug spanning-tree switch** privileged EXEC command to enable debugging of the software interface between the Spanning Tree Protocol (STP) software module and the port manager software module. Use the **no** form of this command to disable debugging output.

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

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

Syntax Description	
all	Enable all the debugging messages.
errors	Enable debugging of error messages for the interface between the spanning-tree software module and the port manager software module.
general	Enable debugging of general events.
helper	Enable debugging of the spanning-tree helper task, which handles bulk spanning-tree updates.
pm	Enable debugging of port manager events.
rx	Display received bridge protocol data unit (BPDU) handling debugging messages. The keywords have these meanings: decode —Enable debugging of received packets. errors —Enable debugging of receive errors. interrupt —Enable debugging of interrupt service requests (ISRs). process —Enable debugging of process receive BPDUs. state —Enable debugging of spanning-tree port state changes.
tx [decode]	Display transmitted BPDU handling debugging messages.

Defaults	Debugging is disabled.						
Command Modes	Privileged EXEC						
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.1(6)EA2</td> <td>This command was first introduced.</td> </tr> <tr> <td>12.1(9)EA1</td> <td>The helper keyword was added.</td> </tr> </tbody> </table>	Release	Modification	12.1(6)EA2	This command was first introduced.	12.1(9)EA1	The helper keyword was added.
Release	Modification						
12.1(6)EA2	This command was first introduced.						
12.1(9)EA1	The helper keyword was added.						

Usage Guidelines	This command can be entered only from the switch console. The undebug spanning-tree switch command is the same as the no debug spanning-tree switch command.
-------------------------	---

■ **debug spanning-tree switch**

Related Commands	Command	Description
	show debugging	Displays information about the types of debugging that are enabled. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference For IOS Release 12.1 > Cisco IOS System Management Commands > Troubleshooting Commands.
	show spanning-tree	Displays spanning-tree state information.

debug spanning-tree uplinkfast

Use the **debug spanning-tree uplinkfast** privileged EXEC command to enable debugging of spanning-tree UplinkFast events. Use the **no** form of this command to disable debugging output.

debug spanning-tree uplinkfast [exceptions]

no debug spanning-tree uplinkfast [exceptions]

Syntax Description	exceptions (Optional) Enable debugging of spanning-tree UplinkFast exceptions.						
Defaults	Debugging is disabled.						
Command Modes	Privileged EXEC						
Command History	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>12.1(6)EA2</td><td>This command was first introduced.</td></tr> </tbody> </table>	Release	Modification	12.1(6)EA2	This command was first introduced.		
Release	Modification						
12.1(6)EA2	This command was first introduced.						
Usage Guidelines	<p>This command can be entered only from the switch console.</p> <p>The undebbug spanning-tree uplinkfast command is the same as the no debug spanning-tree uplinkfast command.</p>						
Related Commands	<table border="1"> <thead> <tr> <th>Command</th><th>Description</th></tr> </thead> <tbody> <tr> <td>show debugging</td><td>Displays information about the types of debugging that are enabled. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference For IOS Release 12.1 > Cisco IOS System Management Commands > Troubleshooting Commands.</td></tr> <tr> <td>show spanning-tree</td><td>Displays spanning-tree state information.</td></tr> </tbody> </table>	Command	Description	show debugging	Displays information about the types of debugging that are enabled. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference For IOS Release 12.1 > Cisco IOS System Management Commands > Troubleshooting Commands .	show spanning-tree	Displays spanning-tree state information.
Command	Description						
show debugging	Displays information about the types of debugging that are enabled. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference For IOS Release 12.1 > Cisco IOS System Management Commands > Troubleshooting Commands .						
show spanning-tree	Displays spanning-tree state information.						

debug sw-vlan

debug sw-vlan

Use the **debug sw-vlan** privileged EXEC command to debug VLAN manager activities. Use the **no** form of this command to disable debugging output.

```
debug sw-vlan {badpmcookies | cfg-vlan {bootup | cli} | events | ifs | management | notification | packets | registries | vtp}
```

```
no debug sw-vlan {badpmcookies | cfg-vlan {bootup | cli} | events | ifs | management | notification | packets | registries | vtp}
```

Syntax Description	
badpmcookies	Display VLAN manager incidents of bad port manager cookies.
cfg-vlan bootup	Debug config-vlan messages generated when the switch is booting up.
cfg-vlan cli	Debug messages generated when the CLI is in config-vlan mode.
events	Debug VLAN manager events.
ifs	Debug VLAN manager IOS file system (IFS) error tests.
management	Debug VLAN manager management of internal VLANs.
notification	Debug VLAN manager notifications.
packets	Debug packet handling and encapsulation processes.
registries	Debug VLAN manager registries.
vtp	Debug the VLAN Trunking Protocol (VTP).

Defaults	Debugging is disabled.
----------	------------------------

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

Command History	Release	Modification
	12.1(6)EA2	This command was first introduced.
	12.1(9)EA1	The cfg-vlan keyword was added.

Usage Guidelines	The undebug sw-vlan command is the same as the no debug sw-vlan command.
------------------	--

Related Commands	Command	Description
	show debugging	Displays information about the types of debugging that are enabled. For syntax information, refer to Cisco IOS Configuration Fundamentals Command Reference For IOS Release 12.1 > Cisco IOS System Management Commands > Troubleshooting Commands .
	show vlan	Displays the parameters for all configured VLANs or one VLAN (if the VLAN name or ID is specified) in the administrative domain.
	show vtp	Displays general information about VTP management domain, status, and counters.

 debug sw-vlan ifs

debug sw-vlan ifs

Use the **debug sw-vlan ifs** privileged EXEC command to enable VLAN manager IOS file system (IFS) error tests. Use the **no** form of this command to disable debugging output.

debug sw-vlan ifs {open {read | write} | read {1 | 2 | 3 | 4} | write}

no debug sw-vlan ifs {open {read | write} | read {1 | 2 | 3 | 4} | write}

Syntax Description	open Enable VLAN manager IFS debugging of errors in an IFS file open operation. read Enable debugging of errors that occurred when opening the IFS VLAN configuration file in order to read it. write Enable debugging of errors that occurred when opening the IFS VLAN configuration file in order to write to it. read Enable debugging of errors that occurred when performing an IFS file read operation. {1 2 3 4} Specify the file read operation. write Enable debugging of errors that occurred when performing an IFS file write operation.
---------------------------	--

Defaults	Debugging is disabled.
-----------------	------------------------

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

Command History	Release	Modification
	12.1(6)EA2	This command was first introduced.

Usage Guidelines	When determining the file read operation, Operation 1 reads the file header, which contains the header verification word and the file version number. Operation 2 reads the main body of the file, which contains most of the domain and VLAN information. Operation 3 reads type length version (TLV) descriptor structures. Operation 4 reads TLV data.
-------------------------	---

The **undebug sw-vlan ifs** command is the same as the **no debug sw-vlan ifs** command.

Related Commands	Command	Description
	show debugging	Displays information about the types of debugging that are enabled. For syntax information, refer to Cisco IOS Configuration Fundamentals Command Reference For IOS Release 12.1 > Cisco IOS System Management Commands > Troubleshooting Commands .
	show vlan	Displays the parameters for all configured VLANs or one VLAN (if the VLAN name or ID is specified) in the administrative domain.

debug sw-vlan notification

Use the **debug sw-vlan notification** privileged EXEC command to enable debugging messages that trace the activation and deactivation of Inter-Link Switch (ISL) VLAN IDs. Use the **no** form of this command to disable debugging output.

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

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

Syntax Description	accfwdchange Enable VLAN manager notification of aggregated access interface Spanning Tree Protocol (STP) forward changes.
	allowedvlancfgchange Enable VLAN manager notification of changes to the allowed VLAN configuration.
	fwdchange Enable VLAN manager notification of STP forwarding changes.
	linkchange Enable VLAN manager notification of interface link-state changes.
	modechange Enable VLAN manager notification of interface mode changes.
	pruningcfgchange Enable VLAN manager notification of changes to the pruning configuration.
	statechange Enable VLAN manager notification of interface state changes.

Defaults	Debugging is disabled.
----------	------------------------

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

Command History	Release	Modification
	12.1(6)EA2	This command was first introduced.

Usage Guidelines	The undebug sw-vlan notification command is the same as the no debug sw-vlan notification command.
------------------	--

Related Commands	Command	Description
	show debugging	Displays information about the types of debugging that are enabled. For syntax information, refer to Cisco IOS Configuration Fundamentals Command Reference For IOS Release 12.1 > Cisco IOS System Management Commands > Troubleshooting Commands .
	show vlan	Displays the parameters for all configured VLANs or one VLAN (if the VLAN name or ID is specified) in the administrative domain.

 debug sw-vlan vtp

debug sw-vlan vtp

Use the **debug sw-vlan vtp** privileged EXEC command to enable debugging messages to be generated by the VLAN Trunking Protocol (VTP) code. Use the **no** form of this command to disable debugging output.

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

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

Syntax Description	events Display general-purpose logic flow and detailed VTP debugging messages generated by the VTP_LOG_RUNTIME macro in the VTP code. packets Display the contents of all incoming VTP packets that have been passed into the VTP code from the IOS VTP platform-dependent layer, except for pruning packets. pruning Enable debugging message to be generated by the pruning segment of the VTP code. packets (Optional) Display the contents of all incoming VTP pruning packets that have been passed into the VTP code from the IOS VTP platform-dependent layer. xmit (Optional) Display the contents of all outgoing VTP packets that the VTP code requests the IOS VTP platform-dependent layer to send. xmit Display the contents of all outgoing VTP packets that the VTP code requests the IOS VTP platform-dependent layer to send, except for pruning packets.				
Defaults	Debugging is disabled.				
Command Modes	Privileged EXEC				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.1(6)EA2</td> <td>This command was first introduced.</td> </tr> </tbody> </table>	Release	Modification	12.1(6)EA2	This command was first introduced.
Release	Modification				
12.1(6)EA2	This command was first introduced.				
Usage Guidelines	If no further parameters are entered after the pruning keyword, VTP pruning debugging messages appear. They are generated by the VTP_PRUNING_LOG_NOTICE, VTP_PRUNING_LOG_INFO, VTP_PRUNING_LOG_DEBUG, VTP_PRUNING_LOG_ALERT, and VTP_PRUNING_LOG_WARNING macros in the VTP pruning code. The undebug sw-vlan vtp command is the same as the no debug sw-vlan vtp command.				

Related Commands	Command	Description
	show debugging	Displays information about the types of debugging that are enabled. For syntax information, refer to Cisco IOS Configuration Fundamentals Command Reference For IOS Release 12.1 > Cisco IOS System Management Commands > Troubleshooting Commands .
	show vtp	Displays general information about VTP management domain, status, and counters.

debug udld

debug udld

Use the **debug udld** privileged EXEC command to display the UniDirectional Link Detection (UDLD) debug messages. Use the **no** form of this command to disable UDLD debugging.

debug udld {events | packets | registries}

no debug udld {events | packets | registries}

Syntax Description	events Enable debugging messages for UDLD process events as they occur. packets Enable debugging messages for the UDLD process as it receives packets from the packet queue and tries to transmit them at the request of the UDLD protocol code. registries Enable debugging messages for the UDLD process as it processes registry calls from the UDLD process-dependent module and other feature modules.
---------------------------	--

Defaults Debugging is disabled.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(6)EA2	This command was first introduced.

Usage Guidelines For **debug udld events**, these debugging messages appear:

- General UDLD program logic flow
- State machine state changes
- Program actions for the set and clear ErrDisable state
- Neighbor cache additions and deletions
- Processing of configuration commands
- Processing of link-up and link-down indications

For **debug udld packets**, these debugging messages appear:

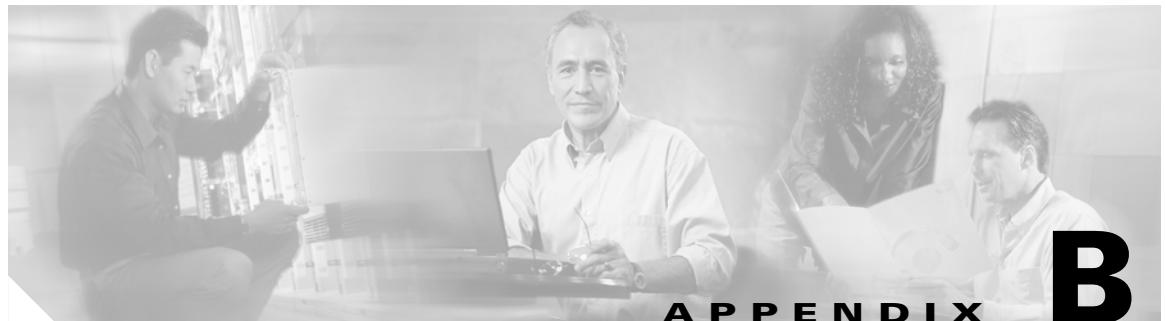
- General packet processing program flow on receipt of an incoming packet
- Indications of the contents of the various pieces of packets received (such as type length versions [TLVs]) as they are examined by the packet reception code
- Packet transmission attempts and the outcome

For **debug udld registries**, these categories of debugging messages appear:

- Sub-block creation
- Fiber-port status changes
- State change indications from the port manager software
- MAC address registry calls

Related Commands	Command	Description
	show debugging	Displays information about the types of debugging that are enabled. For syntax information, refer to Cisco IOS Configuration Fundamentals Command Reference For IOS Release 12.1 > Cisco IOS System Management Commands > Troubleshooting Commands .
	show udld	Displays UDLD administrative and operational status for all ports or the specified port.

■ debug uidl



Boot Loader Commands

During normal boot loader operation, you are not presented with the boot loader command-line prompt. You gain access to the boot loader command line if the switch is set to manually boot, if an error occurs during power-on self test (POST) DRAM testing, or if an error occurs while loading the operating system (a corrupted IOS image). You can also access the boot loader if you have lost or forgotten the switch password.

**Note**

The default configuration for Catalyst 2950 switches allows an end user with physical access to the switch to recover from a lost password by interrupting the boot process while the switch is powering up and then by entering a new password. The password recovery disable feature for Catalyst 2950 Fast Ethernet switches allows the system administrator to protect access to the switch password by disabling part of this functionality and allowing the user to interrupt the boot process only by agreeing to set the system back to the default configuration. With password recovery disabled, the user can still interrupt the boot process and change the password, but the configuration file (config.text) and the VLAN database file (vlan.dat) are deleted. For more information, refer to the software configuration guide for this release.

You can access the boot loader through a switch console connection at 9600 bps. Unplug the switch power cord, and press the switch **Mode** button while reconnecting the power cord. You can release the **Mode** button a second or two after the LED above port 1 goes off. You should then see the boot loader *Switch:* prompt. The boot loader performs low-level CPU initialization, performs POST, and loads a default operating system image into memory.

boot**boot**

Use the **boot** boot loader command to load and boot an executable image and to enter the command-line interface.

boot [-post] filesystem:/file-url ...

Syntax Description

-post	(Optional) Run the loaded image with an extended or comprehensive power-on self-test (POST). Using this keyword causes POST to take longer to complete.
filesystem:	Alias for a Flash file system. Use flash: for the system board Flash device.
/file-url	(Optional) Path (directory) and name of a bootable image. Separate the image names with a semicolon.

Defaults

The switch attempts to automatically boot the system by using information in the BOOT environment variable. If this variable is not set, the switch attempts to load and execute the first executable image it can by performing a recursive, depth-first search throughout the Flash file system. In a depth-first search of a directory, each encountered subdirectory is completely searched before continuing the search in the original directory.

Command Modes

Boot loader

Command History

Release	Modification
12.1(11)YJ	This command was first introduced.

Usage Guidelines

When you enter the **boot** command without any arguments, the switch attempts to automatically boot the system by using the information in the BOOT environment variable, if any. If you supply an image name for the *file-url* variable, the **boot** command attempts to boot the specified image.

When you set boot loader **boot** command options, they are executed immediately and apply only to the current boot loader session. These settings are not saved for the next boot operation.

Filenames and directory names are case sensitive.

Examples

This example shows how to boot the switch using the *new-image.bin* image:

```
switch: boot flash:/new-images/new-image.bin
```

After entering this command, you are prompted to start the setup program.

Related Commands

Command	Description
set	Sets the BOOT environment variable to boot a specific image when the BOOT keyword is appended to the command.

cat

Use the **cat** boot loader command to display the contents of one or more files.

cat *filesystem:/file-url ...*

Syntax Description	<i>filesystem:</i> Alias for a Flash file system. Use flash: for the system board Flash device. <i>/file-url</i> Path (directory) and name of the files to display. Separate each filename with a space.
---------------------------	--

Command Modes	Boot loader
----------------------	-------------

Command History	Release	Modification
	12.1(11)YJ	This command was first introduced.

Usage Guidelines	Filenames and directory names are case sensitive. If you specify a list of files, the contents of each file are sequentially displayed.
-------------------------	--

Examples	This example shows how to display the contents of config.text on Flash memory:
-----------------	--

```
Switch: cat flash:/config.text
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
!
hostname corp-bigboy
!
!
username admin privilege 15 password 0 cisco
!
ip subnet-zero
ip domain-name cisco.com
cluster enable corp-bigboy 0
!
spanning-tree extend system-id
!
controller LongReachEthernet 0
!
controller LongReachEthernet 1
!
controller LongReachEthernet 2
!
!
interface GigabitEthernet0/1
  no ip address
interface GigabitEthernet0/2
```

cat

```

no ip address
!
interface LongReachEthernet0/1
no ip address
!
interface LongReachEthernet0/2
no ip address
cpe type CISCO575-LRE
!
interface LongReachEthernet0/3
no ip address
cpe type CISCO575-LRE
!
interface LongReachEthernet0/4
no ip address
cpe type CISCO575-LRE
!
interface LongReachEthernet0/5
no ip address
cpe type CISCO575-LRE
!
interface LongReachEthernet0/6
no ip address
cpe type CISCO575-LRE
!
interface LongReachEthernet0/7
no ip address
!
interface LongReachEthernet0/8
no ip address
!
interface LongReachEthernet0/9
no ip address
cpe type CISCO585-LRE
!
interface LongReachEthernet0/10
no ip address
cpe type CISCO575-LRE
!
interface LongReachEthernet0/11
no ip address
cpe type CISCO575-LRE
!
interface LongReachEthernet0/12
no ip address
cpe type CISCO585-LRE
!
interface LongReachEthernet0/13
no ip address
!
interface LongReachEthernet0/14
no ip address
!
interface LongReachEthernet0/15
no ip address
!
interface LongReachEthernet0/16
no ip address
!
interface LongReachEthernet0/17
no ip address
!
interface LongReachEthernet0/18
no ip address

```

```

!
interface LongReachEthernet0/19
no ip address
!
interface LongReachEthernet0/20
no ip address
!
interface LongReachEthernet0/21
no ip address
!
interface LongReachEthernet0/22
no ip address
!
interface LongReachEthernet0/23
no ip address
!
interface LongReachEthernet0/24
no ip address
!
interface Vlan1
ip address 172.20.141.76 255.255.255.0
no ip route-cache
!
interface Vlan21
no ip address
no ip route-cache
!
ip http server
!
ip access-list extended CMP-NAT-ACL
dynamic Cluster-HSRP deny ip any any
dynamic Cluster-NAT permit ip any any
!
!
line con 0
session-timeout 3
password cisco
login local
speed 115200
line vty 0 4
session-timeout 3
password cisco
login local
line vty 5 15
session-timeout 3
password cisco
login local
!
end
switch:

```

Related Commands

Command	Description
more	Displays the contents of one or more files.
type	Displays the contents of one or more files.

copy

copy

Use the **copy** boot loader command to copy a file from a source to a destination.

```
copy [-b block-size] filesystem:/source-file-url filesystem:/destination-file-url
```

Syntax Description

-b block-size	(Optional) This option is used only for internal development and testing.
<i>filesystem:</i>	Alias for a Flash file system. Use flash: for the system board Flash device.
<i>/source-file-url</i>	Path (directory) and filename (source) to be copied.
<i>/destination-file-url</i>	Path (directory) and filename of the destination.

Defaults

The default block size is 4 KB.

Command Modes

Boot loader

Command History

Release	Modification
12.1(11)YJ	This command was first introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

Directory names are limited to 45 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

Filenames are limited to 45 characters; the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

If you are copying a file to a new directory, the directory must already exist.

Examples

This example show how to copy a file at the root:

```
switch: copy flash:test1.text flash:test4.text
.
File "flash:test1.text" successfully copied to "flash:test4.text"
```

You can verify that the file was copied by entering the **dir filesystem:** boot loader command.

Related Commands

Command	Description
delete	Deletes one or more files from the specified file system.

delete

Use the **delete** boot loader command to delete one or more files from the specified file system.

delete *filesystem:/file-url* ...

Syntax Description	<i>filesystem:</i> Alias for a Flash file system. Use flash: for the system board Flash device. <i>/file-url</i> Path (directory) and filename to delete. Separate each filename with a space.
---------------------------	--

Command Modes	Boot loader
----------------------	-------------

Command History	Release	Modification
	12.1(11)YJ	This command was first introduced.

Usage Guidelines	Filenames and directory names are case sensitive. The switch prompts you for confirmation before deleting each file.
-------------------------	---

Examples	This example shows how to delete two files:
-----------------	---

```
switch: delete flash:test2.text flash:test5.text
Are you sure you want to delete "flash:test2.text" (y/n)?y
File "flash:test2.text" deleted
Are you sure you want to delete "flash:test5.text" (y/n)?y
File "flash:test2.text" deleted
```

You can verify that the files were deleted by entering the **dir flash:** boot loader command.

Related Commands	Command	Description
	copy	Copies a file from a source to a destination.

dir

dir

Use the **dir** boot loader command to display a list of files and directories on the specified file system.

dir *filesystem:/file-url ...*

Syntax Description

<i>filesystem:</i>	Alias for a Flash file system. Use flash: for the system board Flash device.
<i>/file-url</i>	(Optional) Path (directory) and directory name whose contents you want to display. Separate each directory name with a space.

Command Modes

Boot loader

Command History

Release	Modification
12.1(11)YJ	This command was first introduced.

Usage Guidelines

Directory names are case sensitive.

Examples

This example shows how to display the files in Flash memory:

```
switch: dir flash:
```

[Table B-1](#) describes the fields in the display.

Table B-1 dir Field Descriptions

Field	Description
2	Index number of the file.
-rwx	File permission, which can be any or all of the following: <ul style="list-style-type: none"> • d—directory • r—readable • w—writable • x—executable
1644045	Size of the file.
<date>	Last modification date.
env_vars	Filename.

Related Commands

Command	Description
mkdir	Creates one or more directories.
rmdir	Removes one or more directories.

■ flash_init

flash_init

Use the **flash_init** boot loader command to initialize the Flash file system.

flash_init

Syntax Description This command has no arguments or keywords.

Defaults The Flash file system is automatically initialized during normal system operation.

Command Modes Boot loader

Command History	Release	Modification
	12.1(11)YJ	This command was first introduced.

Usage Guidelines During the normal boot process, the Flash file system is automatically initialized.

Use this command to manually initialize the Flash file system. For example, you use this command during the recovery procedure for a lost or forgotten password.

format

Use the **format** boot loader command to format the specified file system and destroy all data in that file system.

format *filesystem:*

Syntax Description	<i>filesystem:</i> Alias for a Flash file system. Use flash: for the system board Flash device.				
Command Modes	Boot loader				
Command History	<table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>12.1(11)YJ</td><td>This command was first introduced.</td></tr></tbody></table>	Release	Modification	12.1(11)YJ	This command was first introduced.
Release	Modification				
12.1(11)YJ	This command was first introduced.				
<hr/>					
Usage Guidelines	<p> Caution</p> <p>Use this command with care; it destroys all data on the file system and renders your system unusable.</p>				

fsck

Use the **fsck** boot loader command to check the file system for consistency.

fsck [-test | -f] filesystem:

Syntax Description	-test	(Optional) Initialize the file system code and perform extra POST on Flash memory. An extensive, nondestructive memory test is performed on every byte that makes up the file system.
	-f	(Optional) Initialize the file system code and perform a fast file consistency check. Cyclic redundancy checks (CRCs) in the flashfs sectors are not checked.
	<i>filesystem:</i>	Alias for a Flash file system. Use flash: for the system board Flash device.

Defaults

No file system check is performed.

Command Modes

Boot loader

Command History

Release	Modification
12.1(11)YJ	This command was first introduced.

Usage Guidelines

To stop an in-progress file system consistency check, disconnect the switch power and then reconnect the power.

Examples

This example shows how to perform an extensive file system check on Flash memory:

```
switch: fsck -test flash:
```

help

Use the **help** boot loader command to display the available commands.

help

Syntax Description This command has no arguments or keywords.

Command Modes Boot loader

Command History	Release	Modification
	12.1(11)YJ	This command was first introduced.

Usage Guidelines You can also use the question mark (?) to display a list of available boot loader commands.

load_helper

load_helper

Use the **load_helper** boot loader command to load and initialize one or more helper images, which extend or patch the functionality of the boot loader.

load_helper *filesystem:/file-url ...*

Syntax Description	<i>filesystem:</i> Alias for a Flash file system. Use flash: for the system board Flash device. <i>/file-url</i> Path (directory) and a list of loadable helper files to dynamically load during loader initialization. Separate each image name with a semicolon.
---------------------------	--

Defaults	No helper files are loaded.
-----------------	-----------------------------

Command Modes	Boot loader
----------------------	-------------

Command History	Release	Modification
	12.1(11)YJ	This command was first introduced.

Usage Guidelines	The load_helper command searches for loadable files only if the HELPER environment variable is set. Filenames and directory names are case sensitive.
-------------------------	---

memory

Use the **memory** boot loader command to display memory heap utilization information.

memory

Syntax Description This command has no arguments or keywords.

Command Modes Boot loader

Command History	Release	Modification
	12.1(11)YJ	This command was first introduced.

Examples This example shows how to display memory heap utilization information:

```
switch: memory
Text: 0x00700000 - 0x0071cf24 (0x0001cf24 bytes)
Rotext: 0x00000000 - 0x00000000 (0x00000000 bytes)
Data: 0x0071cf24 - 0x00723a0c (0x00006ae8 bytes)
Bss: 0x0072529c - 0x00746f94 (0x00021cf8 bytes)
Stack: 0x00746f94 - 0x00756f94 (0x00010000 bytes)
Heap: 0x00756f98 - 0x00800000 (0x000a9068 bytes)

Bottom heap utilization is 22 percent.
Top heap utilization is 0 percent.
Total heap utilization is 22 percent.
Total bytes: 0xa9068 (692328)
Bytes used: 0x26888 (157832)
Bytes available: 0x827e0 (534496)

Alternate heap utilization is 0 percent.
Total alternate heap bytes: 0x6fd000 (7327744)
Alternate heap bytes used: 0x0 (0)
Alternate heap bytes available: 0x6fd000 (7327744)
```

[Table B-2](#) describes the fields in the display.

Table B-2 Memory Field Descriptions

Field	Description
Text	Beginning and ending address of the text storage area.
Rotext	Beginning and ending address of the read-only text storage area. This part of the data segment is grouped with the Text entry.
Data	Beginning and ending address of the data segment storage area.
Bss	Beginning and ending address of the block started by symbol (Bss) storage area. It is initialized to zero.

Table B-2 Memory Field Descriptions (continued)

Field	Description
Stack	Beginning and ending address of the area in memory allocated to the software to store automatic variables, return addresses, and so forth.
Heap	Beginning and ending address of the area in memory that memory is dynamically allocated to and freed from.

mkdir

Use the **mkdir** boot loader command to create one or more new directories on the specified file system.

mkdir *filesystem:/directory-url* ...

Syntax Description	<i>filesystem:</i> Alias for a Flash file system. Use flash: for the system board Flash device. <i>/directory-url</i> Name of the directories to create. Separate each directory name with a space.
---------------------------	---

Command Modes	Boot loader
----------------------	-------------

Command History	Release	Modification
	12.1(11)YJ	This command was first introduced

Usage Guidelines	Directory names are case sensitive. Directory names are limited to 45 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.
-------------------------	---

Examples	This example shows how to make a directory called Saved_Configs:
	<pre>switch: mkdir flash:Saved_Configs Directory "flash:Saved_Configs" created</pre>

This example shows how to make two directories:

```
switch: mkdir flash:Saved_Configs1 flash:Test
Directory "flash:Saved_Configs1" created
Directory "flash:Test" created
```

You can verify that the directory was created by entering the **dir filesystem:** boot loader command.

Related Commands	Command	Description
	dir	Displays a list of files and directories on the specified file system.
	rmdir	Removes one or more directories from the specified file system.

more

more

Use the **more** boot loader command to display the contents of one or more files.

more *filesystem:/file-url* ...

Syntax Description

<i>filesystem:</i>	Alias for a Flash file system. Use flash: for the system board Flash device.
<i>/file-url</i>	Path (directory) and name of the files to display. Separate each filename with a space.

Command Modes

Boot loader

Command History

Release	Modification
12.1(11)YJ	This command was first introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

If you specify a list of files, the contents of each file is sequentially displayed.

Examples

Related Commands

Command	Description
cat	Displays the contents of one or more files.
type	Displays the contents of one or more files.

rename

Use the **rename** boot loader command to rename a file.

rename *filesystem:/source-file-url filesystem:/destination-file-url*

Syntax Description

<i>filesystem:</i>	Alias for a Flash file system. Use flash: for the system board Flash device.
<i>/source-file-url</i>	Original path (directory) and filename.
<i>/destination-file-url</i>	New path (directory) and filename.

Command Modes

Boot loader

Command History

Release	Modification
12.1(11)YJ	This command was first introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

Directory names are limited to 45 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

Filenames are limited to 45 characters; the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

Examples

This example shows a file named *config.text* being renamed to *config1.text*:

```
switch: rename flash:config.text flash:config1.text
```

You can verify that the file was renamed by entering the **dir** *filesystem:* boot loader command.

Related Commands

Command	Description
copy	Copies a file from a source to a destination.

reset

reset

Use the **reset** boot loader command to perform a hard reset on the system. A hard reset is similar to power-cycling the switch, clearing the processor, registers, and memory.

reset

Syntax Description This command has no arguments or keywords.

Command Modes Boot loader

Command History	Release	Modification
	12.1(11)YJ	This command was first introduced.

Examples This example shows how to reset the system:

```
switch: reset
Are you sure you want to reset the system (y/n)?y
System resetting...
```

Related Commands	Command	Description
	boot	Loads and boots an executable image and enters the command-line interface.

rmdir

Use the **rmdir** boot loader command to remove one or more empty directories from the specified file system.

rmdir *filesystem:/directory-url* ...

Syntax Description	<i>filesystem:</i> Alias for a Flash file system. Use flash: for the system board Flash device. <i>/directory-url</i> Path (directory) and name of the empty directories to remove. Separate each directory name with a space.
---------------------------	--

Command Modes	Boot loader
----------------------	-------------

Command History	Release	Modification
	12.1(11)YP	This command was first introduced.

Usage Guidelines	Directory names are case sensitive and limited to 45 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons. Before removing a directory, you must first delete all the files in the directory. The switch prompts you for confirmation before deleting each directory.
-------------------------	--

Examples	This example shows how to remove a directory: switch: rmdir flash:Test
	You can verify that the directory was deleted by entering the dir filesystem: boot loader command.

Related Commands	Command	Description
	dir	Displays a list of files and directories on the specified file system.
	mkdir	Creates one or more new directories on the specified file system.

set

Use the **set** boot loader command to set or display environment variables, which can be used to control the boot loader or any other software running on the switch.

set *variable value*



Note Under normal circumstances, it is not necessary to alter the setting of the environment variables.

Syntax Description

<i>variable value</i>	<p>Use one of these keywords for <i>variable</i> and <i>value</i>:</p> <p>MANUAL_BOOT—Determines whether the switch automatically or manually boots.</p> <p>Valid values are 1, yes, 0, and no. If it is set to no or 0, the boot loader attempts to automatically boot the system. If it is set to anything else, you must manually boot the switch from the boot loader mode.</p> <p>BOOT filesystem:/file-url—A semicolon-separated list of executable files to try to load and execute when automatically booting.</p> <p>If the BOOT environment variable is not set, the system attempts to load and execute the first executable image it can find by using a recursive, depth-first search through the flash: file system. If the BOOT variable is set but the specified images cannot be loaded, the system attempts to boot the first bootable file that it can find in the Flash file system.</p> <p>ENABLE_BREAK—Determines whether the automatic boot process can be interrupted by using the Break key on the console.</p> <p>Valid values are 1, yes, on, 0, no, and off. If it is set to 1, yes, or on, you can interrupt the automatic boot process by pressing the Break key on the console after the Flash file system has initialized.</p> <p>HELPER filesystem:/file-url—A semicolon-separated list of loadable files to dynamically load during the boot loader initialization. Helper files extend or patch the functionality of the boot loader.</p> <p>PS1 prompt—A string that is used as the command-line prompt in boot loader mode.</p> <p>CONFIG_FILE flash:/file-url—The filename that IOS uses to read and write a nonvolatile copy of the system configuration.</p> <p>CONFIG_BUFSIZE size—The buffer size that IOS uses to hold a copy of the configuration file in memory. The configuration file cannot be larger than the buffer size allocation. The range is from 4096 to 524288 bytes.</p> <p>BAUD rate—The rate in bits per second (bps) used for the console. The IOS software inherits the baud rate setting from the boot loader and continues to use this value unless the configuration file specifies another setting. The range is from 0 to 4294967295 bps. Valid values are 50, 75, 110, 150, 300, 600, 1200, 1800, 2000, 2400, 3600, 4800, 7200, 9600, 14400, 19200, 28800, 38400, 56000, 57600, 115200, and 128000.</p> <p>The most commonly used values are 300, 1200, 2400, 9600, 19200, 57600, and 115200.</p>
-----------------------	---

BOOTHLPR *filesystem:/file-url*—The name of the IOS helper image that is first loaded into memory so that it can then load a second IOS image into memory and launch it. This variable is used only for internal development and testing.

HELPER_CONFIG_FILE *filesystem:/file-url*—The name of the configuration file to be used by the IOS helper image. If this is not set, the file specified by the CONFIG_FILE environment variable is used by all versions of IOS that are loaded, including the helper image. This variable is used only for internal development and testing.

PASSWD_RECOVERY—Enables or disables the password recovery option. Valid values are yes, 1, no, or 2. The default is yes.

REBOOT_AFTER_CRASH—Sets the switch to reboot after an abnormal termination. Valid values are yes, 1, no, or 2. The default is yes.

Defaults

The environment variables have these default values:

MANUAL_BOOT: No (0)

BOOT: Null string

ENABLE_BREAK: No (Off or 0) (the automatic boot process cannot be interrupted by pressing the Break key on the console).

HELPER: No default value (helper files are not automatically loaded).

PS1: switch:

CONFIG_FILE: config.text

CONFIG_BUFSIZE: 32 KB

BAUD: 9600 bps

BOOTHLPR: No default value (no helper images are specified).

HELPER_CONFIG_FILE: No default value (no helper configuration file is specified).



Environment variables that have values are stored in the Flash file system in various files. The format of these files is that each line contains an environment variable name and an equal sign followed by the value of the variable. A variable has no value if it is not listed in this file; it has a value if it is listed in the file even if the value is a null string. A variable that is set to a null string (for example, “ ”) is a variable with a value. Many environment variables are predefined and have default values.

Command Modes

Boot loader

Command History

Release	Modification
12.1(11)YJ	This command was first introduced.

set**Usage Guidelines**

Environment variables are case sensitive and must be entered as documented.

The MANUAL_BOOT environment variable can also be set by using the **boot manual** global configuration command.

The BOOT environment variable can also be set by using the **boot system filesystem:/file-url** global configuration command.

The ENABLE_BREAK environment variable can also be set by using the **boot enable-break** global configuration command.

The HELPER environment variable can also be set by using the **boot helper filesystem:/file-url** global configuration command.

The CONFIG_FILE environment variable can also be set by using the **boot config-file flash:/file-url** global configuration command.

The CONFIG_BUFSIZE environment variable can also be set by using the **boot bufsize size** global configuration command.

The BOOTHLPY environment variable can also be set by using the **boot boothlp filesystem:/file-url** global configuration command.

The HELPER_CONFIG_FILE environment variable can also be set by using the **boot helper-config-file filesystem:/file-url** global configuration command.

The PASSWD_RECOVERY environment variable can be set or reset by using the IOS configuration CLI **service password-recovery** command.

The boot loader prompt string (PS1) can be up to 120 printable characters except the equal sign (=).

Examples

This example shows how to change the boot loader prompt:

```
switch: set PS1 loader:
loader:
```

You can verify your setting by using the **set** boot loader command.

Related Commands

Command	Description
unset	Resets one or more environment variables to its previous setting.

type

Use the **type** boot loader command to display the contents of one or more files.

type *filesystem:/file-url ...*

Syntax Description	<i>filesystem:</i> Alias for a Flash file system. Use flash: for the system board Flash device. <i>/file-url</i> Path (directory) and name of the files to display. Separate each filename with a space.
---------------------------	--

Command Modes	Boot loader
----------------------	-------------

Command History	Release	Modification
	12.1(11)YJ	This command was first introduced.

Usage Guidelines	Filenames and directory names are case sensitive. If you specify a list of files, the contents of each file is sequentially displayed.
-------------------------	---

Examples

Related Commands	Command	Description
	cat	Displays the contents of one or more files.
	more	Displays the contents of one or more files.

unset

Use the **unset** boot loader command to reset one or more environment variables.

unset *variable* ...



Note Under normal circumstances, it is not necessary to alter the setting of the environment variables.

Syntax Description	
	<p><i>variable</i> Use one of these keywords for <i>variable</i>:</p> <p>MANUAL_BOOT—Determines whether the switch automatically or manually boots.</p> <p>BOOT—Resets the list of executable files to try to load and execute when automatically booting. If the BOOT environment variable is not set, the system attempts to load and execute the first executable image it can find by using a recursive, depth-first search through the Flash file system. If the BOOT variable is set but the specified images cannot be loaded, the system attempts to boot the first bootable file that it can find in the Flash file system.</p> <p>ENABLE_BREAK—Determines whether the automatic boot process can be interrupted by using the Break key on the console after the Flash file system has been initialized.</p> <p>HELPER—A semicolon-separated list of loadable files to dynamically load during the boot loader initialization. Helper files extend or patch the functionality of the boot loader.</p> <p>PS1—A string that is used as the command-line prompt in boot loader mode.</p> <p>CONFIG_FILE—Resets the filename that IOS uses to read and write a nonvolatile copy of the system configuration.</p> <p>CONFIG_BUFSIZE—Resets the buffer size that IOS uses to hold a copy of the configuration file in memory.</p> <p>BAUD—Resets the rate in bits per second (bps) used for the console. The IOS software inherits the baud rate setting from the boot loader and continues to use this value unless the configuration file specifies another setting.</p> <p>BOOTHLPR—Resets the name of the IOS helper image that is first loaded into memory so that it can then load a second IOS image into memory and launch it. This variable is used only for internal development and testing.</p> <p>HELPER_CONFIG_FILE—Resets the name of the configuration file to be used by the IOS helper image. If this is not set, the file specified by the CONFIG_FILE environment variable is used by all versions of IOS that are loaded, including the helper image. This variable is used only for internal development and testing.</p> <p>PASSWD_RECOVERY—Resets the password recovery option.</p>

Command Modes

Boot loader

Command History	Release	Modification
	12.1(11)YJ	This command was first introduced.

Usage Guidelines	The MANUAL_BOOT environment variable can also be reset by using the no boot manual global configuration command. The BOOT environment variable can also be reset by using the no boot system global configuration command. The ENABLE_BREAK environment variable can also be reset by using the no boot enable-break global configuration command. The HELPER environment variable can also be reset by using the no boot helper global configuration command. The CONFIG_FILE environment variable can also be reset by using the no boot config-file global configuration command. The CONFIG_FILE_BUFSIZE environment variable can also be reset by using the no boot buffersize global configuration command. The BOOTHLPR environment variable can also be reset by using the no boot boothlpr global configuration command. The HELPER_CONFIG_FILE environment variable can also be reset by using the no boot helper-config-file global configuration command.
-------------------------	--

Examples	This example shows how to reset the prompt string to its previous setting: switch: unset PS1 switch:
-----------------	---

Related Commands	Command	Description
	set	Sets or displays environment variables.

version

version

Use the **version** boot loader command to display the boot loader version.

version

Syntax Description This command has no arguments or keywords.

Command Modes Boot loader

Command History	Release	Modification
	12.1(11)YJ	This command was first introduced.

Examples This example shows how to display the boot loader version:



INDEX

A

aaa authentication command **2-1**
abort command **2-459**
access control entries
 See ACEs
access control lists
 See ACLs
Access Control Parameters
 See ACPs
access groups
 IP **2-108**
 MAC
 applying ACL to interface **2-138**
 displaying **2-298**
access-list (IP extended) command **2-3**
access-list (IP standard) command **2-6**
access-list configuration mode
 deny **2-74**
 entering **2-110**
 permit **2-175**
access ports **2-420**
ACEs **2-78, 2-179**
ACLs
 IP
 applying to interface **2-108**
 deny **2-74**
 displaying **2-204, 2-281**
 permit **2-175**
 MAC
 applying to interface **2-138**
 deny **2-77**
 displaying **2-204**

permit **2-178**
ACPs, displaying **2-307**
aggregate-port learner **2-172**
allowed VLANs, setting **2-432**
apply command **2-459**
archive download-sw command **2-8**
archive tar command **2-10**
archive upload-sw command **2-14**
audience **xiii**
autonegotiation of duplex mode **2-90**
auto qos voip command **2-16**

B

BackboneFast, for STP **2-369**
boot (boot loader) command **B-2**
boot boothlpr command **2-19**
boot buffersize command **2-20**
boot config-file command **2-21**
boot enable-break command **2-22**
boot helper command **2-23**
boot helper-config file command **2-24**
booting
 displaying environment variables **2-209**
 interrupting **2-22**
 IOS image **2-27**
 manually **2-25**
boot loader
 accessing **B-1**
 booting
 helper image **2-23**
 IOS image **B-2**

directories
 creating [B-17](#)
 displaying a list of [B-8](#)
 removing [B-21](#)
 displaying
 available commands [B-13](#)
 memory heap utilization [B-15](#)
 version [B-28](#)
 environment variables
 described [B-22](#)
 displaying settings [B-22](#)
 setting [B-22](#)
 unsetting [B-26](#)
 files
 copying [B-6](#)
 deleting [B-7](#)
 displaying a list of [B-8](#)
 displaying the contents of [B-3, B-18, B-25](#)
 renaming [B-19](#)
 file system
 formatting [B-11](#)
 initializing Flash [B-10](#)
 running a consistency check [B-12](#)
 loading helper images [B-14](#)
 prompt [B-1](#)
 resetting the system [B-20](#)
 boot manual command [2-25](#)
 boot private-config-file command [2-26](#)
 boot system command [2-27](#)
 BPDU filtering, for spanning tree [2-370, 2-402](#)
 BPDU guard, for spanning tree [2-372, 2-402](#)
 broadcast suppression level
 configuring [2-416](#)
 displaying [2-339](#)
 broadcast traffic counters [2-278](#)

C

cat (boot loader) command [B-3](#)
 caution, description [xv](#)
 channel-group command [2-28](#)
 Cisco Technical Assistance Center [xviii](#)
 class command [2-30](#)
 class-map command [2-32](#)
 class maps
 creating [2-32](#)
 defining the match criteria [2-150](#)
 displaying [2-211](#)
 class of service
 See CoS
 clear controllers ethernet-controller command [2-34](#)
 clear controllers lre command [2-36](#)
 clear controllers lre link monitor command [2-37](#)
 clear controllers lre log command [2-38](#)
 clear interface command [2-39](#)
 clear LRE configuration events [2-38](#)
 clear LRE timer events [2-38](#)
 clear mac address-table command [2-41](#)
 clear pagp command [2-43](#)
 clear port-security dynamic command [2-44](#)
 clear port-security sticky command [2-45](#)
 clear spanning-tree detected-protocols command [2-47](#)
 clear vmps statistics command [2-48](#)
 clear vtp counters command [2-49](#)
 cluster commander-address command [2-50](#)
 cluster discovery hop-count command [2-52](#)
 cluster enable command [2-53](#)
 cluster holdtime command [2-54](#)
 cluster management-vlan command [2-55](#)
 cluster member command [2-56](#)
 cluster run command [2-58](#)
 clusters
 adding candidates [2-56](#)
 binding to HSRP [2-59](#)
 building manually [2-56](#)

- communicating with members by using Telnet **2-195**
 displaying
 candidate switches **2-215**
 member switches **2-217**
 status **2-213**
 heartbeat messages
 duration after which switch declared down **2-54**
 interval between **2-61**
 hop-count limit for extended discovery **2-52**
 HSRP standby groups **2-59**
 redundancy **2-59**
 SNMP trap **2-362**
 cluster standby-group command **2-59**
 cluster timer command **2-61**
 command modes defined **1-2**
 command switch
 See clusters
 configuration files
 password recovery disable considerations **B-1**
 setting the NVRAM size for **2-20**
 specifying the name **2-21, 2-26**
 configuring multiple interfaces **2-106 to 2-107**
 config-vlan mode
 commands **2-447**
 description **1-5**
 entering **2-446**
 summary **1-3**
 controller configuration mode **1-2, 1-4**
 controller LongReachEthernet command **2-62**
 conventions
 command **xiv**
 for examples **xiv**
 publication **xiv**
 text **xiv**
 copy (boot loader) command **B-6**
 CoS
 default value, assigning to incoming packets **2-153**
 incoming value, overriding **2-153**
 priority queue, assigning values to **2-477**
 priority queue mapping, displaying **2-359**
 WRR bandwidth allocation, displaying **2-358**
 WRR weights, assigning to CoS priority queues **2-476**
 CoS-to-DSCP map
 default **2-155**
 defining **2-155**
 cpe duplex command **2-63**
 CPE Ethernet ports
 clearing **2-35**
 cpe protected command **2-65**
 cpe shutdown command **2-66**
 cpe speed command **2-68**
 cpe type command **2-70**
 cross-stack UplinkFast, for STP **2-406**
-
- D**
- debug dot1x command **A-2**
 debug etherchannel command **A-3**
 debug lre **A-4**
 debug pagp command **A-5**
 debug pm command **A-6**
 debug spanning-tree backbonefast command **A-10**
 debug spanning-tree bpdu command **A-11**
 debug spanning-tree bpdu-opt command **A-12**
 debug spanning-tree command **A-8**
 debug spanning-tree mstp command **A-13**
 debug spanning-tree switch command **A-15**
 debug spanning-tree uplinkfast command **A-17**
 debug sw-vlan command **A-18**
 debug sw-vlan ifs command **A-20**
 debug sw-vlan notification command **A-21**
 debug sw-vlan vtp command **A-22**
 debug udld command **A-24**
 define interface-range command **2-71**
 delete (boot loader) command **B-7**
 delete command **2-73**
 delete LRE link history **2-38**
 delete LRE link monitor data **2-37**

- deny (access-list configuration) command **2-74**
 deny (MAC access-list configuration) command **2-77**
 dir (boot loader) command **B-8**
 documentation
 feedback **xvi**
 obtaining
 CD-ROM **xvi**
 world wide web **xvi**
 ordering **xvi**
 related **xv**
 document conventions **xiv**
 domain name, VTP **2-466, 2-472**
 dot1x default command **2-80**
 dot1x max-req command **2-81**
 dot1x multiple-hosts command **2-82**
 dot1x port-control command **2-83**
 dot1x re-authenticate command **2-85**
 dot1x re-authentication command **2-86**
 dot1x timeout quiet-period command **2-87**
 dot1x timeout re-authperiod command **2-88**
 dot1x timeout tx-period command **2-89**
 DSCP-to-CoS map
 default **2-155**
 defining **2-155**
 DTP **2-421**
 DTP flap, error recovery timer **2-94**
 duplex command **2-90**
 dynamic-access ports, configuring **2-418**
 Dynamic Trunking Protocol
 See DTP
-
- E**
- EAP-request/identity frame **2-81, 2-89**
 environment variables, displaying **2-209**
 errdisable detect command **2-92**
 errdisable recovery command **2-94**
 EtherChannel
 assigning Ethernet interface to channel group **2-28**
- creating port-channel logical interface **2-105**
 debug messages, displaying **A-3 to A-5**
 displaying **2-265**
 load-distribution methods **2-185**
 PAgP
 aggregate-port learner **2-172**
 clearing channel-group information **2-43**
 debug messages, displaying **A-5**
 displaying **2-321**
 error recovery timer **2-94**
 learn method **2-172**
 modes **2-28**
 priority of interface for transmitted traffic **2-174**
 Ethernet link statistics **2-34**
 Ethernet statistics, collecting **2-199**
 examples, conventions for **xiv**
 exit command **2-459**
 extended discovery of candidate switches **2-52**
 extended-range VLANs
 and allowed VLAN list **2-432**
 and pruning-eligible list **2-432**
 configuring **2-446**
 extended system ID for STP **2-376**
 Extensible Authentication Protocol-request/identity frame
 See EAP-request/identity frame
-
- F**
- fan information, displaying **2-262**
 feedback to Cisco Systems, web **xvi**
 file name, VTP **2-466**
 files, deleting **2-73**
 flash_init (boot loader) command **B-10**
 flowcontrol command **2-96**
 flow-control packets
 receiving **2-96**
 sending **2-96**
 format (boot loader) command **B-11**
 fsck (boot loader) command **B-12**

G

global configuration mode [1-2, 1-4](#)

H

heartbeat messages

duration after which switch declared dead [2-54](#)

interval between [2-61](#)

help (boot loader) command [B-13](#)

holdtime for clusters [2-54](#)

hop-count limit for clusters [2-52](#)

Hot Standby Router Protocol

See HSRP

HSRP

binding HSRP group to cluster [2-59](#)

standby group [2-59](#)

hw-module slot command [2-100](#)

I
IEEE 802.1X commands

authentication methods [2-1](#)

debugging [A-2](#)

displaying settings [2-258](#)

EAP-request/identity frame

response time [2-89](#)

sending [2-81](#)

manual control [2-83](#)

multiple hosts [2-82](#)

quiet state, setting [2-87](#)

reauthenticaton

attempts, interval between [2-88](#)

initiating [2-85](#)

periodic [2-86](#)

resetting parameters [2-80](#)

IGMP snooping

adding ports statically [2-118](#)

configuration, displaying [2-283](#)

enabling [2-113](#)

Immediate-Leave processing [2-115](#)

MAC address tables [2-303](#)

multicast router ports, displaying [2-285](#)

multicast routers [2-116](#)

per VLAN [2-114](#)

images

See software images

Immediate-Leave feature, MVR [2-166](#)

Immediate-Leave processing [2-115](#)

interface command [2-103](#)

interface configuration mode [1-2, 1-4](#)

interface port-channel command [2-105](#)

interface range command [2-106](#)

interface-range macros [2-71](#)

interfaces

assigning Ethernet interface to channel group [2-28](#)

configuring [2-90](#)

configuring multiple [2-106 to 2-107](#)

creating port-channel logical [2-105](#)

disabling [2-360](#)

restarting [2-360](#)

invalid GBIC

error detection for [2-92](#)

error recovery timer [2-94](#)

ip access-group command [2-108](#)

ip access-list command [2-110](#)

ip address command [2-112](#)

ip addresses, setting [2-112](#)

ip igmp snooping command [2-113](#)

ip igmp snooping vlan command [2-114](#)

ip igmp snooping vlan immediate-leave command [2-115](#)

ip igmp snooping vlan mrouter command [2-116](#)

ip igmp snooping vlan static command [2-118](#)

IP multicast addresses [2-163](#)

J

jumbo frames
 displaying setting **2-342**
 setting switch for **2-437**

L

line configuration mode **1-3, 1-6**
 link flap
 enable error detection for **2-92**
 enable timer to recover from error state **2-94**
 link statistics, clearing **2-34**
 load_helper (boot loader) command **B-14**
 load-distribution methods for EtherChannel **2-185**
 local duplex command **2-126**
 local speed command **2-127**
 logging lre command **2-128**
 logical interface **2-105**
 loop guard, for spanning tree **2-378, 2-381**
 LRE-10-1 profile **2-247**
 LRE-10-3 profile **2-247**
 LRE-10-5 profile **2-247**
 LRE-10LL profile **2-247**
 LRE-10 profile **2-246**
 LRE-15-1 profile **2-247**
 LRE-15-3 profile **2-247**
 LRE-15-5 profile **2-247**
 LRE-15LL profile **2-247**
 LRE-15 profile **2-247**
 LRE-2 profile **2-246**
 LRE-3 profile **2-246**
 LRE-4-1 profile **2-246**
 LRE-4 profile **2-246**
 LRE-5LL profile **2-247**
 LRE-5 profile **2-246**
 LRE-7 profile **2-246**
 LRE-8 profiles **2-246**
 LRE-997-10-4 profile **2-246**

LRE-998-15-4 profile **2-246**
 LRE controller, defined **2-62**
 lre profile command **2-130**
 lre rate selection command **2-40**
 lre rate selection sequence command **2-132**
 lre sequence command **2-134**

M

mac access-group command **2-138**
 MAC access-list configuration mode
 deny **2-77**
 entering **2-140**
 permit **2-178**
 mac access-list extended command **2-140**
 MAC ACLs
 deny **2-77**
 permit **2-178**
 MAC addresses
 clearing notification global counters **2-41**
 displaying
 aging time **2-300**
 dynamic **2-300**
 multicast entries **2-303**
 notification setting **2-305**
 number of addresses **2-300**
 per interface **2-300**
 per VLAN **2-300**
 secure **2-325**
 static **2-300**
 dynamic
 aging time **2-142**
 deleting **2-41**
 displaying **2-300**
 enabling MAC address notification **2-144**
 secure
 adding **2-424**
 displaying **2-325**

static
 adding **2-146**
 displaying **2-300**
 sticky
 configuring manually **2-424**
 enabling sticky learning **2-424**
 learning dynamically **2-424**
 mac-address-table aging-time command **2-142**
 mac-address-table notification command **2-144**
 mac-address-table static command **2-146**
 MAC-named extended ACLs **2-140**
 MAC notification feature
 clearing global counters **2-41**
 configuring **2-144**
 enabling **2-144**
 macros, interface range **2-71**
 manual
 audience **xiii**
 organization of **xiv**
 purpose of **xiii**
 maps, QoS
 defining **2-155**
 displaying **2-311**
 margin command **2-148**
 masks
 See ACPs
 match (class-map configuration) command **2-150**
 maximum transmission unit
 See MTU
 media-type command **2-152**
 member switches
 See clusters
 memory (boot loader) command **B-15**
 mkdir (boot loader) command **B-17**
 mls qos cos command **2-153**
 mls qos map command **2-155**
 mls qos trust command **2-157**
 mode, MVR **2-163**
 monitor session command **2-160**
 more (boot loader) command **B-18**
 MSTP
 displaying **2-335**
 interoperability **2-47**
 link type **2-380**
 MST region
 aborting changes **2-384**
 applying changes **2-384**
 configuration name **2-384**
 configuration revision number **2-384**
 current or pending display **2-384**
 displaying **2-335**
 MST configuration mode **2-384**
 VLANs-to-instance mapping **2-384**
 path cost **2-386**
 protocol mode **2-383**
 restart protocol migration process **2-47**
 root port
 loop guard **2-378**
 preventing from becoming designated **2-378**
 restricting which can be root **2-378**
 root guard **2-378**
 root switch
 affects of extended system ID **2-376**
 hello-time **2-389, 2-398**
 interval between BDPU messages **2-391**
 interval between hello BPDU messages **2-389, 2-398**
 max-age **2-391**
 maximum hop count before discarding BPDU **2-393**
 port priority for selection of **2-395**
 primary or secondary **2-398**
 switch priority **2-397**
 state changes
 blocking to forwarding state **2-404**
 enabling BPDU filtering **2-370, 2-402**
 enabling BPDU guard **2-372, 2-402**
 enabling Port Fast **2-402, 2-404**
 forward-delay time **2-388**
 length of listening and learning states **2-388**

rapid transition to forwarding **2-380**
shutting down Port Fast-enabled ports **2-402**
state information display **2-334**

MTU
configuring size **2-437**
displaying global setting **2-342**

multicast groups
See IGMP snooping

multicast groups, MVR **2-164**

multicast router learning method **2-116**

multicast router ports, configuring **2-116**

multicast suppression level
configuring **2-416**
displaying **2-339**
enabling **2-416**

multicast traffic counters **2-278**

multicast VLAN, MVR **2-164**

multicast VLAN registration
See MVR

Multiple Spanning Tree Protocol
See MSTP

MVR
configuring **2-163**
configuring interfaces **2-168**
displaying **2-315**

Immediate Leave feature **2-166**

receiver port **2-168**

source port **2-168**

mvr command **2-163**

mvr group command **2-164**

mvr immediate command **2-166**

mvr type command **2-168**

mvr vlan group command **2-170**

N

native VLANs, configuring **2-432**
normal-range VLANs **2-446, 2-452**
note, description **xv**
no vlan command **2-446, 2-456**

P

PAgP
See EtherChannel

pagp learn-method command **2-172**

pagp port-priority command **2-174**

password, VTP **2-466, 2-470, 2-472**

permit (access-list configuration) command **2-175**

permit (MAC access-list configuration) command **2-178**

persistence **2-180**

PIM-DVMRP, as multicast router learning method **2-116**

police command **2-181**

policy-map command **2-183**

policy maps
applying to an interface **2-201**
creating **2-183**
displaying **2-323**
policers
displaying **2-309**
for a single class **2-181**

traffic classification
defining the class **2-30**
defining the trust states **2-157**
setting DSCP values **2-202**

Port Aggregation Protocol
See EtherChannel

port-channel load-balance command **2-185**

Port Fast, for spanning tree **2-404**

port ranges, defining **2-71**

ports, debug messages, display **A-6**

port security
aging **2-428**

displaying **2-325**
 enabling **2-424**
 violation error recovery timer **2-94**

port trust states for QoS **2-157**
 privileged EXEC mode **1-2 to 1-4**
 profile (interface mode) command **2-187**
 profile (sequence mode) command **2-189**
 profiles, LRE
 default **2-246**
 LRE-10 **2-246**
 LRE-10-1 **2-247**
 LRE-10-3 **2-247**
 LRE-10-5 **2-247**
 LRE-10LL **2-247**
 LRE-15 **2-247**
 LRE-15-1 **2-247**
 LRE-15-3 **2-247**
 LRE-15-5 **2-247**
 LRE-15LL **2-247**
 LRE-2 **2-246**
 LRE-3 **2-246**
 LRE-4 **2-246**
 LRE-4-1 **2-246**
 LRE-5 **2-246**
 LRE-5LL **2-247**
 LRE-5 profile **2-246**
 LRE-7 **2-246**
 LRE-8 **2-246**
 LRE-988-15-4 **2-246**
 LRE-997-10-4 **2-246**

protected ports
 displaying **2-276**
 enabling **2-431**

pruning
 VLANs **2-432**
 VTP
 displaying interface information **2-271**
 enabling **2-466, 2-470, 2-472**

publications, related **xv**

Q

QoS
 ACPs, displaying **2-307**
 automatic configuration **2-16**
 class maps
 creating **2-32**
 defining the match criteria **2-150**
 displaying **2-211**
 configuration information, displaying **2-309**
 defining the CoS value for an incoming packet **2-153**
 displaying configuration information **2-206**
 maps
 defining **2-155**
 displaying **2-311**
 policers, displaying **2-309**
 policy maps
 applying to an interface **2-201**
 creating **2-183**
 defining policers **2-181**
 displaying policy maps **2-323**
 setting DSCP values **2-202**
 traffic classifications **2-30**
 port trust states **2-157**
 queues
 CoS-to-egress-queue map **2-477**
 WRR weights **2-476**
 quality of service
 See QoS
 querytime, MVR **2-163**

R

rate **2-192**
 rate selection, resetting **2-40**
 rate selection command **2-191**
 rate selection profile lock command **2-192**
 rate selection sequence command **2-193**
 rcommand command **2-195**

receiver port, MVR **2-168**
 receiving flow-control packets **2-96**
 recovery mechanism
 causes **2-94**
 display **2-263**
 timer interval **2-94**
 redundancy for cluster switches **2-59**
 remote-span command **2-197**
 Remote Switch Port Analyzer
 See RSPAN
 rename (boot loader) command **B-19**
 reset (boot loader) command **B-20**
 reset command **2-459**
 reset interface **2-36**
 reset LRE rate selection setting **2-40**
 rmdir (boot loader) command **B-21**
 rmon collection stats command **2-199**
 root guard, for spanning tree **2-378**
 RPS status display **2-330**
 RSPAN
 configuring **2-160**
 displaying **2-313**
 remote-span command **2-197**
 sessions
 add interfaces to **2-160**
 display **2-313**
 start new **2-160**

S
 sending flow-control packets **2-96**
 sequence configuration mode **1-3, 1-5**
 service-policy command **2-201**
 set (boot loader) command **B-22**
 set command **2-202**
 SFP **2-152**
 SFP-preferred **2-152**
 show access-lists command **2-204**
 show auto qos command **2-206**
 show boot command **2-209**
 show changes command **2-459**
 show class-map command **2-211**
 show cluster candidates command **2-215**
 show cluster command **2-213**
 show cluster members command **2-217**
 show controllers ethernet-controller command **2-219**
 show controllers lre actual command **2-231**
 show controllers lre admin command **2-234**
 show controllers lre cpe protected command **2-228**
 show controllers lre link monitor errors command **2-236**
 show controllers lre link monitor statistics
 command **2-238, 2-241**
 show controllers lre log **2-38**
 show controllers lre profile names command **2-246, 2-248**
 show controllers lre sequence command **2-250**
 show controllers lre status command **2-253**
 show controllers lre version command **2-257**
 show current command **2-459**
 show dot1x command **2-258**
 show env command **2-262**
 show errdisable recovery command **2-263**
 show etherchannel command **2-265**
 show file command **2-268**
 show interfaces command **2-271**
 show interfaces counters command **2-278**
 show ip access-list command **2-281**
 show ip igmp snooping command **2-283**
 show ip igmp snooping mrouter command **2-285**
 show lre upgrade binaries command **2-287**
 show lre upgrade version command **2-295**
 show mac access-group command **2-298**
 show mac-address-table command **2-300**
 show mac-address-table multicast command **2-303**
 show mac-address-table notification command **2-305**
 show mls masks **2-307**
 show mls qos interface command **2-309**
 show mls qos maps command **2-311**
 show monitor command **2-313**

show mvr command **2-315**
 show mvr interface command **2-317**
 show mvr members command **2-319**
 show pagp command **2-321**
 show policy-map command **2-323**
 show port-security command **2-325**
 show proposed command **2-459**
 show remote lre command **2-328**
 show rps command **2-330**
 show running-config vlan command **2-332**
 show spanning-tree command **2-334**
 show storm-control command **2-339**
 show system mtu command **2-342**
 show udld command **2-343**
 show version command **2-346**
 show vlan command **2-347**
 show vlan command fields **2-348**
 show vmps command **2-351**
 show vtp command **2-353**
 show wrr-queue bandwidth command **2-358**
 show wrr-queue cos-map command **2-359**
 shutdown command **2-360**
 shutdown vlan command **2-361**
 signal to noise ratio **2-148**
 SNMP host, specifying **2-364**
 snmp-server enable traps command **2-362**
 snmp-server host command **2-364**
 snmp trap mac-notification command **2-367**
 SNMP traps
 enable MAC address notification traps **2-362, 2-367**
 enable the sending of traps **2-362**
 enabling MAC address notification **2-144**
 SNR
 definition **2-148**
 margins **2-148**
 software images
 deleting **2-73**
 downloading **2-8**
 upgrading **2-8**
 uploading **2-14**
 software version, displaying **2-346**
 source ports, MVR **2-168**
 SPAN
 configuring **2-160**
 display **2-313**
 displaying **2-313**
 sessions
 add interfaces to **2-160**
 display **2-313**
 start new **2-160**
 spanning-tree backbonefast command **2-369**
 spanning-tree bpdufilter command **2-370**
 spanning-tree bpduguard command **2-372**
 spanning-tree cost command **2-374**
 spanning-tree extend system-id command **2-376**
 spanning-tree guard command **2-378**
 spanning-tree link-type command **2-380**
 spanning-tree loopguard default command **2-381**
 spanning-tree mode command **2-383**
 spanning-tree mst configuration command **2-384**
 spanning-tree mst cost command **2-386**
 spanning-tree mst forward-time command **2-388**
 spanning-tree mst hello-time command **2-389**
 spanning-tree mst max-age command **2-391**
 spanning-tree mst max-hops command **2-393**
 spanning-tree mst port-priority command **2-395**
 spanning-tree mst priority command **2-397**
 spanning-tree mst root command **2-398**
 spanning-tree portfast (global configuration) command **2-402**
 spanning-tree portfast (interface configuration) command **2-404**
 spanning-tree port-priority command **2-400**
 Spanning Tree Protocol
 See STP
 spanning-tree stack-port command **2-406**
 spanning-tree uplinkfast command **2-408**
 spanning-tree vlan command **2-410**

- speed command **2-413**
- static-access ports, configuring **2-418**
- statistics, Ethernet group **2-199**
- sticky learning, enabling **2-424**
- storm control
 - broadcast, enabling **2-416**
 - displaying **2-339**
 - multicast, enabling **2-416**
 - unicast, enabling **2-416**
- storm-control command **2-416**
- STP
 - BackboneFast **2-369**
 - debug message display
 - BackboneFast events **A-10**
 - MSTP **A-13**
 - optimized BPDUs handling **A-12**
 - spanning-tree activity **A-8**
 - switch shim **A-15**
 - transmitted and received BPDUs **A-11**
 - UplinkFast **A-17**
- detection of indirect link failures **2-369**
- extended system ID **2-376**
- path cost **2-374**
- protocol mode **2-383**
- root port
 - accelerating choice of new **2-408**
 - accelerating choice of new root in a stack **2-406**
 - cross-stack UplinkFast **2-406**
 - loop guard **2-378**
 - preventing from becoming designated **2-378**
 - restricting which can be root **2-378**
 - root guard **2-378**
 - UplinkFast **2-408**
- root switch
 - affects of extended system ID **2-376, 2-411**
 - hello-time **2-410**
 - interval between BDPU messages **2-410**
 - interval between hello BPDU messages **2-410**
 - max-age **2-410**
 - port priority for selection of primary or secondary **2-400**
 - primary or secondary **2-410**
 - switch priority **2-410**
 - state changes
 - blocking to forwarding state **2-404**
 - enable timer to recover from error state **2-94**
 - enabling BPDU filtering **2-370, 2-402**
 - enabling BPDU guard **2-372, 2-402**
 - enabling Port Fast **2-402, 2-404**
 - forward-delay time **2-410**
 - length of listening and learning states **2-410**
 - shutting down Port Fast-enabled ports **2-402**
 - state information display **2-334**
 - VLAN options **2-397, 2-410**
 - switching characteristics
 - modifying **2-422**
 - returning to interfaces **2-422**
 - switchport access command **2-418**
 - Switch Port Analyzer
 - See SPAN
 - switchport mode command **2-420**
 - switchport nonegotiate command **2-422**
 - switchport port-security aging command **2-428**
 - switchport port-security command **2-424**
 - switchport priority extend command **2-430**
 - switchport protected command **2-431**
 - switchports, displaying **2-271**
 - switchport trunk command **2-432**
 - switchport voice vlan command **2-435**
 - system-defined profiles
 - LRE-10 **2-246**
 - LRE-10-1 **2-247**
 - LRE-10-3 **2-247**
 - LRE-10-5 **2-247**
 - LRE-10LL **2-247**
 - LRE-15 **2-247**
 - LRE-15-1 **2-247**
 - LRE-15-3 **2-247**
 - LRE-15-5 **2-247**

LRE-15LL **2-247**
 LRE-2 **2-246**
 LRE-3 **2-246**
 LRE-4 **2-246**
 LRE-4-1 **2-246**
 LRE-5 **2-246**
 LRE-5LL **2-247**
 LRE-7 **2-246**
 LRE-8 **2-246**
 LRE-988-15-4 **2-246**
 LRE-997-10-4 **2-246**
 system mtu command **2-437**

T

TAC **xviii**
 tar files, creating, listing, and extracting **2-10**
 technical assistance
 Cisco.com **xvii**
 TAC **xviii**
 toll-free telephone numbers **xviii**
 Telnet to cluster switches **2-195**
 tips, description **xv**
 trunk ports, configuring **2-420**
 trunks, to non-DTP device **2-421**
 trusted boundary for QoS **2-157**
 type (boot loader) command **B-25**

U

UDLD
 aggressive mode **2-439, 2-441**
 debug messages, displaying **A-24**
 enabling globally **2-439**
 enabling per interface **2-441**
 error recovery timer **2-94**
 message timer **2-439**
 normal mode **2-439, 2-441**

resetting shutdown interfaces **2-443**
 status **2-343**
 udld (global interface) command **2-439**
 udld (interface configuration) command **2-441**
 udld reset command **2-443**
 unicast suppression level
 configuring **2-416**
 displaying **2-339**
 enabling **2-416**
 unicast traffic counters **2-278**
 UniDirectional Link Detection
 See UDLD
 unset (boot loader) command **B-26**
 upgrade binary command **2-444**
 upgrade preserve command **2-445**
 upgrading software images **2-8**
 UplinkFast, for STP **2-408**
 URLs, Cisco **xvi**
 user EXEC mode **1-2, 1-3**

V

version (boot loader) command **B-28**
 vlan (global configuration) command **2-446**
 vlan (VLAN configuration) command **2-452**
 VLAN configuration
 rules **2-449, 2-454**
 saving **2-446, 2-456**
 VLAN configuration mode
 commands
 VLAN **2-452**
 VTP **2-472**
 entering **2-458**
 summary **1-3**
 vlan database command **2-458**
 VLAN ID range **2-446, 2-452**
 VLAN Query Protocol
 See VQP
 VLANs

- adding **2-446**
 configuring **2-446, 2-452**
 debug message display
 ISL **A-21**
 VLAN IOS file system error tests **A-20**
 VLAN manager activity **A-18**
 VTP **A-22**
 displaying configurations **2-347**
 extended-range **2-446**
 MAC addresses **2-300**
 media types **2-449, 2-454**
 normal-range **2-446, 2-452**
 saving the configuration **2-446**
 shutting down **2-361**
 SNMP traps for VTP **2-362, 2-365**
 variables **2-452**
- VMPS
 configuring servers **2-464**
 reconfirming dynamic VLAN assignments **2-462**
 vmps reconfirm (global configuration) command **2-461**
 vmps reconfirm (privileged EXEC) command **2-462**
 vmps retry command **2-463**
 vmps server command **2-464**
 voice VLAN
 configure **2-435**
 set port priority **2-430**
- VQP
 and dynamic-access ports **2-419**
 clearing client statistics **2-48**
 displaying information **2-351**
 per-server retry count **2-463**
 reconfirmation interval **2-461**
 reconfirming dynamic VLAN assignments **2-462**
- VTP
 changing characteristics **2-466**
 clearing pruning counters **2-49**
 clearing VTP counters **2-49**
 configuring
 domain name **2-466, 2-472**
 file name **2-466**
 mode **2-466, 2-472**
 password **2-466, 2-470, 2-472**
 counters display fields **2-354**
 displaying information **2-353**
 enabling
 pruning **2-466, 2-470, 2-472**
 version 2 **2-466, 2-470, 2-472**
 mode **2-466, 2-472**
 pruning **2-466, 2-470, 2-472**
 saving the configuration **2-446, 2-456**
 status display fields **2-355**
 vtp (global configuration) command **2-466**
 vtp (privileged EXEC) command **2-470**
 vtp (VLAN configuration) command **2-472**
-
- W**
- WRR, assigning weights to egress queues **2-476**
 wrr-queue bandwidth command **2-476**
 wrr-queue cos-map command **2-477**