



Catalyst 2900 Series XL and Catalyst 3500 Series XL Command Reference

Cisco IOS Release 12.0(5)WC3
January 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-7812155=
Text Part Number: 78-12155-02

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.

AccessPath, AtmDirector, Browse with Me, CCIP, CCSI, CD-PAC, *CiscoLink*, the Cisco *Powered* Network logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, Cisco Unity, Fast Step, Follow Me Browsing, FormShare, FrameShare, IGX, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, MGX, the Networkers logo, ScriptBuilder, ScriptShare, SMARTnet, TransPath, Voice LAN, Wavelength Router, and WebViewer are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and Discover All That's Possible 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, FastHub, FastSwitch, GigaStack, IOS, IP/TV, LightStream, MICA, 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. (0110R)

Catalyst 2900 Series XL and Catalyst 3500 Series XL Command Reference

Copyright © 1998–2002, Cisco Systems, Inc.

All rights reserved.



Preface ix

Audience ix

Purpose ix

Organization x

Conventions x

Related Publications xi

Obtaining Documentation xii

World Wide Web xii

Cisco Documentation CD-ROM xii

Ordering Documentation xii

Documentation Feedback xiii

Obtaining Technical Assistance xiii

Cisco.com xiii

Technical Assistance Center xiv

Contacting TAC by Using the Cisco TAC Website xiv

Contacting TAC by Telephone xiv

CHAPTER 1

Using the Command-Line Interface 1-1

Configuration Tasks 1-1

Type of Memory 1-2

Platforms 1-2

CLI Command Modes 1-2

User EXEC Mode 1-4

Privileged EXEC Mode 1-4

VLAN Database Mode 1-5

Global Configuration Mode 1-5

Interface Configuration Mode 1-6

Line Configuration Mode 1-6

Command Summary 1-7

CHAPTER 2

Cisco IOS Commands 2-1

abort 2-1

apply 2-3

| | |
|---------------------------------------|------|
| cgmp | 2-5 |
| clear cgmp | 2-7 |
| clear controllers ethernet-controller | 2-8 |
| clear ip address | 2-9 |
| clear mac-address-table | 2-10 |
| clear mac-address-table notification | 2-12 |
| clear vmps statistics | 2-13 |
| clear vtp counters | 2-14 |
| cluster commander-address | 2-15 |
| cluster discovery hop-count | 2-17 |
| cluster enable | 2-18 |
| cluster holdtime | 2-20 |
| cluster management-vlan | 2-21 |
| cluster member | 2-22 |
| cluster run | 2-24 |
| cluster setup | 2-25 |
| cluster standby-group | 2-27 |
| cluster timer | 2-29 |
| delete | 2-30 |
| duplex | 2-31 |
| exit | 2-33 |
| flowcontrol | 2-35 |
| interface | 2-36 |
| ip address | 2-38 |
| ip igmp filter | 2-39 |
| ip igmp max-groups | 2-40 |
| ip igmp profile | 2-42 |
| login authentication | 2-44 |
| mac-address-table aging-time | 2-45 |
| mac-address-table dynamic | 2-46 |
| mac-address-table notification | 2-48 |
| mac-address-table secure | 2-50 |
| mac-address-table static | 2-52 |
| management | 2-54 |
| mvr (global configuration) | 2-56 |

| | |
|--------------------------------------|-------|
| mvr (interface configuration) | 2-59 |
| ntp broadcast client | 2-62 |
| ntp broadcast destination | 2-63 |
| ntp broadcast key | 2-64 |
| ntp broadcast version | 2-65 |
| ntp max-associations | 2-66 |
| ntp source | 2-67 |
| port block | 2-68 |
| port group | 2-69 |
| port monitor | 2-71 |
| port network | 2-73 |
| port protected | 2-74 |
| port security | 2-76 |
| port storm-control | 2-78 |
| power inline | 2-80 |
| rcommand | 2-81 |
| reset | 2-83 |
| rmon collection stats | 2-84 |
| session | 2-85 |
| show cgmp | 2-86 |
| show changes | 2-88 |
| show cluster | 2-90 |
| show cluster candidates | 2-92 |
| show cluster members | 2-94 |
| show controllers ethernet-controller | 2-96 |
| show current | 2-98 |
| show diags | 2-100 |
| show env | 2-101 |
| show file systems | 2-102 |
| show interface | 2-103 |
| show ip igmp profile | 2-107 |
| show mac-address-table | 2-108 |
| show mac-address-table notification | 2-110 |
| show mvr | 2-113 |
| show mvr interface | 2-114 |

| | |
|---|-------|
| show mvr members | 2-116 |
| show port block | 2-118 |
| show port group | 2-119 |
| show port monitor | 2-120 |
| show port network | 2-121 |
| show port protected | 2-122 |
| show port security | 2-123 |
| show port storm-control | 2-124 |
| show power inline | 2-125 |
| show proposed | 2-126 |
| show rps | 2-128 |
| show spanning-tree | 2-129 |
| show tacacs | 2-131 |
| show udld | 2-132 |
| show version | 2-135 |
| show vlan | 2-136 |
| show vmps | 2-138 |
| show vmps statistics | 2-139 |
| show vtp | 2-141 |
| shutdown | 2-146 |
| shutdown vlan | 2-147 |
| snmp-server enable traps mac-notification | 2-149 |
| snmp-server enable traps vlan-membership | 2-150 |
| snmp-server enable traps vtp | 2-151 |
| snmp-server host | 2-152 |
| snmp trap mac-notification | 2-154 |
| spanning-tree | 2-155 |
| spanning-tree cost | 2-157 |
| spanning-tree forward-time | 2-159 |
| spanning-tree hello-time | 2-161 |
| spanning-tree max-age | 2-162 |
| spanning-tree portfast | 2-164 |
| spanning-tree port-priority | 2-165 |
| spanning-tree priority | 2-166 |
| spanning-tree protocol | 2-168 |

| | |
|--|-------|
| spanning-tree rootguard | 2-170 |
| spanning-tree stack-port | 2-172 |
| spanning-tree uplinkfast | 2-173 |
| speed | 2-175 |
| switchport access | 2-177 |
| switchport mode | 2-179 |
| switchport multi | 2-181 |
| switchport priority | 2-183 |
| switchport trunk allowed vlan | 2-185 |
| switchport trunk encapsulation | 2-187 |
| switchport trunk native | 2-189 |
| switchport trunk pruning | 2-190 |
| switchport voice vlan | 2-192 |
| tacacs-server attempts | 2-194 |
| tacacs-server dns-alias-lookup | 2-195 |
| udld | 2-196 |
| udld enable | 2-197 |
| udld reset | 2-198 |
| vlan | 2-199 |
| vlan database | 2-205 |
| vmpls reconfirm (privileged EXEC) | 2-206 |
| vmpls reconfirm (global Configuration) | 2-207 |
| vmpls retry | 2-208 |
| vmpls server | 2-209 |
| vtp | 2-211 |
| vtp domain | 2-213 |
| vtp file | 2-214 |
| vtp password | 2-215 |
| vtp pruning | 2-216 |
| vtp v2-mode | 2-217 |



Preface

Audience

The *Catalyst 2900 Series XL and Catalyst 3500 Series XL Command Reference* is for the network manager responsible for configuring the Catalyst 2900 series XL and Catalyst 3500 series XL switches, hereafter referred to as the switches. Before using this reference manual, you should be familiar with the concepts and terminology of Ethernet and local area networking.

Purpose



Note

This guide describes the features for the Catalyst 2900 XL and Catalyst 3500 XL switches that are *not* Long-Reach Ethernet (LRE) switches. The Cisco IOS Release 12.0(5)WC3 software is for non-LRE switches only. Do not install this release on the Catalyst 2900 LRE XL switches. For information about configuring the Catalyst 2900 LRE XL switches, refer to Cisco IOS Release 12.0(5)WC2.

This reference manual provides detailed information about the commands that have been created or changed specifically for the Catalyst 2900 XL or Catalyst 3500 XL switches.

Use this reference manual with other Catalyst 2900 series XL and Catalyst 3500 series XL documents for these topics:

- Software configuration guide: For concepts and procedures for configuring and troubleshooting a switch or switch clusters. It includes descriptions of the management interface options and the features supported by the software.
- Release notes: For the hardware and software requirements and cluster compatibility requirements. For information and procedures for assigning switch IP information and passwords by using the setup program. For information about Cluster Management Suite (CMS) requirements and the procedures for browser configuration and accessing CMS.
- CMS online help: For CMS field-level window descriptions and procedures, refer to the CMS online help.
- Standard Cisco IOS Release 12.0 commands available from the Cisco IOS Release 12.0 documentation on Cisco.com.

Organization

The organization of this reference manual is as follows:

Chapter 1, “Using the Command-Line Interface,” lists the features included in this software release.

Chapter 2, “Cisco IOS Commands,” describes the Cisco IOS commands changed or customized for the switches.

Conventions

This publication uses the following conventions to convey instructions and information:

Command descriptions use these conventions:

- Commands and keywords are in **boldface** font.
- Arguments for which you supply values are in *italic*.
- Alternative keywords are grouped in braces ({}) and separated by vertical bars (|).
- Elements in square brackets ([]) are optional.

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 tip information use the following 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 in equipment damage or loss of data.



Tip

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 the Cisco.com site:

<http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/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 “Ordering Documentation” section on page xii.

- *Release Notes for the Catalyst 2900 Series XL and Catalyst 3500 Series XL Switches* (not orderable but is available on Cisco.com)



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.

- *Catalyst 2900 Series XL and Catalyst 3500 Series XL Software Configuration Guide* (order number DOC-786511=)
- Cluster Management Suite (CMS) online help (available only from the switch CMS software)
- *Catalyst 2900 Series XL Hardware Installation Guide* (order number DOC-786461=)
- *Catalyst 3500 Series XL Hardware Installation Guide* (order number DOC-786456=)
- *Catalyst 2900 Series XL Modules Installation Guide* (order number DOC-CAT2900-IG=)
- *Catalyst 2900 Series XL ATM Modules Installation and Configuration Guide* (order number DOC-785472=)
- *1000BASE-T Gigabit Interface Converter Installation Note* (not orderable but is available on Cisco.com)
- *Catalyst GigaStack Gigabit Interface Converter Hardware Installation Guide* (order number DOC-786460=)

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- <http://www.cisco.com>
- <http://www-china.cisco.com>
- <http://www-europe.cisco.com>

Cisco Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Cisco Documentation CD-ROM is updated monthly and might be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

**Note**

This CD contains the documentation for all Cisco products and is shipped with all Cisco products. This CD is not the same as the Catalyst 2900 XL and Catalyst 3500 XL Documentation CD, which contains only the Catalyst 2900 XL and Catalyst 3500 XL switch documents and related hardware documents.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered 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 corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can send us your comments by completing the online survey. When you display the document listing for this platform, click **Give Us Your Feedback**. If you are using the product-specific CD and you are connected to the Internet, click the pencil-and-paper icon in the toolbar to display the survey. After you display the survey, select the manual that you wish to comment on. Click **Submit** to send your comments to the Cisco documentation group.

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

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc.
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 documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

<http://www.cisco.com>

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

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

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

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

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

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

Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

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

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.



Using the Command-Line Interface

The switches are supported by Cisco IOS software. This chapter describes how to use the switch command-line interface (CLI) to configure features added for the switch. For a complete description of the commands that support these features, see Chapter 2, “Cisco IOS Commands.” For information about the standard Cisco IOS Release 12.0 commands, refer to the Cisco IOS Release 12.0 documentation on Cisco.com.

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, web-based management, and SNMP through devices connected to ports assigned to the management VLAN.



Note

This guide describes the features for the Catalyst 2900 XL and Catalyst 3500 XL switches that are *not* Long-Reach Ethernet (LRE) switches. The Cisco IOS Release 12.0(5)WC3 software is for non-LRE switches only. Do not install this release on the Catalyst 2900 LRE XL switches. For information about configuring the Catalyst 2900 LRE XL switches, refer to Cisco IOS Release 12.0(5)WC2.

Configuration Tasks

You can perform the following configuration tasks on your switches:

- Assign IP information to the switch
- Set port features, including creating Fast EtherChannel and Gigabit EtherChannel port groups
- Classify traffic and provide preferential treatment to certain types of traffic in compliance with the IEEE 802.1P quality of service (QoS) standard
- Manage the switch MAC-address table
- Monitor the MAC addresses of devices that are added or removed from a port
- Configure Spanning Tree Protocol (STP) features
- Enable the Cisco Group Management Protocol (CGMP) Fast-Leave feature
- Create Internet Group Management Group (IGMP) filtering profiles to restrict the flow of multicast traffic
- Assign IGMP filtering profiles to a specific port on the switch
- Configure VLANs

- Configure VLAN Trunking Protocol (VTP)
- Assign ports for static-access, multi-VLAN, or dynamic VLAN membership
- Configure a VLAN trunk
- Add, modify, and remove a VLAN to or from the database
- Configure the management VLAN for clustered and nonclustered switches
- Configure a command switch, build a cluster, and enable command-switch redundancy by using the Hot Standby Router Protocol (HSRP)
- Configure the UniDirectional Link Detection Protocol (UDLD) to help with the detection of spanning-tree loops on logical, one-way connections and disable the affected ports
- Configure enhanced packet-storm suppression to control unicast, broadcast, and multicast storms
- Configure 10/100 Ethernet ports for connection to Cisco IP telephones (control the telephone power on the Catalyst 3524-PWR-XL switch, configure the voice VLAN, and cause the telephone to use the priority received on the other port)
- Configure Network Time Protocol (NTP)
- Configure authentication for user access

For detailed information about completing these tasks, see the *Catalyst 2900 Series XL and Catalyst 3500 Series XL Software Configuration Guide*.

Type of Memory

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

Platforms

Cisco IOS Release 12.0(5)WC3 runs on a variety of Catalyst 2900 XL and Catalyst 3500 XL switches and modules. For a complete list, see the *Release Notes for the Catalyst 2900 Series XL and Catalyst 3500 Series XL Switches* on Cisco.com.



Note

This reference manual describes the features for the Catalyst 2900 XL and Catalyst 3500 XL switches that are *not* Long-Reach Ethernet (LRE) switches. The Cisco IOS Release 12.0(5)WC3 software is for non-LRE switches only. Do not install this release on the Catalyst 2900 LRE XL switches. For configuring the Catalyst 2900 LRE XL switches, refer to Cisco IOS Release 12.0(5)WC2.

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 Cisco IOS command modes:

- User EXEC mode

- Privileged EXEC mode
- VLAN database mode
- Global configuration mode
- Interface configuration mode
- Line configuration mode

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 names *Switch* and *ATM*. The *ATM* prompt appears only if you have an Asynchronous Transfer Mode (ATM) module installed in the 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. (For ATM) Begin a session with the ATM module. | Switch> ATM> | Enter the logout command. |
| Privileged EXEC | From user EXEC mode, enter the enable user EXEC command. | Switch# ATM# | To exit to user EXEC mode, enter the disable command. To enter global configuration mode, enter the configure command. |
| VLAN database | From user EXEC mode, enter the vlan database command. | Switch(vlan)# | To exit to user EXEC mode, enter the exit command. |
| Global configuration | From privileged EXEC mode, enter the configure privileged EXEC command. | Switch (config)# ATM (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 configuration command. |
| Interface configuration | From global configuration mode, specify an interface by entering the interface command. | Switch (config-if)# ATM (config-if)# | To exit to privileged EXEC mode, enter the end command, or press Ctrl-Z . To exit to global configuration mode, enter the exit command. To enter subinterface configuration mode, specify a subinterface with the interface command. On the ATM module, the LAN emulation (LANE) client is considered a subinterface. |
| Line configuration | From global configuration mode, specify a line by entering the line command. | Switch (config-line)# ATM (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, the user EXEC commands allow you to change terminal settings temporarily, perform basic tests, and 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> ?
```

```
ATM> ?
```

**Note**

The **clear** and **set** commands are in the list of commands that appears when you enter a question mark, but they are not supported in user EXEC mode.

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#
```

```
ATM#
```

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

```
Switch> enable
Switch#
```

```
ATM> enable
ATM#
```

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# ?
```

```
ATM# ?
```

**Note**

The **set** command is in the list of commands that appears when you enter a question mark, but it is not supported in privileged EXEC mode.

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

VLAN Database Mode

The VLAN database commands allow you to modify VLAN parameters. Enter the **vlan database** command to access VLAN database 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 VLAN database and to return to privileged EXEC mode.

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]?
```

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

You can specify either the terminal or nonvolatile random-access memory (NVRAM) as the source of configuration commands.

The following example shows you how to access global configuration mode:

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

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

```
ATM(config)# ?  
ATM(config)#
```

To exit global configuration command mode and return to privileged EXEC mode, enter the **end** or **exit** 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 indicates interface configuration mode.

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

```
ATM(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-subif)# ?
```

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

```
ATM(config-subif)# ?
```

```
ATM(config-if)#
```

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

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. These commands are used 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. These examples show how to enter line configuration mode for virtual terminal line 7:

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

```
ATM(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)# ?
```

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

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

Command Summary

Table 1-2 lists and describes the Cisco IOS commands for the Catalyst 2900 XL and Catalyst 3500 XL switches. The commands are sorted by the command modes from which they are entered.

Table 1-2 Command Summary

| Commands | Description |
|--|---|
| User EXEC mode | |
| rcommand | Executes commands on a cluster member from the command switch. |
| show cluster | Displays the cluster status and a summary of the cluster to which the switch belongs. |
| show cluster candidates | Displays switches that are not currently members of the cluster but that could be. |
| show cluster members | Displays information about all members in a cluster. |
| show spanning-tree | Displays STP information. |
| show uddld | Displays UDLD status information for all ports or the specified port. |
| show version | Displays the firmware version for the switch or module. |
| show vlan | Displays information about a VLAN. |
| show vtp counters show vtp status | Displays general information about the VTP management domain, status, and counters. |
| Privileged EXEC mode | |
| clear cgmp | Deletes the multicast addresses and router ports maintained by CGMP. |
| clear controllers ethernet-controller | Deletes the Ethernet link transmit and receive statistics on a Fast Ethernet switch. |
| clear mac-address-table notification | Deletes entries from the MAC address notification table. |
| clear ip address | Deletes the IP address without disabling the IP processing. |
| clear mac-address-table | Deletes all addresses in the MAC address table. |
| clear vmps statistics | Clears the statistics maintained by the VLAN Query Protocol (VQP) client. |
| clear vtp counters | Clears the VTP counters. |
| cluster setup | Automatically builds a cluster. |
| delete | Deletes a file from the file system. |
| session | Logs into an ATM module. |
| show cgmp | Displays the current state of the CGMP-learned multicast groups and routers. |
| show controllers ethernet-controller | Displays the Ethernet link transmit and receive statistics on a Fast Ethernet switch. |
| show diags | Displays the current state of a port or all ports on the switch. |
| show env | Displays the status of the 3524-PWR-XL switch fans and temperature. |
| show file systems | Displays information about local and remote file systems. |
| show interface | Displays the administrative and operational status of a switching port. |
| show ip igmp profile | Displays the details of an IGMP profile entry. |
| show mac-address-table | Displays the MAC address table. |
| show mac-address-table notification | Displays the global parameters for the MAC address table notification feature. |

Table 1-2 Command Summary (continued)

| Commands | Description |
|---|---|
| show mvr | Displays the current multicast VLAN registration (MVR) global parameter values, including whether or not MVR is enabled, the maximum query response time, the maximum number of multicast entries, and the multicast VLAN number. |
| show mvr interface | Displays the MVR receiver and source ports. Use the command with keywords to display MVR parameters for a specific receiver port. |
| show mvr members | Displays all receiver ports that are members of an IP multicast group. |
| show port block | Displays the blocking of unicast and multicast filtering for the port. |
| show port group | Displays the ports that are assigned to groups. |
| show port monitor | Displays the ports that have port monitoring enabled. |
| show port network | Displays the network ports on the switch. |
| show port protected | Displays the ports that are port protected mode. |
| show port security | Displays the ports that have port security enabled. |
| show port storm-control | Displays the setting of broadcast-storm control. |
| show power inline | Displays the power status for the specified port or all ports on the 3524-PWR-XL switch. |
| show rps | Displays the status of the Cisco Redundant Power System (RPS). |
| show spanning-tree | Displays spanning-tree information for the specified spanning-tree instances. |
| show tacacs | Displays various Terminal Access Controller Access Control System Plus (TACACS+) server statistics. |
| show vmps | Displays the VQP version, reconfirmation interval, retry count, server IP addresses, and current and primary servers. |
| show vmps statistics | Displays the VQP client-side statistics. |
| udld reset | Resets all ports that have been shut down by UDLD. |
| vlan database | Enters VLAN database mode. |
| vmps reconfirm (privileged EXEC) | Sends VQP queries to reconfirm all dynamic VLAN assignments with the VLAN Membership Policy Server (VMPS). |
| Global configuration mode | |
| cgmpp | Enables CGMP and other CGMP options. |
| cluster commander-address | Automatically provides the command switch MAC address to member switches. This command is automatically issued. |
| cluster discovery hop-count | Sets the hop-count limit for extended discovery of cluster candidates. |
| cluster enable | Enables the cluster command switch and names the cluster. |
| cluster holdtime | Sets the timer that determines when a command switch declares the other switch down after not receiving a heartbeat message. Used with the cluster timer command. |
| cluster management-vlan | Changes the management VLAN for the entire cluster. |
| cluster member | Adds members to the cluster. |
| cluster run | Enables clustering on a switch. |

Table 1-2 Command Summary (continued)

| Commands | Description |
|--|---|
| cluster standby-group | Enables command switch redundancy by binding an HSPR standby group to the cluster. |
| cluster timer | Specifies the interval between heartbeat messages between the command and member switches. Used with the cluster holdtime command. |
| interface | Selects an interface to configure. Creates a new management VLAN interface. |
| ip igmp profile | Defines a new profile for IGMP filtering or deletes an existing IGMP filtering profile. |
| mac-address-table aging-time | Specifies the length of time that a dynamic entry remains in the MAC address table. |
| mac-address-table dynamic | Adds a dynamic address entry to the MAC address table. |
| mac-address-table notification | Enables the MAC address table notification feature on the switch. |
| mac-address-table secure | Adds a secure address entry to the MAC address table. |
| mac-address-table static | Adds a static address entry to the address table. |
| mvr (global configuration) | Enables the Multicast VLAN Registration (MVR) feature on the switch. |
| ntp max-associations | Specifies the maximum number of NTP associations that are allowed on a server. |
| ntp source | Uses a particular source address in NTP packets. |
| shutdown vlan | Shuts down local traffic on the specified VLAN. |
| snmp-server enable traps mac-notification | Enables SNMP notification for MAC address notification. |
| snmp-server enable traps vlan-membership | Enables SNMP notification for VMPS changes. |
| snmp-server enable traps vtp | Enables SNMP notification for VTP changes. |
| snmp-server host | Specifies the host that receives SNMP traps. |
| spanning-tree | Enables a spanning-tree instance. |
| spanning-tree forward-time | Specifies the forward delay interval for the switch. |
| spanning-tree hello-time | Specifies the interval between hello Bridge Protocol Data Units (BPDUs). |
| spanning-tree max-age | Changes the interval the switch waits to receive BPDUs from the root switch. |
| spanning-tree priority | Configures the bridge priority for the specified spanning-tree instance. |
| spanning-tree protocol | Defines the type of STP. |
| spanning-tree uplinkfast | Accelerates the choice of a new root port when a link or switch fails or when STP reconfigures itself. |
| tacacs-server attempts | Controls the number of login attempts that can be made on a line configured for TACACS, Extended TACACS, or TACACS+ verification. |
| tacacs-server dns-alias-lookup | Enables IP Domain Name System alias lookup for TACACS+. |
| udld enable | Enables UDLD on all switch ports. |
| vmmps reconfirm (global Configuration) | Changes the reconfirmation interval for the VQP client. |
| vmmps retry | Configures the per-server retry count for the VQP client. |
| vmmps server | Configures the primary VMPS and up to three secondary servers. |

Table 1-2 Command Summary (continued)

| Commands | Description |
|--------------------------------------|---|
| vtp file | Modifies the VTP configuration storage filename. |
| VLAN database mode | |
| abort | Abandons the proposed VLAN database and returns to privileged EXEC mode. |
| apply | Implements the proposed VLAN database, propagates it throughout the administrative domain, and remains in VLAN database mode. |
| exit | Implements the proposed VLAN database, propagates it throughout the administrative domain, and returns to privileged EXEC mode. |
| reset | Abandons the proposed VLAN database and remains in VLAN database mode. |
| show changes | Displays the differences between the current VLAN database on the switch and the proposed VLAN database. |
| show current | Displays the current VLAN database on the switch or a single selected VLAN from it. |
| show proposed | Displays the proposed VLAN database or a single selected VLAN from it. |
| vlan | Configures a VLAN by its VLAN ID. |
| vtp | Configures the VTP mode. |
| vtp domain | Configures the VTP administrative domain. |
| vtp password | Configures the VTP password. |
| vtp pruning | Enables pruning in the VTP administrative domain. |
| vtp v2-mode | Enables VTP version 2 mode in the administrative domain. |
| Interface configuration mode | |
| duplex | Specifies the duplex mode of operation for a port. |
| flowcontrol | Controls traffic rates during congestion. |
| ip address | Specifies a primary or secondary IP address of a VLAN interface. |
| ip igmp filter | Applies a specific IGMP filtering profile to an interface. |
| ip igmp max-groups | Specifies the maximum number of IGMP profiles that can be active on a port. |
| management | Shuts down the management VLAN interface. |
| mvr (interface configuration) | Configures a port as an MVR receiver or source port, specifies the Immediate-Leave feature, and configures the port threshold. |
| ntp broadcast client | Allows the system to receive NTP broadcast packets on a port. |
| ntp broadcast destination | Configures an NTP server or peer to restrict broadcast of NTP frames to the IP address of a designated client or a peer. |
| ntp broadcast key | Configures an NTP server or peer to broadcast NTP frames with the authentication key embedded in the NTP packet. |
| ntp broadcast version | Specifies a port to send NTP broadcast packets. |
| port block | Prevents the flooding of unknown destination MAC addresses and multicast addresses on this port. |
| port group | Places a port into a port aggregation group. |
| port monitor | Implements port monitoring on this port. |

Table 1-2 Command Summary (continued)

| Commands | Description |
|---------------------------------------|---|
| port network | Enables a port as the network port for a VLAN. |
| port protected | Isolates unicast, multicast, and broadcast traffic at Layer 2 from other protected ports on the same switch. |
| port security | Enables port security on a port. |
| port storm-control | Disables broadcast, multicast, or unicast traffic if too many packets are seen on this port. |
| power inline | Specifies how inline power is applied to the device on the specified Fast Ethernet port of the 3524-PWR-XL switch. |
| rmon collection stats | Collects Ethernet group statistics. |
| shutdown | Disables a port. |
| snmp trap mac-notification | Enables or disables the MAC notification feature on a specific port. |
| spanning-tree cost | Specifies a different path cost. |
| spanning-tree portfast | Enables the Port Fast option on the switch. |
| spanning-tree port-priority | Configures the STP priority of a port. |
| spanning-tree rootguard | Enables the root guard feature for all the VLANs associated with the specified port. Controls which ports can be STP root ports. |
| 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 STP reconfigures itself. |
| speed | Specifies the speed of a port. |
| switchport access | Configures a port as an access or dynamic VLAN port. |
| switchport mode | Configures the VLAN membership mode of a port. |
| switchport multi | Configures a port to be a multi-VLAN port. |
| switchport priority | Configures a port priority for untagged (native Ethernet) frames to provide quality of service (QoS). Also sets the priority of frames received by the appliance connected to the specified port. |
| switchport trunk allowed vlan | Controls which VLANs can receive and transmit traffic on the trunk. |
| switchport trunk encapsulation | Sets the encapsulation format on the trunk. |
| switchport trunk native | Sets the native VLAN for untagged traffic when in IEEE 802.1Q trunking mode. |
| switchport trunk pruning | Sets the list of VLANs enabled for VTP pruning when the port is in trunking mode. |
| switchport voice vlan | Sets the voice VLAN on the port. |
| udld | Enables or disables UDLD on a port. |
| Line configuration mode | |
| login local | Changes a login username. |
| login tacacs | Configures the switch to use TACACS user authentication. |

For detailed command syntax and descriptions, see Chapter 2, “Cisco IOS Commands.” For task-oriented configuration steps, see the software configuration documentation that came with the switch.



Cisco IOS Commands

abort

Use the **abort** VLAN database command to abandon the proposed VLAN database, exit VLAN database mode, and return to privileged EXEC mode.

abort

| | |
|---------------------------|--|
| Syntax Description | This command has no arguments or keywords. |
|---------------------------|--|

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

| | |
|----------------------|---------------|
| Command Modes | VLAN database |
|----------------------|---------------|

| | | |
|------------------------|----------------|------------------------------------|
| Command History | Release | Modification |
| | 11.2(8)SA4 | This command was first introduced. |

| | |
|-------------------------|---|
| Usage Guidelines | If you have added, deleted, or modified VLAN parameters in VLAN database mode but you do not want to keep the changes, the abort command causes all the changes to be abandoned. The VLAN configuration that was running before you entered VLAN database mode continues to be used. |
|-------------------------|---|

| | |
|-----------------|---|
| Examples | This example shows how to abandon the proposed VLAN database and to exit to the privileged EXEC mode: |
|-----------------|---|

```
Switch(vlan)# abort
Switch#
```

You can verify that no VLAN database changes occurred by entering the **show vlan brief** user EXEC command.

| Related Commands | Command | Description |
|------------------|----------------------|--|
| | apply | Implements the proposed VLAN database, increments the database configuration revision number, propagates it throughout the administrative domain, and remains in VLAN database mode. |
| | exit | Implements the proposed VLAN database, increments the database configuration number, propagates it throughout the administrative domain, and returns to privileged EXEC mode. |
| | reset | Abandons the proposed VLAN database and remains in VLAN database mode. Resets the proposed database to the currently implemented VLAN database on the switch. |
| | show vlan | Displays the parameters for all configured VLANs in the administrative domain. |
| | shutdown vlan | Shuts down (suspends) local traffic on the specified VLAN. |
| | vlan database | Enters VLAN database mode from the command-line interface (CLI). |

apply

Use the **apply** VLAN database command to implement the proposed VLAN database to increment the database configuration revision number, to propagate it throughout the administrative domain, and to remain in VLAN database mode.

apply

| | |
|---------------------------|--|
| Syntax Description | This command has no arguments or keywords. |
|---------------------------|--|

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

| | |
|----------------------|---------------|
| Command Modes | VLAN database |
|----------------------|---------------|

| Command History | Release | Modification |
|-----------------|------------|------------------------------------|
| | 11.2(8)SA4 | This command was first introduced. |

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

You cannot use this command when the switch is in the VLAN Trunking Protocol (VTP) client mode.

| | |
|-----------------|---|
| Examples | This example shows how to implement the proposed VLAN database as the running database: |
|-----------------|---|

```
Switch(vlan)# apply
```

You c**g**ow **vlan** user EXEC command.

| Related Commands | Command | Description |
|------------------|----------------------|--|
| | apply | Implements the proposed VLAN database, increments the database configuration revision number, propagates it throughout the administrative domain, and remains in VLAN database mode. |
| | exit | Implements the proposed VLAN database, increments the database configuration number, propagates it throughout the administrative domain, and returns to privileged EXEC mode. |
| | reset | Abandons the proposed VLAN database and remains in VLAN database mode. Resets the proposed database to the currently implemented VLAN database on the switch. |
| | show vlan | Displays the parameters for all configured VLANs in the administrative domain. |
| | shutdown vlan | Shuts down (suspends) local traffic on the specified VLAN. |
| | vlan database | Enters VLAN database mode from the command-line interface (CLI). |

cgmp

Use the **cgmp** global configuration command to enable Cisco Group Management Protocol (CGMP) and other CGMP options. Use the **no** form of this command to disable CGMP and its options.

cgmp {**leave-processing** | **holdtime** *time* / **reserved**}

no cgmp {**leave-processing** | **holdtime** | **reserved**}

| | | |
|--------------------|-----------------------------|--|
| Syntax Description | leave-processing | Enable Fast Leave processing on the switch. |
| | holdtime <i>time</i> | Number of seconds a router connection is retained before the switch ceases to exchange messages with it. You can enter a number from 10 to 6000 (seconds). |
| | reserved | Allow reserved addresses from 0100.5E00.0000 to 0100.5E00.00FF to join as group destination addresses. |

| | |
|----------|--|
| Defaults | CGMP is enabled. Fast Leave is disabled. The hold time is 300 seconds. Reserved addresses are allowed as group destination addresses. |
|----------|--|

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

| | | |
|-----------------|----------------|--|
| Command History | Release | Modification |
| | 11.2(8)SA3 | This command was first introduced. |
| | 12.0(5)XP | The reserved keyword was added. |

| | |
|------------------|---|
| Usage Guidelines | CGMP must be enabled before the Fast Leave option can be enabled. |
|------------------|---|

Examples

This example shows how to disable CGMP:

```
Switch(config)# no cgmp
```

This example shows how to disable the Fast Leave option:

```
Switch(config)# no cgmp leave-processing
```

This example shows how to set 400 seconds as the length of time the switch waits before ceasing to exchange messages with a router:

```
Switch(config)# cgmp holdtime 400
```

This example shows how to remove the amount of time the switch waits before ceasing to exchange messages with a router:

```
Switch(config)# no cgmp holdtime
```

This example shows how to exclude reserved addresses from the group destination address for compatibility with Catalyst 5000 series switches.

```
Switch(config)# no cgmp reserved
```

You can verify the previous commands by entering the **show cgmp** user EXEC command.

Related Commands

| Command | Description |
|-------------------|--|
| clear cgmp | Deletes information that the switch learned by using CGMP. |
| show cgmp | Displays the state of the CGMP-learned multicast groups and routers. |

clear cgmp

Use the **clear cgmp** privileged EXEC command to delete information that was learned by the switch by using the Cisco Group Management Protocol (CGMP).

clear cgmp [**vlan** *vlan-id*] | [**group** *address*] | **router** *address*]

| | | |
|--------------------|------------------------------|--|
| Syntax Description | vlan <i>vlan-id</i> | (Optional) VLAN for which the CGMP groups or routers are to be deleted. Valid IDs are from 1 to 1001; do not enter leading zeroes. |
| | group <i>address</i> | Delete all known multicast groups and their destination ports. Limited to a VLAN if the vlan keyword is entered. Limited to a specific group if the <i>address</i> parameter (MAC address of the group or router) is entered. |
| | router <i>address</i> | (Optional) Delete all routers, their ports, and expiration times. Limited to a given VLAN if the vlan keyword is entered. Limited to a specific router if the <i>address</i> parameter is entered. |

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

| | | |
|-----------------|------------|------------------------------------|
| Command History | Release | Modification |
| | 11.2(8)SA3 | This command was first introduced. |

| | |
|------------------|--|
| Usage Guidelines | Using clear cgmp with no arguments deletes all groups and routers in all VLANs. |
|------------------|--|

| | |
|----------|--|
| Examples | This example shows how to delete all groups and routers on VLAN 2: |
|----------|--|

```
Switch# clear cgmp vlan 2
```

This example shows how to delete all groups on all VLANs:

```
Switch# clear cgmp group
```

This example shows how to delete a router address on VLAN 2:

```
Switch# clear cgmp vlan 2 router 0012.1234.1234
```

You can verify the previous commands by entering the **show cgmp** user EXEC command.

| | | |
|------------------|------------------|---|
| Related Commands | Command | Description |
| | cgmp | Enables CGMP and the Fast Leave option and sets the router port aging time. |
| | show cgmp | Displays the state of the CGMP-learned multicast groups and routers. |

clear controllers ethernet-controller

Use the **clear controllers ethernet-controller** privileged EXEC command to delete the Ethernet link transmit and receive statistics on a Fast Ethernet switch.

clear controllers ethernet-controller *interface-id*

| | | |
|--------------------|---------------------|-------------------------------|
| Syntax Description | <i>interface-id</i> | ID of the Fast Ethernet port. |
|--------------------|---------------------|-------------------------------|

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

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

| Command History | Release | Modification |
|-----------------|------------|------------------------------------|
| | 12.0(5)WC1 | This command was first introduced. |

| | |
|------------------|--|
| Usage Guidelines | <p>Using the clear controllers ethernet-controller command without specifying a Fast Ethernet port deletes the Ethernet link statistics of all ports on the switch.</p> <p>It takes the switch several seconds to clear all of the ports.</p> |
|------------------|--|

| | |
|-----------|---|
| Examples. | <p>This example shows how to use the clear controllers ethernet-controller command to delete the Ethernet link statistics on Fast Ethernet port 0/1:</p> <pre>Switch# clear controllers ethernet-controller FastEthernet 0/1 Switch#</pre> <p>You can verify that information was deleted by entering the show controllers ethernet-controller user EXEC command.</p> |
|-----------|---|

| Related Commands | Command | Description |
|------------------|---|--|
| | show controllers ethernet-controller | Displays the Ethernet link transmit and receive statistics on a Fast Ethernet. |

clear ip address

Use the **clear ip address** privileged EXEC command to delete an IP address for a switch without disabling the IP processing.

clear ip address [**vlan** *vlan-id*]

Syntax Description

| | |
|----------------------------|--|
| vlan <i>vlan-id</i> | (Optional) Delete an IP address only within the specified VLAN. Valid IDs are from 1 to 1000; do not enter leading zeroes. |
|----------------------------|--|

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|------------|------------------------------------|
| 11.2(8)SA | This command was first introduced. |
| 11.2(8)SA3 | The vlan keyword was added. |

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 your switch receives its IP address from a Bootstrap Protocol (BOOTP) or Dynamic Host Configuration Protocol (DHCP) server and you delete the switch IP address by using the **clear ip address** command, the BOOTP or DHCP server reassigns the address.

Examples

This example shows how to clear the IP address for the switch on VLAN 1:

```
Switch# clear ip address vlan 1
```

You can verify the previous commands by entering the **show running-config** privileged EXEC command.

Related Commands

| Command | Description |
|----------------------------|---|
| show running-config | Displays the running configuration on the switch. |

clear mac-address-table

Use the **clear mac-address-table** privileged EXEC command to delete entries from the MAC address table.

```
clear mac-address-table [static | dynamic | secure] [address hw-addr] [interface interface]
[atm slot/port] [vlan vlan-id]
```

| | | |
|--------------------|-----------------------------------|---|
| Syntax Description | static | (Optional) Delete only static addresses. |
| | dynamic | (Optional) Delete only dynamic addresses. |
| | secure | (Optional) Delete only secure addresses. |
| | address <i>hw-addr</i> | (Optional) Delete the address <i>hw-addr</i> of type static, dynamic, and secure as specified. |
| | interface <i>interface</i> | (Optional) Delete an address on the interface <i>interface</i> of type static, dynamic, or secure as specified. |
| | atm <i>slot/port</i> | (Optional) Delete only ATM addresses on this slot and port. |
| | vlan <i>vlan-id</i> | (Optional) Delete all the MAC addresses for <i>vlan-id</i> . Valid IDs are from 1 to 1005; do not enter leading zeroes. |

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

| Command History | Release | Modification |
|-----------------|------------|------------------------------------|
| | 11.2(8)SA | This command was first introduced. |
| | 11.2(8)SA3 | The vlan keyword was added. |
| | 11.2(8)SA5 | The atm keyword was added. |

| | |
|------------------|--|
| Usage Guidelines | This command deletes entries from the global MAC address table. Specific subsets can be deleted by using the optional keywords and values. If more than one optional keyword is used, all of the conditions in the argument must be true for that entry to be deleted. |
|------------------|--|

Examples

This example shows how to delete static addresses on port fa0/7:

```
Switch# clear mac-address-table static interface fa0/7
```

This example shows how to delete all secure addresses in VLAN 3:

```
Switch# clear mac-address-table secure vlan 3
```

This example shows how to delete address 0099.7766.5544 from all ports in all VLANs. If the address exists in multiple VLANs or multiple ports, all the instances are deleted.

```
Switch# clear mac-address-table address 0099.7766.5544
```

This example shows how to delete address 0099.7766.5544 only in VLAN 2:

```
Switch# clear mac-address-table address 0099.7766.5544 vlan 2
```

This example shows how to delete the secure MAC address 00c0.00a0.03fa associated with the ATM port in expansion slot 2:

```
Switch(config)# clear mac-address-table secure 00c0.00a0.03fa atm 2/1
```

This example shows how to delete the static address 00c0.00a0.03fa associated with the ATM port in expansion slot 2:

```
Switch(config)# clear mac-address-table static 00c0.00a0.03fa atm 2/1
```

You can verify the previous commands by entering the **show mac-address-table** user EXEC command.

Related Commands

| Command | Description |
|-------------------------------|---------------------------------|
| show mac-address-table | Displays the MAC address table. |

clear mac-address-table notification

Use the **clear mac-address-table notification** privileged EXEC command to clear the addresses maintained by the MAC address notification feature.

clear mac-address-table notification

| | |
|--------------------|--|
| Syntax Description | This command has no keywords or options. |
|--------------------|--|

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

| Command History | Release | Modification |
|-----------------|------------|-------------------------|
| | 12.0(5)WC3 | This feature was added. |

| | |
|------------------|--|
| Usage Guidelines | This command clears the counters for the MAC addresses added, the MAC addresses removed, and the number of traps sent to the NMS counters on the switch. This command does <i>not</i> clear the history table on the switch. |
|------------------|--|

| Related Commands | Command | Description |
|------------------|-------------------------------|---------------------------------|
| | show mac-address-table | Displays the MAC address table. |

clear vmmps statistics

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

clear vmmps statistics

| | |
|---------------------------|--|
| Syntax Description | This command has no arguments or keywords. |
|---------------------------|--|

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

| | | |
|------------------------|----------------|------------------------------------|
| Command History | Release | Modification |
| | 11.2(8)SA4 | This command was first introduced. |

| | |
|-----------------|---|
| Examples | This example shows how to clear VLAN Membership Policy Server (VMPS) statistics: Switch# clear vmmps statistics |
| | You can verify the previous command by entering the show vmmps statistics privileged EXEC command. |

| | | |
|-------------------------|------------------------------|---|
| Related Commands | Command | Description |
| | show vmmps statistics | Displays the VLAN Query Protocol (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. |
|---------------------------|--|

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

| | | |
|------------------------|----------------|------------------------------------|
| Command History | Release | Modification |
| | 11.2(8)SA4 | This command was first introduced. |

| | |
|-----------------|---|
| Examples | This example shows how to clear the VTP counters: |
|-----------------|---|

```
Switch# clear vtp counters
```

You can verify the previous command by entering the **show vtp counters** user EXEC command.

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

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. |
| | member <i>number</i> | Number of member switch. The range is from 0 to 15. |
| | name <i>name</i> | Name of the cluster up to 31 characters. |
| | no | Remove a switch from the cluster. Entered on the member switch. |
| | default | Remove a switch from the cluster. Entered on the member switch. |

| | |
|----------|--|
| Defaults | The switch is not a member of any cluster. |
|----------|--|

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

| Command History | Release | Modification |
|-----------------|------------|--|
| | 11.2(8)SA6 | This command was first introduced. |
| | 12.0(5)XU | The member and name keywords were added. |

| | |
|------------------|---|
| Usage Guidelines | <p>A cluster member can belong to only one command switch.</p> <p>The member switch retains the identity of the command switch during a system reload by using the <i>mac-address</i> parameter.</p> <p>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 <i>n</i> global configuration command on the command switch.</p> <p>When a standby command-switch becomes active (becomes the command switch), it removes the cluster commander-address line from its configuration.</p> |
|------------------|---|

Examples

This is partial sample output from the running configuration of a cluster member.

```
Switch(config)# show running-configuration
```

```
<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-es3# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Switch-es3(config)# no cluster commander-address
```

You can verify the previous command by entering the **show cluster** command in user EXEC mode.

Related Commands

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

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

default 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. |
| | no | Set the hop count to the default value (3). |
| | default | Set the hop count to the default value (3). |

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

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

| Command History | Release | Modification |
|-----------------|-----------|------------------------------------|
| | 12.0(5)XU | This command was first introduced. |

| | |
|------------------|--|
| Usage Guidelines | <p>Enter this command only on the command switch. This command does not operate on member switches.</p> <p>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.</p> |
|------------------|--|

| | |
|----------|---|
| Examples | <p>This example shows how to set the hop count limit to 4. This command is entered on the command switch.</p> |
|----------|---|

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

You can verify the previous command by entering the **show cluster** command in user EXEC mode.

| 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 to make the command switch a candidate switch.

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

no cluster enable

default cluster enable

| | | |
|--------------------|-------------------------------------|--|
| Syntax Description | <i>name</i> | Name of the cluster up to 31 characters. Valid characters include only alphanumerics, dashes, and underscores. |
| | <i>command-switch-member-number</i> | (Optional) Assign a member number to the command switch of the cluster. The range is from 0 to 15. |
| | no | Remove all member switches, and make the command switch a candidate. |
| | default | Switch is not a command switch. |

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 |
|------------|---|
| 11.2(8)SA6 | This command was first introduced. |
| 12.0(5)XU | The <i>command-switch-member-number</i> variable was added. |

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, to name the cluster, and to set the command switch member number to 4.

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

You can verify the previous command by entering the **show cluster** command in user EXEC mode 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

default 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. |
| | no | Set the holdtime to the default value (80 seconds). |
| | default | Set the holdtime to the default value (80 seconds). |

Defaults The holdtime is 80 seconds.

Command Modes Global configuration

| Command History | Release | Modification |
|-----------------|-----------|------------------------------------|
| | 12.0(5)XU | This command was first 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.

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 the previous commands by entering the **show cluster** command in user EXEC mode.

| 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

default cluster management-vlan

| | | |
|--------------------|----------------|--|
| Syntax Description | <i>n</i> | VLAN ID of the new management VLAN. Valid VLAN IDs are from 1 to 1001. |
| | no | Set the management VLAN to VLAN 1. |
| | default | Set the management VLAN to VLAN 1. |

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

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

| Command History | Release | Modification |
|-----------------|-----------|------------------------------------|
| | 12.0(5)XU | This command was first introduced. |

| | |
|------------------|--|
| Usage Guidelines | Enter this command only on the command switch. This command is not written to the configuration file. |
|------------------|--|

| | |
|----------|---|
| Examples | <p>This example shows how to change the management VLAN to VLAN 5 on the entire cluster.</p> <pre>Switch(config)# cluster management-vlan 5</pre> <p>You can verify the previous command by entering the show interface vlan number user EXEC command.</p> |
|----------|---|

| Related Commands | Command | Description |
|------------------|-------------------|---|
| | management | Shuts down the management VLAN interface and enables the new management VLAN interface on an individual switch. |

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*]

no cluster member *n*

default cluster member *n*

| | | |
|--------------------|--|--|
| Syntax Description | <i>n</i> | (Optional) The number that identifies a cluster member. The range is from 0 to 15. |
| | mac-address <i>H.H.H</i> | MAC address of the member switch in hexadecimal format. |
| | password <i>enable-password</i> | Enable password of the candidate switch. The password is not required if there is no password on the candidate switch. |
| | no | Remove the specified member from the cluster. |
| | default | Remove the specified member from the cluster. |

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

Command Modes Global configuration

| | | |
|-----------------|----------------|------------------------------------|
| Command History | Release | Modification |
| | 11.2(8)SA6 | This command was first introduced. |

Usage Guidelines

Enter this command only on the command switch to add a member to or remove a member from the cluster. If a switch is not commanding a cluster, this command displays an error message.

You do not need to enter a member number. The command switch selects the next available member number and assigns it to the switch 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.

Examples

This example shows how to add a switch as member 2 with MAC address 00E0.1E00.2222 and the password grandkey to a cluster.

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

This example shows how to add a switch with MAC address 00E0.1E00.3333 to the cluster. 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 the previous command by entering the **show cluster members** command in user EXEC mode 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

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

default cluster run

| | | |
|--------------------|----------------|---------------------------------|
| Syntax Description | no | Disable clustering on a switch. |
| | default | Enable clustering on a switch. |

| | |
|----------|--|
| Defaults | Clustering is enabled on all switches. |
|----------|--|

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

| Command History | Release | Modification |
|-----------------|-----------|------------------------------------|
| | 12.0(5)XU | This command was first 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 is incapable of becoming 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 is incapable of becoming 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 the previous command by entering the show cluster command in user EXEC mode. |

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

cluster setup

Use the **cluster setup** privileged EXEC command on the command switch to automatically build a cluster.

cluster setup

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|------------|------------------------------------|
| | 11.2(8)SA6 | This command was first introduced. |

Usage Guidelines You can use the **cluster setup** command to add new switches to an existing cluster. The **cluster setup** command provides a high-level view of the configuration and guides you through the configuration change process. You can only see candidate switches that are one hop away from the command switch and that have no IP address. To see devices farther away, use the **show cluster members** or **show cluster candidates** command.

If a candidate switch has a password, this information is not passed to the cluster.

Examples This is an example of the **cluster setup** command output:

```
Switch# cluster setup
```

```
--- Cluster Configuration Dialog ---
```

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

```
This switch is already configured as cluster command switch:
Command Switch Name:m217, contains 7 members
```

```
Continue with cluster configuration dialog? [yes/no]:yes
The suggested Cluster configuration is as follows:
```

| | | | | | ---Upstream--- | | | |
|----|----------------|-----------|--------|----------|----------------|--------|-----|----------|
| SN | MAC Address | Name | PortIf | FEC Hops | SN | PortIf | FEC | State |
| 0 | 00d0.796d.2f00 | 3524-24 | | 0 | | | | Cmdr |
| 1 | 00d0.7960.66c0 | 3508 | Gi0/4 | 1 | 0 | Gi0/1 | | Up |
| 2 | 00d0.7961.c4c0 | 3512-12 | Fa0/3 | 1 | 0 | Fa0/13 | | Up |
| 3 | 00e0.1e9f.8300 | 2924M | Fa0/11 | 2 | 2 | Fa0/12 | | Up |
| 4 | 00e0.1e9f.7a00 | 2924-24 | Fa0/5 | 1 | 0 | Fa0/3 | | Up |
| 5 | 00e0.1e9f.8c00 | 2912-12-2 | Fa0/4 | 1 | 0 | Fa0/7 | | Up |
| 6 | 00e0.1e9f.8c40 | 2912-12-1 | Fa0/1 | 1 | 0 | Fa0/9 | | Up |
| 7* | 0010.7bb6.1cc0 | 2912MF | Fa2/1 | 3 | 3 | Fa0/24 | | Candidat |

The following configuration command script was created:

```
cluster member 7 mac-address 0010.7bb6.1cc0
!
end
```

Use this configuration? [yes/no]:yes

Building configuration...

[OK]

Use the enabled mode 'configure' command to modify this configuration.

Switch#

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

Related Commands

| Command | Description |
|--------------------------------|---|
| cluster enable | Enables a switch as the cluster command switch, assigns a cluster name, and optionally assigns a member number to it. |
| 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 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

default 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. |
| | no | Unbind the cluster from the HSRP standby group. |
| | default | Unbind the cluster from the HSRP standby group. |

| | |
|----------|---|
| Defaults | The cluster is not bound to any HSRP group. |
|----------|---|

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

| Command History | Release | Modification |
|-----------------|-----------|------------------------------------|
| | 12.0(5)XU | This command was first introduced. |

| | |
|------------------|--|
| Usage Guidelines | <p>You must enter this command only on the command switch. If you enter it on a member switch, an error message appears.</p> <p>The command switch propagates the cluster-HSRP binding information to all members. Each member switch stores the binding information in its nonvolatile RAM (NVRAM).</p> <p>The HSRP group name must be a valid standby group; otherwise, the command exits with an error.</p> |
|------------------|--|

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 group 'my_hsrp' doesn't exist
```

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 only on the command switch
```

You can verify the previous commands by entering the **show cluster** command in user EXEC mode.

Related Commands

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

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

default cluster timer

Syntax Description

| | |
|-------------------------|---|
| <i>interval-in-secs</i> | Interval in seconds between heartbeat messages. The range is from 1 to 300 seconds. |
| no | Set the interval to the default value (8 seconds). |
| default | Set the interval to the default value (8 seconds). |

Defaults

The interval is 8 seconds.

Command Modes

Global configuration

Command History

| Release | Modification |
|-----------|------------------------------------|
| 12.0(5)XU | This command was first 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.

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 the previous commands by entering the **show cluster** user EXEC command.

Related Commands

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

delete

Use the **delete** privileged EXEC command to delete a file from the file system.

delete {*device:*}*filename*

| | | |
|--------------------|-----------------|--|
| Syntax Description | <i>device:</i> | Device containing the file to be deleted. Valid devices include the switch Flash memory and Asynchronous Transfer Mode (ATM) module files. To access the ATM module, specify the slot number (1 or 2). |
| | <i>filename</i> | Name of file. |

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

| | | |
|-----------------|------------|------------------------------------|
| Command History | Release | Modification |
| | 11.2(8)SA6 | This command was first introduced. |

| | |
|------------------|--|
| Usage Guidelines | A colon (:) follows the <i>device</i> variable. Do not enter spaces after the colon. |
|------------------|--|

| | |
|----------|--|
| Examples | This example shows how to delete the file <i>atm_image</i> from the file system for an ATM module installed in slot 1: |
| | Switch# delete slot1:atm_image |
| | This example shows how to delete a file from the switch Flash memory: |
| | Switch# delete flash:filename |
| | You can verify that the file was removed by entering the show flash: user EXEC command. |

| | | |
|------------------|------------------|--|
| Related Commands | Command | Description |
| | copy tftp | Downloads a file from a TFTP server to a device. |

duplex

Use the **duplex** interface configuration command to specify the duplex mode of operation for Fast Ethernet and Gigabit Ethernet ports. Use the **no** form of this command to return the port to its default value.

duplex { full | half | auto }

no duplex

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

| | |
|----------|------------------------------|
| Defaults | The default is auto . |
|----------|------------------------------|

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

| Command History | Release | Modification |
|-----------------|-----------|------------------------------------|
| | 11.2(8)SA | This command was first introduced. |

| | |
|------------------|--|
| Usage Guidelines | <p>Certain ports can be configured as either full duplex or half duplex. Applicability of this command depends on the device to which the switch is attached.</p> <p>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.</p> <p>For Gigabit Ethernet ports, setting the port to auto has the same effect as specifying full if the attached device does not autonegotiate the duplex parameter.</p> <p>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.</p> <p>If both the speed and duplex are set to specific values, autonegotiation is disabled.</p> |
|------------------|--|

**Note**

For guidelines on setting the switch speed and duplex parameters, see the *Catalyst 2900 Series XL Hardware Installation Guide* and the *Catalyst 3500 Series XL Hardware Installation Guide*.

This command is not supported on the ATM module.

Examples

This example shows how to set port 1 on a Fast Ethernet module installed in slot 2 to full duplex:

```
Switch(config)#interface fastethernet2/1  
Switch(config-if)#duplex full
```

This example shows how to set port 1 on a Gigabit Ethernet module installed in slot 2 to full duplex:

```
Switch(config)# interface gigabitethernet2/1  
Switch(config-if)# duplex full
```

You can verify the previous commands by entering the **show running-config** privileged EXEC command.

Related Commands

| Command | Description |
|----------------------------|---|
| show running-config | Displays the running configuration on the switch. |
| speed | Specifies the speed of a Fast Ethernet port. |

exit

Use the **exit** VLAN database command to implement the proposed VLAN database, to increment the database configuration number, to propagate it throughout the administrative domain, and to return to privileged EXEC mode.

exit

| | |
|---------------------------|--|
| Syntax Description | This command has no arguments or keywords. |
|---------------------------|--|

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

| | |
|----------------------|---------------|
| Command Modes | VLAN database |
|----------------------|---------------|

| Command History | Release | Modification |
|-----------------|------------|------------------------------------|
| | 11.2(8)SA4 | This command was first introduced. |

| | |
|-------------------------|--|
| Usage Guidelines | The exit command implements all the configuration changes that you made since you entered VLAN database mode and uses them for the running configuration. This command returns you to privileged EXEC mode. |
|-------------------------|--|

| | |
|-----------------|---|
| Examples | This example shows how to implement the proposed VLAN database and to exit to privileged EXEC mode: |
|-----------------|---|

```
Switch(vlan)# exit  
Switch#
```

You can verify the previous command by entering the **show vlan brief** user EXEC command.

| Related Commands | Command | Description |
|------------------|----------------------|--|
| | abort | Abandons the proposed VLAN database, exits VLAN database mode, and returns to privileged EXEC mode. |
| | apply | Implements the proposed VLAN database, increments the database configuration revision number, propagates it throughout the administrative domain, and remains in VLAN database mode. |
| | reset | Abandons the proposed VLAN database and remains in VLAN database mode. Resets the proposed database to the currently implemented VLAN database on the switch. |
| | show vlan | Displays the parameters for all configured VLANs in the administrative domain. |
| | shutdown vlan | Shuts down (suspends) local traffic on the specified VLAN. |
| | vlan database | Enters VLAN database mode from the command-line interface (CLI). |

flowcontrol

Use the **flowcontrol** interface configuration command on Gigabit Ethernet ports to control traffic rates during congestion. Use the **no** form of this command to disable flow control on the port.

flowcontrol {asymmetric | symmetric}

no flowcontrol

| | | |
|--------------------|---|---|
| Syntax Description | asymmetric | Enable the local port to perform flow control of the remote port. If the local port is congested, it can request the remote port to stop transmitting. The local port requests that the remote port begin transmitting after the congestion clears. |
| | symmetric | Enable the local port to perform flow control only if the remote port can also perform flow control of the local port. If the remote port cannot perform flow control, the local port also does not. |
| Defaults | The default is asymmetric. | |
| Command Modes | Interface configuration | |
| Command History | Release | Modification |
| | 11.2(8)SA6 | This command was first introduced. |
| Examples | <p>This example shows how to configure the local port to support any level of flow control by the remote port:</p> <pre>Switch(config-if)# flowcontrol</pre> <p>This example shows how to configure the local port to control the traffic flow from the remote port:</p> <pre>Switch(config-if)# flowcontrol asymmetric</pre> <p>You can verify the previous commands by entering the show running-config privileged EXEC command.</p> | |
| Related Commands | Command | Description |
| | show interface [interface-id] flow-control | Displays flow-control information for the specified port. |

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 *type slot/port* | **vlan** *number*

no interface *type slot/port* | **vlan** *number*

Syntax Description

| | |
|---------------------------|--|
| <i>type</i> | Type of interface to be configured. Can be Fast Ethernet, Gigabit Ethernet, or Asynchronous Transfer Mode (ATM). |
| <i>slot</i> | Slot number (0, 1, or 2). For an ATM module, use slot number 1 or 2. |
| <i>port</i> | Port ID. |
| vlan <i>number</i> | VLAN number from 1 to 1001 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 |
|------------|------------------------------------|
| 11.2(8)SA | This command was first introduced. |
| 11.2(8)SA3 | The vlan keyword was added. |

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.

Before bringing up a new management VLAN interface with the **no shutdown** command, you must enter the **shutdown** command to disable the old one.

You can use the **management** command to shut down the active management VLAN interface and to enable the newly created management VLAN interface.

You can configure the management VLAN interface on static-access, multi-VLAN, dynamic-access, and trunk ports.

Examples

This example shows how to enable the switch to act on ATM interface 1/2:

```
Switch(config)# interface atm 1/2
Switch(config-if)#
```

This example shows how to change the management VLAN from VLAN 1 to VLAN 3. Enter this series of commands only from the console. If you enter these commands through a Telnet session, the **shutdown** command disconnects the session, and you cannot to use IP to access the system.

```
Switch#configure terminal
Switch(config)# interface vlan 3
Switch(config-subif)# ip address 172.20.128.176 255.255.255.0
Switch(config-subif)# exit
Switch(config-if)# exit
Switch(config)# interface vlan 1
Switch(config-subif)# shutdown
Switch(config-subif)# exit
Switch(config-if)# exit
Switch(config)# interface vlan 3
Switch(config-subif)# no shutdown
Switch(config-subif)# exit
Switch(config-if)# exit
```

This example shows how to change the management VLAN from VLAN 1 to VLAN 3 through a Telnet session. In this situation, the **management** command shuts down VLAN 1 and brings up VLAN 3. The Telnet session must be re-established through the new management VLAN.

```
Switch# configure terminal
Switch(config)# interface vlan 3
Switch(config-subif)# ip address 172.20.128.176 255.255.255.0
Switch(config-subif)# management
```

This example shows how to copy the IP address and the network mask information from the current management VLAN to VLAN 3 and to make VLAN 3 the new management VLAN:

```
Switch# configure terminal
Switch(config)# interface vlan 3
Switch(config-subif)# management
```

You can verify the previous commands by entering the **show interface** and **show interface vlan number** commands in user EXEC mode.

Related Commands

| Command | Description |
|-----------------------|---|
| management | Shuts down the current management VLAN interface and enables the new management VLAN interface. |
| show interface | Displays the administrative and operational status of a switching (nonrouting) port. |
| shutdown | Disables a port and shuts down the management VLAN. |

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 |
|-----------|------------------------------------|
| 11.2(8)SA | This command was first 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 session, your connection to the switch will be lost.

If your switch receives its IP address from a Bootstrap Protocol (BOOTP) or Dynamic Host Configuration 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 the previous commands by entering the **show running-config** privileged EXEC command.

Related Commands

| Command | Description |
|----------------------------|---|
| show running-config | Displays the running configuration on the switch. |
| clear ip address | Deletes an IP address for a switch without disabling the IP processing. |

ip igmp filter

Use the **ip igmp filter** interface configuration command to apply an Internet Group Management Protocol (IGMP) profile to an interface and to prevent hosts on an interface from joining one or more IP multicast groups. Use the **no** form of this command to remove a specified profile from an interface.

ip igmp filter *profile number*

no ip igmp filter *profile number*

Syntax Description

profile number The range is from 1 to 4294967295.

Defaults

No IGMP filtering profiles are assigned to an interface.

Command Modes

Interface configuration

Command History

| Release | Modification |
|------------|------------------------------------|
| 12.0(5)WC3 | This command was first introduced. |

Usage Guidelines

The same IGMP profile can be applied to more than one switch port interface.

Examples

This example shows how to apply an IGMP filtering profile to an interface:

```
Switch(config-if)# ip igmp filter 30
```

You can verify your settings by entering the **show ip igmp profile** *profile number* user EXEC command.

Related Commands

| Command | Description |
|--|--|
| ip igmp profile | Defines a new IGMP filtering profile. |
| show ip igmp profile | Displays the details of an IGMP filtering profile entry. |
| show running-config interface <i>interface name</i> | Displays the running configuration on the switch, including any profiles assigned to a port. |

ip igmp max-groups

Use the **ip igmp max-groups** interface configuration command to specify the maximum number of Internet Group Management Protocol (IGMP) groups that can be active on a port.

ip igmp max-groups *number*

| Syntax Description | <i>number</i> | The maximum number of IGMP filtering groups that can be active on a port. The range is from 0 to 256. |
|--------------------|---------------|---|
|--------------------|---------------|---|

| | |
|----------|---|
| Defaults | No maximum number of IGMP groups are defined. |
|----------|---|

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

| Command History | Release | Modification |
|-----------------|------------|------------------------------------|
| | 12.0(5)WC3 | This command was first introduced. |

| | |
|------------------|---|
| Usage Guidelines | <p>There is no limit to the number of multicast groups that a port can join.</p> <p>If 0 is specified as the maxgroups value for an interface, that interface cannot join <i>any</i> multicast groups.</p> |
|------------------|---|

| | |
|----------|--|
| Examples | <p>This example shows how to limit the number of IGMP groups that an interface can join to 25.</p> |
|----------|--|

```
Switch(config)# interface fastethernet 0/12
Switch(config-if)# ip igmp max-groups 25
```

You can verify your setting by using the **show running-configuration** privileged EXEC command and by specifying an interface.

```
Switch# show running-config interface fastethernet 0/12
Building configuration...
```

```
Current configuration :124 bytes
!
interface FastEthernet0/12
  no ip address
  shutdown
  snmp trap link-status
  ip igmp max-groups 25
  ip igmp filter 22
end
```

You can verify your settings by entering the **show running-config interface** interface configuration command.

Related Commands

| | |
|---|--|
| ip igmp profile | Applies an IGMP filtering profile to an interface. |
| show ip igmp profile | Displays the details of an IGMP filtering profile entry. |
| show running-config <i>interface</i> | Displays the running configuration on the switch, including any profiles assigned to a port. |

ip igmp profile

Use the **ip igmp profile** global configuration command to create an Internet Group Management Protocol (IGMP) profile and to enter IGMP profile configuration mode. From this mode, you can specify the configuration of the IGMP profile. Use the **no** form of this command and a profile number to delete an IGMP profile.

ip igmp profile *profile number*

no ip igmp profile *profile number*

| | | |
|--------------------|---|------------------------------------|
| Syntax Description | <i>profile number</i> The IGMP profile being created. The range is 1 to 4294967295. | |
| Defaults | No IGMP profiles are defined. When a profile configured, the default action is to deny the addresses in the profile. | |
| Command Modes | Global configuration | |
| Command History | Release | Modification |
| | 12.0(5)WC3 | This command was first introduced. |
| Usage Guidelines | <p>When you are in IGMP profile configuration mode, you can create the profile by using these keywords:</p> <ul style="list-style-type: none"> • deny: specifies that matching addresses are denied; this is the default. • permit: specifies that matching address are permitted. • range: adds a range to the set range of IP address. This can be a single IP address or a range with start and end addresses. • exit: saves changes to the IGMP profile and exits from IGMP profile configuration mode. • no: negates the command or sets it to the defaults. | |
| Examples | <p>This example shows how to create an IGMP filtering profile:</p> <pre> host1# config terminal Enter configuration commands, one per line. End with CNTL/Z. host1(config)# ip igmp profile 30 host1(config-igmp-profile)# host1(config-igmp-profile)# deny host1(config-igmp-profile)# range 233.1.1.1 233.255.255.255 host1(config-igmp-profile)# range 235.1.1.1 235.255.255.255 host1(config-igmp-profile)# end host1# </pre> | |

| Related Commands | Command | Description |
|------------------|---|--|
| | ip igmp profile | Applies an IGMP filtering profile to an interface. |
| | show ip igmp profile | Displays the details of an IGMP filtering profile entry. |
| | show running-config <i>interface</i> | Displays the running configuration on the switch, including any profiles assigned to a port. |

login authentication

Use the **login authentication** line configuration command to enable authentication, authorization, and accounting (AAA) for logins. Use the **no** form of this command to either disable Terminal Access Controller Access Control System Plus (TACACS+) authentication for logins or to return to the default.

login authentication { **default** | *list-name* }

no login { **default** | *list-name* }

| | | |
|--------------------|------------------|--|
| Syntax Description | default | Use the default list created with the AAA authentication login command. |
| | <i>list-name</i> | Use the indicated list created with the AAA authentication login command. |

Defaults Login authentication is disabled.

Command Modes Line configuration

| | | |
|-----------------|----------------|------------------------------------|
| Command History | Release | Modification |
| | 11.2(8)SA6 | This command was first introduced. |

Usage Guidelines To create a default list that is used if no list is specified in the **login authentication** command, use the **default** keyword followed by the methods that you want used in default situations. The default method list is automatically applied to all interfaces.

Examples This example shows how to specify TACACS+ as the default method for user authentication during login:

```
Switch(config)# aaa new-model
Switch(config)# aaa authentication login default tacacs
Switch(config)# line vty 0 4
Switch(config-line)# login authentication default tacacs
```

You can verify the previous commands by entering the **show running-config** privileged EXEC command.

| | | |
|------------------|----------------------------|---|
| Related Commands | Command | Description |
| | enable password | Specifies a local password to control access to various privilege levels. |
| | password | Specifies a password on a line. |
| | show running-config | Displays the running configuration on the switch. |
| | username | Establishes a username-based authentication system. |

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 use the default aging-time interval. The aging time applies to all VLANs.

mac-address-table aging-time *age*

no mac-address-table aging-time

| | | |
|--------------------|---|--|
| Syntax Description | <i>age</i> Number from 10 to 1000000 (seconds). | |
| Defaults | The default is 300 seconds. | |
| Command Modes | Global configuration | |
| Command History | Release | Modification |
| | 11.2(8)SA | This command was first introduced. |
| Usage Guidelines | If hosts do not transmit continuously, increase the aging time to record the dynamic entries for a longer time. This can reduce the possibility of flooding when the hosts transmit again. | |
| Examples | <p>This example shows how to set the aging time to 200 seconds:</p> <pre>Switch(config)# mac-address-table aging-time 200</pre> <p>You can verify the previous command by entering the show mac-address-table user EXEC command.</p> | |
| Related Commands | Command | Description |
| | clear mac-address-table | Deletes entries from the MAC address table. |
| | mac-address-table dynamic | Adds dynamic addresses to the MAC address table. |
| | mac-address-table secure | Adds secure addresses to the MAC address table. |
| | port block | Blocks the flooding of unknown unicast or multicast packets to a port. |
| | show cgmp | Displays the state of the CGMP-learned multicast groups and routers. |
| | show mac-address-table | Displays the MAC address table. |

mac-address-table dynamic

Use the **mac-address-table dynamic** global configuration command to add dynamic addresses to the MAC address table. Dynamic addresses are automatically added to the address table and dropped from it when they are not in use. Use the **no** form of this command to remove dynamic entries from the MAC address table.

mac-address-table dynamic *hw-addr* interface [**atm** *slot/port*] [**vlan** *vlan-id*]

no mac-address-table dynamic *hw-addr* [**vlan** *vlan-id*]

| | | |
|--------------------|-----------------------------|---|
| Syntax Description | <i>hw-addr</i> | MAC address added to or removed from the table. |
| | <i>interface</i> | Port to which packets destined for <i>hw-addr</i> are forwarded. |
| | atm <i>slot/port</i> | (Optional) Add dynamic addresses to ATM module <i>in slot 1 or 2</i> . The port is always 0 for an ATM interface. |
| | vlan <i>vlan-id</i> | <p>(Optional) The <i>interface</i> and vlan parameters together specify a destination to which packets destined for <i>hw-addr</i> are forwarded.</p> <p>The vlan keyword is optional if the port is a static-access or dynamic-access VLAN port. The VLAN assigned to the port is then assumed to be that of the port associated with the MAC address.</p> <p>Note When this command is entered on a dynamic-access port, queries to the VLAN Membership Policy Server (VMPS) do not occur. The VMPS cannot verify that the address is allowed or determine to which VLAN the port should be assigned. Use this command only for testing purposes.</p> <p>The vlan keyword is required for multi-VLAN and trunk ports. This keyword is required on trunk ports to specify to which VLAN the dynamic address is assigned.</p> <p>The <i>vlan-id</i> is the ID of the VLAN to which packets destined for <i>hw-addr</i> are forwarded. Valid IDs are 1 to 1005; do not enter leading zeroes.</p> |

Command Modes Global configuration

| Command History | Release | Modification |
|-----------------|------------|------------------------------------|
| | 11.2(8)SA | This command was first introduced. |
| | 11.2(8)SA3 | The vlan keyword was added. |
| | 11.2(8)SA5 | The atm keyword was added. |

Usage Guidelines If the variable *vlan-id* is omitted and the **no** form of the command is used, the MAC address is removed from all VLANs.

Examples

This example shows how to add a MAC address on port fa1/1 to VLAN 4:

```
Switch(config)# mac-address-table dynamic 00c0.00a0.03fa fa1/1 vlan 4
```

You can verify the previous command by entering the **show mac-address-table** user EXEC command.

Related Commands

| Command | Description |
|-------------------------------------|--|
| clear mac-address-table | Deletes entries from the MAC address table. |
| mac-address-table aging-time | Specifies the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated. |
| mac-address-table static | Adds static addresses to the MAC address table. |
| show mac-address-table | Displays the MAC address table. |

mac-address-table notification

Use the **mac-address-table notification** global configuration command to enable the MAC address notification feature and to configure the notification-trap interval or history table. Use the **no** form of this command to disable this feature or return to the default setting.

mac-address-table notification [*interval seconds*] | [*history-size value*]

no mac-address-table notification [*interval seconds*] | [*history-size value*]

Syntax Description

| | |
|---------------------------------|--|
| interval <i>interval</i> | (Optional) Configures the notification trap interval in seconds. The range is from 0 to 2147483647. The switch sends notification traps only after this interval has elapsed. |
| history-size <i>size</i> | (Optional) Configures the maximum number of entries in the MAC notification history table. The range is from 1 to 500. When this command is issued, the previous table is deleted, and a new table is created. |

Defaults

MAC notification feature is disabled.
 The default trap interval value is one second.
 The default number of entries in the history table is one.

Command Modes

Global configuration

Command History

| Release | Modification |
|------------|------------------------------------|
| 12.0(5)WC3 | This command was first introduced. |

Usage Guidelines

The MAC notification feature sends SNMP traps when a MAC address is learned or deleted from the forwarding tables.



Note

You must use the **snmp-server enable traps mac-notification** global configuration command to enable MAC address traps on the switch before enabling the MAC notification feature.

Use the **mac-address-table notification** command without keywords to enable or disable the feature.

Use this command with the **interval** or **history-size** keywords to configure the trap interval or the maximum number of entries in the MAC notification history table.



Note

The **interval seconds** and **history-size value** keywords must be entered as separate commands.

Use the **no mac-address-table notification interval** global configuration command to reset the MAC notification history table size to the default of 1 second.

Use the **no mac-address-table notification *history-size*** global configuration command to reset the MAC notification history table size to the default of one.

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 this command by entering the **show mac-address-table notification** user EXEC command.

Related Commands

| | |
|--|---|
| snmp-server enable traps mac-notification | Enables the MAC-notification traps on a port. |
| show mac-address-table notification | Displays MAC-notification parameters. |

mac-address-table secure

Use the **mac-address-table secure** global configuration command to add secure addresses to the MAC address table. Use the **no** form of this command to remove secure entries from the MAC address table.

mac-address-table secure *hw-addr interface* [**atm slot/port**] [**vlan vlan-id**]

no mac-address-table secure *hw-addr* [**vlan vlan-id**]

| | | |
|--------------------|----------------------|--|
| Syntax Description | <i>hw-addr</i> | MAC address that is added to the table. |
| | <i>interface</i> | Port to which packets destined for <i>hw-addr</i> are forwarded. |
| | atm slot/port | (Optional) Add secure address to the Asynchronous Transfer Mode (ATM) module in slot 1 or 2. The port is always 0 for an ATM interface. |
| | vlan vlan-id | (Optional) The <i>interface</i> and vlan parameters together specify a destination to which packets destined for <i>hw-addr</i> are forwarded. The vlan keyword is optional if the port is a static-access VLAN port. The VLAN assigned to the port is then assumed to be that of the port associated with the MAC address. This keyword is required for multi-VLAN and trunk ports. The <i>vlan-id</i> is the ID of the VLAN to which secure entries are added. Valid IDs are 1 to 1005; do not enter leading zeroes. |

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

| Command History | Release | Modification |
|-----------------|------------|------------------------------------|
| | 11.2(8)SA | This command was first introduced. |
| | 11.2(8)SA3 | The vlan keyword was added. |
| | 11.2(8)SA5 | The atm keyword was added. |

| | |
|------------------|--|
| Usage Guidelines | Secure addresses can be assigned only to one port at a time. Therefore, if a secure address table entry for the specified MAC address and VLAN already exists on another port, it is removed from that port and assigned to the specified one. Dynamic-access ports cannot be configured with secure addresses. |
|------------------|--|

Examples

This example shows how to add a secure MAC address to VLAN 6 of port fa1/1:

```
Switch(config)# mac-address-table secure 00c0.00a0.03fa fa1/1 vlan 6
```

This example shows how to add a secure MAC address to ATM port 2/1:

```
Switch(config)# mac-address-table secure 00c0.00a0.03fa atm 2/1
```

You can verify the previous command by entering the **show mac-address-table** user EXEC command.

Related Commands

| Command | Description |
|-------------------------------------|--|
| clear mac-address-table | Deletes entries from the MAC address table. |
| mac-address-table aging-time | Specifies the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated. |
| mac-address-table dynamic | Adds dynamic addresses to the MAC address table. |
| mac-address-table static | Adds static addresses to the MAC address table. |
| show mac-address-table | Displays the MAC address table. |

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 *hw-addr in-port out-port-list* [**atm** *slot/port*] [**vlan** *vlan-id*]

no mac-address-table static *hw-addr* [**in-port** *in-port*] [**out-port-list** *out-port-list*] [**vlan** *vlan-id*]

| | | |
|--------------------|-----------------------------|---|
| Syntax Description | <i>hw-addr</i> | MAC address to add to the address table. |
| | <i>in-port</i> | Input port from which packets received with a destination address of <i>hw-addr</i> are forwarded to the list of ports in the <i>out-port-list</i> . The <i>in-port</i> must belong to the same VLAN as all the ports in the <i>out-port-list</i> . |
| | <i>out-port-list</i> | List of ports to which packets received on ports in <i>in-port</i> are forwarded. All ports in the list must belong to the same VLAN. |
| | atm <i>slot/port</i> | (Optional) Add static addresses to Asynchronous Transfer Mode (ATM) module in slot 1 or 2. The port is always 0 for an ATM interface. |
| | vlan <i>vlan-id</i> | <p>(Optional) The <i>interface</i> and vlan parameters together specify a destination to which packets destined for the specified MAC address are forwarded.</p> <p>The vlan keyword is optional if all the ports specified by <i>in-port</i> and <i>out-port-list</i> are static-access VLAN ports. The VLAN assigned to the ports is assumed. This keyword is required for multi-VLAN and trunk ports.</p> <p>Dynamic-access ports cannot be included in static addresses as either the source (inport) or destination (outport).</p> <p>The vlan keyword is required on trunk ports to specify to which VLAN the static address is assigned.</p> <p>The <i>vlan-id</i> is the ID of the VLAN to which static address entries are forwarded. Valid IDs are 1 to 1005; do not enter leading zeroes.</p> |

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

| Command History | Release | Modification |
|-----------------|------------|------------------------------------|
| | 11.2(8)SA | This command was first introduced. |
| | 11.2(8)SA3 | The vlan keyword was added. |
| | 11.2(8)SA5 | The atm keyword was added. |

Usage Guidelines

When a packet is received on the input port, it is forwarded to the VLAN of each port that you specify for the *out-port-list*. Different input ports can have different output-port lists for each static address. Adding a static address already defined as one modifies the port map (*vlan* and *out-port-list*) for the input port specified.

If the variable *vlan-id* is omitted and the **no** form of the command is used, the MAC address is removed from all VLANs.

Traffic from a static address is only accepted from a port defined in the *in-port* variable.

Dynamic-access ports cannot be configured as the source or destination port in a static address entry.

Examples

This example shows how to add a static address with port 1 as an input port and ports 2 and 8 of VLAN 4 as output ports:

```
Switch(config)# mac-address-table static c2f3.220a.12f4 fa0/1 fa0/2 fa0/8 vlan 4
```

You can verify the previous command by entering the **show mac-address-table** user EXEC command.

Related Commands

| Command | Description |
|-------------------------------------|--|
| clear mac-address-table | Deletes entries from the MAC address table. |
| mac-address-table aging-time | Specifies the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated. |
| mac-address-table dynamic | Adds dynamic addresses to the MAC address table. |
| mac-address-table secure | Adds secure addresses to the MAC address table. |
| show mac-address-table | Displays the MAC address table. |

management

Use the **management** interface configuration command to shut down the current management VLAN interface and to enable the new management VLAN interface. The management VLAN is the VLAN used for managing a cluster of switches. To use this VLAN for switch management, apply this VLAN to a switched virtual interface or to the management interface. The default management VLAN is VLAN 1; however, it can be changed to a new management interface on a different VLAN with valid IDs from 1 to 1001.

This command also copies the current management VLAN IP information to the new management VLAN interface if no new IP address or network mask is provided. It also copies the cluster standby group configuration to the new management VLAN.

management

| | |
|---------------------------|--|
| Syntax Description | This command has no arguments or keywords. |
|---------------------------|--|

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

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

| | | |
|------------------------|----------------|------------------------------------|
| Command History | Release | Modification |
| | 12.0(5)XP | This command was first introduced. |

| | |
|-------------------------|---|
| Usage Guidelines | No default management or no management command exists to return the management VLAN to its default state. |
|-------------------------|---|

The management command is not written to the configuration file, and it is not displayed in the output of the **show running-config** privileged EXEC command.

Before entering the **management** command, make sure that these conditions exist:

- You must be able to move your network management station to a switch port assigned to the same VLAN as the new management VLAN. (Depending on your network topology, you might not need to move your network management station: for example, you have ISL routing configured on a router between two VLANs.)
- Connectivity through the network must exist from the network management station to all switches involved in the management VLAN change.
- The switch must already have a port assigned to the same VLAN as the management VLAN.

Use the management command to change the management VLAN on a single switch. Use the global **cluster management-vlan n** configuration command on the command switch to change the management VLAN on the entire cluster.

Examples

This example shows how to shut down the current management VLAN interface and start VLAN 2 as the management VLAN:

```
Switch# configure terminal
Switch(config)# interface vlan 2
Switch(config-subif)# ip address 172.20.128.176 255.255.255.0
Switch(config-subif)# management
Switch(config-subif)# exit
Switch(config)#
```

This example shows how to copy the IP address and network mask from the current management VLAN to VLAN 2 and make VLAN 2 the management VLAN:

```
Switch# configure terminal
Switch(config)# interface vlan 2
Switch(config-subif)# management
Switch(config-subif)# exit
Switch(config)#
```

You can verify the previous command by entering the **show interface vlan *number*** user EXEC command.

Related Commands

| Command | Description |
|--|--|
| cluster management-vlan | Changes the management VLAN for the entire cluster. |
| interface vlan | Configures an interface type, creates a switch virtual interface to be used as the management VLAN interface, and enters interface configuration mode. |
| show interface vlan <i>number</i> | Displays the administrative and operational status of a switching (nonrouting) port. |

mvr (global configuration)

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 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 commands to return the switch to the default settings.

mvr [**group** *ip-address* [*count*] [**querytime** *value*] [**vlan** *vlan-id*]]

no mvr [**group** *ip-address* [*count*] [**querytime** *value*] [**vlan** *vlan-id*]]

| | | |
|--------------------|--------------------------------|---|
| Syntax Description | group <i>ip-address</i> | 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. |
| | querytime <i>value</i> | (Optional) Set the maximum time to wait for IGMP report memberships on a receiver port. This time only applies to receiver-port leave processing. When an IGMP query is sent from a receiver port, the switch waits for the default or configured MVR querytime 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 0.5 second. Use the no form of the command to return to the default setting. |
| | vlan <i>vlan-id</i> | 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. |
| | | |

Defaults

MVR is disabled.

The switch hardware determines the maximum number of MVR entries.

No IP multicast addresses are configured on the switch.

The default count is 1.

The default query response time is 0.5 second.

The default multicast VLAN is VLAN 1.

Command Modes

Global configuration

Command History

| Release | Modification |
|-----------|------------------------------------|
| 12.0(5)XW | This command was first introduced. |

Usage Guidelines

The switch hardware determines the maximum number of MVR entries.

Use the **mvr group** command to statically set 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 that have registered to receive data on that IP multicast address.

**Note**

The **mvr group** command prevents adding IP multicast addresses that cause address aliasing. 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, the command fails.

The **mvr querytime** parameter applies only to receiver ports. You should configure the query time before enabling MVR and configuring the static multicast groups. You can change the query time after MVR is enabled, but you receive a warning message:

Warning: Changing MVR query response time while MVR is running.

Set the MVR multicast VLAN before the multicast addresses are configured. If it is necessary to change the multicast VLAN, disable MVR, change the VLAN number, and then reenables MVR. Previously configured groups are restored.

Examples

This example shows how to enable MVR:

```
Switch(config)# mvr
```

This example shows how to disable MVR:

```
Switch(config)# no mvr
```

Use the **show mvr** privileged EXEC command to display the setting for maximum multicast groups.

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
```

Use the command **show mvr members** to display the IP multicast group addresses configured on the switch.

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 0.5 second:

```
Switch(config)# no mvr querytime
```

This example shows how to set VLAN 2 as the multicast VLAN:

```
Switch(config)# mvr vlan 2
```

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

Related Commands

| Command | Description |
|--------------------------------------|---|
| mvr (interface configuration) | Configures MVR source or receiver ports. |
| show mvr | Displays MVR global parameters or port parameters. |
| show mvr members | Displays all receiver ports that are members of an MVR multicast group. |
| show mvr interface | Displays the configured MVR interfaces. |

mvr (interface configuration)

Use the **mvr** interface configuration command to configure a port as a multicast VLAN registration (MVR) receiver or source port and set the Immediate Leave feature.

Use the **no** form of the commands to return the port to the default settings.

```
mvr {type {source | receiver} | immediate}
```

```
no mvr {type {source | receiver} | immediate}
```

| Syntax Description | type <i>value</i> | (Optional) Configure the port as an MVR receiver port or source port. The default port type is neither an MVR source nor receiver port. The no mvr type command resets the port to the default. |
|--------------------|--------------------------|---|
| | source | Configure the port as an uplink port that can send and receive multicast data for the configured multicast groups. All source ports on a switch belong to a single multicast VLAN. |
| | receiver | Configure the port as a subscriber port that can only receive multicast data. Receiver ports cannot belong to the multicast VLAN. |
| | immediate | Enable the Immediate Leave feature of MVR on a port. Use the no form of this command to disable the feature. |

Defaults

A port is configured as neither receiver nor source.
The Immediate Leave feature is disabled on all ports.
No receiver port is a member of any configured multicast group.

Command Modes

Interface configuration

Command History

| Release | Modification |
|-----------|------------------------------------|
| 12.0(5)XW | This command was first 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.



Note

For the Catalyst 2900 XL and Catalyst 3500 XL switches, all receiver ports must belong to the same VLAN and must not be trunk ports.

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.

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 IGMP leave message from a group on a receiver port, it sends out 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 Immediate Leave, 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.

Enable the Immediate Leave feature only on receiver ports to which a single receiver device is connected.

All receiver ports must be on the same VLAN and cannot be trunk ports. A receiver configured as a static member of a multicast group remains a member until statically removed from membership.

MVR does not support IGMP dynamic joins. You must configure static multicast addresses for receiver ports.

The receiver VLAN is the VLAN to which the first configured receiver port belongs. If the first receiver port is a dynamic port with an unassigned VLAN, it becomes an inactive receiver port and does not take part in MVR until it is assigned to the receiver VLAN. The receiver VLAN is reset whenever there are no remaining receiver ports on the switch (active or inactive), which means that the receiver VLAN might change every time the first receiver port is configured.

Examples

This example shows how to configure port 0/1 as an MVR receiver port:

```
Switch(config)# interface FastEthernet 0/1
Switch(config-if)# mvr type receiver
```

This example shows how to configure port 0/3 as an MVR source port:

```
Switch(config)# interface FastEthernet 0/3
Switch(config-if)# mvr type source
```

This example shows how to remove port 0/1 from taking part in MVR:

```
Switch(config)# interface FastEthernet 0/1
Switch(config-if)# no mvr
```

This example shows how to display configured receiver ports and source ports.:

```
Switch# show mvr interface

MVR PORTS
Port: Fa0/1 Type: RECEIVER Status: ACTIVE
Port: Fa0/2 Type: RECEIVER Status: ACTIVE
Port: Fa0/3 Type: SOURCE Status: ACTIVE
```

This example shows how to enable Immediate Leave on Fast Ethernet port 0/1:

```
Switch(config)# interface FastEthernet 0/1
Switch(config-if)# mvr immediate
```

This example shows how to disable Immediate Leave on port 0/1:

```
Switch(config)# interface FastEthernet 0/1
Switch(config-if)# no mvr immediate
```

To display whether or not Immediate Leave is enabled on an interface, use the command **show mvr** for the interface as in this example:

```
Switch# show mvr interface fastethernet 0/1
Interface: Fa0/1
      Immediate Leave: FALSE
```

Use the **show mvr members** privileged EXEC command to display the multicast group address, the VLAN, and the receiver port.

Related Commands

| Command | Description |
|-----------------------------------|---|
| mvr (global configuration) | Enables multicast VLAN registration on the switch. |
| show mvr | Displays MVR global parameters or port parameters. |
| show mvr members | Displays all receiver ports that are members of an MVR multicast group. |
| show mvr interface | Displays the configured MVR ports. |

ntp broadcast client

Use the **ntp broadcast client** interface configuration command to allow the system to receive Network Time Protocol (NTP) broadcast packets on an interface. Use the **no** form of the command to disable this capability.

ntp broadcast client

no ntp broadcast client

| | |
|---------------------------|--|
| Syntax Description | This command has no arguments or keywords. |
|---------------------------|--|

| | |
|-----------------|------------------------------------|
| Defaults | Broadcast client mode is disabled. |
|-----------------|------------------------------------|

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

| | | |
|------------------------|----------------|------------------------------------|
| Command History | Release | Modification |
| | 11.2(8)SA6 | This command was first introduced. |

| | |
|-------------------------|--|
| Usage Guidelines | Use this command to allow the system to listen to broadcast packets on an interface-by-interface basis. Enter this command on the management VLAN interface. By default, the management VLAN is VLAN 1, but you can configure a different VLAN as the management VLAN. |
|-------------------------|--|

| | |
|-----------------|--|
| Examples | This example shows how to synchronize the router to NTP packets that are broadcast on interface VLAN1: |
|-----------------|--|

```
Switch(config-if)# interface vlan1
Switch(config-if)# ntp broadcast client
```

You can verify the previous commands by entering the **show running-config** privileged EXEC command.

| | | |
|-------------------------|----------------------------|---|
| Related Commands | Command | Description |
| | show running-config | Displays the running configuration on the switch. |

ntp broadcast destination

Use the **ntp broadcast destination** interface configuration command to configure a Network Time Protocol (NTP) server or peer to restrict the broadcast of NTP frames to the IP address of a designated client or a peer. Use the **no** form of the command to return the setting to its default.

ntp broadcast destination *IP-address*

no ntp broadcast destination

| | | |
|--------------------|--|---|
| Syntax Description | <i>IP-address</i> IP address or host name of a designated client or a peer. | |
| Defaults | No IP address or host name is assigned. | |
| Command Modes | Interface configuration | |
| Command History | Release | Modification |
| | 11.2(8)SA6 | This command was first introduced. |
| Usage Guidelines | Enter this command on the management VLAN interface. By default, the management VLAN is VLAN 1, but you can configure a different VLAN as the management VLAN. | |
| Examples | This example shows how to restrict the broadcast of NTP frames to a specific IP address: | |
| | Switch(config-if)# interface vlan1 Switch(config-if)# ntp broadcast destination 172.20.128.176 | |
| Related Commands | Command | Description |
| | ntp broadcast client | Allows the system to receive NTP broadcast packets on an interface. |

ntp broadcast key

Use the **ntp broadcast key** interface configuration command to configure a Network Time Protocol (NTP) server or peer to broadcast NTP frames with the authentication key that is embedded in the NTP packet. Use the **no** form of the command to return the setting to its default.

ntp broadcast key *number*

no ntp broadcast key

| Syntax Description | <i>number</i> The NTP authentication key that is embedded in the NTP packet. The range is from 0 to 4294967295. | | | | | |
|-----------------------------|---|--|---------|--------------|-----------------------------|---|
| Defaults | No NTP broadcast key is defined. | | | | | |
| Command Modes | Interface configuration | | | | | |
| Command History | <table><tr><th>Release</th><th>Modification</th></tr><tr><td>11.2(8)SA6</td><td>This command was first introduced.</td></tr></table> | | Release | Modification | 11.2(8)SA6 | This command was first introduced. |
| Release | Modification | | | | | |
| 11.2(8)SA6 | This command was first introduced. | | | | | |
| Usage Guidelines | Enter this command on the management VLAN interface. By default, the management VLAN is VLAN 1, but you can configure a different VLAN as the management VLAN. | | | | | |
| Examples | This example shows how to assign an authentication key to outgoing NTP frames: Switch(config)# interface vlan1 Switch(config-if)# ntp broadcast key 1 | | | | | |
| Related Commands | <table><tr><th>Command</th><th>Description</th></tr><tr><td>ntp broadcast client</td><td>Allows the system to receive NTP broadcast packets on an interface.</td></tr></table> | | Command | Description | ntp broadcast client | Allows the system to receive NTP broadcast packets on an interface. |
| Command | Description | | | | | |
| ntp broadcast client | Allows the system to receive NTP broadcast packets on an interface. | | | | | |

ntp broadcast version

Use the **ntp broadcast** interface configuration command to specify that a specific interface should send Network Time Protocol (NTP) broadcast packets. Use the **no** form of the command to disable this capability.

ntp broadcast version *number*

no ntp broadcast

| | | |
|--------------------|---------------|----------------------|
| Syntax Description | <i>number</i> | The range is 1 to 3. |
|--------------------|---------------|----------------------|

| | |
|----------|---------------------------|
| Defaults | Version 3 is the default. |
|----------|---------------------------|

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

| Command History | Release | Modification |
|-----------------|------------|------------------------------------|
| | 11.2(8)SA6 | This command was first introduced. |

| | |
|------------------|--|
| Usage Guidelines | Cisco IOS uses NTP version 3 by default. If the network (NTP server) is using NTP version 2, and synchronization does not occur, use NTP version 2. |
| | Enter this command on the management VLAN interface. By default, the management VLAN is VLAN 1, but you can configure a different VLAN as the management VLAN. |

| | |
|----------|---|
| Examples | This example shows how to configure interface VLAN 1 to send NTP version 2 packets: |
|----------|---|

```
Switch(config-if)# interface vlan1  
Switch(config-if)# ntp broadcast version 2
```

You can verify the previous commands by entering the **show running-config** privileged EXEC command.

| Related Commands | Command | Description |
|------------------|-----------------------------|---|
| | ntp broadcast client | Allows the system to receive NTP broadcast packets on an interface. |
| | show running-config | Displays the running configuration on the switch. |

ntp max-associations

Use the **ntp max-associations** global configuration command to set the maximum number of Network Time Protocol (NTP) associations that are allowed on a server. Use the **no** form of this command to disable this feature.

ntp max-associations [*number*]

no ntp max-associations

| | | |
|--------------------|--|---|
| Syntax Description | <i>number</i> (Optional) Specify the number of NTP associations. The range is from 0 to 4294967295. | |
| Defaults | The number of NTP associations is 100. | |
| Command Modes | Global configuration | |
| Command History | Release | Modification |
| | 11.2(8)SA6 | This command was first introduced. |
| Usage Guidelines | This command can control the number of peers that can use the switch to synchronize to it through NTP. After you enable a switch as an NTP server, use this command to set the maximum number of associations that are allowed on a server. | |
| Examples | <p>This example shows how to set the maximum number of NTP associations to 44:</p> <pre>Switch(config)# ntp max-associations 44</pre> <p>You can verify the previous command by entering the show running-config privileged EXEC command.</p> | |
| Related Commands | Command | Description |
| | show running-config | Displays the running configuration on the switch. |

ntp source

Use the **ntp source** global configuration command to use a particular source address in Network Time Protocol (NTP) packets. Use the **no** form of this command to remove the specified source address.

ntp source *interface*

no ntp source

| | | |
|--------------------|------------------|----------------------------------|
| Syntax Description | <i>interface</i> | Any valid system interface name. |
|--------------------|------------------|----------------------------------|

| | |
|----------|-------------------------------|
| Defaults | No source address is defined. |
|----------|-------------------------------|

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

| Command History | Release | Modification |
|-----------------|------------|------------------------------------|
| | 11.2(8)SA6 | This command was first introduced. |

| | |
|------------------|--|
| Usage Guidelines | Use this command when you want to use a particular source IP address for all NTP packets. The address is taken from the specified interface. This command is useful if the address on an interface cannot be used as the destination for reply packets. If the source keyword is present on an ntp server or ntp peer command, that value overrides the global value. |
|------------------|--|

| | |
|----------|--|
| Examples | This example shows how to configure the switch to use the IP address of VLAN1 as the source address of all outgoing NTP packets: |
|----------|--|

```
Switch(config)# ntp source vlan1
```

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

| Related Commands | Command | Description |
|------------------|----------------------------|---|
| | ntp source | Allows the switch system clock to be synchronized by a time server. |
| | show running-config | Displays the running configuration on the switch. |

port block

Use the **port block** interface configuration command to block the flooding of unknown unicast or multicast packets to a port. Use the **no** form of this command to resume normal forwarding.

port block {unicast | multicast}

no port block {unicast | multicast}

Syntax Description

| | |
|------------------|--|
| unicast | Packets with unknown unicast addresses are not forwarded to this port. |
| multicast | Packets with unknown multicast addresses are not forwarded to this port. |

Defaults

Flood unknown unicast and multicast packets to all ports.

Command Modes

Interface configuration

Command History

| Release | Modification |
|-----------|------------------------------------|
| 11.2(8)SA | This command was first introduced. |

Usage Guidelines

The **port block** command cannot be entered for a network port.

If a trunk port is not a network port, the **unicast** keyword applies. The **multicast** keyword is supported on trunk ports. Both port block features affect all the VLANs associated with the trunk port.

Examples

This example shows how to block the forwarding of multicast and unicast packets to a port:

```
Switch(config-if)# port block unicast
Switch(config-if)# port block multicast
```

You can verify the previous commands by entering the **show port block** user EXEC command.

Related Commands

| Command | Description |
|------------------------|---|
| show port block | Displays the blocking of unicast or multicast flooding to a port. |

port group

Use the **port group** interface configuration command to assign a port to a Fast EtherChannel or Gigabit EtherChannel port group. Up to 12 port groups can be created on a switch. Any number of ports can belong to a destination-based port group. Up to eight ports can belong to a source-based port group. Use the **no** form of this command to remove a port from a port group.

port group *group-number* [**distribution** {**source** | **destination**}]

no port group

| | |
|--------------------|---|
| Syntax Description | <i>group-number</i> Port group number to which the port belongs. The range is from 1 to 12. |
| | distribution { source destination } (Optional) Forwarding method for the port group. <ul style="list-style-type: none"> • source—Set the port to forward traffic to a port group based on the packet source address. This is the default forwarding method. • destination—Set the port to forward traffic to a port group based on the packet destination address. |

| | |
|----------|---|
| Defaults | Port does not belong to a port group. The default forwarding method is source. |
|----------|---|

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

| | | |
|-----------------|----------------|------------------------------------|
| Command History | Release | Modification |
| | 11.2(8)SA3 | This command was first introduced. |

| | |
|------------------|---|
| Usage Guidelines | An Asynchronous Transfer Mode (ATM) port is the only port that <i>cannot</i> belong to a port group. For all other ports, these restrictions apply: <ul style="list-style-type: none"> • Do not group Fast Ethernet and Gigabit ports together. • No port group member can be configured for Switched Port Analyzer (SPAN) port monitoring. • No port group member can be enabled for port security. • You can create up to 12 port groups. You can have source-based port groups and destination-based source groups. A source-based port group can have up to eight ports in its group. A destination-based port group can contain an unlimited number of ports in its group. You cannot mix source-based and destination-based ports in the same group. You can independently configure port groups that link switches, but you must consistently configure both ends of a port group. |
|------------------|---|

- Port group members must belong to the same set of VLANs and must be all static-access, all multi-VLAN, or all trunk ports.
- Dynamic-access ports cannot be grouped with any other port, not even with other dynamic-access ports.

When a group is first formed, the switch automatically sets these parameters to be the same on all ports:

- VLAN membership of ports in the group
- VLAN mode (static, multi, trunk) of ports in the group
- Encapsulation method of the trunk
- Native VLAN configuration if the trunk uses IEEE 802.1Q
- Allowed VLAN list configuration of the trunk port
- Spanning Tree Protocol (STP) Port Fast option
- STP port priority
- STP path cost
- Network port configuration for source-based port group
- Protected port

Configuration of the first port added to the group is used when setting the above parameters for other ports in the group. After a group is formed, changing any parameter in the above list changes the parameter on all other ports.

Use the **distribution** keyword to customize the port group to your particular environment. The forwarding method you choose depends on how your network is configured. However, source-based forwarding works best for most network configurations.

This command is not supported on the ATM modules.

Examples

This example shows how to add a port to a port group by using the default source-based forwarding:

```
Switch(config-if)# port group 1
```

This example shows how to add a port to a group by using destination-based forwarding:

```
Switch(config-if)# port group 2 distribution destination
```

You can verify the previous commands by entering the **show port group** user EXEC command.

Related Commands

| Command | Description |
|------------------------|---|
| show port group | Displays the ports that belong to a port group. |

port monitor

Use the **port monitor** interface configuration command to enable Switch Port Analyzer (SPAN) port monitoring on a port. Use the **no** form of this command to return the port to its default value.

port monitor [*interface* / **vlan** *vlan-id*]

no port monitor [*interface* / **vlan** *vlan-id*]

| | | |
|--------------------|--|--|
| Syntax Description | <i>interface</i> | (Optional) Module type, slot, and port number for the SPAN to be enabled. The interface specified is the port to be monitored. |
| | vlan <i>vlan-id</i> | (Optional) ID of the VLAN to be monitored. |
| | Note VLAN 1 is the only valid option. | |

Defaults Port does not monitor any other ports.

Command Modes Interface configuration

| | | |
|-----------------|----------------|------------------------------------|
| Command History | Release | Modification |
| | 11.2(8)SA | This command was first introduced. |
| | 11.2(8)SA3 | The vlan keyword was added. |

Usage Guidelines

Enabling port monitoring without specifying a port causes all other ports in the same VLAN to be monitored.

Entering the **port monitor vlan 1** command causes monitoring of all traffic to and from the IP address configured on VLAN 1.

Asynchronous Transfer Mode (ATM) ports are the only ports that *cannot* be monitor ports. However, you can monitor ATM ports. The following restrictions apply for ports that have port-monitoring capability:

- A monitor port cannot be in a Fast EtherChannel or Gigabit EtherChannel port group.
- A monitor port cannot be enabled for port security.
- A monitor port cannot be a multi-VLAN port.
- A monitor port must be a member of the same VLAN as the port monitored. VLAN membership changes are not allowed on monitor ports and ports being monitored.
- A monitor port cannot be a dynamic-access port or a trunk port. However, a static-access port can monitor a VLAN on a trunk, a multi-VLAN port, or a dynamic-access port. The VLAN monitored is the one associated with the static-access port.
- Port monitoring does not work if both the monitor and monitored ports are protected ports.

Examples

This example shows how to enable port monitoring on port fa0/2:

```
Switch(config-if)# port monitor fa0/2
```

You can verify the previous command by entering the **show port monitor** user EXEC command.

Related Commands

| Command | Description |
|--------------------------|---|
| show port monitor | Displays the ports for which SPAN port monitoring is enabled. |

port network

Use the **port network** interface configuration command to define a port as the switch network port. All traffic with unknown unicast addresses is forwarded to the network port on the same VLAN. Use the **no** form of this command to return the port to the default value.

port network

no port network

| | |
|---------------------------|--|
| Syntax Description | This command has no arguments or keywords. |
|---------------------------|--|

| | |
|-----------------|-----------------------------|
| Defaults | No network port is defined. |
|-----------------|-----------------------------|

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

| Command History | Release | Modification |
|------------------------|------------|------------------------------------|
| | 11.2(8)SA4 | This command was first introduced. |

| | |
|-------------------------|---|
| Usage Guidelines | The following restrictions apply to network ports: |
| | <ul style="list-style-type: none">• A network port can be a static-access port, a multi-VLAN port, a port group, or a trunk port. Both the multi-VLAN port and the trunk port become the network port for all the VLANs associated with that port.• A network port cannot be an Asynchronous Transfer Mode (ATM), a secure, a monitor, a protected, or a dynamic-access port. You can assign a dynamic-access port to a VLAN in which another port is the network port.• Each VLAN can have one network port.• A network port cannot be in a destination-based port group.• A network port cannot be on an ATM module.• A network port cannot be a protected port. |

| | |
|-----------------|---|
| Examples | This example shows how to set a port as a network port: |
|-----------------|---|

Switch(config-if)# **port network**

You can verify the previous command by entering the **show port network** privileged EXEC command.

| Related Commands | Command | Description |
|-------------------------|--------------------------|---|
| | show port network | Displays the network port defined for the switch or VLAN. |

port protected

Use the **port 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 the command to disable the protected port.

port protected

no port protected

Syntax Description

This command has no keywords or arguments.

Defaults

No protected port is defined.

A protected port does not forward any unicast, multicast, or broadcast traffic to any other protected port.

A protected port continues to forward and receive unicast, multicast, and broadcast traffic to and from unprotected ports.

Command Modes

Interface configuration

Command History

| Release | Modification |
|-----------|------------------------------------|
| 12.0(5)XU | This command was first introduced. |

Usage Guidelines

The port 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 cannot be a network port.

Port monitoring does not work if both the monitor and monitored ports are protected ports.

A protected port is different from a secure port.

Examples

This example shows how to enable a protected port on interface fa0/3:

```
Switch(config)# interface fa0/3
Switch(config-if)# port protected
```

You can verify the previous command by entering **the show port protected** user EXEC command.

Related Commands

| Command | Description |
|----------------------------|---|
| show port protected | Displays the ports that are in port-protected mode. |

port security

Use the **port security** interface configuration command to enable port security on a port and restrict the use of the port to a user-defined group of stations. Use the **no** form of this command to return the port to its default value.

port security [**action** {**shutdown** | **trap**} | **max-mac-count** *addresses*]

no port security

| | | |
|--------------------|---|--|
| Syntax Description | action { shutdown trap } | (Optional) Action to take when an address violation occurs on this port. <ul style="list-style-type: none"> • shutdown—Disable the port when a security violation occurs. • trap—Generate a Simple Network Management Protocol (SNMP) trap when a security violation occurs. |
| | max-mac-count <i>addresses</i> | (Optional) The maximum number of secure addresses that this port can support. The range is from 1 to 132. |

Defaults

Port security is disabled.

When enabled, the default action is to generate an SNMP trap.

Command Modes

Interface configuration

Command History

| Release | Modification |
|-----------|------------------------------------|
| 11.2(8)SA | This command was first introduced. |

Usage Guidelines

If you specify **trap**, use the **snmp-server host** global configuration command to configure the SNMP trap host to receive traps.

The following restrictions apply to secure ports:

- A secure port cannot belong to a Fast EtherChannel or Gigabit EtherChannel port group.
- A secure port cannot have Switched Port Analyzer (SPAN) port monitoring enabled on it.
- A secure port cannot be a multi-VLAN port.
- A secure port cannot be a network port.
- A secure port cannot be an Asynchronous Transfer Mode (ATM) port.
- A secure port cannot be a dynamic-access port or a trunk port.

Examples

This example shows how to enable port security and what action the port takes in case of an address violation (shutdown).

```
Switch(config-if)# port security action shutdown
```

This example shows how to set the maximum number of addresses that the port can learn to 8.

```
Switch(config-if)# port security max-mac-count 8
```

You can verify the previous commands by entering the **show port security** privileged EXEC command.

Related Commands

| Command | Description |
|---------------------------|---|
| show port security | Displays the port security settings defined for the port. |

port storm-control

Use the **port storm-control** interface configuration command to enable broadcast, multicast, or unicast storm control on a port. Use the **no** form of this command to disable storm control or one of the storm-control parameters on the port.

port storm-control {**broadcast** | **multicast** | **unicast**} [{**action** {**filter** | **shutdown**} | **threshold** {**rising** *rising-number* **falling** *falling-number*} | **trap**}]

no port storm-control {**broadcast** | **multicast** | **unicast**}

| | |
|--------------------|--|
| Syntax Description | <p>{broadcast multicast unicast} Determine the type of packet-storm suppression.</p> <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. |
| | <p>{action {filter shutdown} (Optional) Determine the type of action to perform.</p> <ul style="list-style-type: none"> • filter—Filter traffic during a storm. • shutdown—Disable the port during a storm. |
| | <p>threshold {rising <i>rising-number</i> falling <i>falling-number</i>} Defines the rising and falling thresholds.</p> <ul style="list-style-type: none"> • rising <i>rising-number</i>—Block the flooding of storm packets when the value specified for <i>rising-number</i> is reached. The <i>rising-number</i> is 0 to 4294967295 packets per second. • falling <i>falling-number</i>—Restart the normal transmission of broadcast packets when the value specified for <i>falling-number</i> is reached. The <i>falling-number</i> is 0 to 4294967295 packets per second. |
| | <p>trap (Optional) Generate a Simple Network Management Protocol (SNMP) trap when the traffic on the port crosses the rising or falling threshold. Traps are generated only for broadcast traffic and not for unicast or multicast traffic.</p> |

Defaults

Broadcast, multicast, and unicast storm control are disabled.

The rising thresholds are 500 broadcast packets per second, 2500 multicast packets per second, and 5000 unicast packets per second.

The falling thresholds are 250 broadcast packets per second, 1200 multicast packets per second, and 2500 unicast packets per second.

Command Modes

Interface configuration

| Command History | Release | Modification |
|-----------------|-----------|--|
| | 11.2(8)SA | This command was first introduced. |
| | 12.0(5)XU | The multicast , unicast , action , and shutdown keywords were added. |

Usage Guidelines Do not set the rising and falling thresholds to the same value.

Examples This example shows how to enable broadcast storm control on a port. In this example, transmission is inhibited when the number of broadcast packets arriving on the port reaches 1000 and is restarted when the number drops to 200.

```
Switch(config-if)# port storm-control broadcast threshold rising 1000 falling 200
```

You can verify the previous command by entering the **show port storm-control** user EXEC command.

| Related Commands | Command | Description |
|------------------|--------------------------------|--|
| | show port storm-control | Displays the packet storm-control information. |

power inline

Use the **power inline** interface configuration command to determine how inline power is applied to the device on the specified Fast Ethernet port of the 3524-PWR-XL switch. Use the **no** form of this command to return the setting to its default.

power inline { auto | never }

no power inline

| | | |
|--------------------|--------------|--|
| Syntax Description | auto | Automatically detect and power inline devices. |
| | never | Never apply inline power. |

| | |
|----------|---|
| Defaults | Power is applied when a telephone is detected on the port (auto). |
|----------|---|

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

| | | |
|-----------------|-----------|------------------------------------|
| Command History | Release | Modification |
| | 12.0(5)XU | This command was first introduced. |

Examples

This example shows how to always apply power to the port:

```
Switch(config-if)# power inline auto
```

You can verify the previous command by entering the **show power inline** privileged EXEC command.

| | | |
|------------------|-----------------------------------|--|
| Related Commands | Command | Description |
| | show power inline | Displays the power status for the specified port or for all ports. |
| | switchport priority extend | Determines how the telephone connected to the specified port handles priority traffic received on its incoming port. |
| | switchport voice vlan | Configures the voice VLAN on the port. |

rcommand

Use the **rcommand** user EXEC command to start a Telnet session and to enter commands on a member switch from the command switch. To end the session, enter the **exit** command.

rcommand { *n* | **commander** | **mac-address** *hw-addr* }

| | | |
|--------------------|-----------------------------------|---|
| Syntax Description | <i>n</i> | 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 <i>hw-addr</i> | MAC address of the member switch. |

| | |
|---------------|-----------|
| Command Modes | User EXEC |
|---------------|-----------|

| | | |
|-----------------|------------|------------------------------------|
| Command History | Release | Modification |
| | 11.2(8)SA6 | This command was first introduced. |

Usage Guidelines

If the switch is the command switch but the member switch *n* does not exist, an error message appears. To obtain the switch number, enter the **show cluster members** privileged EXEC command from 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 and Catalyst 3500 XL 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 Catalyst 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 Catalyst 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.

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. |

reset

Use the **reset** VLAN database command to abandon the proposed VLAN database and to remain in VLAN database mode. This command resets the proposed database to the currently implemented VLAN database on the switch.

reset

| | |
|---------------------------|--|
| Syntax Description | This command has no arguments or keywords. |
|---------------------------|--|

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

| | |
|----------------------|---------------|
| Command Modes | VLAN database |
|----------------------|---------------|

| Command History | Release | Modification |
|-----------------|------------|------------------------------------|
| | 11.2(8)SA4 | This command was first introduced. |

| | |
|-----------------|--|
| Examples | <p>This example shows how to abandon the proposed VLAN database and to reset to the VLAN database:</p> <pre>Switch(vlan)# reset Switch(vlan)#</pre> |
|-----------------|--|

You can verify the previous command by entering the **show changes** and **show proposed** VLAN database commands.

| Related Commands | Command | Description |
|------------------|----------------------|--|
| | abort | Abandons the proposed VLAN database, exits VLAN database mode, and returns to privileged EXEC mode. |
| | apply | Implements the proposed VLAN database, increments the database configuration revision number, propagates it throughout the administrative domain, and remains in VLAN database mode. |
| | exit | Implements the proposed VLAN database, increments the database configuration number, propagates it throughout the administrative domain, and returns to privileged EXEC mode. |
| | show changes | Displays the differences between the VLAN database currently on the switch and the proposed VLAN database. |
| | show proposed | Displays the proposed VLAN database or a selected VLAN from it. |
| | shutdown vlan | Shuts down (suspends) local traffic on the specified VLAN. |
| | vlan database | Enters VLAN database mode from the command-line interface (CLI). |

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 from 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)WC1 | This command was first 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 interface fa01:

```
Switch(config)# interface fa0/1
Switch(config-if)# rmon collection stats 2 owner root
```

You can verify this command by entering the **show rmon statistics** command in user EXEC mode.

| | | |
|------------------|-----------------------------|---|
| Related Commands | Command | Description |
| | show rmon statistics | Displays RMON statistics. Refer to the Cisco IOS Release 12.0 documentation on Cisco.com for information about this command. |

session

Use the **session** privileged EXEC command to log into the Asynchronous Transfer Mode (ATM) module operating system and to start a command-line interface (CLI) session. Enter the **exit** command, or press **Ctrl-G** to return to the switch command-line interface.

session *number*

| | | |
|--------------------|--|---|
| Syntax Description | <i>number</i> | Slot number (1 or 2). |
| Command Modes | Privileged EXEC | |
| Command History | Release | Modification |
| | 11.2(8)SA5 | This command was first introduced. |
| Examples | This example shows how to log in to the ATM module number 1: Switch# session 1 | |
| Related Commands | Command | Description |
| | exit | Exits the session with the ATM module and returns you to the CLI. |

show cgmp

Use the **show cgmp** user EXEC command to display the state of the Cisco Group Management Protocol (CGMP)-learned multicast groups and routers.

show cgmp [**state** | **holdtime** | [**vlan** *vlan-id*] | [**group** *address*] | **router** *address*]]

| | | |
|--------------------|------------------------------|--|
| Syntax Description | state | (Optional) Display whether CGMP is enabled or not, whether Fast Leave is enabled or not, and the router port timeout value. |
| | holdtime | (Optional) Display the router port timeout value in seconds. |
| | vlan <i>vlan-id</i> | (Optional) Limit the display to the specified VLAN. Valid IDs are from 1 to 1001; do not enter leading zeroes. |
| | group <i>address</i> | (Optional) Display all known multicast groups and the destination ports. Limited to given VLAN if vlan keyword is entered; limited to a specific group if the <i>address</i> variable is entered. The <i>address</i> is the MAC address of the group. |
| | router <i>address</i> | (Optional) Display all routers, their ports, and expiration times. Limited to a given VLAN if the vlan keyword entered; limited to a specific router if the <i>address</i> variable is entered. The <i>address</i> is the MAC address of the router. |

| | |
|---------------|-----------|
| Command Modes | User EXEC |
|---------------|-----------|

| | | |
|-----------------|----------------|------------------------------------|
| Command History | Release | Modification |
| | 11.2(8)SA3 | This command was first introduced. |

| | |
|------------------|---|
| Usage Guidelines | This command displays CGMP information about known routers and groups, as well as whether CGMP is enabled, whether Fast Leave is enabled, and the value of the router timeout. If show cgmp is entered with no arguments, all information appears. |
|------------------|---|

Examples

This is an example of output from the **show cgmp** command.

```
Switch> show cgmp
```

```
CGMP is running.
CGMP Fast Leave is not running.
CGMP Allow reserved address to join GDA.
Default router timeout is 300 sec.
```

| vLAN | IGMP MAC Address | Interfaces |
|------|------------------|------------|
| 1 | 0100.5e01.0203 | Fa0/8 |
| 1 | 0100.5e00.0128 | Fa0/8 |

| vLAN | IGMP Router | Expire | Interface |
|------|----------------|---------|-----------|
| 1 | 0060.5cf3.d1b3 | 197 sec | Fa0/8 |

Related Commands

| Command | Description |
|-------------------|---|
| cgmp | Enables CGMP. Also enables and disables the Fast Leave parameter and sets the router port aging time. |
| clear cgmp | Deletes information that was learned by the switch by using CGMP. |

show changes

Use the **show changes** VLAN database command to display the differences between the VLAN database on the switch and the proposed VLAN database. You can also display the differences between the two for a selected VLAN.

show changes [*vlan-id*]

| | | |
|---------------------------|----------------|--|
| Syntax Description | <i>vlan-id</i> | (Optional) ID of the VLAN in the current or proposed database. If this variable is omitted, all the differences between the two VLAN databases are displayed, including the pruning state and Version 2 mode. Valid IDs are from 1 to 1005; do not enter leading zeroes. |
|---------------------------|----------------|--|

| | |
|----------------------|---------------|
| Command Modes | VLAN database |
|----------------------|---------------|

| | | |
|------------------------|----------------|------------------------------------|
| Command History | Release | Modification |
| | 11.2(8)SA4 | This command was first introduced. |

Examples This is an example of output from the **show changes** command. It displays the differences between the current and proposed databases.

```
Switch(vlan)# show changes
```

```
DELETED:
```

```
VLAN ISL Id: 4
  Name: VLAN0004
  Media Type: Ethernet
  VLAN 802.10 Id: 100004
  State: Operational
  MTU: 1500
```

```
DELETED:
```

```
VLAN ISL Id: 6
  Name: VLAN0006
  Media Type: Ethernet
  VLAN 802.10 Id: 100006
  State: Operational
  MTU: 1500
```

```
MODIFIED:
```

```
VLAN ISL Id: 7
  Current State: Operational
  Modified State: Suspended
```

This is an example of output from the **show changes 7** command. It displays the differences between VLAN 7 in the current and proposed database.

```
Switch(vlan)# show changes 7

MODIFIED:
  VLAN ISL Id: 7
    Current State: Operational
    Modified State: Suspended
```

Related Commands

| Command | Description |
|----------------------|--|
| show current | Displays the VLAN database on the switch or a selected VLAN from it. |
| show proposed | Displays the proposed VLAN database or a selected VLAN from it. |

show cluster

Use the **show cluster** user 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

| | |
|---------------------------|--|
| Syntax Description | This command has no arguments or keywords. |
|---------------------------|--|

| | |
|----------------------|-----------|
| Command Modes | User EXEC |
|----------------------|-----------|

| | | |
|------------------------|----------------|------------------------------------|
| Command History | Release | Modification |
| | 11.2(8)SA6 | This command was first introduced. |

| | |
|-------------------------|--|
| Usage Guidelines | If the switch is not a command switch or a member switch, the command displays an empty line at the prompt. |
| | 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 number of members. It also shows the cluster status and length of 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 <code>Not a management cluster member</code> appears. |

| | |
|-----------------|---|
| Examples | This is an example of output when this command is entered on the active command switch: |
|-----------------|---|

```
Switch> show cluster
Command switch for cluster "Ajang"
  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:             Ajang_standby
    Standby Group Number:      110
  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:

```
Switch1> show cluster
Member switch for cluster "mcluster"
  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 "mcluster"
  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 is separated from member 1:

```
3524-24> show cluster
Command switch for cluster "Ajang"
  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 is separated from the command switch:

```
3512-12> show cluster
Member switch for cluster "mcluster"
  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** user EXEC command on the command switch to display a list of candidate switches.

show cluster candidates [**mac-address** *H.H.H.* | **detail**]

| | | |
|--------------------|----------------------------------|---|
| Syntax Description | mac-address <i>H.H.H.</i> | (Optional) MAC address of the cluster candidate. |
| | detail | (Optional) Display detailed information for all candidates. |

| | |
|---------------|-----------|
| Command Modes | User EXEC |
|---------------|-----------|

| | | |
|-----------------|----------------|--------------------------------------|
| Command History | Release | Modification |
| | 11.2(8)SA6 | This command was first introduced. |
| | 12.0(5)XU | The detail keyword was added. |

| | |
|------------------|---|
| Usage Guidelines | Enter this command only on a command switch. |
| | If the switch is not a command switch, the command line displays an empty line at the prompt. |
| | The SN in the display means <i>switch member number</i> . If E appears in the SN column, it means that the switch is discovered through extended discovery. The hop count is the number of devices that the candidate is from the command switch. |
| | |

| | |
|----------|---|
| 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 3512-12      WS-C3512-XL    Fa0/3    1   0   Fa0/13
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 2924-24      WS-C2924-XL    Fa0/5    1   0   Fa0/3
00e0.1e9f.8c00 2912-12-2    WS-C2912-XL    Fa0/4    1   0   Fa0/7
00e0.1e9f.8c40 2912-12-1    WS-C2912-XL    Fa0/1    1   0   Fa0/9
0050.2e4a.9fb0   murali-132    WS-C3508-XL                      E
0050.354e.7cd0   murali-134    WS-C2924-XL                      E

```

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 '3512-12' with mac address number 00d0.7961.c4c0
Device type:                cisco WS-C3512-XL
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 '2912MF' with mac address number 0010.7bb6.1cc0
Device type:          cisco WS-C2912MF-XL
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 '3512-12' with mac address number 00d0.7961.c4c0
Device type:          cisco WS-C3512-XL
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 '2924-24' 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** user EXEC command on the command switch to display information about the cluster members.

show cluster members [*n* | **detail**]

| | | |
|--------------------|---------------|--|
| Syntax Description | <i>n</i> | (Optional) Number that identifies a cluster member. The range is from 0 to 15. |
| | detail | (Optional) Display detailed information for all cluster members. |

| | |
|---------------|-----------|
| Command Modes | User EXEC |
|---------------|-----------|

| Command History | Release | Modification |
|-----------------|------------|--------------------------------------|
| | 11.2(8)SA6 | This command was first introduced. |
| | 12.0(5)XU | The detail keyword was added. |

| | |
|------------------|---|
| Usage Guidelines | You should enter this command only on a command switch. |
| | If the cluster has no members, an empty line appears at the prompt. |

| | |
|----------|---|
| Examples | This is an example of output from the show cluster members command. The SN in the display means <i>switch number</i> . |
|----------|---|

```
Switch> show cluster members
```

```

                                     |---Upstream---|
SN MAC Address      Name           PortIf FEC Hops   SN PortIf  FEC  State
0  00d0.796d.2f00  3524-24                        0                               Up (Cmdr)
1  00d0.7960.66c0                               255                             Down
2  00e0.1e9f.8c00  2912-12-2 Fa0/4             1    0 Fa0/7             Up (Standby)
3  00e0.1e9f.7a00  2924-24 Fa0/5             1    0 Fa0/3             Up
4  00d0.bbf5.e900  ldf-dist-128 Fa0/7           1    0 Fa0/24            Up
5  00d0.7961.c4c0  3512-12 Fa0/3             1    0 Fa0/13            Up
6  00e0.1e9f.8c40  2912-12-1 Fa0/1           1    0 Fa0/9             Up
7  00e0.1e7e.be80  1900_Switch 3             0    1    0 Fa0/11            Up
8  00e0.1e9f.8300  2924M Fa0/11             2    5 Fa0/12            Up
9  0010.7bb6.1cc0  2912MF Fa2/1              3    8 Fa0/24            Up
10 00e0.1e87.2140  2820-01 24             0    4    9 Fa2/3             Up

```

This is an example of output from the **show cluster members** for cluster member 3:

```

Switch> show cluster members 3
Device '2924-24' with member number 3
  Device type:      cisco WS-C2924M-XL
  MAC address:      00e0.1e9f.9440
  Upstream MAC address: 00d0.796d.2e00 (Cluster member 0)
  Local port:      Fa0/18 FEC number:
  Upstream port:   Fa0/20 FEC Number:
  Hops from command device: 1

```


This is an example of output from the **show cluster members detail** command:

```
Switch> show cluster members detail
Device '3524-24' with member number 0 (Command Switch)
  Device type:          cisco WS-C3524-XL
  MAC address:          00d0.7964.1f00
  Upstream MAC address:
  Local port:           FEC number:
  Upstream port:        FEC Number:
  Hops from command device: 0
'Unknown'device with member number 1
  Device type:
  MAC address:
  Upstream MAC address:
  Local port:           FEC number:
  Upstream port:        FEC Number:
  Hops from command device: 255
Device '2912-12-2' with member number 2
  Device type:          cisco WS-C3548-XL
  MAC address:          00d0.5868.f5c0
  Upstream MAC address: 00d0.7964.1f00 (Cluster member 0)
  Local port:          Fa0/7   FEC number: 1
  Upstream port:        Fa0/6   FEC Number:
  Hops from command device: 1
Device '2924-24' with member number 3
  Device type:          cisco WS-C3508G-XL
  MAC address:          00d0.7968.5380
  Upstream MAC address: 00d0.7964.1f00 (Cluster member 0)
  Local port:          Gi0/6   FEC number:
  Upstream port:        Gi0/1   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 transmit and receive statistics on a Fast Ethernet switch.

show controllers ethernet-controller *interface-id*

| | | |
|--------------------|---------------------|-------------------------------|
| Syntax Description | <i>interface-id</i> | ID of the Fast Ethernet port. |
|--------------------|---------------------|-------------------------------|

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

| | | |
|-----------------|------------|------------------------------------|
| Command History | Release | Modification |
| | 12.0(5)WC1 | This command was first introduced. |

| | |
|------------------|--|
| Usage Guidelines | Using the show controllers ethernet-controller command without specifying a Fast Ethernet port displays the Ethernet link statistics of all ports on the switch. The output shows the internal switch statistics. |
|------------------|--|

| | |
|----------|--|
| Examples | This is an example of output from the show controllers ethernet-controller command on Fast Ethernet port 1: |
|----------|--|

Switch# **show controllers ethernet-controller fa0/1**

| | |
|------------------------|-----------------------------|
| Transmit | Receive |
| 877634 Bytes | 8834435 Bytes |
| 3853 Unicast frames | 5212 Unicast frames |
| 606 Multicast frames | 20600 Multicast frames |
| 3496 Broadcast frames | 32756 Broadcast frames |
| 0 Discarded frames | 0 No bandwidth frames |
| 0 Too old frames | 0 No buffers frames |
| 0 Deferred frames | 10697 No dest, unicast |
| 0 1 collision frames | 42555 No dest, multicast |
| 0 2 collision frames | 0 No dest, broadcast |
| 0 3 collision frames | 0 Alignment errors |
| 0 4 collision frames | 0 FCS errors |
| 0 5 collision frames | 0 Collision fragments |
| 0 6 collision frames | 0 Undersize frames |
| 0 7 collision frames | 33602 Minimum size frames |
| 0 8 collision frames | 75929 65 to 127 byte frames |
| 0 9 collision frames | 760 128 to 255 byte frames |
| 0 10 collision frames | 1527 256 to 511 byte frames |
| 0 11 collision frames | 2 512 to 1023 byte frames |
| 0 12 collision frames | 0 1024 to 1518 byte frames |
| 0 13 collision frames | 0 Oversize frames |
| 0 14 collision frames | |
| 0 15 collision frames | |
| 0 Excessive collisions | |
| 0 Late collisions | |

| Related Commands | Command | Description |
|------------------|--|--|
| | clear controllers ethernet-controller | Deletes the Ethernet link transmit and receive statistics on a Fast Ethernet switch. |

show current

Use the **show current** VLAN database command to display the current VLAN database on the switch or a selected VLAN from it.

show current [*vlan-id*]

Syntax Description

| | |
|----------------|---|
| <i>vlan-id</i> | (Optional) ID of the VLAN in the current database. If this variable is omitted, the entire VLAN database displays, including the pruning state and Version 2 mode. Valid IDs are from 1 to 1005; do not enter leading zeroes. |
|----------------|---|

Command Modes

VLAN database

Command History

| Release | Modification |
|------------|------------------------------------|
| 11.2(8)SA4 | This command was first introduced. |

Examples

This is an example of output from the **show current** command. It displays the current VLAN database.

```
Switch(vlan)# show current
```

```
VLAN ISL Id: 1
  Name: default
  Media Type: Ethernet
  VLAN 802.10 Id: 100001
  State: Operational
  MTU: 1500
  Translational Bridged VLAN: 1002
  Translational Bridged VLAN: 1003
```

```
VLAN ISL Id: 2
  Name: VLAN0002
  Media Type: Ethernet
  VLAN 802.10 Id: 100002
  State: Operational
  MTU: 1500
```

```
VLAN ISL Id: 3
  Name: VLAN0003
  Media Type: Ethernet
  VLAN 802.10 Id: 100003
  State: Operational
  MTU: 4000
```

```
VLAN ISL Id: 4
  Name: VLAN0004
  Media Type: Ethernet
  VLAN 802.10 Id: 100004
  State: Operational
  MTU: 1500
```

```
VLAN ISL Id: 5
  Name: VLAN0005
  Media Type: Ethernet
  VLAN 802.10 Id: 100005
  State: Operational
  MTU: 1500
```

```
VLAN ISL Id: 6
  Name: VLAN0006
  Media Type: Ethernet
  VLAN 802.10 Id: 100006
  State: Operational
  MTU: 1500
```

This is an example of output from the **show current 2** command. It displays only VLAN 2 of the current database.

```
Switch(vlan)# show current 2
```

```
VLAN ISL Id: 2
  Name: VLAN0002
  Media Type: Ethernet
  VLAN 802.10 Id: 100002
  State: Operational
  MTU: 1500
```

Related Commands

| Command | Description |
|----------------------|--|
| show changes | Displays the differences between the VLAN database currently on the switch and the proposed VLAN database. |
| show proposed | Displays the proposed VLAN database or a selected VLAN from it. |

show diags

Use the **show diags** user EXEC command to display the state of a port or all ports on the switch.

show diags [**addr-move** | **link-flap**] *interface-id*

| | | |
|--------------------|---------------------|---|
| Syntax Description | addr-move | Show learned address movement count and rate. |
| | link-flap | Show link up/down count and rate. |
| | <i>interface-id</i> | ID of the Fast Ethernet or Long-Reach Ethernet (LRE) port number. |

| | |
|---------------|-----------|
| Command Modes | User EXEC |
|---------------|-----------|

| | | |
|-----------------|----------------|------------------------------------|
| Command History | Release | Modification |
| | 12.0(5)XU | This command was first introduced. |

| | |
|------------------|--|
| Usage Guidelines | Use the show diags command without specifying a port to show the state of all ports on the switch. |
| | Use the show diags link-flap command to check if link flapping on a port is occurring. Link flapping can be caused by a loose connection to a port or by numerous changes to a port connection. |
| | Use the show diags addr-move command to check if address flapping is occurring. Address flapping can be caused when the switch learns the same MAC address on different ports on the same VLAN. The address table keeps changing because the MAC address is first learned on one interface, is learned on another interface, and then relearned on the previous interface, and so on. This can be caused by a loop that Spanning Tree Protocol (STP) has not blocked. |

| | |
|----------|--|
| Examples | This is an example of output from the show link-flap command. |
|----------|--|

```
Switch> show diags link-flap fa0/1
Interface                Total    Last Min
-----
FastEthernet0/1          14         0
FastEthernet0/2          12         0
FastEthernet0/3           1         0
FastEthernet0/7           6         0
FastEthernet0/12          6         0
```

show env

Use the **show env** privileged EXEC command to display fan and temperature information for the 3524-PWR-XL switch.

show env {all | fan | temperature}

| | | |
|--------------------|--------------------|--|
| Syntax Description | all | Display both fan and temperature environmental status. |
| | fan | Display the switch fan status. |
| | temperature | Display the switch temperature status. |

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

| | | |
|-----------------|----------------|------------------------------------|
| Command History | Release | Modification |
| | 12.0(5)XU | This command was first introduced. |

Examples

This is an example of output from the **show env all** command:

```
Switch# show env all
FAN 1 is OK

FAN 2 is OK

FAN 3 is OK

FAN 4 is OK

FAN 5 is OK

TEMPERATURE is OK
```

This is an example of output from the **show env fans** command:

```
FAN 1 is OK

FAN 2 is OK

FAN 3 is OK

FAN 4 is FAULTY

FAN 5 is OK
```

show file systems

Use the **show file systems** privileged EXEC command to display file system information.

show file systems

Syntax Description The command has no arguments or keywords.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|------------|------------------------------------|
| | 11.2(8)SA5 | This command was first introduced. |

Examples 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 |
|---|---------|---------|---------|-------|----------|
| * | 3612672 | 1234432 | flash | rw | flash: |
| | 3612672 | 1234432 | unknown | rw | zflash: |
| | - | - | opaque | ro | bs: |
| | 32768 | 30917 | nvram | rw | nvram: |
| | - | - | network | rw | tftp: |
| | - | - | opaque | rw | null: |
| | - | - | opaque | rw | system: |
| | - | - | network | rw | rcp: |

show interface

Use the **show interface** privileged EXEC command to display the administrative and operational status of a switching (nonrouting) port.

show interface [*interface-id* / **vlan number**] [**flow-control** | **pruning** | **status** | **switchport** [**allowed-vlan** | **prune-elig** | **native-vlan**]]

| Syntax Description | |
|---------------------|---|
| <i>interface-id</i> | ID of the module and port. |
| vlan number | VLAN number of the management VLAN. Valid IDs are from 1 to 1000. Do not enter leading zeroes. |
| flow-control | Displays flowcontrol information for the specified port. |
| pruning | (Optional) Display pruning information for the trunk port. |
| status | (Optional) Display the status of the interface. |
| switchport | (Optional) Display the administrative and operational status of a switching (nonrouting) port. <ul style="list-style-type: none"> • allowed-vlan—Display the VLAN IDs that receive and transmit all types of traffic on the trunk port. By default, all VLAN IDs are included. • prune-elig—Display the VLAN ID whose flood traffic can be pruned. By default, all VLANs, except VLAN 1 and 1002 through 1005, are pruning-eligible on the trunk. • native-vlan—Display the native VLAN ID for untagged traffic when the port is in 802.1Q trunking mode. |

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

| Command History | Release | Modification |
|-----------------|------------|---|
| | 11.2(8)SA4 | This command was first introduced. |
| | 11.2(8)SA5 | The native-vlan keyword was added. |
| | 12.0(5)XP | The vlan number keyword was added. |
| | 12.0(5)XU | The pruning keyword was added. |
| | 12.0(5)XW | The status keyword was added. |

Examples

This is an example of output from the **show interface gi0/1 flow-control** command.

```
Switch# show interface gi0/1 flow-control
Any, Input only
```

The display shows two values separated by a comma. The first value is the value that you configured by using the **flowcontrol** command or the Cluster Management Suite (CMS) (or the default value if you did not configure it). The first value can be one of these settings:

- None—Flow control is not enabled.
- Asymmetric—Only the transmit or receive flow control is enabled.
- Symmetric—Both the transmit and receive flow control are enabled.
- Any—Any type of flow control is supported.

The second value represents the flow control value that is autonegotiated with the link partner and can be one of these settings:

- None—Flow control with the link partner does not occur.
- Output only—The interface can only transmit pause frames but not receive any.
- Input only—The interface can only receive pause frames but not transmit any.
- Output and Input—The interface can transmit and receive pause frames.



Note

If you enter the **show interface *interface-id* flow-control** command on a GigaStack Gigabit Interface Converter (GBIC), the first value in the display is the setting for both GigaStack GBIC ports, and the second value is the autonegotiated setting for both ports.

This is an example of output from the **show interface fa0/2 switchport** command. Table 2-1 describes each field in the display.

```
Switch# show interface fa0/2 switchport
Name: fa0/2
Switchport: Enabled
Administrative Mode: Trunk
Operational Mode: Trunk
Administrative Trunking Encapsulation: ISL
Operational Trunking Encapsulation: ISL
Negotiation of Trunking: Disabled
Access Mode VLAN: 0 (inactive)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: 1-30, 50, 100-1005
Trunking VLANs Active: 1-4
Pruning VLANs Enabled: 2-1001

Priority for untagged frames: 0
Voice VLAN: none
Appliance trust: none
```

Table 2-1 Show Interface fa0/2 Switchport Field Descriptions

| Field | Description |
|--|--|
| Name | Displays the port name. |
| Switchport | Displays the administrative and operational status of the port. In this display, the port is in switch port mode. |
| Administrative Mode Operational Mode | Displays the administrative and operational mode. |
| Administrative Trunking Encapsulation Operation Trunking Encapsulation Negotiation of Trunking | Displays the administrative and operational encapsulation method. Also displays whether trunking negotiation is enabled. |
| Access Mode VLAN | Displays the VLAN ID to which the port is configured. |
| Trunking Native Mode VLAN Trunking VLANs Enabled Trunking VLANs Active | 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. |
| Pruning VLANs Enabled | Lists the VLANs that are pruning-eligible. |
| Priority for untagged frames | Displays the port priority on incoming untagged frames. |
| Voice VLAN | Displays the voice VLAN. |
| Appliance trust | Displays how the appliance (telephone) connected to the specified port handles priority traffic that is received on its incoming port. |

This is an example of output from the **show interface fa0/9 pruning** command when pruning is enabled in the VTP domain:

```
Switch# show interface fa0/9 pruning
Port      Vlans pruned for lack of request by neighbor
Fa0/9     3,4

Port      Vlans traffic requested of neighbor
Fa0/9     1-3
```

This is an example of output from the **show interface status** command:

```
Switch# show interface status
Port      Name              Status      Vlan      Duplex Speed  Type
-----
Fa0/1     Fa0/1              connected   trunk     A-Full  A-100  100BASE-TX/FX
Fa0/2     Fa0/2              notconnect  1         Auto    Auto    100BASE-TX/FX
Fa0/3     Fa0/3              notconnect  1         Auto    Auto    100BASE-TX/FX
Fa0/4     Fa0/4              notconnect  1         Auto    Auto    100BASE-TX/FX
Fa0/5     Fa0/5              notconnect  1         Auto    Auto    100BASE-TX/FX
Fa0/6     Fa0/6              notconnect  1         Auto    Auto    100BASE-TX/FX
Fa0/7     Fa0/7              notconnect  1         Auto    Auto    100BASE-TX/FX
Fa0/8     Fa0/8              notconnect  1         Auto    Auto    100BASE-TX/FX
Fa0/9     Fa0/9              notconnect  1         Auto    Auto    100BASE-TX/FX
<output truncated>
```

| Related Commands | Command | Description |
|------------------|------------------------------------|---|
| | switchport access | Configures a port as a static-access or dynamic-access port. |
| | switchport mode | Configures the VLAN membership mode of a port. |
| | switchport multi | Configures a list of VLANs to which the port is associated. |
| | switchport priority default | Provides a default port priority for the incoming untagged frames. |
| | switchport trunk pruning | Configures the VLAN pruning-eligible list for ports in trunking mode. |
| | switchport voice vlan | Configures the voice VLAN on the port. |

show ip igmp profile

Use the **show ip igmp profile** privileged EXEC command to display the details of an Internet Group Management Protocol (IGMP) profile entry.

show ip igmp profile [*profile number*] | [{**begin** | **exclude** | **include**} *expression*]

Syntax Description

| | |
|-----------------------|--|
| <i>profile number</i> | The IGMP profile to be displayed. The range is from 1 to 4294967295. |
| 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)WC3 | This command was first introduced. |

Usage Guidelines

Use the **show ip igmp profile** command with an IGMP filter profile to display parameters for a specific IGMP profile.

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 ip igmp profile** command:

```
host1# show ip igmp profile 30
IGMP Profile 30
range 233.1.1.1 233.255.255.255
range 235.1.1.1 235.255.255.255
host1#
```

Related Commands

| Command | Description |
|--------------------------------------|--|
| ip igmp filter | Apply a specific IGMP profile to an interface. |
| ip igmp profile | Define an IGMP profile. |
| show running-config interface | Displays the running configuration on the switch, including any profiles assigned to a port. |

show mac-address-table

Use the **show mac-address-table** user EXEC command to display the MAC address table.

show mac-address-table [**static** | **dynamic** | **secure** | **self** | **aging-time** | **count**]
 [**address** *hw-addr*] [**interface** *interface*] [**atm** *slot/port*] [**vlan** *vlan-id*]

Syntax Description

| | |
|-----------------------------------|---|
| static | (Optional) Display only the static addresses. |
| dynamic | (Optional) Display only the dynamic addresses. |
| secure | (Optional) Display only the secure addresses. |
| self | (Optional) Display only addresses added by the switch itself. |
| aging-time | (Optional) Display aging-time for dynamic addresses for all VLANs. |
| count | (Optional) Display a count for different kinds of MAC addresses. |
| address <i>hw-addr</i> | (Optional) Display information for a specific address. |
| interface <i>interface</i> | (Optional) Display addresses for a specific port. |
| atm <i>slot/port</i> | (Optional) Add dynamic addresses to ATM module <i>slot/port</i> . Use 1 or 2 for the slot number. Use 0 as the port number. |
| vlan <i>vlan-id</i> | (Optional) Display addresses for a specific VLAN. Valid IDs are from 1 to 1005; do not enter leading zeroes. |

Command Modes

User EXEC

Command History

| Release | Modification |
|------------|--|
| 11.2(8)SA | This command was first introduced. |
| 11.2(8)SA3 | The self , aging-time , count , and vlan <i>vlan-id</i> keywords were added. |
| 11.2(8)SA5 | The atm <i>slot/port</i> keywords were added. |

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, then all of the conditions must be true in order for that entry to be displayed.

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 |

Related Commands

| Command | Description |
|--------------------------------|---|
| clear mac-address-table | Deletes entries from the MAC address table. |

show mac-address-table notification

Use the **show mac-address-table notification** privileged EXEC command to display the global parameters for the MAC address notification feature.

show mac-address-table notification [**interface** *interface id*] | [{**begin** | **exclude** | **include**} *expression*]

| | | |
|--------------------|--------------------------------------|--|
| Syntax Description | interface <i>interface-id</i> | (Optional) Specify a 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 Privileged EXEC

| | | |
|-----------------|----------------|--|
| Command History | Release | Modification |
| | 12.0(5)WC3 | The notification keyword was added. |

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* are not displayed, but the lines that contain *Output* are displayed.

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 Enabled on the switch
Interval between Notification Traps : 10 secs
Number of MAC Addresses Added : 18
Number of MAC Addresses Removed : 15
Number of Notifications sent to NMS : 28
Maximum Number of entries configured in History Table : 5
Current History Table Length : 5
MAC Notification Traps are Enabled
History Table contents
-----
History Index 3, Entry Timestamp 1790800, Despatch Timestamp 1790800
MAC Changed Message :
Operation: Deleted Vlan: 1      MAC Addr: 00c0.4301.101b Dot1dBasePort:16
```



```

History Index 4, Entry Timestamp 1794810, Despatch Timestamp 1794810
MAC Changed Message :
Operation: Added   Vlan: 1       MAC Addr: 00c0.4301.101b Module: 0   Port: 2

History Index 0, Entry Timestamp 1825868, Despatch Timestamp 1825868
MAC Changed Message :
Operation: Deleted Vlan: 1       MAC Addr: 00c0.4301.101b Module: 0   Port: 2

History Index 1, Entry Timestamp 1850929, Despatch Timestamp 1850929
MAC Changed Message :
Operation: Added   Vlan: 1       MAC Addr: 00c0.4301.101b Module: 0   Port: 2

History Index 2, Entry Timestamp 1880988, Despatch Timestamp 1880988
MAC Changed Message :
Operation: Deleted Vlan: 1       MAC Addr: 00c0.4301.101b Module: 0   Port: 2

```

Switch#

This is an example of output from the **show mac-address-table notification interface** command for all interfaces on a switch:

```

MAC Notification Flags For All Ethernet Interfaces :
-----
Interface          MAC Added Trap  MAC Removed Trap
-----
FastEthernet0/1    Disabled        Disabled
FastEthernet0/2    Disabled        Disabled
FastEthernet0/3    Disabled        Disabled
FastEthernet0/4    Enabled         Enabled
FastEthernet0/5    Disabled        Disabled
FastEthernet0/6    Disabled        Disabled
FastEthernet0/7    Disabled        Disabled
FastEthernet0/8    Disabled        Disabled
FastEthernet0/9    Disabled        Disabled
FastEthernet0/10   Disabled        Disabled
FastEthernet0/11   Disabled        Disabled
FastEthernet0/12   Disabled        Disabled
FastEthernet0/13   Disabled        Disabled
FastEthernet0/14   Disabled        Disabled
FastEthernet0/15   Disabled        Disabled
FastEthernet0/16   Disabled        Disabled
FastEthernet0/17   Disabled        Disabled
FastEthernet0/18   Disabled        Disabled
FastEthernet0/19   Disabled        Disabled
FastEthernet0/20   Disabled        Disabled
FastEthernet0/21   Disabled        Disabled
FastEthernet0/22   Disabled        Disabled
FastEthernet0/23   Disabled        Disabled
FastEthernet0/24   Disabled        Disabled

```

This is an example of output from the **show mac-address-table notification interface *interface-id*** command for one interface on a switch:

```

Interface          MAC Added Trap  MAC Removed Trap
-----
FastEthernet0/4    Enabled         Enabled

Switch#

```

| Related Commands | Command | Description |
|------------------|---|---|
| | clear mac-address-table notification | Clears the counters maintained by the MAC address notification feature. |
| | mac-address-table notification | Enables the MAC notification feature. |
| | snmp trap mac-notification | Enables MAC-notification traps on a 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 maximum query response time, and the multicast VLAN number.

show mvr

| | |
|--------------------|-------------------------------|
| Syntax Description | This command has no keywords. |
|--------------------|-------------------------------|

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

| Command History | Release | Modification |
|-----------------|-----------|------------------------------------|
| | 12.0(5)XW | This command was first introduced. |

| | |
|----------|---|
| Examples | This example shows how to view the MVR global parameter values: |
|----------|---|

```
Switch# show mvr
MVR Enabled
MVR multicast vlan: 2
MVR Current multicast groups: 1
MVR Global query response time: 100 (tenths of sec)
```

| Related Commands | Command | Description |
|------------------|---|---|
| | show mvr interface | Displays the configured MVR interfaces or displays the multicast groups to which a receiver port belongs. |
| | show mvr members | Displays all receiver ports that are members of an MVR multicast group. |
| | mvr (global configuration) (global configuration mode) | Enables and configures multicast VLAN registration on the switch. |
| | mvr (interface configuration) (interface configuration mode) | Configures MVR ports. |

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*]]]

Syntax Description

| | |
|----------------------------|---|
| <i>interface-id</i> | (Optional) Enter a receiver port identification to display parameters for the specified port. |
| members | (Optional) Display all MVR groups that the specified receive port is a member of. |
| vlan <i>vlan-id</i> | (Optional) Display the VLAN to which the receiver port belongs. |

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 and per port parameters, such as maximum threshold and Immediate Leave setting.

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|-----------|------------------------------------|
| 12.0(5)XW | This command was first introduced. |

Examples

This example shows how to display all MVR interfaces:

```
Switch# show mvr interface
MVR PORTS
Port: Fa0/1 Type: RECEIVER Status: ACTIVE
Port: Fa0/2 Type: RECEIVER Status: ACTIVE
Port: Fa0/3 Type: SOURCE   Status: ACTIVE
```

This example shows how to view the MVR parameters for Fast Ethernet port 0/1:

```
Switch# show mvr interface fastethernet 0/1
Interface: Fa0/1
    Threshold: 20
    Immediate Leave: Disabled
    Multicast packets received: 13
```

This example shows the response displayed when the entered port is not a receiver port:

```
Switch# show mvr fastethernet 0/3
Sorry, Cannot display parameter information for non-receiver port
```

| Related Commands | Command | Description |
|------------------|---|---|
| | 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. |
| | mvr (global configuration) (global configuration mode) | Enables and configures multicast VLAN registration on the switch. |
| | mvr (interface configuration) (interface configuration mode) | Configures MVR ports. |

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*]

| 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 are displayed. If no address is entered, all members of all MVR groups are listed. |
|--------------------|-------------------|---|
|--------------------|-------------------|---|

| Usage Guidelines | The show mvr members command only applies to receiver ports. All source ports are members of all multicast groups. |
|------------------|---|
|------------------|---|

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

| Command History | Release | Modification |
|-----------------|-----------|------------------------------------|
| | 12.0(5)XW | This command was first introduced. |

Examples This example shows how to view the members of any IP multicast group:

```
Switch# show mvr members
MVR Group IP:239.255.0.1
      Vlan 2 Interface:Fa0/16 DYNAMIC ACTIVE
      Vlan 2 Interface:Fa0/17 DYNAMIC ACTIVE

MVR Group IP:239.255.0.2
      Vlan 2 Interface:Fa0/15 DYNAMIC ACTIVE
      Vlan 2 Interface:Fa0/17 DYNAMIC ACTIVE
      Vlan 2 Interface:Fa0/20 DYNAMIC ACTIVE

MVR Group IP:239.255.0.3
      Vlan 2 Interface:Fa0/23 DYNAMIC ACTIVE
      Vlan 2 Interface:Fa0/16 DYNAMIC ACTIVE

MVR Group IP:239.255.0.4
      Vlan 2 Interface:Fa0/26 DYNAMIC ACTIVE
      Vlan 2 Interface:Fa0/16 DYNAMIC ACTIVE
      Vlan 2 Interface:Fa0/23 DYNAMIC ACTIVE

MVR Group IP:239.255.0.5
      Vlan 2 Interface:Fa0/15 DYNAMIC ACTIVE
      Vlan 2 Interface:Fa0/14 DYNAMIC ACTIVE

MVR Group IP:239.255.0.6
      Vlan 2 Interface:Fa0/17 DYNAMIC ACTIVE
      Vlan 2 Interface:Fa0/18 DYNAMIC ACTIVE
      Vlan 2 Interface:Fa0/20 DYNAMIC ACTIVE
      Vlan 2 Interface:Fa0/23 DYNAMIC ACTIVE
      Vlan 2 Interface:Fa0/15 DYNAMIC ACTIVE
```

This example shows how to view the members of the IP multicast group 239.255.0.4:

```
Switch# show mvr members 239.255.0.4
MVR Group IP:239.255.0.4
      Vlan 2 Interface:Fa0/26 DYNAMIC ACTIVE
      Vlan 2 Interface:Fa0/16 DYNAMIC ACTIVE
      Vlan 2 Interface:Fa0/23 DYNAMIC ACTIVE
```

| Related Commands | Command | Description |
|------------------|---|---|
| | show mvr | Displays the global MVR configuration on the switch. |
| | show mvr interface | Displays the configured MVR interfaces or displays the multicast groups to which a receiver port belongs. |
| | mvr (global configuration) (global configuration mode) | Enables and configures multicast VLAN registration on the switch. |
| | mvr (interface configuration) (interface configuration mode) | Configures MVR ports. |

show port block

Use the **show port block** privileged EXEC command to display the blocking of unicast or multicast flooding to a port.

show port block {**unicast** | **multicast**} [*interface-id* / **vlan number**]

| | | |
|--------------------|---------------------|---|
| Syntax Description | unicast | Display whether or not ports are blocking unicast packets. |
| | multicast | Display whether or not ports are blocking multicast packets. |
| | <i>interface-id</i> | (Optional) ID of the module and port. |
| | vlan number | (Optional) VLAN number from 1 to 1000. Do not enter leading zeroes. |

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

| | | |
|-----------------|----------------|------------------------------------|
| Command History | Release | Modification |
| | 11.2(8)SA | This command was first introduced. |

| | |
|------------------|---|
| Usage Guidelines | If the variable <i>interface</i> is omitted, the show port block unicast and show port block multicast commands display packet blocking information on all ports. |
|------------------|---|

| | |
|----------|---|
| Examples | This is an example of output from the show port block command: |
|----------|---|

```
Switch# show port block unicast fa0/8
```

```
FastEthernet0/8 is blocked from unknown unicast addresses
```

| | | |
|------------------|-------------------|--|
| Related Commands | Command | Description |
| | port block | Blocks the flooding of unknown unicast or multicast packets to a port. |

show port group

Use the **show port group** privileged EXEC command to display the ports that belong to a port group.

show port group [*group-number*]

| | | |
|--------------------|--|---|
| Syntax Description | <i>group-number</i> (Optional) Port group to which the port is assigned. | |
| Command Modes | Privileged EXEC | |
| Command History | Release | Modification |
| | 11.2(8)SA3 | This command was first introduced. |
| Usage Guidelines | If the variable <i>group-number</i> is omitted, the show port group command displays all port groups on the switch. | |
| Examples | This is an example of output from the show port group command: | |
| | <pre>Switch# show port group 1 Group Interface ----- - 1 FastEthernet0/1 1 FastEthernet0/4</pre> | |
| Related Commands | Command | Description |
| | port group | Assigns a port to a Fast EtherChannel or Gigabit EtherChannel port group. |

show port monitor

Use the **show port monitor** privileged EXEC command to display the ports for which Switched Port Analyzer (SPAN) port monitoring is enabled.

show port monitor [*interface-id* / **vlan** *number*]

| | | |
|--------------------|---------------------------|---|
| Syntax Description | <i>interface-id</i> | (Optional) ID of the module and port enabled for SPAN. |
| | vlan <i>number</i> | (Optional) VLAN number from 1 to 1000. Do not enter leading zeroes. |

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

| Command History | Release | Modification |
|-----------------|-----------|------------------------------------|
| | 11.2(8)SA | This command was first introduced. |

| | |
|------------------|---|
| Usage Guidelines | If the variable <i>interface</i> is omitted, the show port monitor command displays all monitor ports on the switch. |
|------------------|---|

Examples This is an example of output from the **show port monitor** command:

```
Switch# show port monitor fa0/8
```

```

Monitor Port      Port Being Monitored
-----
FastEthernet0/8   FastEthernet0/1
FastEthernet0/8   FastEthernet0/2
FastEthernet0/8   FastEthernet0/3
FastEthernet0/8   FastEthernet0/4
```

| Related Commands | Command | Description |
|------------------|---------------------|---|
| | port monitor | Enables SPAN port monitoring on a port. |

show port network

Use the **show port network** privileged EXEC command to display the network port defined for the switch or VLAN.

show port network [*interface-id* / **vlan** *number*]

Syntax Description

| | |
|---------------------------|---|
| <i>interface-id</i> | (Optional) ID of the module and port. |
| vlan <i>number</i> | (Optional) VLAN number from 1 to 1000. Do not enter leading zeroes. |

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|------------|------------------------------------|
| 11.2(8)SA4 | This command was first introduced. |

Usage Guidelines

If the variable *interface* is omitted, the **show port network** command displays all network ports on the switch.

Examples

This is an example of output from the **show port network** command:

```
Switch# show port network

Network Port      VLAN ID
-----
FastEthernet0/11  1
```

Related Commands

| Command | Description |
|---------------------|--|
| port network | Defines a port as the switch network port. All traffic with unknown unicast addresses is forwarded to the network port on the same VLAN. |

show port protected

Use the **show port protected** privileged EXEC command to display the port protected mode for all ports.

show port protected

| | |
|---------------------------|--|
| Syntax Description | This command has no keywords or options. |
|---------------------------|--|

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

| | | |
|------------------------|----------------|------------------------------------|
| Command History | Release | Modification |
| | 12.0(5)XU | This command was first introduced. |

| | |
|-----------------|---|
| Examples | This is an example of output from the show port protected command: |
|-----------------|---|

```
Switch# show port protected
```

```
FastEthernet0/3 is in protected mode  
GigabitEthernet1/1 is in protected mode
```

| | | |
|-------------------------|-----------------------|--|
| Related Commands | Command | Description |
| | port protected | Isolates unicast, multicast, and broadcast traffic at Layer 2 from other protected ports on the same switch. |

show port security

Use the **show port security** privileged EXEC command to display the port security settings defined for the port.

show port security [*interface-id* / **vlan number**]

| | | |
|--------------------|---------------------|---|
| Syntax Description | <i>interface-id</i> | (Optional) ID of the module and port. |
| | vlan number | (Optional) VLAN number from 1 to 1000. Do not enter leading zeroes. |

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

| Command History | Release | Modification |
|-----------------|-----------|------------------------------------|
| | 11.2(8)SA | This command was first introduced. |

| | |
|------------------|---|
| Usage Guidelines | If the variable <i>interface</i> is omitted, the show port security command displays all secure ports on the switch. |
|------------------|---|

Examples This is an example of output from the **show port security** command for fixed port 07:

Switch# **show port security fa0/7**

| Secure Port | Secure Addr Cnt (Current) | Secure Addr Cnt (Max) | Security Reject Cnt | Security Action |
|-----------------|------------------------------|--------------------------|------------------------|-----------------|
| FastEthernet0/7 | 0 | 132 | 0 | Send Trap |

| Related Commands | Command | Description |
|------------------|----------------------|----------------------------------|
| | port security | Enables port security on a port. |

show port storm-control

Use the **show port storm-control** privileged 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 port storm-control [*interface*] [{**broadcast** | **multicast** | **unicast** | **history**}]

| | | |
|--------------------|------------------|---|
| Syntax Description | <i>interface</i> | (Optional) Port for which information is to be displayed. |
| | broadcast | (Optional) Display broadcast storm information. |
| | multicast | (Optional) Display multicast storm information. |
| | unicast | (Optional) Display unicast storm information. |
| | history | (Optional) Display storm history on a per-port basis. |

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

| | | |
|-----------------|-----------|--|
| Command History | Release | Modification |
| | 11.2(8)SA | This command was first introduced. |
| | 12.0(5)XU | The broadcast , multicast , unicast , and history keywords were added. |

| | |
|------------------|---|
| Usage Guidelines | If the variable <i>interface</i> is omitted, the show port storm-control command displays storm control settings on all ports on the switch. |
| | You can display broadcast, multicast, or unicast packet-storm information by using the corresponding keyword. |

| | |
|----------|---|
| Examples | This is an example of output from the show port storm-control command: |
|----------|---|

Switch# **show port storm-control**

| Interface | Filter State | Trap State | Rising | Falling | Current | Traps Sent |
|-----------|--------------|------------|--------|---------|---------|------------|
| Fa0/1 | <inactive> | <inactive> | 1000 | 200 | 0 | 0 |
| Fa0/2 | <inactive> | <inactive> | 500 | 250 | 0 | 0 |
| Fa0/3 | <inactive> | <inactive> | 500 | 250 | 0 | 0 |
| Fa0/4 | <inactive> | <inactive> | 500 | 250 | 0 | 0 |

| | | |
|------------------|---------------------------|---|
| Related Commands | Command | Description |
| | port storm-control | Enables broadcast, multicast, or unicast storm control on a port. |

show power inline

Use the **show power inline** privileged EXEC command to display the power status for the specified port or for all ports on the 3524-PWR-XL switch.

show power inline [*interface-id*] [**actual** | **configured**]

| Syntax Description | <i>interface-id</i> | (Optional) ID of the module and port. |
|--------------------|---------------------|---|
| | actual | (Optional) Display the current power status, which might not be the same as the configured power. |
| | configured | (Optional) Display the configured power status. |

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

| Command History | Release | Modification |
|-----------------|-----------|------------------------------------|
| | 12.0(5)XU | This command was first introduced. |

Examples This is an example of output from the **show power inline fa0/4 actual** command:

```
Switch# show power inline fa0/4 actual
Interface           Power
-----
FastEthernet0/4    no
```

| Related Commands | Command | Description |
|------------------|---------------------|--|
| | power inline | Determines how inline power is applied to devices on the specified Fast Ethernet port of the 3524-PWR-XL switch. |

show proposed

Use the **show proposed** VLAN database command to display the proposed VLAN database or a selected VLAN from it.

show proposed [*vlan-id*]

| | | |
|---------------------------|----------------|---|
| Syntax Description | <i>vlan-id</i> | (Optional) ID of the VLAN in the proposed database. If this variable is omitted, the entire VLAN database displays, included the pruning state and Version 2 mode. Valid IDs are from 1 to 1005; do not enter leading zeroes. |
|---------------------------|----------------|---|

| | |
|----------------------|---------------|
| Command Modes | VLAN database |
|----------------------|---------------|

| | | |
|------------------------|----------------|------------------------------------|
| Command History | Release | Modification |
| | 11.2(8)SA4 | This command was first introduced. |

| | |
|-------------------------|--|
| Usage Guidelines | <p>If the variable <i>vlan-id</i> is omitted, the show proposed command displays the entire proposed VLAN database.</p> <p>The proposed VLAN database is not the running configuration until you use the exit or apply command.</p> |
|-------------------------|--|

| | |
|-----------------|---|
| Examples | This is an example of output from the show proposed command: |
|-----------------|---|

```
Switch(vlan)# show proposed
```

```
VLAN ISL Id: 1
  Name: default
  Media Type: Ethernet
  VLAN 802.10 Id: 100001
  State: Operational
  MTU: 1500
  Translational Bridged VLAN: 1002
  Translational Bridged VLAN: 1003
```

```
VLAN ISL Id: 2
  Name: VLAN0002
  Media Type: FDDI Net
  VLAN 802.10 Id: 100002
  State: Operational
  MTU: 1500
  STP Type: IBM
```

```
VLAN ISL Id: 1002
  Name: fddi-default
  Media Type: FDDI
  VLAN 802.10 Id: 101002
  State: Operational
  MTU: 1500
  Bridge Type: SRB
  Translational Bridged VLAN: 1
  Translational Bridged VLAN: 1003
```



```
VLAN ISL Id: 1003
  Name: trcrf-default
  Media Type: TRCRF
  VLAN 802.10 Id: 101003
  State: Operational
  MTU: 4472
  Bridge Type: SRB
  Ring Number: 3276
  Bridge Number: 1
  Parent VLAN: 1005
  Maximum ARE Hop Count: 7
  Maximum STE Hop Count: 7
  Backup CRF Mode: Disabled
  Translational Bridged VLAN: 1
  Translational Bridged VLAN: 1002

VLAN ISL Id: 1004
  Name: fddinet-default
  Media Type: FDDI Net
  VLAN 802.10 Id: 101004
  State: Operational
  MTU: 1500
  Bridge Type: SRB
  Bridge Number: 1
  STP Type: IBM

VLAN ISL Id: 1005
  Name: trbrf-default
  Media Type: TRBRF
  VLAN 802.10 Id: 101005
  State: Operational
  MTU: 4472
  Bridge Type: SRB
  Bridge Number: 15
  STP Type: IBM
```

| Related Commands | Command | Description |
|------------------|---------------------|--|
| | show changes | Displays the differences between the VLAN database currently on the switch and the proposed VLAN database. |
| | show current | Displays the VLAN database on the switch or a selected VLAN from it. |

show rps

Use the **show rps** user EXEC command to display the status of the Cisco Redundant Power System (RPS).

show rps

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC

| Command History | Release | Modification |
|-----------------|-----------|------------------------------------|
| | 12.0(5)XU | This command was first introduced. |

Examples This is an example of output from the **show rps** command. Table 2-2 describes the possible display output.

```
Switch> show rps
ACTIVATED
```

Table 2-2 Show RPS Display Output Description

| Display | Description | Switch RPS LED Color |
|---|--|--|
| NA | The RPS is off or not installed. | Off (all switch and RPS models) |
| ACTIVATED | The internal power supply of the switch is down. The switch is operating through the RPS. | Blinking amber (3524-PWR switch connected to RPS 300) Solid green (all Catalyst 2900 XL and Catalyst 3500 XL switches, except the 3524-PWR, connected to the Cisco RPS) |
| DEACTIVATED | The RPS is connected, operational, and in standby mode. The switch is operating from its own internal power supply. | Solid green (3524-PWR switch connected to RPS 300) Blinking green (all Catalyst 2900 XL and Catalyst 3500 XL switches, except the 3524-PWR, connected to the Cisco RPS) |
| FAULTY | The RPS is connected but not operating correctly (faulty). One of the power supplies in the RPS could be powered down or a fan on the RPS could have failed. | Solid amber (all switch and RPS models) |
| NOT AVAILABLE (only for 3524-PWR switch) | The RPS is backing up another switch; power redundancy is lost. | Blinking green (3524-PWR switch connected to RPS 300) |

show spanning-tree

Use the **show spanning-tree** user EXEC command to display spanning-tree information for the specified spanning-tree instances.

show spanning-tree [**brief**] | [**summary**] | [**vlan** *stp-list*] | [**interface** *interface-list*]

| Syntax Description | | |
|--|--|---|
| brief | | Display a brief status of the spanning tree. |
| summary | | Display a summary of the spanning-tree states. |
| vlan <i>stp-list</i> | | (Optional) List of spanning-tree instances. Each spanning-tree instance is associated with a VLAN ID. Enter each VLAN ID separated by a space. Valid IDs are from 1 to 1005; do not enter leading zeroes. Ranges are not supported. |
| interface <i>interface-list</i> | | List of ports for which spanning-tree information appears. Enter each port separated by a space. Ranges are not supported. |

Command Modes User EXEC

| Command History | Release | Modification |
|-----------------|------------|--|
| | 11.2(8)SA3 | This command was first introduced. |
| | 12.0(5)XW | The brief and summary keywords were added. |

Usage Guidelines If the variable *stp-list* is omitted, the command applies to the spanning-tree instance associated with VLAN 1.

Examples This is an example of output from the **show spanning-tree** command for VLAN 1:

```
Switch> show spanning-tree vlan 1
Spanning tree 1 is executing the IEEE compatible Spanning Tree protocol
Bridge Identifier has priority 49152, address 00b0.6476.08c0
Configured hello time 2, max age 20, forward delay 15
Current root has priority 32768, address 0001.42cd.a200
Root port is 31, cost of root path is 42
Topology change flag not set, detected flag not set, changes 1
Times: hold 1, topology change 35, notification 2
       hello 2, max age 20, forward delay 15
Timers: hello 0, topology change 0, notification 0
Fast uplink switchover is enabled
Stack port is GigabitEthernet0/1

Interface Fa0/1 (port 13) in Spanning tree 1 is down
Port path cost 3100, Port priority 128
Designated root has priority 32768, address 0001.42cd.a200
Designated bridge has priority 49152, address 00b0.6476.08c0
Designated port is 13, path cost 42
Timers: message age 0, forward delay 0, hold 0
BPDU: sent 0, received 0
<output truncated>
```

This is an example of output from the **show spanning-tree interface** command for port 3:

```
Switch> show spanning-tree interface fa0/3
```

```
Interface Fa0/3 (port 3) in Spanning tree 1 is down
  Port path cost 100, Port priority 128
  Designated root has priority 6000, address 0090.2bba.7a40
  Designated bridge has priority 32768, address 00e0.1e9f.4abf
  Designated port is 3, path cost 410
  Timers: message age 0, forward delay 0, hold 0
  BPDU: sent 0, received 0
```

This is an example of output from the **show spanning-tree summary** command:

```
Switch> show spanning-tree summary
```

```
UplinkFast is enabled
```

```
Stack port is GigabitEthernet0/1
```

| 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>

Related Commands

| Command | Description |
|------------------------------------|--|
| spanning-tree | Enables STP on a VLAN. |
| spanning-tree forward-time | Specifies the forwarding-time for the specified spanning-tree instances. |
| spanning-tree max-age | Changes the interval between messages that the spanning tree receives from the root switch. |
| spanning-tree port-priority | Configures a port priority, which is used when two switches tie for position as the root switch. |
| spanning-tree protocol | Specifies the STP version to be used for specified spanning-tree instances. |

show tacacs

Use the **show tacacs** user EXEC command to display various Terminal Access Controller Access Control System Plus (TACACS+) server statistics.

show tacacs

| | |
|---------------------------|--------------------------------|
| Syntax Description | This command has no arguments. |
|---------------------------|--------------------------------|

| | |
|----------------------|-----------|
| Command Modes | User EXEC |
|----------------------|-----------|

| | | |
|------------------------|----------------|------------------------------------|
| Command History | Release | Modification |
| | 11.2(8)SA6 | This command was first introduced. |

| | |
|-----------------|---|
| Examples | This is an example of output from the show tacacs command: |
|-----------------|---|

```
Switch> show tacacs
```

```
Server:172.20.128.113/49:opens=4 closes=4 aborts=0 errors=0
      packets in=6 packets out=6
      no connection
```

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*]

| | | |
|--------------------|---------------------|--|
| Syntax Description | <i>interface-id</i> | (Optional) ID of the module and port or a VLAN ID. Valid IDs are from 1 to 1000. |
|--------------------|---------------------|--|

| | |
|---------------|-----------|
| Command Modes | User EXEC |
|---------------|-----------|

| | | |
|-----------------|-----------|------------------------------------|
| Command History | Release | Modification |
| | 12.0(5)XU | This command was first introduced. |

Examples This is an example of output from the **show udld fa0/11** command. In this display, UDLD is enabled on both ends of the link, and UDLD detects that the link is bidirectional. Table 2-3 describes the fields in this display.

```
Switch> show udld fa0/11
Interface Fa0/11
Port enable configuration setting: Follows global setting
Operational enable state: Enabled
Current bidirectional state: Bidirectional
Message interval: 60
Message timer: 38
Current operational state: Advertisement
Time out interval: 5
Time out timer: 0
Restart counter: 0
Neighbors counter: 1
Probe counter: 0
No multiple neighbors detected
Current pool id: 1
---
Cache entry 1 (0x69D8E4)
Device name: aunguyen-1.cisco.com
Device MAC address: 00:E0:1E:9F:85:80
Port ID: Fa1/1
Expiration time: 159
Cache device ID: 1
Resynch flag clear
Current neighbor state: Bidirectional
Most recent message type received: Probe
Message interval: 5
    Neighbor echo 1 device: 00:50:0F:08:A4:00
    Neighbor echo 1 port: Fa0/11
```

Table 2-3 Show UDLD Field Descriptions

| Field | Description |
|-----------------------------------|--|
| Interface | The interface on the local device configured for UDLD. |
| Port enable configuration setting | How UDLD is configured on the port. If UDLD is enabled or disabled, the port enable configuration setting is the same as operational enable state. Otherwise, the enable operational setting depends on the global enable setting. |
| Operational enable state | Operational state that indicates 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. |
| Message interval | How often advertisement messages are sent from the local device. Measured in seconds. |
| Message timer | The length of time before the next advertisement is sent from the local device. Measured in seconds. |
| Current operational state | The current phase of the UDLD state machine. For a normal bidirectional link, the state machine is usually in the Advertisement phase. |
| Time out interval | The time period, in seconds, that UDLD waits for echoes from a neighbor device during the detection window. |
| Time out timer | The remaining time in seconds in the detection window. This setting is meaningful only if UDLD is in the detection phase. |
| Restart counter | The number of times UDLD sends probe messages in the detection phase. |
| Neighbors counter | The number of neighbors detected. For point-to-point links, this value should always be one. It is greater than one only when the port is connected to a hub. |
| Probe counter | The remaining number of probe messages to send in the detection window. This setting is meaningful only if UDLD is in the detection phase. |
| Current pool id | An internal index number on the local device. |
| Cache entry 1 | Information from the first cache entry, which contains a copy of echo information received from the neighbor. |
| Device name | The neighbor device name. |
| Device MAC address | The neighbor MAC address. |
| Port ID | The neighbor port ID enabled for UDLD. |
| Expiration time | The amount of time in seconds remaining before this cache entry is aged out. |
| Cache device ID | The ID of the cache device. |
| Resynch flag clear | There are no outstanding requests from neighbors to resynchronize cache data. |

Table 2-3 Show UDLD Field Descriptions (continued)

| Field | Description |
|-----------------------------------|--|
| Current neighbor state | The neighbor's current state. If both the local and neighbor devices are running UDLD normally, the neighbor state and local state should be bidirectional. If the link is down or the neighbor is not UDLD-capable, no cache entries are displayed. |
| Most recent message type received | The type of message received from the neighbor. |
| Message interval | The rate, in seconds, at which the neighbor is sending advertisement messages. |
| Neighbor echo 1 device | The MAC address of the neighbors neighbor from which the echo originated. |
| Neighbor echo 1 port | The port ID of the neighbor from which the echo originated. |

Related Commands

| Command | Description |
|--------------------|---|
| udld | Enables UDLD on a port. |
| udld enable | Enables UDLD on all ports on the switch. |
| udld reset | Resets any interface that has been shut down by UDLD. |

show version

Use the **show version** user EXEC command to display version information for the hardware and firmware.

show version

| | |
|---------------------------|-------------------------------|
| Syntax Description | The command has no arguments. |
|---------------------------|-------------------------------|

| | |
|----------------------|-----------|
| Command Modes | User EXEC |
|----------------------|-----------|

| | | |
|------------------------|----------------|------------------------------------|
| Command History | Release | Modification |
| | 11.2(8)SA | This command was first introduced. |

| | |
|-----------------|--|
| Examples | This is an example of output from the show version command: |
|-----------------|--|

```
Switch> show version
```

```
Cisco Internetwork Operating System Technology Software
IOS Technology(tm) C3500XL Software (C3500XL-C3H2S-M), Version 12.0
Copyright (c) 1986-1998 by cisco Systems, Inc.
Compiled Mon 22-Nov-99 10:51 by mollyn
Image text-base: 0x00003000, data-base: 0x0031B6B4
```

```
ROM: Bootstrap program is C3500XL boot loader
```

```
Switch uptime is 1 hour, 32 minutes
System returned to ROM by reload
System image file is "flash:c3500XL-c3h2s-mz-120.0.0.29-XU.bin"
```

```
cisco WS-C3524-XL (PowerPC403) processor (revision 0x01) with 8192K/1024K bytes
of memory.
Processor board ID 0x12, with hardware revision 0x00
Last reset from warm-reset
```

```
Processor is running Enterprise Edition Software
Cluster command switch capable
Cluster member switch capable
24 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:D0:79:6D:2F:00
Motherboard assembly number: 73-3904-08
Power supply part number: 34-0851-02
Motherboard serial number: FAA03269NLK
Power supply serial number: PHI031200D2
Model revision number: A0
Model number: WS-C3524-XL-A
System serial number: FAA0328K01G
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) in the administrative domain.

show vlan [**brief** | **id** *vlan-id* / **name** *vlan-name*]

| | | |
|--------------------|------------------------------|--|
| Syntax Description | brief | (Optional) Display one line for each VLAN with the VLAN name, status, and its ports |
| | id <i>vlan-id</i> | (Optional) ID of the VLAN displayed. Valid IDs are from 1 to 1005; do not enter leading zeroes. |
| | name <i>vlan-name</i> | (Optional) Name of the VLAN displayed. The VLAN name is an ASCII string from 1 to 32 characters. |

| | |
|---------------|-----------|
| Command Modes | User EXEC |
|---------------|-----------|

| | | |
|-----------------|----------------|---|
| Command History | Release | Modification |
| | 11.2(8)SA3 | This command was first introduced. |
| | 11.2(8)SA4 | The name <i>vlan-name</i> keywords were added. |

Examples This is an example of output from the **show vlan** command:

```
Switch> show vlan
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,
                                   Fa0/13, Fa0/14, Fa0/15, Fa0/16,
                                   Fa0/17, Fa0/18, Fa0/19, Fa0/20,
                                   Fa0/21, Fa0/22, Fa0/23, Fa0/24,
                                   Gi0/1, Gi0/2
1002 fddi-default          active
1003 token-ring-default    active
1004 fddinet-default       active
1005 trnet-default         active

VLAN Type  SAID      MTU    Parent RingNo BridgeNo  Stp    Trans1  Trans2
-----
1    enet   100001    1500   -       -       -        -     1002    1003
6    fdnet  100006    1500   -       -       -        ieee  0       0
7    trnet  100007    1500   -       -       5        ieee  0       0
1002 fddi   101002    1500   -       -       -        -     1       1003
1003 tr    101003    1500   1005   3276    -        -     1       1002
1004 fdnet  101004    1500   -       -       1        ibm   0       0
1005 trnet  101005    1500   -       -       15       ibm   0       0
```

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, Fa0/5, Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa1/1, Fa1/2, Fa1/3, Fa1/4, Fa2/3, Fa2/4 |
| 2 | VLAN0002 | active | |
| 3 | VLAN0003 | active | |
| 6 | VLAN0006 | active | |
| 7 | VLAN0007 | active | |
| 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 6** or **show vlan name VLAN006** command:

```
Switch> show vlan id 6
```

| VLAN | Name | Status | Ports |
|------|----------|--------|-------|
| 6 | VLAN0006 | active | |

| VLAN | Type | SAID | MTU | Parent | RingNo | BridgeNo | Stp | Trans1 | Trans2 |
|------|-------|--------|------|--------|--------|----------|------|--------|--------|
| 6 | fdnet | 100006 | 1500 | - | - | - | ieee | 0 | 0 |

Related Commands

| Command | Description |
|------------------------|--|
| switchport mode | Configures the VLAN membership mode of a port. |
| vlan | Configures VLAN characteristics. |

show vmps

Use the **show vmps** user EXEC command to display the VLAN Query Protocol (VQP) version, the reconfirmation interval, the retry count, the VLAN Membership Policy Server (VMPS) IP addresses, and the current and primary servers.

show vmps

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC

| Command History | Release | Modification |
|-----------------|------------|------------------------------------|
| | 11.2(8)SA4 | This command was first introduced. |

Examples This is an example of output from the **show vmps** command:

```
Switch> show vmps

VQP Client Status:
-----
VMPS VQP Version: 1
Reconfirm Interval: 60 min
Server Retry Count: 3
VMPS domain server: 172.20.128.86 (primary, current)
                   172.20.128.87

Reconfirmation status
-----
VMPS Action:          No Dynamic Port
```

| Related Commands | Command | Description |
|------------------|--|--|
| | vmps reconfirm (privileged EXEC) | Sends VQP queries to reconfirm all dynamic VLAN assignments with the VMPS. |
| | and | |
| | vmps reconfirm (global Configuration) | |
| | 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 vmps statistics

Use the **show vmps statistics** privileged EXEC command to display the VLAN Query Protocol (VQP) client-side statistics and counters.

show vmps statistics

| | |
|---------------------------|--|
| Syntax Description | This command has no arguments or keywords. |
|---------------------------|--|

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

| | | |
|------------------------|----------------|------------------------------------|
| Command History | Release | Modification |
| | 11.2(8)SA4 | This command was first introduced. |

| | |
|-----------------|---|
| Examples | This is an example of output from the show vmps statistics command. Table 2-4 describes each field in the display. |
|-----------------|---|

```
Switch# show vmps statistics
```

```
VMPS Client Statistics
-----
VQP  Queries:           0
VQP  Responses:         0
VMPs  Changes:          0
VQP  Shutdowns:         0
VQP  Denied:            0
VQP  Wrong Domain:      0
VQP  Wrong Version:     0
VQP  Insufficient Resource: 0
```

Table 2-4 Show VMPS Statistics Field Descriptions

| Field | Description |
|---------------------------|---|
| VQP Queries | Number of queries sent by the client to the VLAN Membership Policy Server (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 that 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 re-enable the port to restore connectivity. |
| VQP Denied | Number of times that the VMPS denied the client request for security reasons. When the VMPS response is to deny 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 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 that 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 that 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 switch sends only VMPS version 1 requests. |
| VQP Insufficient Resource | Number of times that 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 vmmps statistics | Clears the statistics maintained by the VQP client. |

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}

| | | |
|--------------------|-----------------|--|
| Syntax Description | counters | Display the VTP counters for the switch. |
| | status | Display general information about the VTP management domain. |

| | |
|---------------|-----------|
| Command Modes | User EXEC |
|---------------|-----------|

| | | |
|-----------------|----------------|------------------------------------|
| Command History | Release | Modification |
| | 11.2(8)SA4 | This command was first introduced. |

Examples This is an example of output from the **show vtp counters** command. Table 2-5 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 |

Table 2-5 *Show VTP Counters Field Descriptions*

| Field | Description |
|--------------------------------------|--|
| Summary Advts 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 Advts 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 Advts 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 Advts 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 Advts 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 Advts 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. |
| No. 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 2-5 Show VTP Counters Field Descriptions (continued)

| Field | Description |
|--|---|
| No. of Configuration Digest Errors | <p>Number of MD5 digest errors.</p> <p>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 that the VTP password on all switches is the same.</p> <p>These errors mean that the switch is filtering incoming advertisements, which causes the VTP database to become unsynchronized across the network.</p> |
| No. of V1 Summary Errors | <p>Number of version 1 errors.</p> <p>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.</p> |
| Join Transmitted | Number of VTP pruning messages transmitted 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 2-6 describes each field in the display.

```
Switch> show vtp status
```

```

VTP Version           : 2
Configuration Revision : 1
Maximum VLANs supported locally : 68
Number of existing VLANs : 7
VTP Operating Mode     : Server
VTP Domain Name        : test1
VTP Pruning Mode       : Disabled
VTP V2 Mode            : Disabled
VTP Traps Generation   : Disabled
MD5 digest             : 0x3D 0x02 0xD4 0x3A 0xC4 0x46 0xA1 0x03
Configuration last modified by 172.20.130.52 at 3-4-93 22:25:

```

Table 2-6 Show VTP Status Field Descriptions

| Field | Description |
|---------------------------------|--|
| VTP Version | Displays the VTP version operating on the switch. By default, Catalyst 2900 XL and Catalyst 3500 XL switches implement version 1 but can be set to version 2. |
| Configuration Revision | Configuration revision number on this switch. |
| Maximum VLANs Supported Locally | Maximum number of VLANs supported locally. |
| Number of Existing VLANs | Number of existing VLANs. |
| 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 VTP database from nonvolatile storage after reboot. By default, every switch is a VTP server.</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 transmit 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 transmit 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. The configuration of multi-VLAN ports causes the switch to automatically enter transparent mode.</p> <p>Note Catalyst 2912MF, 2924M, and Catalyst 3500 XL switches support up to 250 VLANs. All other Catalyst 2900 XL switches support up to 64 VLANs. If you define more than 250 or 64 or if the switch receives an advertisement that contains more than 250 or 64 VLANs, the switch automatically enters VTP transparent mode and operates with the VLAN configuration preceding the one that sent it into transparent mode.</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. |

Table 2-6 Show VTP Status Field Descriptions (continued)

| Field | Description |
|-----------------------------|---|
| VTP Traps Generation | Displays whether VTP traps are transmitted 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 | Configures the VTP mode. |

shutdown

Use the **shutdown** interface configuration command to disable a port and to shut down the management VLAN. Use the **no** form of this command to restart 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 |
|-----------------|-----------|--|
| | 11.2(8)SA | This command was first introduced. |
| | 12.0(5)XP | Command functionality extended to the management VLAN interface. |

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, the active management VLAN interface is the one with the **shutdown** command displayed.

Examples These examples show how to disable fixed port fa0/8 and how to re-enable it:

```
Switch(config)# interface fa0/8
Switch(config-if)# shutdown
```

```
Switch(config-if)# no shutdown
```

You can verify the previous commands by entering the **show interface** user EXEC command.

| Related Commands | Command | Description |
|------------------|-------------------|---|
| | management | Shuts down the current management VLAN interface and enables the new management VLAN interface. |

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, excluding VLANs defined as default VLANs under the VLAN Trunking Protocol (VTP). The default VLANs are 1 and 1002 to 1005. Do not enter leading zeroes. |
| Defaults | No default is defined. | |
| Command Modes | Global configuration | |
| Command History | Release | Modification |
| | 11.2(8)SA4 | This command was first introduced. |
| Usage Guidelines | The shutdown vlan command does not change the VLAN information in VTP database. It shuts down traffic locally, but the switch still advertises VTP information. | |
| Examples | <p>This example shows how to shutdown traffic on VLAN 2:</p> <pre>Switch(config)# shutdown vlan 2</pre> <p>You can verify the previous command by entering the show vlan user EXEC command.</p> | |
| Related Commands | Command | Description |
| | abort | Abandons the proposed VLAN database, exits VLAN database mode, and returns to privileged EXEC mode. |
| | apply | Implements the proposed VLAN database, increments the database configuration revision number, propagates it throughout the administrative domain, and remains in VLAN database mode. |
| | exit | Implements the proposed VLAN database, increments the database configuration number, propagates it throughout the administrative domain, and returns to privileged EXEC mode. |

| Command | Description |
|----------------------|---|
| reset | Abandons the proposed VLAN database and remains in VLAN database mode. Resets the proposed database to the currently implemented VLAN database on the switch. |
| vlan database | Enters VLAN database mode from the command-line interface (CLI). |

snmp-server enable traps mac-notification

Use the **snmp-server enable traps mac-notification** global configuration command to enable Simple Network Management Protocol (SNMP) traps used by the MAC address notification feature. Use the **no** form of this command to disable SNMP MAC address traps.

snmp-server enable traps mac-notification

no snmp-server enable traps mac-notification

Syntax Description This command has no arguments or keywords.

Defaults SNMP traps for the MAC notification feature are disabled.

Command Modes Global configuration

| Command History | Release | Modification |
|-----------------|--------------|------------------------------------|
| | 12.0(5)WC(3) | This command was first introduced. |

Usage Guidelines Traps are generated only when these conditions are met:

- The MAC address notification feature is enabled.
- The appropriate interface flag for address addition or deletion is enabled.
- Global MAC notification traps are enabled.

Examples This example shows how to enable SNMP traps used by the MAC address notification feature:

```
Switch(config)# snmp-server enable trap traps notification
```

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

| Related Commands | Command | Description |
|------------------|---------------------------------------|--|
| | mac-address-table notification | Enables the MAC address notification feature. |
| | show running-config | Displays the running configuration on the switch. |
| | snmp-server host | Specifies the host that receives SNMP traps. |
| | snmp trap mac-notification | Enables or disables MAC notification traps on a specific port. |

snmp-server enable traps vlan-membership

Use the **snmp-server enable traps vlan-membership** global configuration command to enable Simple Network Management Protocol (SNMP) notification for VLAN Membership Policy Server (VMPS) changes. Use the **no** form of this command to disable the VMPS trap notification.

snmp-server enable traps vlan-membership

no snmp-server enable traps vlan-membership

Syntax Description

This command has no arguments or keywords.

Defaults

SNMP traps for VMPS are disabled.

Command Modes

Global configuration

Command History

| Release | Modification |
|------------|------------------------------------|
| 11.2(8)SA4 | This command was first introduced. |

Usage Guidelines

Specify the host that receives the traps by using the **snmp-server host** global configuration command.

Examples

This example shows how to enable VMPS to send trap notifications:

```
Switch(config)# snmp-server enable trap vlan-membership
```

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

Related Commands

| Command | Description |
|----------------------------|---|
| show running-config | Displays the running configuration on the switch. |
| snmp-server host | Specifies the host that receives SNMP traps. |

snmp-server enable traps vtp

Use the **snmp-server enable traps vtp** global configuration command to enable Simple Network Management Protocol (SNMP) notification for VLAN Trunking Protocol (VTP) changes. Use the **no** form of this command to disable VTP trap notification.

snmp-server enable traps vtp

no snmp-server enable traps vtp

| | |
|---------------------------|--|
| Syntax Description | This command has no arguments or keywords. |
|---------------------------|--|

| | |
|-----------------|----------------------------------|
| Defaults | SNMP traps for VTP are disabled. |
|-----------------|----------------------------------|

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

| | | |
|------------------------|----------------|------------------------------------|
| Command History | Release | Modification |
| | 11.2(8)SA4 | This command was first introduced. |

| | |
|-------------------------|---|
| Usage Guidelines | Specify the host that receives the traps by using the snmp-server host global configuration command. |
|-------------------------|---|

| | |
|-----------------|---|
| Examples | This example shows how to enable VTP to send trap notifications: Switch(config)# snmp-server enable trap vtp |
| | You can verify the previous command by entering the show vtp status user EXEC command or the show running-config privileged EXEC command. |

| | | |
|-------------------------|----------------------------|--|
| Related Commands | Command | Description |
| | show running-config | Displays the running configuration on the switch. |
| | show vtp status | Displays general information about the VTP management domain and status. |
| | snmp-server host | Specifies the host that receives SNMP traps. |

snmp-server host

Use the **snmp-server host** global configuration command to specify the host that receives Simple Network Management Protocol (SNMP) traps. Use the **no** form of this command to remove the specified host.

snmp-server host *host-address community-string* [**c2900** | **config** | **snmp** | **tty** | **udp-port** *port-number* | **vlan-membership** | **vtp**]

no snmp-server host *host-address community-string*

| | | |
|--------------------|------------------------------------|---|
| Syntax Description | <i>host-address</i> | IP address or name of the SNMP trap host. |
| | <i>community-string</i> | Password-like community string sent with the trap operation. |
| | c2900 | (Optional) Send SNMP Catalyst 2900 XL or Catalyst 3500 XL switch traps. |
| | config | (Optional) Send SNMP configuration traps. |
| | snmp | (Optional) Send SNMP-type traps. |
| | tty | (Optional) Send Cisco enterprise-specific traps when a Transmission Control Protocol (TCP) connection closes. |
| | udp-port <i>port-number</i> | (Optional) UDP port of the host to use. The default is 162. |
| | vlan-membership | (Optional) Send SNMP VLAN Membership Policy Server (VMPS) traps |
| | vtp | (Optional) Send SNMP VLAN Trunking Protocol (VTP) traps. |

Defaults

The SNMP trap host address and community string are not defined.
Traps are disabled.

Command Modes

Global configuration

| | | |
|-----------------|----------------|------------------------------------|
| Command History | Release | Modification |
| | 11.2(8)SA4 | This command was first introduced. |

Usage Guidelines

Use the **snmp-server host** global configuration command with the **snmp-server enable traps** global commands to generate traps.

Examples

This example shows how to configure an SNMP host to receive VTP traps:

```
Switch(config)# snmp-server host 172.20.128.178 traps vtp
```

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

Related Commands

| Command | Description |
|---|---|
| snmp-server enable traps vlan-membership | Enables SNMP notification for VMPS changes. |
| snmp-server enable traps vtp | Enables SNMP notification for VTP changes. |

snmp trap mac-notification

Use the **snmp trap mac-notification** interface configuration command to enable or disable the MAC notification traps on a particular port. Use the **no** form of the command 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 whenever a MAC address is added on this port. |
| | removed | (Optional) Enable MAC notification traps whenever a MAC address is removed from this port. |
| Defaults | The SNMP address-addition and address-removal traps are disabled. | |
| Command Modes | Interface configuration | |
| Command History | Release | Modification |
| | 12.0(5)WC3 | This command was first introduced. |
| Usage Guidelines | Even though the notification trap is enabled for a particular port, the trap is actually generated only when the global MAC trap flag is also enabled. To enable the global trap flag, use the snmp-server enable traps mac-notification global configuration command. | |
| 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 | |
| Related Commands | You can verify the previous commands by entering the show running-config privileged EXEC command. | |
| | mac-address-table notification | Enables the MAC notification feature on a switch. |
| | show mac-address-table notification | Displays MAC-notification parameters. |

spanning-tree

Use the **spanning-tree** global configuration command to enable Spanning Tree Protocol (STP) on a VLAN. Use the **no** form of the command to disable STP on a VLAN.

spanning-tree [**vlan** *stp-list*]

no spanning-tree [**vlan** *stp-list*]

| Syntax Description | vlan <i>stp-list</i> (Optional) List of spanning-tree instances. Each spanning-tree instance is associated with a VLAN ID. Valid IDs are from 1 to 1005. Enter each VLAN ID separated by a space. Do not enter leading zeroes. Ranges are not supported. | | | | | |
|--------------------|---|--|---------|--------------|------------|------------------------------------|
| Defaults | STP is enabled. | | | | | |
| Command Modes | Global configuration | | | | | |
| Command History | <table><tr><th>Release</th><th>Modification</th></tr><tr><td>11.2(8)SA3</td><td>This command was first introduced.</td></tr></table> | | Release | Modification | 11.2(8)SA3 | This command was first introduced. |
| Release | Modification | | | | | |
| 11.2(8)SA3 | This command was first introduced. | | | | | |
| Usage Guidelines | <p>Disabling STP causes the VLAN or a list of VLANs to stop participating in STP. Ports that are administratively down remain down. Received Bridge Protocol Data Units (BPDUs) are forwarded like other multicast frames. The VLAN does not detect and prevent loops when STP is disabled.</p> <p>You can disable STP on a VLAN that is not active and verify the change by using the privileged EXEC show running-config or the show spanning-tree vlan <i>stp-list</i> privileged EXEC commands. The setting takes effect when the VLAN is activated.</p> <p>If the variable <i>stp-list</i> is omitted, the command applies to the STP instance associated with VLAN 1.</p> <p>You can enable STP on a VLAN that has no ports assigned to it.</p> | | | | | |
| Examples | <p>This example shows how to disable STP on VLAN 5:</p> <pre>Switch(config)# no spanning-tree vlan 5</pre> <p>You can verify the previous command by entering the show spanning-tree user EXEC command. In this instance, VLAN 5 does not appear in the list.</p> | | | | | |

| Related Commands | Command | Description |
|------------------|------------------------------------|--|
| | show spanning-tree | Displays spanning-tree information for the specified spanning-tree instances. |
| | spanning-tree forward-time | Specifies the forwarding-time for the specified spanning-tree instances. |
| | spanning-tree max-age | Changes the interval between messages the spanning tree receives from the root switch. |
| | spanning-tree port-priority | Configures a port priority, which is used when two switches tie for position as the root switch. |
| | spanning-tree protocol | Specifies the STP version to be used for specified spanning-tree instances. |

spanning-tree cost

Use the **spanning-tree cost** interface configuration command to set the path cost for Spanning Tree Protocol (STP) calculations. In the event of a loop, spanning tree considers the path cost when selecting an interface to place into the forwarding state. Use the **no** form of this command to return to the default value.

spanning-tree [vlan *stp-list*] cost *cost*

no spanning-tree [vlan *stp-list*] cost

| | | |
|--------------------|-----------------------------|---|
| Syntax Description | vlan <i>stp-list</i> | (Optional) List of spanning-tree instances. Each spanning-tree instance is associated with a VLAN ID. Valid IDs are from 1 to 1005. Enter each VLAN ID separated by a space. Do not enter leading zeroes. Ranges are not supported. |
| | cost | Path cost can range from 1 to 65535, with higher values indicating higher costs. This range applies whether or not the IEEE STP has been specified. |

| | |
|----------|---|
| Defaults | <p>The default path cost is computed from the interface bandwidth setting. These are the IEEE default path cost values:</p> <ul style="list-style-type: none"> • 10 Mbps – 100 • 100 Mbps – 19 • 155 Mbps – 14 • 1 Gbps – 4 • 10 Gbps – 2 • Speeds greater than 10 Gbps – 1 |
|----------|---|

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

| Command History | Release | Modification |
|-----------------|------------|------------------------------------|
| | 11.2(8)SA3 | This command was first introduced. |

| | |
|------------------|--|
| Usage Guidelines | <p>If the variable <i>stp-list</i> is omitted, the command applies to the spanning-tree instance associated with VLAN 1.</p> <p>You can set a cost for a port or on a VLAN that does not exist. The setting takes effect when the VLAN exists.</p> |
|------------------|--|

| | |
|----------|---|
| Examples | <p>This example shows how to set a path cost value of 250 for VLAN 1:</p> <pre>Switch(config-if)# spanning-tree vlan 1 cost 250</pre> <p>You can verify the previous command by entering the show spanning-tree user EXEC command.</p> |
|----------|---|

| Related Commands | Command | Description |
|------------------|-------------------------------|---|
| | show spanning-tree | Displays spanning-tree information for the specified spanning-tree instances. |
| | spanning-tree portfast | Enables the Port Fast feature on a port in all its associated VLANs. |
| | spanning-tree priority | Configures the switch priority for the specified spanning-tree instance. |

spanning-tree forward-time

Use the **spanning-tree forward-time** global configuration command to set the forwarding-time for the specified spanning-tree instances. The forwarding time determines how long each of the listening and learning states last before the port begins forwarding. Use the **no** form of this command to return to the default value.

spanning-tree [**vlan** *stp-list*] **forward-time** *seconds*

no spanning-tree [**vlan** *stp-list*] **forward-time**

| | | |
|--------------------|---|---|
| Syntax Description | vlan <i>stp-list</i> | (Optional) List of spanning-tree instances. Each spanning-tree instance is associated with a VLAN ID. Valid IDs are from 1 to 1005. Enter each VLAN ID separated by a space. Do not enter leading zeroes. Ranges are not supported. |
| | <i>seconds</i> | Forward-delay interval from 4 to 200 seconds. |
| Defaults | The default forwarding-time for IEEE Spanning Tree Protocol (STP) is 15 seconds. The default for IBM STP is 4 seconds. | |
| Command Modes | Global configuration | |
| Command History | Release | Modification |
| | 11.2(8)SA3 | This command was first introduced. |
| Usage Guidelines | If the variable <i>stp-list</i> is omitted, the command applies to the STP instance associated with VLAN 1. You can set the forwarding-time on a VLAN that has no ports assigned to it. The setting takes effect when you assign ports to it. | |
| Examples | This example shows how to set the spanning-tree forwarding time to 18 seconds for VLAN 20: | |
| | <pre>Switch(config)# spanning-tree vlan 20 forward-time 18</pre> | |
| | You can verify the previous command by entering the show spanning-tree user EXEC command. | |

| Related Commands | Command | Description |
|------------------|------------------------------------|--|
| | show spanning-tree | Displays spanning-tree information for the specified spanning-tree instances. |
| | spanning-tree max-age | Changes the interval between messages the spanning tree receives from the root switch. |
| | spanning-tree port-priority | Configures a port priority, which is used when two switches tie for position as the root switch. |
| | spanning-tree protocol | Specifies the STP version to be used for specified spanning-tree instances. |

spanning-tree hello-time

Use the **spanning-tree hello-time** global configuration command to specify the interval between hello Bridge Protocol Data Units (BPDUs). Use the **no** form of this command to return to the default interval.

spanning-tree [**vlan** *stp-list*] **hello-time** *seconds*

no spanning-tree [**vlan** *stp-list*] **hello-time**

| | | |
|--------------------|-----------------------------|---|
| Syntax Description | vlan <i>stp-list</i> | (Optional) List of spanning-tree instances. Each spanning-tree instance is associated with a VLAN ID. Valid IDs are from 1 to 1005. Enter each VLAN ID separated by a space. Do not enter leading zeroes. Ranges are not supported. |
| | <i>seconds</i> | Interval from 1 to 10 seconds. |

Defaults The default hello time for IEEE Spanning Tree Protocol (STP) and IBM STP is 2 seconds.

Command Modes Global configuration

| Command History | Release | Modification |
|-----------------|------------|------------------------------------|
| | 11.2(8)SA3 | This command was first introduced. |

Usage Guidelines If the variable *stp-list* is omitted, the command applies to the STP instance associated with VLAN 1. You can set the hello time on a VLAN that has no ports assigned to it. The setting takes effect when you assign ports to it.

Examples 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
```

You can verify the previous command by entering the **show spanning-tree** user EXEC command.

| Related Commands | Command | Description |
|------------------|------------------------------------|--|
| | show spanning-tree | Displays spanning-tree information for the specified spanning-tree instances. |
| | spanning-tree | Enables STP on a VLAN. |
| | spanning-tree port-priority | Configures a port priority, which is used when two switches tie for position as the root switch. |
| | spanning-tree protocol | Specifies the STP version to be used for specified spanning-tree instances. |

spanning-tree max-age

Use the **spanning-tree max-age** global configuration command to change the interval between messages 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 Protocol (STP) topology. Use the **no** form of this command to return to the default interval.

spanning-tree [*vlan stp-list*] **max-age** *seconds*

no spanning-tree [*vlan stp-list*] **max-age**

| | | |
|--------------------|----------------------|---|
| Syntax Description | vlan stp-list | (Optional) List of spanning-tree instances. Each spanning-tree instance is associated with a VLAN ID. Valid IDs are from 1 to 1005. Enter each VLAN ID separated by a space. Do not enter leading zeroes. Ranges are not supported. |
| | <i>seconds</i> | Interval the switch waits between receiving BPDUs from the root switch. Enter a number from 6 to 200. |

Defaults The default max-age for IEEE STP is 20 seconds. The default for IBM STP is 10 seconds.

Command Modes Global configuration

| Command History | Release | Modification |
|-----------------|------------|------------------------------------|
| | 11.2(8)SA3 | This command was first introduced. |

Usage Guidelines The **max-age** setting must be greater than the **hello-time** setting.

If the variable *stp-list* is omitted, the command applies to the STP instance associated with VLAN 1.

You can set the **max-age** on a VLAN that has no ports assigned to it. The setting takes effect when you assign ports to the VLAN.

Examples 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 instances 100 through 102:

```
Switch(config)# no spanning-tree vlan 100 101 102 max-age
```

You can verify the previous commands by entering the **show spanning-tree** user EXEC command.

| Related Commands | Command | Description |
|------------------|------------------------------------|--|
| | show spanning-tree | Displays spanning-tree information for the specified spanning-tree instances. |
| | spanning-tree forward-time | Specifies the forwarding-time for the specified spanning-tree instances. |
| | spanning-tree hello-time | Specifies the interval between hello Bridge Protocol Data Units (BPDUs). |
| | spanning-tree port-priority | Configures a port priority, which is used when two switches tie for position as the root switch. |
| | spanning-tree protocol | Specifies the STP version to be used for specified spanning-tree instances. |

spanning-tree portfast

Use the **spanning-tree portfast** interface configuration command to enable the Port Fast feature on a port in all its associated VLANs. 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 Protocol (STP) status changes. Use the **no** form of this command to return the port to default operation.

spanning-tree portfast

no spanning-tree portfast

| | |
|---------------------------|--|
| Syntax Description | This command has no keywords or arguments. |
|---------------------------|--|

| | |
|-----------------|--|
| Defaults | The Port Fast feature is disabled; however, it is automatically enabled on dynamic-access ports. |
|-----------------|--|

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

| | | |
|------------------------|----------------|------------------------------------|
| Command History | Release | Modification |
| | 11.2(8)SA3 | This command was first introduced. |

| | |
|-------------------------|--|
| Usage Guidelines | <p>This feature is not supported on the Asynchronous Transfer Mode (ATM) modules.</p> <p>Use this feature only on ports that connect to end stations.</p> <p>This feature affects all VLANs on the port.</p> <p>A port with the Port Fast feature enabled is moved directly to the spanning-tree forwarding state.</p> |
|-------------------------|--|

| | |
|-----------------|---|
| Examples | <p>This example shows how to enable the Port Fast feature on fixed port 2.</p> <pre>Switch(config-if)# interface FastEthernet 0/2 Switch(config-if)# spanning-tree portfast</pre> <p>You can verify the previous commands by entering the show running-config in privileged EXEC mode.</p> |
|-----------------|---|

| | | |
|-------------------------|------------------------------------|--|
| Related Commands | Command | Description |
| | show spanning-tree | Displays spanning-tree information for the specified spanning-tree instances. |
| | spanning-tree port-priority | Configures a port priority, which is used when two switches tie for position as the root switch. |

spanning-tree port-priority

Use the **spanning-tree port-priority** interface configuration command to configure a port priority that is used when two switches tie for position as the root switch. Use the **no** form of this command to return to the default value.

spanning-tree [**vlan** *stp-list*] **port-priority** *port-priority*

no spanning-tree [**vlan** *stp-list*] **port-priority**

Syntax Description

| | |
|-----------------------------|---|
| vlan <i>stp-list</i> | (Optional) List of spanning-tree instances. Each spanning-tree instance is associated with a VLAN ID. Valid IDs are from 1 to 1005. Enter each VLAN ID separated by a space. Do not enter leading zeroes. Ranges are not supported. |
| <i>port-priority</i> | Number from 0 to 255. The lower the number, the higher the priority. |

Defaults

The default port-priority for IEEE STP and IBM STP is 128.

Command Modes

Interface configuration

Command History

| Release | Modification |
|------------|------------------------------------|
| 11.2(8)SA3 | This command was first introduced. |

Usage Guidelines

If the variable *stp-list* is omitted, the command applies to the STP instance associated with VLAN 1. You can set the port priority on a VLAN that has no ports assigned to it. The setting takes effect when you assign ports to the VLAN.

Examples

This example shows how to increase the likelihood that the spanning-tree instance 20 is chosen as the root switch on port fa0/2:

```
Switch(config)# interface fa0/2
Switch(config-if)# spanning-tree vlan 20 port-priority 0
```

You can verify the previous commands by entering the **show spanning-tree** user EXEC command.

Related Commands

| Command | Description |
|-------------------------------|---|
| show spanning-tree | Displays spanning-tree information for the specified spanning-tree instances. |
| spanning-tree protocol | Specifies the STP version to be used for specified spanning-tree instances. |

spanning-tree priority

Use the **spanning-tree priority** global configuration command to configure the switch priority for the specified spanning-tree instance. This changes the likelihood that the switch is selected as the root switch. Use the **no** form of this command to revert to the default value.

spanning-tree [**vlan** *stp-list*] **priority** *bridge-priority*

no spanning-tree [**vlan** *stp-list*] **priority**

Syntax Description

| | |
|-----------------------------|---|
| vlan <i>stp-list</i> | (Optional) List of spanning-tree instances. Each spanning-tree instance is associated with a VLAN ID. Valid IDs are from 1 to 1005. Enter each VLAN ID separated by a space. Do not enter leading zeroes. Ranges are not supported. |
| <i>bridge-priority</i> | A number from 0 to 65535. The lower the number, the more likely the switch will be chosen as root. |

Defaults

The default bridge priority for IEEE STP and IBM STP is 32768.

Command Modes

Global configuration

Command History

| Release | Modification |
|------------|------------------------------------|
| 11.2(8)SA3 | This command was first introduced. |

Usage Guidelines

If the variable *stp-list* is omitted, the command applies to the STP instance associated with VLAN 1. You can configure the switch priority on a VLAN that has no ports assigned to it. The setting takes effect when you assign ports to the VLAN.

Examples

This example shows how to set the spanning-tree priority to 125 for a list of VLANs:

```
Switch(config)# spanning-tree vlan 20 100 101 102 priority 125
```

You can verify the previous command by entering the **show spanning-tree** user EXEC command.

| Related Commands | Command | Description |
|------------------|-----------------------------------|--|
| | show spanning-tree | Displays spanning-tree information for the specified spanning-tree instances. |
| | spanning-tree forward-time | Specifies the forwarding-time for the specified spanning-tree instances. |
| | spanning-tree hello-time | Specifies the interval between hello Bridge Protocol Data Units (BPDUs). |
| | spanning-tree max-age | Changes the interval between messages the spanning tree receives from the root switch. |
| | spanning-tree protocol | Specifies the STP version to be used for specified spanning-tree instances. |

spanning-tree protocol

Use the **spanning-tree protocol** global configuration command to specify the Spanning Tree Protocol (STP) to be used for specified spanning-tree instances. Use the **no** form of this command to use the default protocol.

spanning-tree [*vlan stp-list*] **protocol** {*ieee* | *ibm*}

no spanning-tree [*vlan stp-list*] **protocol**

| | | |
|--------------------|----------------------|---|
| Syntax Description | vlan stp-list | (Optional) List of spanning-tree instances. Each spanning-tree instance is associated with a VLAN ID. Valid IDs are from 1 to 1005. Enter each VLAN ID separated by a space. Do not enter leading zeroes. Ranges are not supported. |
| | ieee | IEEE Ethernet STP. |
| | ibm | IBM STP. |

Defaults The default protocol is **ieee**.

Command Modes Global configuration

| | | |
|-----------------|----------------|------------------------------------|
| Command History | Release | Modification |
| | 11.2(8)SA3 | This command was first introduced. |

Usage Guidelines Changing the **spanning-tree protocol** command changes spanning-tree parameters to change to the default values of the new protocol.

If the variable *stp-list* is omitted, this command applies to the spanning-tree instance associated with VLAN 1.

You can change the protocol on a VLAN that has no ports assigned to it. The setting takes effect when you assign ports to it.

Examples This example shows how to change the STP version for VLAN 20 to the IBM version of STP:

```
Switch(config)# spanning-tree vlan 20 protocol ibm
```

You can verify the previous command by entering the **show spanning-tree** user EXEC command.

| Related Commands | Command | Description |
|------------------|------------------------------------|---|
| | show spanning-tree | Displays spanning-tree information for the specified spanning-tree instances. |
| | spanning-tree | Enables STP on a VLAN. |
| | spanning-tree forward-time | Specifies the forwarding-time for the specified spanning-tree instances. |
| | spanning-tree max-age | Changes the interval between messages that the spanning tree receives from the root switch. |
| | spanning-tree port-priority | Configures a port priority, that is used when two switches tie for position as the root switch. |

spanning-tree rootguard

Use the **spanning-tree rootguard** interface configuration command to enable the root guard feature for all the VLANs associated with the selected port. Root guard restricts which port is allowed to be the Spanning Tree Protocol (STP) root port or the path-to-the root for the switch. The root port provides the best path from the switch to the root switch. Use the **no** form of this command to disable this feature.

spanning-tree rootguard

no spanning-tree rootguard

Syntax Description This command has no keywords or arguments.

Defaults The root guard feature is disabled.

Command Modes Interface configuration

| Command History | Release | Modification |
|-----------------|-----------|------------------------------------|
| | 12.0(5)XU | This command was first introduced. |

Usage Guidelines

When the root guard feature 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.

When the **no spanning-tree rootguard** command is entered, the root guard feature is disabled for all VLANs on the selected port. If this port is in the root-inconsistent (blocked) state, the port automatically transitions to the listening state.

Do not enable the root guard on ports that will be used by the UplinkFast feature. With UplinkFast, the backup ports (in the blocked state) replace the root port in the case of a failure. However, if root guard is also enabled, all the backup ports used by the UplinkFast feature are placed in the root-inconsistent state (blocked) and prevented from reaching the forwarding state.

Examples

This example shows how to enable the root guard feature on all the VLANs associated with interface fa0/3:

```
Switch(config)# interface fa0/3
Switch(config-if)# spanning-tree rootguard
```

You can verify the previous commands by entering the **show running-config** privileged EXEC command.

| Related Commands | Command | Description |
|------------------|------------------------------------|---|
| | show running-config | Displays the current operating configuration. |
| | show spanning-tree | Displays spanning-tree information for the specified spanning-tree instances. |
| | spanning-tree cost | Specifies the path cost for STP calculations. In the event of a loop, spanning tree considers the path cost when selecting an interface to place into the forwarding state. |
| | spanning-tree port-priority | Configures a port priority that is used when two switches tie for position as the root switch. |
| | spanning-tree priority | Configures the switch priority for the specified spanning-tree instance and affects the likelihood that the switch is selected as the root switch. |

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 Protocol (STP) 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 |
| | 12.0(5)XW | This command was first introduced. |

| | |
|-------------------------|---|
| Usage Guidelines | <p>This command is effective only if you enable the UplinkFast feature by using the spanning-tree uplinkfast global configuration command.</p> <p>Use this command only on access switches.</p> <p>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.</p> <p>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.</p> |
|-------------------------|---|

| | |
|-----------------|---|
| Examples | The following command shows how to enable CSUF on the GBIC interface gi0/1: |
|-----------------|---|

```
Switch(config)# interface gi0/1
Switch(config-if)# spanning-tree stack-port
```

You can verify the previous command by entering the **show spanning-tree** user EXEC command.

| | | |
|-------------------------|---------------------------|---|
| Related Commands | Command | Description |
| | show spanning-tree | Displays spanning-tree information for the specified spanning-tree instances. |

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 Spanning Tree Protocol (STP) reconfigures itself. Use the **no** form of this command to return to the default value.

spanning-tree uplinkfast [**max-update-rate** *pkts-per-second*]

no spanning-tree uplinkfast [**max-update-rate** *pkts-per-second*]

| | | |
|--------------------|---|---|
| Syntax Description | max-update-rate <i>pkts-per-second</i> | The number of packets per second at which stations address update packets are sent. The range is 0 to 1000. |
|--------------------|---|---|

| | |
|----------|-------------------------|
| Defaults | UplinkFast is disabled. |
|----------|-------------------------|

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

| Command History | Release | Modification |
|-----------------|------------|------------------------------------|
| | 11.2(8)SA6 | This command was first introduced. |

| | |
|------------------|---|
| Usage Guidelines | When you enable UplinkFast, it is enabled for the entire switch and cannot be enabled for individual VLANs. |
| | When you enable UplinkFast, the bridge priority of all VLANs is set to 49152, and the path cost of all ports and VLAN trunks is increased by 3000. This change reduces the chance that the switch will become the root switch. |
| | When you disable UplinkFast, the bridge priorities of all VLANs and path costs are set to their default values. |
| | Do not enable the root guard on ports that will be used by the UplinkFast feature. With UplinkFast, the backup ports (in the blocked state) replace the root port in the case of a failure. However, if root guard is also enabled, all the backup ports used by the UplinkFast feature are placed in the root-inconsistent state (blocked) and prevented from reaching the forwarding state. |

Examples

The following command shows how to enable UplinkFast:

```
Switch(config)#spanning-tree uplinkfast
```

You can verify the previous command by entering the **show spanning-tree** user EXEC command.

Related Commands

| Command | Description |
|---------------------------|---|
| show spanning-tree | Displays spanning-tree information for the specified spanning-tree instances. |

speed

Use the **speed** interface configuration command to specify the speed of a Fast Ethernet port. Use the **no** form of this command to return the port to its default value.

speed {10 | 100 | auto}

no speed

Syntax Description

| | |
|-------------|--|
| 10 | Port runs at 10 Mbps. |
| 100 | Port runs at 100 Mbps. |
| auto | Port automatically detects whether it should run at 10 or 100 Mbps on Fast Ethernet ports. |

Defaults

For Fast Ethernet ports, the default is **auto**.

For Gigabit Ethernet ports, the speed is 1000 Mbps and is not configurable.

For Asynchronous Transfer Mode (ATM) ports, the speed is 155 Mbps and is not configurable.

Command Modes

Interface configuration

Command History

| Release | Modification |
|-----------|------------------------------------|
| 11.2(8)SA | This command was first introduced. |

Usage Guidelines

Certain ports can be configured to be either 10 or 100 Mbps. Applicability of this command is hardware-dependent.

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

For guidelines on setting the switch speed and duplex parameters, see the *Catalyst 2900 Series XL and Catalyst 3500 Series XL Software Configuration Guide*.

Examples

This example shows how to set port 1 on module 2 to 100 Mbps:

```
Switch(config)# interface fastethernet2/1  
Switch(config-if)# speed 100
```

You can verify the previous commands by entering the **show running-config** in privileged EXEC mode.

Related Commands

| Command | Description |
|---------------|--|
| duplex | Specifies the duplex mode of operation for Fast Ethernet and Gigabit Ethernet ports. |

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 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 vlan {*vlan-id* | **dynamic**}

| Syntax Description | vlan <i>vlan-id</i> | ID of the VLAN. Valid IDs are from 1 to 1001. Do not enter leading zeroes. |
|--------------------|----------------------------|---|
| | dynamic | Port is assigned to a VLAN based on the source MAC address of a host (or hosts) connected to that port. The switch sends every new source MAC address received to the VLAN Membership Policy Server (VMPS) 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.

A dynamic-access port is initially a member of no VLAN and receives its assignment based on the packets it receives.

Command Modes

Interface configuration

Command History

| Release | Modification |
|------------|---------------------------------------|
| 11.2(8)SA3 | This command was first introduced. |
| 11.2(8)SA4 | The dynamic keyword was added. |

Usage Guidelines

The port must be in access mode before the **switchport access vlan** *vlan-id* or **switchport access vlan dynamic** command can take effect. For more information, see the “switchport mode” section on page 2-179.

An access port can be assigned to only one VLAN.

When the **no switchport access vlan** form is used, the access mode is reset to static access on VLAN 1.

The following restrictions apply to dynamic-access ports:

- The software implements the VLAN Query Protocol (VQP) client, which can query a VMPS such as a Catalyst 5000 series switch. Catalyst 2900 XL and Catalyst 3500 XL 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 STP does not put the dynamic-access port into 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:
 - The source or destination port in a static address entry.
 - A network port (dynamic-access ports can be assigned to a VLAN in which one of the other ports is a network port).
 - A port group (dynamic-access ports cannot be grouped with any other port including other dynamic ports).
 - A secure port.
 - A port with a secure address.
 - A monitor port.

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
```

This example shows how to assign a port already in access mode to dynamic:

```
Switch(config-if)# switchport access vlan dynamic
```

This example shows how to reconfigure a dynamic-access port to a static-access port:

```
Switch(config-if)# no switchport access vlan dynamic
```

You can verify the previous commands by entering the **show interface *interface-id* switchport** command in privileged EXEC mode and examining information in the Administrative Mode and Operational Mode rows.

Related Commands

| Command | Description |
|-------------------------|---|
| switchport mode | Configures the VLAN membership mode of a port. |
| switchport multi | Configures a list of VLANs to which the port is associated. |

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 | multi | trunk}

no switchport mode {access | multi | trunk}

| Syntax Description | | |
|--------------------|--|--|
| access | | Set the port to access mode (either static-access or dynamic-access depending on the setting of the switchport access vlan command). The port operates as a nontrunking, single VLAN interface that transmits and receives nonencapsulated frames. An access port can be assigned to only one VLAN. |
| multi | | Set the port to multi-VLAN port mode. The port operates as a nontrunking VLAN interface that transmits and receives nonencapsulated frames. A multi-VLAN port can be assigned to one or more VLANs. |
| trunk | | Set the port to 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 All ports are static-access ports in VLAN 1.

Command Modes Interface configuration

| Command History | Release | Modification |
|-----------------|------------|-------------------------------------|
| | 11.2(8)SA3 | This command was first introduced. |
| | 11.2(8)SA4 | The trunk keyword was added. |

Usage Guidelines The **access**, **multi**, or **trunk** keywords take effect only when you change the port to the corresponding mode by using the **switchport mode** command. The static-access, multi-VLAN, and trunk configurations are saved, but only one configuration is active at a time.

The **no switchport mode** form resets the mode to static access.

Only these combinations of port modes can appear on a single switch:

- Multi-VLAN and access ports
- Trunk and access ports

Trunk and multi-VLAN ports cannot coexist on the same switch. If you want to change a multi-VLAN or trunk port into another mode, you must first change it to an access port and then reassign it to the new mode.

Examples

This example shows how to configure a port for access mode:

```
Switch(config-if)# switchport mode access
```

This example shows how to configure a port for multi-VLAN mode:

```
Switch(config-if)# switchport mode multi
```

This example shows how to configure a port for trunk mode:

```
Switch(config-if)# switchport mode trunk
```

You can verify the previous commands by entering the **show interface *interface-id* switchport** command in privileged EXEC mode and examining information in the Administrative Mode and Operational Mode rows.

Related Commands

| Command | Description |
|--------------------------|--|
| switchport access | Configures a port as a static-access or dynamic-access port. |
| switchport multi | Configures a list of VLANs to which the port is associated. |

switchport multi

Use the **switchport multi** interface configuration command to configure a list of VLANs to which the port is associated. If the mode is set to multi, the port operates as a member of all VLANs in the list. Use the **no** form of this command to reconfigure the port as an access port.

switchport multi vlan {**add** *vlan-list* / **remove** *vlan-list*}

no switchport multi vlan

Syntax Description

| | |
|--------------------------------|---|
| vlan | Indicate the VLAN to which the port is associated. |
| add <i>vlan-list</i> | List of VLAN IDs to add. Valid IDs are from 1 to 1001. Separate nonconsecutive VLAN IDs with a comma and no spaces; use a hyphen to designate a range of IDs. Do not enter leading zeroes. |
| remove <i>vlan-list</i> | List of VLAN IDs to remove. Valid IDs are from 1 to 1001. Separate nonconsecutive VLAN IDs with a comma and no spaces; use a hyphen to designate a range of IDs. Do not enter leading zeroes. |

Defaults

The default for VLAN membership of a multi-VLAN port is VLAN 1.

Command Modes

Interface configuration

Command History

| Release | Modification |
|------------|------------------------------------|
| 11.2(8)SA3 | This command was first introduced. |

Usage Guidelines

The **switchport mode multi** command must be entered before the **switchport multi vlan** *vlan-list* command can take effect.

In the variable *vlan-list*, separate nonconsecutive VLAN IDs with a comma; use a hyphen to designate a range of IDs.

A multi-VLAN port cannot be a secure port or a monitor port.

A multi-VLAN port cannot coexist with a trunk port on the same switch.



Caution

To avoid loss of connectivity, do not connect multi-VLAN ports to hubs or switches. Connect multi-VLAN ports to routers or servers.

Examples

This example shows how to assign a multi-VLAN port already in multimode to two VLANs:

```
Switch(config-if)# switchport multi vlan 2,4
```

This example shows how to assign a multi-VLAN port already in multimode to a range of VLANs:

```
Switch(config-if)# switchport multi vlan 5-10
```

This example shows how to reset the VLAN list of a multi-VLAN port to the default (VLAN 1 only):

```
Switch(config-if)# no switchport multi vlan
```

You can verify the previous commands by entering the **show interface *interface-id* switchport** command in privileged EXEC mode and examining information in the Administrative Mode and Operational Mode rows.

Related Commands

| Command | Description |
|--------------------------|--|
| switchport access | Configures a port as a static-access or dynamic-access port. |
| switchport mode | Configures the VLAN membership mode of a port. |

switchport priority

Use the **switchport priority** interface configuration command to set a port priority for the incoming untagged frames or the priority of frames received by the appliance connected to the specified port. Use the **no** form of this command to return the setting to its default.

switchport priority {**default** *default-priority-id* / **extend** {**cos** *value* | **none** | **trust**} / **override**}

no switchport priority {**default** *default-priority-id* | **extend** / **override**}

| | | |
|--------------------|----------------------------|---|
| Syntax Description | <i>default-priority-id</i> | The priority number for untagged traffic. The priority is a number from 0 to 7. Seven is the highest priority. |
| | extend | Set the 802.1P priority of the switch. <ul style="list-style-type: none"> cos <i>value</i>—Override the 802.1p priority of devices connected to the switch. The cos value is a number from 0 to 7. Seven is the highest priority. The cos keyword only applies to the 3524-PWR and the 3548 XL switches. none—The switch is not instructed what to do with the priority. trust—Specify that the switch should trust (honor) the received 802.1P priority from devices connected to it. |
| | override | Override the priority of tagged frames with the default value. |
| | | |

Defaults The port priority is not set, and the default value for untagged frames received on the port is zero. The appliance connected to the port is not instructed (none) what to do with the priority.

Command Modes Interface configuration

| Command History | Release | Modification |
|-----------------|-----------|---|
| | 12.0(5)XP | This command was first introduced. |
| | 12.0(5)XU | The extend keyword and its options were added. |

Usage Guidelines The default port priority applies if the incoming frame is an untagged frame received from a VLAN trunk or static-access port. This port priority does not apply to the ISL or IEEE 802.1Q VLAN tagged frames. If the incoming frame is an IEEE 802.1Q VLAN tagged frame, the IEEE 802.1P User Priority bits will be used.

The **cos** keyword only applies to the 3524-PWR and 3548 XL switches.

Examples

This example shows how to set a default priority on port 3.

```
Switch(config)# interface fa0/3
Switch(config-if)# switchport priority default 7
```

All untagged frames received from this port will have the same priority value. You can verify the previous commands by entering the **show interface *interface-id* switchport** privileged EXEC command.

This example shows how to configure the appliance connected to the specified port to honor the received 802.1P priority:

```
Switch(config-if)# switchport priority extend trust
```

You can verify the previous command by entering the **show interface *interface-id* switchport** privileged EXEC command.

Related Commands

| Command | Description |
|------------------------------|---|
| power inline | Determines how inline power is applied to the specified port on the 3524-PWR-XL switch. |
| show interface | Displays the administrative and operational status of a switching (nonrouting) port. |
| switchport access | Configures a port as a static-access or dynamic-access port. |
| switchport mode | Configures the VLAN membership mode of a port. |
| switchport voice vlan | Configures the voice VLAN on the port. |

switchport trunk allowed vlan

Use the **switchport trunk allowed vlan** interface configuration command to control which VLANs can receive and transmit traffic on the trunk. Use the **no** form of this command to reset the allowed list to the default value.

switchport trunk allowed vlan {**add** *vlan-list* / **all** / **except** *vlan-list* / **remove** *vlan-list*}

no switchport trunk allowed vlan

Syntax Description

| | |
|--------------------------------|--|
| add <i>vlan-list</i> | List of VLAN IDs to add. Valid IDs are from 1 to 1001. Separate nonconsecutive VLAN IDs with a comma and no spaces; use a hyphen to designate a range of IDs. Do not enter leading zeroes. |
| all | Add all VLAN IDs to the list. |
| except <i>vlan-list</i> | List of exception VLAN IDs. VLANs are added except the ones specified. Valid IDs are from 1 to 1001. Separate nonconsecutive VLAN IDs with a comma and no spaces; use a hyphen to designate a range of IDs. Do not enter leading zeroes. |
| remove <i>vlan-list</i> | List of VLAN IDs to remove. Valid IDs are from 1 to 1001. Separate nonconsecutive VLAN IDs with a comma and no spaces; use a hyphen to designate a range of IDs. Do not enter leading zeroes. |

Defaults

All VLANs are included in the allowed list.

Command Modes

Interface configuration

Command History

| Release | Modification |
|------------|------------------------------------|
| 11.2(8)SA4 | This command was first introduced. |

Usage Guidelines

When you use the **no switchport trunk allowed vlan** form, the allowed list resets to the default list, which includes all VLANs.

In the variable *vlan-list*, separate nonconsecutive VLAN IDs with a comma; use a hyphen to designate a range of IDs. You cannot remove VLANs 1 or 1002 to 1005 from the list.

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.

If a trunk port is identified as a network port, the trunk port becomes the network port for all the VLANs associated with the port.

Examples

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
```

You can verify the previous command by entering the **show interface *interface-id* switchport** privileged EXEC command.

Related Commands

| Command | Description |
|---------------------------------------|--|
| switchport mode | Configures the VLAN membership mode of a port. |
| switchport trunk encapsulation | Specifies the encapsulation format on the trunk port. |
| switchport trunk native | Specifies the native VLAN for untagged traffic when in 802.1Q trunking mode. |

switchport trunk encapsulation

Use the **switchport trunk encapsulation** interface configuration command to set the encapsulation format on the trunk port. Use the **no** form of this command to reset the format to the default.

switchport trunk encapsulation {isl / dot1q}

no switchport trunk encapsulation

| | | |
|--------------------|--------------|---|
| Syntax Description | isl | Set the encapsulation format to Inter-Switch Link (ISL). The switch encapsulates all received and transmitted packets with an ISL header. The switch filters native frames received from an ISL trunk port. |
| | dot1q | Set the tagging format to IEEE 802.1Q. With this format, the switch supports simultaneous tagged and untagged traffic on a port. |

| | |
|----------|--|
| Defaults | The default encapsulation format is ISL. |
|----------|--|

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

| Command History | Release | Modification |
|-----------------|------------|-------------------------------------|
| | 11.2(8)SA4 | This command was first introduced. |
| | 11.2(8)SA5 | The dot1q keyword was added. |

| | |
|------------------|---|
| Usage Guidelines | You cannot configure one end of the trunk as an 802.1Q trunk and the other end as an ISL or nontrunk port. However, you can configure one port as an ISL trunk and another port on the same switch as a 802.1Q trunk. |
|------------------|---|

This command is only applicable on switch platforms and port hardware that support both formats.

Examples

This example shows how to configure the encapsulation format to 802.1Q:

```
Switch(config-if)# switchport trunk encapsulation dot1q
```

You can verify the previous command by entering the **show interface *interface-id* switchport** privileged EXEC command.

Related Commands

| Command | Description |
|--------------------------------------|--|
| switchport mode | Configures the VLAN membership mode of a port. |
| switchport trunk allowed vlan | Controls which VLANs can receive and transmit traffic on the trunk. |
| switchport trunk native | Specifies the native VLAN for untagged traffic when in 802.1Q trunking mode. |

switchport trunk native

Use the **switchport trunk native** interface configuration command to set the native VLAN for untagged traffic when in 802.1Q trunking mode. Use the **no** form of this command to reset the native VLAN to the default.

switchport trunk native vlan *vlan-id*

no switchport trunk native

| | | |
|--------------------|--|---|
| Syntax Description | vlan <i>vlan-id</i> ID of the VLAN that is sending and receiving untagged traffic on the trunk port. Valid IDs are from 1 to 1001. Do not enter leading zeroes. | |
| Defaults | VLAN 1 is the default native VLAN ID on the port. | |
| Command Modes | Interface configuration | |
| Command History | Release | Modification |
| | 11.2(8)SA4 | This command was first introduced. |
| Usage Guidelines | <p>All untagged traffic received on the 802.1Q trunk port is forwarded with the native VLAN configured for the port.</p> <p>If a packet has a VLAN ID that is the same as the sending port native VLAN ID, the packet is transmitted untagged; otherwise, the switch transmits the packet with a tag.</p> | |
| Examples | <p>This example shows how to configure VLAN 3 as the default port to send all untagged traffic:</p> <pre>Switch(config-if)# switchport trunk native vlan 3</pre> <p>You can verify the previous command by entering the show interface <i>interface-id</i> switchport privileged EXEC command.</p> | |
| Related Commands | Command | Description |
| | switchport mode | Configures the VLAN membership mode of a port. |
| | switchport trunk allowed vlan | Controls which VLANs can receive and transmit traffic on the trunk. |
| | switchport trunk encapsulation | Specifies the encapsulation format on the trunk port. |

switchport trunk pruning

Use the **switchport trunk pruning** interface configuration command to configure the VLAN pruning-eligible list for ports in trunking mode. Use the **no** form of this command to return the pruning list to the default setting.

switchport trunk pruning vlan {**add** *vlan-list* / **all** / **except** *vlan-list* / **remove** *vlan-list*}

no switchport trunk pruning

| | | |
|--------------------|--------------------------------|---|
| Syntax Description | add <i>vlan-list</i> | List of VLAN IDs to add. Valid IDs are from 2 to 1001. Separate nonconsecutive VLAN IDs with a comma and no spaces; use a hyphen to designate a range of IDs. Do not enter leading zeroes. |
| | all | Add all VLAN IDs to the list. |
| | except <i>vlan-list</i> | List of exception VLAN IDs (VLANs are added except the specified ones). Valid IDs are from 2 to 1001. Separate nonconsecutive VLAN IDs with a comma and no spaces; use a hyphen to designate a range of IDs. Do not enter leading zeroes. |
| | remove <i>vlan-list</i> | List of VLAN IDs to remove. Valid IDs are from 2 to 1001. Separate nonconsecutive VLAN IDs with a comma and no spaces; use a hyphen to designate a range of IDs. Do not enter leading zeroes. |
| | no | Set the pruning list to the default. |
| | | |

Defaults VLANs 2 through 1001 are pruning eligible.

Command Modes Interface configuration

| | | |
|-----------------|----------------|------------------------------------|
| Command History | Release | Modification |
| | 12.0(5)XU | This command was first introduced. |

Usage Guidelines

- 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.

Examples

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 the previous command by entering the **show interface interface-id switchport** privileged EXEC command.

| Related Commands | Command | Description |
|------------------|--|--|
| | show interface <i>interface-id</i> pruning | Displays pruning information for the trunk port. |
| | show interface <i>interface-id</i> switchport | Displays the administrative and operational status of a switching (nonrouting) port. |
| | vtp pruning | Enables pruning in the VLAN Trunking Protocol (VTP) administrative domain. |

switchport voice vlan

Use the **switchport voice vlan** interface configuration command to configure the voice VLAN on the port. Use the **no** form of this command to return the setting to its default.

switchport voice vlan {*vlan-id* | **dot1p** | **none** | **untagged**}

no switchport voice vlan

| Syntax Description | | |
|--------------------|-----------------|---|
| | <i>vlan-id</i> | VLAN used for voice traffic. Valid IDs are from 1 to 1001 (IDs 1002 to 4094 are not supported on Catalyst 2900 XL and Catalyst 3500 XL switches). Do not enter leading zeroes. The switch port is an 802.1Q trunk port. |
| | dot1p | The telephone uses priority tagging and uses VLAN 0 (the native VLAN). The switch port is an 802.1Q trunk port. |
| | 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 switch port can be an access port or an 802.1Q trunk port. |

| 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 |
|-----------------|-----------|------------------------------------|
| | 12.0(5)XU | This command was first introduced. |

| Usage Guidelines | Ports that are not configured as trunk ports but have a configured voice VLAN are access ports with a voice VLAN ID (VVID). |
|------------------|---|
|------------------|---|

Examples

This example shows how to configure VLAN 2 as the voice VLAN:

```
Switch(config-if)# switchport voice vlan 2
```

You can verify the previous command by entering the **show interface *interface-id* switchport** privileged EXEC command.

Related Commands

| Command | Description |
|--|--|
| power inline | Determines how inline power is applied to the specified port on the 3524-PWR-XL switch. |
| show interface <i>interface-id</i> switchport | Displays the administrative and operational status of a switching (nonrouting) port. |
| switchport priority extend | Determines how the appliance connected to the specified port handles priority traffic received on its incoming port. |

tacacs-server attempts

Use the **tacacs-server attempts** global configuration command to control the number of login attempts that can be made on a line set up for Terminal Access Controller Access Control System (TACACS), Extended TACACS, or TACACS+ verification. Use the **no** form of this command to disable this feature and to restore the default.

tacacs-server attempts *count*

no tacacs-server attempts

| | | |
|--------------------|---|--|
| Syntax Description | <i>count</i> Integer that sets the number of attempts. The range is from 1 to 1000. | |
| Defaults | The default number of login attempts is 3. | |
| Command Modes | Global configuration | |
| Command History | Release | Modification |
| | 11.2(8)SA6 | This command was first introduced. |
| Examples | <p>This example shows how to change the login attempt to just one:</p> <pre>Switch(config)# tacacs-server attempts 1</pre> <p>You can verify the previous command by entering the show running-config privileged EXEC command.</p> | |
| Related Commands | Command | Description |
| | login tacacs | Configures the switch to use TACACS user authentication. |
| | show tacacs | Displays various TACACS+ server statistics. |
| | tacacs-server directed request | Sends only a username to a specified server when a direct request is issued in association with TACACS, Extended TACACS, and TACACS+. |
| | tacacs-server host | Specifies a TACACS, Extended TACACS, or TACACS+ host. |
| | tacacs-server key | Specifies the authentication encryption key used for all TACACS+ communications between the access server and the TACACS+ daemon. |
| | tacacs-server last-resort | Causes the network access server to request the privileged password as verification for TACACS or Extended TACACS or to allow successful login without further user input. |
| | udld | Specifies the interval that the server waits for a TACACS, Extended TACACS, or TACACS+ server to reply. |

tacacs-server dns-alias-lookup

Use the **tacacs-server dns-alias-lookup** global configuration command to enable IP Domain Name System alias lookup for Terminal Access Controller Access Control System Plus (TACACS+). Use the **no** form of this command to disable this feature.

tacacs-server dns-alias-lookup

no tacacs-server dns-alias-lookup

| | |
|---------------------------|--|
| Syntax Description | This command has no keywords or arguments. |
|---------------------------|--|

| | |
|-----------------|-----------------------------------|
| Defaults | The DNS alias lookup is disabled. |
|-----------------|-----------------------------------|

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

| | | |
|------------------------|----------------|------------------------------------|
| Command History | Release | Modification |
| | 11.2(8)SA6 | This command was first introduced. |

| | |
|-----------------|--|
| Examples | This example shows how to enable the IP DNS alias lookup: Switch(config)# tacacs-server dns-alias-lookup |
| | You can verify the previous command by entering the show running-config privileged EXEC command. |

| | | |
|-------------------------|-----------------------|---|
| Related Commands | Command | Description |
| | ip domain-name | Defines a default domain name that is used to complete unqualified host names (names without a dotted-decimal domain name). |
| | ip name-server | Specifies the address of one or more name servers to use for name and address resolution. |

udld

Use the **udld** interface configuration command to enable UniDirectional Link Detection (UDLD) on a port to assist with the detection of spanning-tree loops on logical one-way connections. Use the **no** form of this command to return the port setting to the global setting.

udld {enable | disable}

no udld {enable | disable}

| | | |
|--------------------|--|---|
| Syntax Description | enable | Enable UDLD on the specified port. |
| | disable | Disable UDLD on the specified port. |
| Defaults | UDLD follows the setting of the udld enable global configuration command and is disabled on all ports. | |
| Command Modes | Interface configuration | |
| Command History | Release | Modification |
| | 12.0(5)XU | This command was first introduced. |
| Usage Guidelines | <p>UDLD is supported on fiber- and copper-based Ethernet ports.</p> <p>UDLD is not supported on ATM interfaces.</p> <p>A UDLD-capable port cannot detect a unidirectional link if it is connected to a UDLD-incapable port of another switch.</p> <p>Setting UDLD on an interface overrides the global UDLD configuration for that specific interface.</p> | |
| Examples | <p>This example shows how to enable UDLD on port 2:</p> <pre>Switch(config)# interface fastethernet 0/2 Switch(config-if)# udld enable</pre> <p>You can verify the previous command by entering the show running-config or the show udld interface command in privileged EXEC mode.</p> | |
| Related Commands | Command | Description |
| | show running-config | Displays the running configuration on the switch. |
| | udld enable | Enables UDLD on all ports on the switch. |
| | udld reset | Resets any interface that has been shut down by UDLD. |

udld enable

Use the **udld enable** global configuration command to enable UniDirectional Link Detection (UDLD) on all ports on the switch to assist with the detection of spanning-tree loops on logical one-way connections. Use the **no** form of this command to return the switch setting to its default value.

udld enable

no udld enable

| | |
|---------------------------|--|
| Syntax Description | This command has no keywords or arguments. |
|---------------------------|--|

| | |
|-----------------|---------------------------------|
| Defaults | UDLD is disabled on the switch. |
|-----------------|---------------------------------|

| | |
|----------------------|---------------------------|
| Command Modes | Global configuration mode |
|----------------------|---------------------------|

| Command History | Release | Modification |
|------------------------|-----------|------------------------------------|
| | 12.0(5)XU | This command was first introduced. |

| | |
|-------------------------|--|
| Usage Guidelines | UDLD is supported on fiber- and copper-based Ethernet ports. |
| | UDLD is not supported on Asynchronous Transfer Mode (ATM) interfaces. |
| | A UDLD-capable port cannot detect a unidirectional link if it is connected to a UDLD-incapable port of another switch. |
| | The udld enable global configuration command setting is overwritten by each specific port UDLD configuration. |

| | |
|-----------------|---|
| Examples | This example shows how to enable UDLD on the switch: Switch(config)# udld enable |
| | You can verify the previous command by entering the show running-config in privileged EXEC mode. |

| Related Commands | Command | Description |
|-------------------------|----------------------------|---|
| | show running-config | Displays the running configuration on the switch. |
| | udld | Enables UDLD on a port. |
| | udld reset | Resets any interface that has been shut down by UDLD. |

uddl reset

Use the **uddl reset** privileged EXEC command to reset all interfaces that have been shut down by UniDirectional Link Detection (UDLD).

uddl reset

Syntax Description This command has no keywords or arguments.

Command Modes Privileged EXEC mode

| Command History | Release | Modification |
|-----------------|-----------|------------------------------------|
| | 12.0(5)XU | This command was first introduced. |

Examples This example shows how to reset all interfaces that have been shut down by UDLD:

```
Switch# uddl reset
1 ports shutdown by UDLD were reset.
```

You can verify the previous command by entering the **show uddl** user EXEC command.

| Related Commands | Command | Description |
|------------------|----------------------------|---|
| | show running-config | Displays the running configuration on the switch. |
| | uddl | Enables UDLD on a port. |
| | uddl enable | Enables UDLD on all ports on the switch. |

vlan

Use the **vlan** VLAN database command to configure VLAN characteristics. Use the **no** form of this command to delete a VLAN and its configured characteristics.

```
vlan vlan-id [name vlan-name] [media {ethernet | fddi | fdi-net | tokenring | tr-net}]
[state {suspend | active}] [said said-value] [mtu mtu-size] [ring ring-number]
[bridge bridge-number / type {srb | srt}] [parent parent-vlan-id]
[stp type {ieee | ibm | auto}] [are are-number] [ste ste-number]
[backupcrf {enable | disable}] [tb-vlan1 tb-vlan1-id] [tb-vlan2 tb-vlan2-id]
```

```
no vlan vlan-id [name vlan-name] [media {ethernet | fddi | fdi-net | tokenring | tr-net}]
[state {suspend | active}] [said said-value] [mtu mtu-size] [ring ring-number]
[bridge bridge-number / type {srb | srt}] [parent parent-vlan-id]
[stp type {ieee | ibm | auto}] [are are-number] [ste ste-number]
[backupcrf {enable | disable}] [tb-vlan1 tb-vlan1-id] [tb-vlan2 tb-vlan2-id]
```



Note

Catalyst 2900 XL and Catalyst 3500 XL switches support 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.

Table 2-7 lists the valid syntax for each media type.

Table 2-7 Valid Syntax for Different Media Types

| Media Type | Valid Syntax |
|--|--|
| Ethernet | vlan <i>vlan-id</i> [name <i>vlan-name</i>] media ethernet [state { suspend active }] [said <i>said-value</i>] [mtu <i>mtu-size</i>] [tb-vlan1 <i>tb-vlan1-id</i>] [tb-vlan2 <i>tb-vlan2-id</i>] |
| FDDI | vlan <i>vlan-id</i> [name <i>vlan-name</i>] media fddi [state { suspend active }] [said <i>said-value</i>] [mtu <i>mtu-size</i>] [ring <i>ring-number</i>] [parent <i>parent-vlan-id</i>] [tb-vlan1 <i>tb-vlan1-id</i>] [tb-vlan2 <i>tb-vlan2-id</i>] |
| FDDI-NET | vlan <i>vlan-id</i> [name <i>vlan-name</i>] media fdi-net [state { suspend active }] [said <i>said-value</i>] [mtu <i>mtu-size</i>] [bridge <i>bridge-number</i>] [stp type { ieee ibm auto }] [tb-vlan1 <i>tb-vlan1-id</i>] [tb-vlan2 <i>tb-vlan2-id</i>] If VTP V2 mode is disabled, do not set the stp type to auto . |
| Token Ring | VTP V2 mode is disabled. vlan <i>vlan-id</i> [name <i>vlan-name</i>] media tokenring [state { suspend active }] [said <i>said-value</i>] [mtu <i>mtu-size</i>] [ring <i>ring-number</i>] [parent <i>parent-vlan-id</i>] [tb-vlan1 <i>tb-vlan1-id</i>] [tb-vlan2 <i>tb-vlan2-id</i>] |
| Token Ring concentrator relay function (TRCRF) | VTP V2 mode is enabled. vlan <i>vlan-id</i> [name <i>vlan-name</i>] media tokenring [state { suspend active }] [said <i>said-value</i>] [mtu <i>mtu-size</i>] [ring <i>ring-number</i>] [parent <i>parent-vlan-id</i>] [bridge type { srb srt }] [are <i>are-number</i>] [ste <i>ste-number</i>] [backupcrf { enable disable }] [tb-vlan1 <i>tb-vlan1-id</i>] [tb-vlan2 <i>tb-vlan2-id</i>] |

Table 2-7 Valid Syntax for Different Media Types (continued)

| Media Type | Valid Syntax |
|--|---|
| Token Ring-NET | VTP V2 mode is disabled. vlan <i>vlan-id</i> [name <i>vlan-name</i>] media tr-net [state { suspend active }] [said <i>said-value</i>] [mtu <i>mtu-size</i>] [bridge <i>bridge-number</i>] [stp type { ieee ibm }] [tb-vlan1 <i>tb-vlan1-id</i>] [tb-vlan2 <i>tb-vlan2-id</i>] |
| Token Ring bridge relay function (TRBRF) | VTP V2 mode is enabled. vlan <i>vlan-id</i> [name <i>vlan-name</i>] media tr-net [state { suspend active }] [said <i>said-value</i>] [mtu <i>mtu-size</i>] [bridge <i>bridge-number</i>] [stp type { ieee ibm auto }] [tb-vlan1 <i>tb-vlan1-id</i>] [tb-vlan2 <i>tb-vlan2-id</i>] |

VLAN Configuration Rules

Table 2-8 describes the rules for configuring VLANs.

Table 2-8 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. |
| VTP V2 mode is enabled, and you are configuring a TRBRF VLAN media type. | Specify a bridge number. Do not leave this field blank. |

Table 2-8 VLAN Configuration Rules (continued)

| Configuration | Rule |
|---|--|
| VTP V2 mode is disabled. | 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). |

Syntax Description

| | |
|-------------------|---|
| <i>vlan-id</i> | ID of the configured VLAN. Valid IDs are from 1 to 1005 and must be unique within the administrative domain. Do not enter leading zeroes. |
| name | (Optional) Keyword to be followed by the VLAN name. |
| <i>vlan-name</i> | ASCII string from 1 to 32 characters that must be unique within the administrative domain. |
| media | (Optional) Keyword to be followed by the VLAN media type. |
| ethernet | Ethernet media type. |
| fddi | FDDI media type. |
| fddi-net | FDDI network entity title (NET) media type. |
| tokenring | Token Ring media type if the VTP V2 mode is disabled. TRCRF media type if the VTP V2 mode is enabled. |
| tr-net | Token Ring network entity title (NET) media type if the VTP V2 mode is disabled. TRBRF media type if the VTP V2 mode is enabled. |
| state | (Optional) Keyword to be followed by the VLAN state. |
| active | VLAN is operational. |
| suspend | VLAN is suspended. Suspended VLANs do not pass packets. |
| said | (Optional) Keyword to be followed by the security association identifier (SAID) as documented in IEEE 802.10. |
| <i>said-value</i> | Integer from 1 to 4294967294 that must be unique within the administrative domain. |
| mtu | (Optional) Keyword to be followed by the maximum transmission unit (packet size in bytes). |
| <i>mtu-size</i> | Packet size in bytes from 1500 to 18190 that the VLAN can use. |

| | |
|---|--|
| ring | (Optional) Keyword to be followed by the logical ring for an FDDI, Token Ring, or TRCRF VLAN. |
| <i>ring-number</i> | Integer from 1 to 4095. |
| bridge | (Optional) Keyword to be followed by the logical distributed source-routing bridge. This bridge that interconnects all logical rings having this VLAN as a parent VLAN in FDDI-NET, Token Ring-NET, and TRBRF VLANs. |
| <i>bridge-number</i> | Integer from 0 to 15. |
| type | Keyword to be followed by the bridge type. Applies only to TRCRF VLANs. |
| srb | Source-route bridging VLAN. |
| srt | Source-route transparent bridging VLAN. |
| parent | (Optional) Keyword to be followed by 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. |
| <i>parent-vlan-id</i> | Integer from 0 to 1005. |
| stp type | (Optional) Keyword to be followed by the spanning-tree type for FDDI-NET, Token Ring-NET, or TRBRF VLAN. |
| ieee | IEEE Ethernet STP running source-route transparent (SRT) bridging. |
| ibm | IBM STP running source-route bridging (SRB). |
| auto | STP running a combination of source-route transparent bridging (IEEE) and source-route bridging (IBM). |
| are | Keyword to be followed by the number of all-routes explorer (ARE) hops. This keyword applies only to TRCRF VLANs. |
| <i>are-number</i> | Integer from 0 to 13 that defines the maximum number of ARE hops for this VLAN. |
| ste | Keyword to be followed by the number of spanning-tree explorer (STE) hops. This keyword applies only to TRCRF VLANs. |
| <i>ste-number</i> | Integer from 0 to 13 that defines the maximum number of STE hops for this VLAN. |
| backupcrf | Keyword to be followed by the backup CRF mode. This keyword applies only to TRCRF VLANs. |
| enable | Enable backup CRF mode for this VLAN. |
| disable | Disable backup CRF mode for this VLAN. |
| tb-vlan1 and tb-vlan2 | (Optional) Keyword to be followed by the first and second VLAN to which this VLAN is translationally bridged. Translational VLANs translate FDDI or Token Ring to Ethernet, for example. |
| <i>tb-vlan1-id</i> and <i>tb-vlan2-id</i> | Integer that ranges from 0 to 1005. |

Defaults

The *vlan-name* variable is *VLANxxxx*, where *xxxx* represents four numeric digits (including leading zeroes) equal to the VLAN ID number.

The **media** type is **ethernet**.

The state is **active**.

The *said value* is 100000 plus the VLAN ID.

The *mtu size* for Ethernet, FDDI, and FDDI-NET VLANs is 1500 bytes. The MTU size for Token Ring and Token Ring-NET VLANs is 1500 bytes. The MTU size for TRBRF and TRCRF VLANs is 4472 bytes.

The *ring number* for Token Ring VLANs is zero. For FDDI VLANs, there is no default. For TRCRF VLANs, you must specify a ring number.

The bridge number is zero (no source-routing bridge) for FDDI-NET and Token Ring-NET VLANs. For TRBRF VLANs, you must specify a bridge number.

The parent VLAN ID is zero (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 STP type is **ieee** for FDDI-NET VLANs. For Token Ring-NET and TRBRF VLANs, the default is **ibm**.

The ARE value is 7.

The STE value is 7.

Backup CRF is disabled.

The *tb-vlan1-id* and *tb-vlan2-id* variables are zero (no translational bridging).

Command Modes

VLAN database

Command History

| Release | Modification |
|------------|------------------------------------|
| 11.2(8)SA4 | This command was first introduced. |

Usage Guidelines

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* **name** *vlan-name* form is used, the VLAN name returns to the default name (VLANxxxx, where xxxx represent four numeric digits (including leading zeroes) equal to the VLAN ID number).

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**, and **tb-vlan2** keywords, or any combination are also present in the command.

When the **no vlan** *vlan-id* **state** form is used, the VLAN state returns to the default (**active**).

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* **mtu** form is used, the VLAN MTU returns to the default for the applicable VLAN media type. You can also modify the MTU by using the **media** keyword.

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* bridge** form is used, the VLAN source-routing bridge number returns to the default (0). The **vlan *vlan-id* bridge** command is only used for FDDI-NET and Token Ring-NET VLANs and is ignored in other VLAN types.

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* 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 zeroes) 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**. The VLAN is added if it did not already exist; otherwise, this command does nothing.

```
Switch(vlan)# vlan 2
```

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 the previous commands by entering the **show vlan** user 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 database

Use the **vlan database** privileged EXEC command to enter VLAN database mode from the command-line interface (CLI). From the CLI, you can add, delete, and modify VLAN configurations and globally propagate these changes by using the VLAN Trunking Protocol (VTP).

vlan database

| | |
|---------------------------|--|
| Syntax Description | This command has no arguments or keywords. |
|---------------------------|--|

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

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

| | | |
|------------------------|----------------|------------------------------------|
| Command History | Release | Modification |
| | 11.2(8)SA4 | This command was first introduced. |

| | |
|-------------------------|---|
| Usage Guidelines | To return to the privileged EXEC mode from the VLAN database 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** commands. 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**.

| | |
|-----------------|---|
| Examples | This example shows how to enter the VLAN database mode from the privileged EXEC mode: |
|-----------------|---|

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

| | | |
|-------------------------|----------------------|--|
| Related Commands | Command | Description |
| | abort | Abandons the proposed VLAN database, exits VLAN database mode, and returns to privileged EXEC mode. |
| | apply | Implements the proposed VLAN database, increments the database configuration revision number, propagates it throughout the administrative domain, and remains in VLAN database mode. |
| | reset | Abandons the proposed VLAN database and remains in VLAN database mode. Resets the proposed database to the currently implemented VLAN database on the switch. |
| | shutdown vlan | Shuts down (suspends) local traffic on the specified VLAN. |

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 |
| | 11.2(8)SA4 | This command was first introduced. |

| | |
|-----------------|---|
| Examples | This example shows how to immediately send VQP queries to the VMPS: |
|-----------------|---|

```
Switch# vmps reconfirm
```

You can verify the previous command by entering the **show vmps** user 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 reconfirmation timer expiring or because the **vmps reconfirm** command was entered.

| | | |
|-------------------------|---|--|
| Related Commands | Command | Description |
| | show vmps | Displays VQP and VMPS information. |
| | vmps reconfirm (privileged EXEC) | Sends VQP queries to reconfirm all dynamic VLAN assignments with the VMPS. |
| | and vmps reconfirm (global Configuration) | |

vmmps reconfirm (global Configuration)

Use the **vmmps reconfirm** global configuration command to change the reconfirmation interval for the VLAN Query Protocol (VQP) client.

vmmps 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 |
|-----------------|------------|------------------------------------|
| | 11.2(8)SA4 | This command was first introduced. |

| Examples | <p>This example shows how to set the VQP client to reconfirm dynamic VLAN entries every 20 minutes:</p> <pre>Switch(config)# vmmps reconfirm 20</pre> <p>You can verify the previous command by entering the show vmmps user EXEC command and examining information in the Reconfirm Interval row.</p> |
|----------|--|
|----------|--|

| Related Commands | Command | Description |
|------------------|--|--|
| | show vmmps | Displays VQP and VMPS information. |
| | vmmps reconfirm (privileged EXEC) and | Sends VQP queries to reconfirm all dynamic VLAN assignments with the VMPS. |
| | vmmps reconfirm (global Configuration) | |

vmps retry

Use the **vmps retry** global configuration command to configure the per-server retry count for the VLAN Query Protocol (VQP) client.

vmps retry *count*

Syntax Description

| <i>count</i> | Description |
|--------------|--|
| | 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 |
|------------|------------------------------------|
| 11.2(8)SA4 | This command was first introduced. |

Examples

This example shows how to set the retry count to 7:

```
Switch(config)# vmps retry 7
```

You can verify the previous command by entering the **show vmps** user EXEC command and examining information in the Server Retry Count row.

Related Commands

| Command | Description |
|------------------|------------------------------------|
| show vmps | 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 | <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. |
| | primary | (Optional) Determines whether primary or secondary VMPS servers are being configured. |

| | |
|----------|---|
| Defaults | No primary or secondary VMPS servers are defined. |
|----------|---|

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

| Command History | Release | Modification |
|-----------------|------------|------------------------------------|
| | 11.2(8)SA4 | This command was first introduced. |

| | |
|------------------|---|
| Usage Guidelines | <p>The first server entered is automatically selected as the primary server whether or not primary 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

This example shows how to configure the server with IP address 191.10.49.20 as the primary VMPS server. The servers with IP addresses 191.10.49.21 and 191.10.49.22 are configured as secondary servers:

```
Switch(config)# vmps server 191.10.49.20 primary
Switch(config)# vmps server 191.10.49.21
Switch(config)# vmps server 191.10.49.22
```

This example shows how to delete the server with IP address 191.10.49.21:

```
Switch(config)# no vmps server 191.10.49.21
```

You can verify the previous commands by entering the **show vmps** user EXEC command and examining information in the VMPS Domain Server row.

Related Commands

| Command | Description |
|------------------|------------------------------------|
| show vmps | Displays VQP and VMPS information. |

vtp

Use the **vtp** VLAN database command to configure the VLAN Trunking Protocol (VTP) mode. Use the **no** form of this command to return to the default setting.

vtp {server | client | transparent}

no vtp {server | client | transparent}

| Syntax Description | | |
|--------------------|--|--|
| 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 VTP database from nonvolatile storage after reboot. |
| 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 transmit VTP advertisements until it receives advertisements to initialize its VLAN database. |
| transparent | | Place the switch in VTP transparent mode. A switch in VTP transparent mode is disabled for VTP, does not transmit 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. The configuration of multi-VLAN ports causes the switch to automatically enter transparent mode. |



Note

The switch supports up to 250 VLANs on the Catalyst 2912MF, 2924M, and Catalyst 3500 XL switches. All other Catalyst 2900 XL switches support up to 64 VLANs. If you define more than 250 or 64, respectively, or if the switch receives an advertisement that contains more than 250 or 64 VLANs, the switch automatically enters VTP transparent mode and operates with the VLAN configuration preceding the one that put it into transparent mode. The count of 250 or 64 VLANs always includes VLAN 1 but never includes VLANs 1002 to 1005. The switch can have 250 or 64 active VLANs, plus VLANs 1002 through 1005, which are inactive.

Defaults

Server mode is the default mode.

Command Modes

VLAN database

Command History

| Release | Modification |
|------------|------------------------------------|
| 11.2(8)SA4 | This command was first introduced. |

Usage Guidelines

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.

Examples

This example shows how to place the switch in VTP transparent mode:

```
Switch(vlan)# vtp transparent
```

You can verify the previous commands by entering the **show vtp status** privileged EXEC command.

Related Commands

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

vtp domain

Use the **vtp domain** VLAN database command to configure the VLAN Trunking Protocol (VTP) administrative domain.

vtp domain *domain-name*

| Syntax Description | <i>domain-name</i> ASCII string from 1 to 32 characters that identifies the VTP administrative domain for the switch. The domain name is case sensitive. |
|--------------------|--|
|--------------------|--|

| Defaults | No domain name is defined. |
|----------|----------------------------|
|----------|----------------------------|

| Command Modes | VLAN database |
|---------------|---------------|
|---------------|---------------|

| Command History | Release | Modification |
|-----------------|------------|------------------------------------|
| | 11.2(8)SA4 | This command was first introduced. |

| Usage Guidelines | <p>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 transmit 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 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 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.</p> |
|------------------|---|
|------------------|---|

Domain names are case sensitive.

Once you configure a domain name, it cannot be removed. You can only reassign it to a different domain.

| Examples | This example shows how to set the administrative domain for the switch: |
|----------|---|
|----------|---|

```
Switch(vlan)# vtp domain OurDomainName
```

You can verify the previous commands by entering the **show vtp status** user EXEC command.

| Related Commands | Command | Description |
|------------------|------------------------|---|
| | show vtp status | Displays general information about the VTP management domain, status, and counters. |
| | vtp password | Configures the VTP administrative domain password. |

vtp file

Use the **vtp file** global configuration command to modify the VLAN Trunking Protocol (VTP) configuration storage filename. Use the **no** form of this command to return the filename to its default name.

vtp file *ifsfilename*

no vtp file

| | | |
|--------------------|--|------------------------------------|
| Syntax Description | <i>ifsfilename</i> The IOS IFS filename where the VTP VLAN configuration is stored. | |
| Defaults | The default filename is <i>flash:vlan.dat</i> . | |
| Command Modes | Global configuration | |
| Command History | Release | Modification |
| | 11.2(8)SA4 | This command was first introduced. |
| Usage Guidelines | This command cannot be used to load a new database; it only renames the file in which the existing database is stored. | |
| Examples | This example shows how to rename the filename for VTP configuration storage to <i>vtpfilename</i> : Switch(config)# vtp file vtpfilename | |
| Related Commands | Command | Description |
| | vtp | Configures the VTP mode. |

vtp password

Use the **vtp password** VLAN database command to configure the VLAN Trunking Protocol (VTP) administrative domain password. Use the **no** form of this command to remove the password.

vtp password *password-value*

no vtp password *password-value*

| | | |
|--------------------|--|--|
| Syntax Description | password | Set the 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. |
| | <i>password-value</i> | ASCII string from 8 to 64 characters. The password is case sensitive. |
| Defaults | No password is defined. | |
| Command Modes | VLAN database | |
| Command History | Release | Modification |
| | 11.2(8)SA4 | This command was first introduced. |
| Usage Guidelines | <p>Passwords are case sensitive. Passwords should match on all switches in the same domain.</p> <p>When the no vtp password form of the command is used, the switch returns to the no-password state.</p> | |
| Examples | <p>This example shows how to configure the VTP domain password:</p> <pre>Switch(vlan)# vtp password ThisIsOurDomainsPassword</pre> | |
| Related Commands | Command | Description |
| | vtp domain | Configures the VTP administrative domain. |

vtp pruning

Use the **vtp pruning** VLAN database command to enable pruning in the VLAN Trunking Protocol (VTP) administrative domain. Use the **no** form of this command to disable pruning.

vtp pruning

no vtp pruning

Syntax Description This command has no arguments or keywords.

Defaults Pruning is disabled.

Command Modes VLAN database

| Release | Modification |
|------------|------------------------------------|
| 11.2(8)SA4 | This command was first introduced. |

Usage Guidelines

- 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.
- VLANs 2 through 1001 are pruning-eligible on Catalyst 2900 XL and Catalyst 3500 XL trunk ports.
- Pruning is supported with VTP version 1 and version 2.

Examples

This example shows how to enable pruning in the proposed VLAN database:

```
Switch(vlan)# vtp pruning
```

You can verify the previous commands by entering the **show vtp status** user EXEC command.

| Command | Description |
|---|---|
| show interface <i>interface-id</i> pruning | Displays pruning information for the trunk port. |
| show vtp status | Displays general information about the VTP management domain, status, and counters. |
| switchport trunk pruning | Configures the VLAN pruning-eligible list for ports in trunking mode. |

vtp v2-mode

Use the **vtp v2-mode** VLAN database command to enable VLAN Trunking Protocol (VTP) version 2 in the administrative domains. Use the **no** form of this command to disable V2 mode.

vtp v2-mode

no vtp v2-mode

| | |
|---------------------------|--|
| Syntax Description | This command has no arguments or keywords. |
|---------------------------|--|

| | |
|-----------------|----------------------------|
| Defaults | VTP version 2 is disabled. |
|-----------------|----------------------------|

| | |
|----------------------|---------------|
| Command Modes | VLAN database |
|----------------------|---------------|

| | | |
|------------------------|----------------|------------------------------------|
| Command History | Release | Modification |
| | 11.2(8)SA4 | This command was first introduced. |

| | |
|-------------------------|---|
| Usage Guidelines | <p>Toggling the V2 mode state modifies certain parameters of certain default VLANs.</p> <p>Each VTP switch automatically detects the capabilities of all the other VTP devices. To use V2 mode, all VTP switches in the network must support version 2; otherwise, you must configure them to operate in VTP version 1 mode (no vtp v2-mode).</p> <p>If you are using VTP in a Token Ring environment, VTP V2 mode must be enabled.</p> <p>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.</p> <p>If you are configuring a Token Ring or Token Ring-NET VLAN media type, you must use version 1.</p> |
|-------------------------|---|

| | |
|-----------------|---|
| Examples | This example shows how to enable V2 mode in the proposed VLAN database: |
|-----------------|---|

```
Switch(vlan)# vtp v2-mode
```

You can verify the previous commands by entering the **show vtp status** user EXEC command.

| | | |
|-------------------------|------------------------|---|
| Related Commands | Command | Description |
| | show vtp status | Displays general information about the VTP management domain, status, and counters. |
| | vtp | Configures the VTP mode. |
| | vtp pruning | Enables pruning in the VTP administrative domain. |

