Catalyst 2950 Desktop Switch Command Reference

Cisco IOS Release 12.0(5)WC(1)
April 2001

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-7811381=
Text Part Number: 78-11381-01

Catalyst 2950 Desktop Switch Command Reference

Preface

The *Catalyst 2950 Desktop Switch Command Reference* describes the commands for the Catalyst 2950 switches (hereafter referred to as the 2950 switch).

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more up to date than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or http://www-europe.cisco.com.

If you are reading Cisco product documentation on the World Wide Web, you can submit comments electronically. Click **Feedback** in the toolbar, and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco. We appreciate your comments.

Audience and Scope

This document is for the networking professional managing a 2950 switch from the Cisco IOS command-line interface (CLI). We assume that you have experience working with Cisco IOS and are familiar with the concepts and terminology of Ethernet and local area networking.

This guide provides the information you need to configure features added to this software release.

Organization

This guide is organized into the following chapters:

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.

Examples use these conventions:

- Terminal sessions and system displays are in `screen` font.
- Information you enter is in **`boldface screen`** font.
- Angle brackets (< >) indicate nonprinting characters such as passwords.

Related Publications

You can order printed copies of documents with a DOC-xxxxxx= number. For more information, see the "Obtaining Documentation" section on page xi.

The following publications provide more information about the switches:

- Cisco Catalyst 2950 Desktop Switch Documentation CD

  This CD is shipped with the switch and contains the following documents:

  – *This Catalyst 2950 Desktop Switch Command Reference, Cisco IOS Release 12.0(5)WC(1)* (order number DOC-7811381=)

  – The *Catalyst 2950 Desktop Switch Software Configuration Guide, Cisco IOS Release 12.0(5)WC(1)* (order number DOC-7811380=)

  – *The Catalyst 2950 Desktop Switch Hardware Installation Guide* (order number DOC-7811157=)

- *Release Notes for the Catalyst 2950 Cisco IOS Release 12.0(5)WC(1)*

Notes and Cautions

Notes and cautions 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 equipment damage or loss of data.

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

Documentation CD-ROM

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

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 an 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.

CHAPTER 1

Using the Command-Line Interface

The Catalyst 2950 switches are supported by Cisco IOS software. These switches support Cisco IOS Release 12.0(5)WC(1). This chapter describes how to use the switch command-line interface (CLI) to configure the software. For a complete description of the commands that support these features, see Chapter 2, "Cisco IOS Commands." For more information on Cisco IOS Release 12.0, refer to the *Cisco IOS Release 12.0 Command Summary.*

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.

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.(5)WC(1) runs on a variety of 2950 switches. For a complete list, see the *Release Notes for Catalyst 2950 Series, Cisco IOS Release 12.0(5)WC(1).*

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. The Cisco IOS command modes are as follows:

- 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 will see in that mode, and how to exit that mode. The prompts listed assume the default name *Switch*.

Table 1-1 Command Modes Summary

Command Mode	Access Method	Prompt	Exit or Access Next Mode
User EXEC	This is the first level of access. (For the switch) Change terminal settings, perform basic tasks, and list system information.	`Switch>`	Enter the **logout** command.
Privileged EXEC	From user EXEC mode, enter the **enable** user EXEC command.	`Switch#`	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)#`	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)#`	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.
Line configuration	From global configuration mode, specify a line by entering the **line** command.	`Switch (config-line)#`	To exit to global configuration mode, enter the **exit** command. To return to privileged EXEC mode, enter the **end** command, or press **Ctrl-Z**.

User EXEC Mode

After you access the device, you are automatically in user EXEC command mode. The EXEC commands available at the user level are a subset of those available at the privileged level. In general, 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> ?
```

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 is not displayed on the screen and is case sensitive.

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

```
Switch#
```

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

```
Switch> enable
Switch#
```

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

```
Switch# ?
```

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

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 new VLAN database and 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, the console prompts you for the source of the configuration commands:

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

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

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

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

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

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

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)#
```

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.

The following examples shows how to enter line configuration mode for virtual terminal line 7:

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

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

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

To exit line configuration mode and 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**.

Searching and Filtering Output of show and more Commands

You can search and filter the output for **show** and **more** commands. This functionality is useful when you need to sort through large amounts of output or if you want to exclude output that you do not need to see.

To use this functionality, enter a **show** or **more** command followed by the *pipe* character (|), one of the keywords **begin**, **include**, or **exclude**, and an expression that you want to search for or filter out:

command **|** {**begin** | **include** | **exclude**} *regular-expression*

The following is an example of the **show igmp snooping** command where the display begins with the lines that match the expression *vlan 2*.

```
switch# show ip igmp snooping | begin vlan 2
vlan 2
----------
IGMP snooping is globally enabled
IGMP snooping is enabled on this Vlan
IGMP snooping immediate-leave is disabled on this Vlan
IGMP snooping mrouter learn mode is pim-dvmrp on this Vlan
IGMP snooping is running in IGMP_ONLY mode on this Vlan
vlan 3
----------
IGMP snooping is globally enabled
IGMP snooping is enabled on this Vlan
IGMP snooping immediate-leave is disabled on this Vlan
IGMP snooping mrouter learn mode is pim-dvmrp on this Vlan
```

The following is an example of the **show igmp snooping** command where the display excludes the lines that match the expression *globally*.

```
switch# show ip igmp snooping | exclude globally
IGMP snooping is enabled on this Vlan
IGMP snooping immediate-leave is disabled on this Vlan
IGMP snooping mrouter learn mode is cgmp on this Vlan
IGMP snooping is running in IGMP_CGMP mode on this Vlan
vlan 2
----------
IGMP snooping is enabled on this Vlan
IGMP snooping immediate-leave is disabled on this Vlan
IGMP snooping mrouter learn mode is pim-dvmrp on this Vlan
IGMP snooping is running in IGMP_ONLY mode on this Vlan
vlan 3
----------
IGMP snooping is enabled on this Vlan
IGMP snooping immediate-leave is disabled on this Vlan
IGMP snooping mrouter learn mode is pim-dvmrp on this Vlan
```

The following is an example of the **show igmp snooping** command where the display includes the lines that match the expression *disabled*.

```
switch# show ip igmp snooping | include disabled
IGMP snooping immediate-leave is disabled on this Vlan
IGMP snooping immediate-leave is disabled on this Vlan
IGMP snooping immediate-leave is disabled on this Vlan
```

Command Summary

Table 1-2 lists and describes the Cisco IOS commands for the 2950 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 could be.
show cluster members	Displays information about all members in a cluster.
show ntp associations	Displays the status of NTP associations.
show ntp status	Displays the status of NTP.
show spanning-tree	Displays Spanning Tree Protocol (STP) information.
show udld	Displays UniDirectional Link Detection (UDLD) status information for all or the specified port.
show vlan	Displays information about a VLAN.
show version	Displays the firmware version for the switch or module.
show vtp counters **show vtp status**	Displays general information about the VTP management domain, status, and counters.
show wrr-queue bandwidth	Displays the weighted round-robin (WRR) bandwidth allocation for the four class of service (CoS) priority queues.
show wrr-queue cos-map	Displays the mapping of the CoS values to the CoS priority queues.
Privileged EXEC mode	
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 vtp counters	Clears the VLAN Trunk Protocol (VTP) counters.
cluster setup	Automatically builds a cluster.
delete	Deletes a file from the file system.

Table 1-2 Command Summary (continued)

Commands	Description
show env	Displays the status of the switch fans.
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 snooping	Displays the IGMP snooping for all VLANs.
show ip igmp snooping vlan	Displays the IGMP snooping configuration of the VLAN.
show ip igmp snooping mrouter	Displays the statically and dynamically learned multicast router ports.
show mac-address-table	Displays the MAC address table.
show mac-address-table multicast	Displays the Layer 2 multicast entries for a VLAN.
show port group	Displays the ports that are assigned to groups.
show port monitor	Displays the ports that have port monitoring enabled.
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 rps	Displays the status of the Cisco Redundant Power System (RPS).
show tacacs	Displays various Terminal Access Controller Access Control System Plus (TACACS+) server statistics.
udld reset	Resets any port that has been shut down by UDLD.
vlan database	Enters VLAN database mode.
Global configuration mode	
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.
cluster standby-group	Enables command switch redundancy by binding an Hot Standby Router Protocol (HSPR) standby group to the cluster.
cluster timer	Sets the interval between heartbeat messages between the command and member switches. Used with the **cluster holdtime** command.

Table 1-2 Command Summary (continued)

Commands	Description
enable last-resort	Specifies what happens if the Terminal Access Controller Access Control System (TACACS) and Extended TACACS servers used by the **enable** command do not respond.
enable use-tacacs	Enables the use of TACACS to determine whether a user can access the privileged command level.
interface	Selects an interface to configure. Creates a new management VLAN interface.
ip igmp snooping	Enables IGMP snooping.
ip igmp snooping vlan	Enables IGMP snooping on the VLAN interface.
ip igmp snooping vlan immediate-leave	Configures IGMP Immediate-Leave processing.
ip igmp snooping vlan mrouter	Configures a Layer 2 port as a multicast router port.
ip igmp snooping vlan static	Configures a Layer 2 port as a member of a group.
mac-address-table aging-time	Sets the length of time that a dynamic entry remains in the address table.
mac-address-table secure	Adds a secure address entry to the address table.
mac-address-table static	Adds a static address entry to the address table.
ntp access-group	Controls access to the system's NTP services.
ntp authenticate	Enables NTP authentication.
ntp authentication-key	Defines an authentication key for NTP.
ntp broadcastdelay	Sets the estimated round-trip delay between the Cisco IOS software and an NTP broadcast server.
ntp clock-period	Determines the clock error.
ntp max-associations	Sets the maximum number of NTP associations that are allowed on a server.
ntp peer	Configures the router system clock to synchronize a peer or to be synchronized by a peer.
ntp server	Allows the router system clock to be synchronized by a time server.
ntp source	Uses a particular source address in NTP packets.
ntp trusted-key	Authenticates the identity of a system to which NTP will synchronize.
shutdown vlan	Shuts down local traffic on the specified VLAN.
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 an instance of STP.
spanning-tree forward-time	Specifies the forward delay interval for the switch.

Table 1-2 Command Summary (continued)

Commands	Description
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 set up for TACACS, Extended TACACS, or TACACS+ verification.
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 dns-alias-lookup	Enables IP Domain Name System alias lookup for TACACS+.
tacacs-server extended	Enables an extended TACACS mode.
tacacs-server host	Specifies a TACACS, Extended TACACS, or TACACS+ host.
tacacs-server key	Sets 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 input from the user.
tacacs-server login-timeout	Specifies the maximum amount of time in seconds to wait for a TACACs login.
tacacs-server optional-passwords	Specifies that the first TACACS request to a TACACS or Extended TACACS server be made without password verification.
tacacs-server retransmit	Specifies the number of times the Cisco IOS software searches the list of TACACS or Extended TACACS server hosts before giving up.
tacacs-server timeout	Sets the interval that the server waits for a TACACS, Extended TACACS, or TACACS+ server to reply.
udld enable	Enables UDLD on all switch ports.
vtp file	Modify the VTP configuration storage filename.
wrr-queue bandwidth	Assigns WRR weights to the four CoS priority queues.
wrr-queue cos-map	Assigns CoS values to the CoS priority queues.

Table 1-2 Command Summary (continued)

Commands	Description
VLAN database mode	
abort	Abandons the proposed new VLAN database, and return to privileged EXEC mode.
apply	Implements the proposed new VLAN database, propagate it throughout the administrative domain, and remain in VLAN database mode.
exit	Implements the proposed new VLAN database, propagate it throughout the administrative domain, and return to privileged EXEC mode.
reset	Abandons the proposed new VLAN database, and remain in VLAN database mode.
show changes	Displays the differences between the currently implemented VLAN database on the switch and the proposed new VLAN database.
show current	Displays the currently implemented VLAN database on the switch or a single selected VLAN from it.
show proposed	Displays the proposed new 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 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.
management	Shuts down the current management VLAN interface.
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 into the NTP packet.
ntp broadcast version	Specifies a port to send NTP broadcast packets.
ntp disable	Prevents a port from receiving NTP packets.
ip address	Sets a primary or secondary IP address of a VLAN interface.
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 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.
rmon collection stats	Collect Ethernet group statistics.
shutdown	Disables a port.
spanning-tree cost	Sets 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 are allowed to be STP root ports.
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 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 native	Sets the native VLAN for untagged traffic when in IEEE 802.1Q trunking mode.
udld	Enables or disables UDLD on a port.
Line configuration mode	
login authentication	Applies the authentication list to a line or set of lines.
login local	Changes a login username.
login tacacs	Configures your 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 *Catalyst 2950 Desktop Switch Software Configuration Guide, Cisco IOS Release 12.0(5)WC(1)*.

CHAPTER 2

Cisco IOS Commands

abort

Use the **abort** VLAN database command to abandon the proposed new 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
12.0(5)WC(1)	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

The following example shows how to abandon the proposed new VLAN database and 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** command in privileged EXEC mode.

Related Commands

Command	Description
apply	Implements the proposed new VLAN database, increments the database configuration revision number, propagates it throughout the administrative domain, and remains in VLAN database mode.
exit	Implements the proposed new 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 new VLAN database, increment the database configuration revision number, propagate it throughout the administrative domain, and 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
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

The **apply** command implements the configuration changes 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 Trunk Protocol (VTP) client mode.

Examples

The following example shows how to implement the proposed new VLAN database and recognize it as the current database:

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

You can verify that VLAN database changes occurred by entering the **show vlan** command in privileged EXEC mode.

Related Commands

Command	Description
apply	Implements the proposed new VLAN database, increments the database configuration revision number, propagates it throughout the administrative domain, and remains in VLAN database mode.
exit	Implements the proposed new 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.

Command	Description
shutdown vlan	Shuts down (suspends) local traffic on the specified VLAN.
vlan database	Enters VLAN database mode from the command-line interface (CLI).

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 *vlan-id*	(Optional) Delete an IP address only within the specified VLAN. Valid IDs are from 1 to 1001; do not enter leading zeroes.

Defaults

No IP address is defined for the switch.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)WC(1)	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 your switch receives its IP address from a Bootstrap Protocol (BOOTP) or a Dynamic Host Configured Protocol (DHCP) server and you clear the switch IP address by using the **clear ip address** command, the BOOTP or DHCP server reassigns the IP address.

Examples

The following 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** command in privileged EXEC mode.

Related Commands

Command	Description
show running-config	Displays the configuration information currently running 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** |**secure**] [**address** *hw-addr*] [**interface** *interface*] [**vlan** *vlan-id*]

Syntax Description

static	(Optional) Delete only static addresses.
secure	(Optional) Delete only secure addresses.
address *hw-addr*	(Optional) Delete the address *hw-addr* of type static, dynamic, and secure as specified.
interface *interface*	(Optional) Delete an address on the interface *interface* of type static, dynamic, or secure as specified.
vlan *vlan-id*	(Optional) Delete all the MAC addresses for *vlan-id.* Valid IDs are from 1 to 1001; do not enter leading zeroes.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

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

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

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

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

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

The following 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
```

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

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

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

Related Commands

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

clear vtp counters

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

clear vtp counters

Syntax Description

This command has no arguments or keywords.

Defaults

No default is defined.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Examples

The following example shows how to clear the VTP counters:

```
Switch# clear vtp counters
```

You can verify the previous command by entering the **show vtp counters** command in privileged EXEC mode.

Related Commands

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

cluster commander-address

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. You do not need to enter this command. Enter the **no** form of this global configuration command on a member switch 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

default cluster commander-address

Syntax Description

mac-address	MAC address of the cluster command switch.
member *number*	Number of member switch. The range is from 0 to 15.
name *name*	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
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

A cluster member can have only one command switch.

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

You can enter the **no** form on a member switch to remove it from the cluster only during debugging or recovery procedures. However, with normal switch configuration, we recommend that you remove member switches only by entering the **no cluster member** *n* command on the command switch.

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

Examples

The following is sample text from the running configuration of a cluster member.

```
Switch(config)# cluster commander-address 00e0.9bc0.a500 member 4 name my_cluster
```

The following 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

number	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)WC(1)	This command was first introduced.

Usage Guidelines

Enter this command only on the command switch. This command does not operate on member switches.

If the hop count is set to 1, it disables extended discovery. The command switch discovers only candidates that are one hop from the edge of the cluster. The edge of the cluster is the point between the last discovered member switch and the first discovered candidate switch.

Examples

The following example shows how to set hop count limit to 4. This command is executed on the command switch.

```
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 make the command switch a candidate switch.

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

no cluster enable

default cluster enable

Syntax Description

name	Name of the cluster up to 31 characters. Valid characters include only alphanumerics, dashes, and underscores.
command-switch-member-number	(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
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

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

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

Examples

The following example shows how to enable the command switch, name the cluster, and set the command switch member number to 4.

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

You can verify 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

holdtime-in-secs	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)WC(1)	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

The following 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

n	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)WC(1)	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

The following example shows how to change the management VLAN to VLAN 5 on the entire cluster.

```
Switch(config)# cluster management-vlan 5
```

You can verify the previous command by entering the **show interface vlan** *number* command in privileged EXEC mode.

Related Commands

Command	Description
management	Shuts down the current 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

n	(Optional) The number that identifies a cluster member. The range is from 0 to 15.
mac-address *H.H.H*	MAC address of the member switch in hexadecimal format.
password *enable-password*	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
12.0(5)WC(1)	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

The following 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
```

The following 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)WC(1)	This command was first introduced.

Usage Guidelines

When you enter the **no cluster run** command on a command switch, the command switch is disabled.

When you enter the **no cluster run** command on a member switch, it is removed from the cluster.

When you enter the **no cluster run** command on a switch, it disables clustering on that switch. This switch is then incapable of becoming a candidate switch.

Examples

The following 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
12.0(5)WC(1)	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 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 will not be passed to the cluster.

Examples

The following 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:clus1, contains 1 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  0030.0002.0240 c2950-1                 0                    Up   (Cmdr)
1* 0001.96e4.e580 c2950-2    Fa0/1       1     0  Fa0/9       Up
2* 0001.96e4.e580 c2950-2    Fa0/3       1     0  Fa0/3       Up
3* 0001.96e4.e580 c2950-2    Fa0/5       1     0  Fa0/5       Up
4* 0050.2ae6.2e00 2900-1     Fa0/1       1     0  Fa0/1       Up
```

```
The following configuration command script was created:
cluster member 1 mac-address 0001.96e4.e580
cluster member 2 mac-address 0001.96e4.e580
cluster member 3 mac-address 0001.96e4.e580
cluster member 4 mac-address 0050.2ae6.2e00
!
end

Use this configuration? [yes/no]:yes

Building configuration...
[OK]
Use the enabled mode 'configure' command to modify this configuration.

Switch#
```

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

HSRP-group-name	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)WC(1)	This command was first introduced.

Usage Guidelines

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

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

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

Examples

The following example shows how to bind the HSRP group named my_hsrp to the cluster. This command is executed on the command switch.

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

The following example shows the error message when this command is executed 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
```

The following example shows the error message when this command is executed 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

interval-in-secs	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)WC(1)	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

The following 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** 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.

delete

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

delete {*device***:**}***filename***

Syntax Description

*device***:**	Device containing the file to be deleted. Valid devices include the switch Flash memory.
filename	Name of file.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

A colon (:) follows the *device* variable. Do not enter spaces after the colon.

Examples

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

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

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 or 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
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

Certain ports can be configured to be either full duplex or half duplex. Applicability of this command depends on the device to which the switch is attached.

For Fast Ethernet ports, setting the port to **auto** has the same effect as specifying **half** if the attached device does not autonegotiate the duplex parameter.

If the speed is set to auto, the switch negotiates with the device at the other end of the link for the speed setting and then forces the speed setting to the negotiated value. The duplex setting remains as configured on each end of the link, which could result in a duplex setting mismatch.

Note The Gigabit Ethernet ports can operate in either half- or full-duplex mode when they are set to 10 or 100 Mbps, but when they are set to1000 Mbps, they can only operate in the full-duplex mode.

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 2950 Desktop Switch Hardware Installation Guide.*

Examples

The following example shows how to set port 1 (Fast Ethernet port) to full duplex:

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

The following example shows how to set port 1 (Gigabit Ethernet port) 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** command in privileged EXEC mode.

Related Commands

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

enable last-resort

Use the **enable last-resort** global configuration command to specify what happens if the Terminal Access Controller Access Control System (TACACS) and Extended TACACS servers used by the **enable** command do not respond. Use the **no** form of this command to restore the default.

enable last-resort {**password** | **succeed**}

no enable last-resort

Syntax Description

password	Provide access to enable mode with entry of the privileged command level password. A password must contain from 1 to 25 uppercase and lowercase alphanumeric characters.
succeed	Provide access to enable mode without further question.

Defaults

Authentication is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

This secondary authentication is used only if the first attempt fails.

Note This command is not used with Terminal Access Controller Access Control System Plus (TACACS+), a Cisco proprietary protocol that instead uses the authentication, authorization, and accounting (AAA) suite of commands.

Examples

In the following example, if the TACACS servers do not respond to the **enable** command, you can enable access by entering the privileged-level password:

```
Switch(config)# enable last-resort <password>
```

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

Related Commands

Command	Description
enable	Accesses privileged EXEC mode.
show running-config	Displays the running configuration on the switch.

enable use-tacacs

Use the **enable use-tacacs** global configuration command to enable the use of Terminal Access Controller Access Control System (TACACS) to determine whether a user can access the privileged command level. Use the **no** form of this command to disable TACACS verification.

enable use-tacacs

no enable use-tacacs

Tips If you use the **enable use-tacacs** command, you must also use the **tacacs-server authenticate enable** command, or you will be locked out of the privileged command level.

Syntax Description

This command has no arguments or keywords.

Defaults

TACACS verification is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

When you add this command to the configuration file, the **enable** privilege EXEC command prompts for a new username and password. This pair is then passed to the TACACS server for authentication. If you are using Extended TACACS, it also sends any existing UNIX user identification code to the server.

Note This command initializes TACACS. Use the **tacacs server-extended** command to initialize Extended TACACS or use the **aaa new-model** command to initialize authentication, authorization, and accounting (AAA) and Terminal Access Controller Access Control System Plus (TACACS+).

Examples

The following example sets TACACS verification on the privileged EXEC login sequence:

```
Switch(config)# enable use-tacacs
Switch(config)# tacacs-server authenticate enable
```

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

Related Commands

Command	Description
show running-config	Displays the running configuration on the switch.
tacacs-server authenticate enable	Indicates whether users can perform an attempted action under TACACS and extended TACACS.

exit

Use the **exit** VLAN database command to implement the proposed new VLAN database, increment the database configuration number, propagate it throughout the administrative domain, and 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
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

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

Examples

The following example shows how to implement the proposed new VLAN database and exit to privileged EXEC mode:

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

You can verify the previous command by entering the **show vlan brief** command in privileged EXEC mode.

Related Commands

Command	Description
abort	Abandons the proposed new VLAN database, exits VLAN database mode, and returns to privileged EXEC mode.
apply	Implements the proposed new 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.

Command	Description
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. When the congestion clears, the local port requests that the remote port begin transmitting.
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
12.0(5)WC(1)	This command was first introduced.

Examples

The following example shows how to configure the local port to support any level of flow control by the remote port:

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

The following example shows how to configure the local port to control the traffic flow from the remote port:

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

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

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, create a switch virtual interface to be used as the management VLAN interface, and to enter interface configuration mode.

interface *type port* | **vlan** *number*

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

Syntax Description

type	Type of interface to be configured. Can be Fast Ethernet or Gigabit Ethernet.
port	Port ID.
vlan *number*	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
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

When creating a management VLAN interface, a space between **vlan** and *number* is accepted.

Only one management VLAN interface can be active.

You cannot delete the management VLAN 1 interface.

Before bringing up a new management VLAN interface with the **no shutdown** command, you must issue 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 and trunk ports.

Examples

The following example shows how to enable the switch to configure interface 2:

```
Switch(config)# interface fa0/2
Switch(config-if)#
```

The following example shows how to change the management VLAN from VLAN 1 to VLAN 3. This series of commands should only be executed from the console. If these commands are executed through a Telnet session, the **shutdown** command disconnects the session, and there is no way to use IP to access the system.

```
Switch# configure terminal
```

```
Switch(config)# interface vlan 3
Switch(config-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
```

The following 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
```

The following example shows how to copy the IP address and network mask information from the current management VLAN to VLAN 3 and 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* command in privilege 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

ip-address	IP address.
subnet-mask	Mask for the associated IP subnet.

Defaults

No IP address is defined for the switch.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)WC(1)	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 a Dynamic Host Configured Protocol (DHCP) server and you remove the switch IP address by using the **no ip address** command, IP processing is disabled, and the BOOTP or DHCP server cannot reassign the address.

Examples

The following 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** command in privileged EXEC mode.

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 snooping

Use the **ip igmp snooping** global configuration command to globally enable Internet Group Management Protocol (IGMP) snooping. Use the **no** form of this command to disable IGMP snooping.

ip igmp snooping

no ip igmp snooping

Syntax Description

This command has no arguments or keywords.

Defaults

By default, IGMP snooping is globally enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

When IGMP snooping is globally enabled, it enables IGMP snooping on all the existing VLAN interfaces. When IGMP snooping is globally disabled, it disables IGMP snooping on all the existing VLAN interfaces.

The configuration is saved in nonvolatile RAM (NVRAM).

Examples

The following example shows how to globally enable IGMP snooping:

```
Switch(config)# ip igmp snooping
```

The following example shows how to globally disable IGMP snooping:

```
Switch(config)# no ip igmp snooping
```

You can verify the previous commands by entering the **show ip igmp snooping** command in the privileged EXEC mode.

Related Commands

Command	Description
ip igmp snooping vlan	Enables IGMP snooping an a VLAN interface.
ip igmp snooping vlan immediate-leave	Enables the IGMP Immediate-Leave processing.
ip igmp snooping vlan mrouter	Configures a Layer 2 port as a multicast router port.
ip igmp snooping vlan static	Configures a Layer 2 port as a member of a group.
show ip igmp snooping	Displays the IGMP snooping configuration.

ip igmp snooping vlan

Use the **ip igmp snooping vlan** global configuration command to enable Internet Group Management Protocol (IGMP) snooping on a specific VLAN. Use the **no** form of this command to disable IGMP snooping on a VLAN interface.

ip igmp snooping vlan *vlan-id*

no ip igmp snooping vlan *vlan-id*

Syntax Description

vlan_id	VLAN ID value. The range is from 1 to 1001.

Defaults

By default, IGMP snooping is enabled when each VLAN is created.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

This command automatically configures the VLAN if it is not already configured. This information is saved in nonvolatile RAM (NVRAM).

Examples

The following example shows how to enable IGMP snooping on VLAN 2:

```
Switch(config)# ip igmp snooping vlan 2
```

The following example shows how to disable IGMP snooping on VLAN 2:

```
Switch(config)# no ip igmp snooping vlan 2
```

You can verify the previous commands by entering the **show ip igmp snooping vlan** command in the privileged EXEC mode.

Related Commands

Command	Description
ip igmp snooping	Globally enables IGMP snooping. IGMP snooping must be globally enabled in order to be enabled on a VLAN.
ip igmp snooping vlan immediate-leave	Enables the IGMP Immediate-Leave processing.
ip igmp snooping vlan mrouter	Configures a Layer 2 port as a multicast router port.
ip igmp snooping vlan static	Configures a Layer 2 port as a member of a group.
show ip igmp snooping	Displays the snooping configuration.

ip igmp snooping vlan immediate-leave

Use the **ip igmp snooping immediate-leave** global configuration command to enable Internet Group Management Protocol (IGMP) Immediate-Leave processing on a VLAN interface. Use the **no** form of this command to disable Immediate-Leave processing on the VLAN interface.

ip igmp snooping vlan *vlan-id* **immediate-leave**

no ip igmp snooping vlan *vlan-id* **immediate-leave**

Syntax Description

vlan-id	VLAN ID value. The range is between 1 to 1001.

Defaults

By default, IGMP Immediate-Leave processing is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

Use the Immediate-Leave feature only when there is a only one IP multicast receiver present on every port in the VLAN. The Immediate Leave configuration is saved in nonvolatile RAM (NVRAM).

Immediate Leave is supported only with IGMP version 2 hosts.

Examples

The following example shows how to enable IGMP Immediate-Leave processing on VLAN 1:

```
Switch(config)# ip igmp snooping vlan 1 immediate-leave
```

The following example shows how to disable IGMP Immediate-Leave processing on VLAN 1:

```
Switch(config)# no ip igmp snooping vlan 1 immediate-leave
```

You can verify the previous commands by entering the **show ip igmp snooping vlan** command in the privileged EXEC mode.

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping.
ip igmp snooping vlan mrouter	Configures a Layer 2 port as a multicast router port.
ip igmp snooping vlan static	Configures a Layer 2 port as a member of a group.
show ip igmp snooping	Displays the snooping configuration.
show mac-address-table multicast	Displays the Layer 2 multicast entries for a VLAN.

ip igmp snooping vlan mrouter

Use the **ip igmp snooping vlan mrouter** global configuration command to add a multicast router port and to configure the multicast router learning method. Use the **no** form of this command to remove the configuration.

ip igmp snooping vlan *vlan-id* **mrouter** *interface* **|** { **learn** {**cgmp | pim-dvmrp**}}

no ip igmp snooping vlan *vlan-id* **mrouter** *interface* **|** { **learn** {**cgmp | pim-dvmrp**}}

Syntax Description

vlan-id	Specify the VLAN ID. The range is from 1 to 1001.
interface	Specify the Fast Ethernet port that is configured to a static router port.
learn	Specify the multicast router learning method.
cgmp	Specify the multicast router snooping CGMP packets.
pim-dvmrp	Specify the multicast router snooping PIM-DVMRP packets.

Defaults

The default is **pim-dvmrp**.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

The CGMP learning method is useful for controlling traffic in Cisco router environments.

The configured learning method is saved in nonvolatile RAM (NVRAM).

Static connections to multicast routers are supported only on switch ports.

Examples

The following example shows how to configure Fast Ethernet interface 0/6 as a multicast router port:

```
Switch(config)# ip igmp snooping vlan 1 mrouter fa0/6
```

The following example shows how to specify the multicast router learning method as CGMP:

```
Switch(config)# no ip igmp snooping vlan 1 mrouter learn cgmp
```

You can verify the previous commands by entering the **show ip igmp snooping mrouter** command in the privileged EXEC mode.

Related Commands

Command	Description
ip igmp snooping	Globally enables IGMP snooping.
ip igmp snooping vlan	Enables Internet Group Management Protocol (IGMP) snooping on the VLAN interface.
ip igmp snooping vlan immediate-leave	Configures IGMP Immediate-Leave processing.
ip igmp snooping vlan static	Configures a Layer 2 port as a member of a group.
show ip igmp snooping mrouter	Displays the statically and dynamically learned multicast router ports.

ip igmp snooping vlan static

Use the **ip igmp snooping vlan** *vlan-id* **static** global configuration command to add a Layer 2 port as a member of a multicast group. Use the **no** form of this command to remove the configuration.

ip igmp snooping vlan *vlan-id* **static** *mac-address interface*

no ip igmp snooping vlan *vlan-id* **static** *mac-address interface*

Syntax Description

vlan-id	VLAN ID value. The range is 1 to 1001.
static	Keyword to define the static group address.
mac-address	Group MAC address.
interface	Keyword to specify the Fast Ethernet port that is configured to a static router port.

Defaults

None configured.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

The command is used to statically configure the IP multicast group member ports.

The static ports and groups are saved in nonvolatile RAM (NVRAM).

Static connections to multicast routers are supported only on switch ports.

Examples

The following example shows how to statically configure a host on an interface:

```
Switch(config)# ip igmp snooping vlan 1 static 0100.5e02.0203 fa0/6
Configuring port FastEthernet 0/6 on group 0100.5e02.0203
```

You can verify the previous commands by entering the **show mac-address-table multicast** command in the privileged EXEC mode.

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping.
ip igmp snooping vlan	Enables IGMP snooping on the VLAN interface.
ip igmp snooping vlan immediate-leave	Configures IGMP Immediate-Leave processing.

Command	Description
ip igmp snooping vlan mrouter	Configures a Layer 2 port as a multicast router port.
show mac-address-table multicast	Displays the Layer 2 multicast entries for a VLAN.

login

Use the **login** line configuration command to enable password checking at login. Use the **no** form of this command to disable password checking and to allow connections without a password.

login [**local** | **tacacs**]

no login

Syntax Description

local	(Optional) Select local password checking. Authentication is based on the username specified with the **username** global configuration command.
tacacs	(Optional) Select the Terminal Access Controller Access Control System (TACACS)-style user ID and password-checking mechanism.

Defaults

No password is assigned, and you cannot access the switch through Telnet. Virtual terminals require a password. If you do not set a password for a virtual terminal, it responds to attempted connections by displaying an error message and closing the connection.

Command Modes

Line configuration

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

If you specify the login command without the **local** or **tacacs** option, authentication is based on the password specified with the line configuration **password** command.

Note This command cannot be used with authentication, authorization, and accounting (AAA) and TACACS+. Use the **login authentication** command instead.

Examples

The following example shows how to set the password letmein on virtual terminal line 4:

```
Switch(config-line)# line vty 4
Switch(config-line)# password letmein
Switch(config-line)# login
```

The following example shows how to enable the TACACS-style user ID and password-checking mechanism:

```
Switch(config-line)# line 0
Switch(config-line)# password <mypassword>
Switch(config-line)# login tacacs
```

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

Related Commands

Command	Description
enable password	Sets 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.

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.
list-name	Use the indicated list created with the AAA **authentication login** command.

Defaults

Login authentication is disabled.

Command Modes

Line configuration

Command History

Release	Modification
12.0(5)WC(1)	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 you want used in default situations. The default method list is automatically applied to all interfaces.

Examples

The following 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** command in privileged EXEC mode.

Related Commands

Command	Description
enable password	Sets 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

age	Number from 10 to 1000000 (seconds).

Defaults

The default is 300 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)WC(1)	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

The following example shows how to set the aging time to 200 seconds:

```
Switch(config)# mac-address-table aging-time 200
```

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

Related Commands

Command	Description
clear mac-address-table	Deletes entries from 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.

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* [**vlan** *vlan-id*]

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

Syntax Description

hw-addr	MAC address that is added to the table.
interface	Port to which packets destined for *hw-addr* are forwarded.
vlan *vlan-id*	(Optional) The *interface* and **vlan** parameters together specify a destination to which packets destined for *hw-addr* are forwarded. The **vlan** keyword is optional if the port is a static-access VLAN port. In this case, the VLAN assigned to the port is assumed to be that of the port associated with the MAC address. This keyword is required for trunk ports. The *vlan-id* is the ID of the VLAN to which secure entries are added. Valid IDs are 1 to 1001; do not enter leading zeroes.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

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.

Examples

The following 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
```

You can verify this command by entering the **show mac-address-table** command in privileged EXEC mode.

Related Commands

Command	Description
clear mac-address-table	Deletes entries from the MAC address table.
mac-address-table aging-time	Sets the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated.
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 *mac_addr* **interface** *out-ports-lists* **vlan** *vlan-id*

no mac-address-table static *mac_addr* **interface** *out-ports-lists* **vlan** *vlan-id*

Syntax Description

mac_addr	MAC address added to the address table.
interface	Keyword for the output port interfaces.
out-port-list	List of ports to which packets received on ports in a VLAN are forwarded. All ports in the list must belong to the same VLAN.
vlan *vlan-id*	The *vlan-id* is the ID of the VLAN to which static address entries are forwarded. Valid IDs are 1 to 1001; do not enter leading zeroes.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

When a packet is received on any port in the VLAN, it is forwarded to all the ports specified by the out-ports-lists in the same VLAN.

Examples

The following example shows how to statically configure a host on an interface:

```
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** command in privileged EXEC mode.

Related Commands

Command	Description
clear mac-address-table	Deletes entries from the MAC address table.
mac-address-table aging-time	Sets the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated.
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 used to manage a cluster of switches. To use it for cluster management, apply it to a switched virtual interface or the management interface. The default management VLAN is VLAN 1; however, the management VLAN can be changed to a new management interface by using a different VLAN (one with 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)WC(1)	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** command.

Before entering the **management** command, make sure the following 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.
- The network management station must have network connectivity 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 configuration command **cluster management-vlan** *n* on the command switch to change the management VLAN on the entire cluster.

Examples

The following 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)#
```

The following 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* command in privileged EXEC mode.

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 *number*	Displays the administrative and operational status of a switching (nonrouting) port.

ntp access-group

Use the **ntp access-group** global configuration command to control access to the system Network Time Protocol (NTP) services. Use the **no** form of the command to remove access control to the system NTP services.

ntp access-group {**query-only** | **serve-only** | **serve** | **peer**} *access-list-number*

no ntp access-group {**query-only** | **serve** | **peer**}

Syntax Description

query-only	Enable only NTP control queries. See RFC 1305 (NTP version 3).
serve-only	Enable only time requests.
serve	Enable time requests and NTP control queries, but does not enable the system to synchronize to the remote system.
peer	Enable time requests and NTP control queries; enable the system to synchronize to the remote system.
access-list-number	Number (1 to 99) of a standard IP access list.

Defaults

NTP is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

The access group options are scanned in the following order from least restrictive to most restrictive:

1. peer
2. serve
3. serve-only
4. query-only

Access is granted for the first match that is found. If no access groups are specified, all access is granted to all sources. If any access groups are specified, only the specified access is granted. This facility provides minimal security for the time services of the system. If tighter security is desired, use the NTP authentication facility.

Examples

The following example shows how to configure the system to be synchronized by a peer from access list 99.

However, the system restricts access to allow time requests only from access list 42:

```
Switch(config)# ntp access-group peer 99
Switch(config)# ntp access-group serve-only 42
```

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

Related Commands

Command	Description
access-list	Differentiates one packet from another so that different treatment can be applied.
show running-config	Displays the running configuration on the switch.

ntp authenticate

Use the **ntp authenticate** global configuration command to enable Network Time Protocol (NTP) authentication. Use the **no** form of this command to disable the feature.

ntp authenticate

no ntp authenticate

Syntax Description

This command has no keywords or arguments.

Defaults

NTP authentication is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

Use this command if you want authentication. If this command is specified, the system will not synchronize to a system unless it carries one of the authentication keys specified in the **ntp trusted-key** command.

Examples

The following example shows how to enable NTP authentication:

```
Switch(config)# ntp authenticate
```

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

Related Commands

Command	Description
ntp authentication-key	Defines an authentication key for NTP.
ntp trusted-key	Authenticates the identity of a system to which NTP will synchronize.
show running-config	Displays the running configuration on the switch.

ntp authentication-key

Use the **ntp authentication-key** global configuration command to define an authentication key for Network Time Protocol (NTP). Use the **no** form of this command to remove the authentication key for NTP.

ntp authentication-key *number* **md5** *value*

no ntp authentication-key *number*

Syntax Description

number	Key number (1 to 4294967295).
md5	Use MD5 authentication.
value	Key value (an arbitrary string of up to eight characters, with the exception of control or escape characters).

Defaults

No authentication key is defined.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

Use this command to define authentication keys for use with other NTP commands for greater security.

Examples

The following example shows how to set authentication key 10 to *aNiceKey*:

```
Switch(config)# ntp authentication-key 10 md5 aNiceKey
```

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

Note When this command is written to nonvolatile RAM (NVRAM), the key is encrypted so that it is not displayed when the configuration is viewed.

Related Commands

Command	Description
ntp authenticate	Enables NTP authentication.
ntp peer	Configures the switch system clock to synchronize a peer or to be synchronized by a peer.
ntp server	Allows the switch system clock to be synchronized by a time server.
ntp trusted-key	Authenticates the identity of a system to which NTP will synchronize.
show running-config	Displays the running configuration on the switch.

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
12.0(5)WC(1)	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. You must configure 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

The following example shows how to synchronize the router to NTP packets that are broadcast on interface VLAN 1:

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

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

Related Commands

Command	Description
ntp broadcastdelay	Sets the estimated round-trip delay between the IOS software and an NTP broadcast server.
show running-config	Displays the running configuration on the switch.

ntp broadcastdelay

Use the **ntp broadcastdelay** global configuration command to set the estimated round-trip delay between the IOS software and a Network Time Protocol (NTP) broadcast server. Use the **no** form of this command to revert to the default value.

ntp broadcastdelay *microseconds*

no ntp broadcastdelay

Syntax Description

microseconds	Estimated round-trip time (in microseconds) for NTP broadcasts. The range is from 1 to 999999.

Defaults

The default is 3000 microseconds.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

Use this command when the switch is configured as a broadcast client and the round-trip delay on the network is other than 3000 microseconds.

Examples

The following example shows how to configure the estimated round-trip delay between the switch and the broadcast client to 5000 microseconds:

```
Switch(config)# ntp broadcastdelay 5000
```

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

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 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

IP-address	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
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

You must configure 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.

Related Commands

Command	Description
ntp broadcast client	Allows the system to receive NTP broadcast packets on an interface.
ntp broadcastdelay	Sets the estimated round-trip delay between the IOS software and an NTP broadcast server.

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 embedded into 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

number	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

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

You must configure 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.

Related Commands

Command	Description
ntp broadcast client	Allows the system to receive NTP broadcast packets on an interface.
ntp broadcastdelay	Sets the estimated round-trip delay between the IOS software and an NTP broadcast server.

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

number	Number from 1 to 3.

Defaults

Version 3 is the default.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

If you are using version 2 and the NTP synchronization does not occur, use NTP version 2.

You must configure 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

The following 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** command in privileged EXEC mode.

Related Commands

Command	Description
ntp broadcast client	Allows the system to receive NTP broadcast packets on an interface.
ntp broadcastdelay	Sets the estimated round-trip delay between the IOS software and an NTP broadcast server.
show running-config	Displays the running configuration on the switch.

ntp clock-period

Do not enter this command; it is documented for informational purposes only. The system automatically generates this command as the Network Time Protocol (NTP) determines the clock error and compensates.

As the NTP compensates for the error in the system clock, it keeps track of the correction factor for this error. The system automatically saves this value into the system configuration using the **ntp clock-period** global configuration command. The system uses the **no** form of this command to revert to the default.

ntp clock-period *value*

no ntp clock-period

Syntax Description

value	Amount to add to the system clock for each clock hardware tick (in units of 2 to 32 seconds).

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

If a **write memory** command is entered to save the configuration to nonvolatile RAM (NVRAM), this command is automatically added to the configuration. It is a good idea to perform this task after NTP has been running for a week or so; NTP synchronizes more quickly if the system is restarted.

ntp disable

Use the **ntp disable** interface configuration command to prevent an interface from receiving Network Time Protocol (NTP) packets. To enable receipt of NTP packets on an interface, use the **no** form of the command.

ntp disable

no ntp disable

Syntax Description

This command has no arguments or keywords.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

You must configure 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.

The preferred command to disable NTP is **no ntp**.

Examples

The following example shows how to prevent interface VLAN 1 from receiving NTP packets:

```
Switch(config-if)# interface vlan1
Switch(config-if)# ntp disable
```

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

Related Commands

Command	Description
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

number	(Optional) Specify the number of NTP associations. The range is from 0 to 4294967295.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

This command provides a simple method to 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

The following example shows how to set the maximum number of NTP associations to 44:

```
Switch(config)# ntp max-associations 44
```

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

Related Commands

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

ntp peer

Use the **ntp peer** global configuration command to configure the switch system clock to synchronize a peer or to be synchronized by a peer. Use the **no** form of the command to disable this capability.

ntp peer *ip-address* [**version** *number*] [**key** *keyid*] [**source** *interface*] [**prefer**]

no ntp peer *ip-address*

Syntax Description

ip-address	IP address of the peer providing, or being provided, the clock synchronization.
version *number*	(Optional) Define the Network Time Protocol (NTP) version number as version 1, 2, or 3.
key *keyid*	(Optional) Define the authentication key, which is used when sending packets to this peer. The range is from 0 to 4294967295.
source *interface*	(Optional) Authentication key to use when sending packets to this peer. Also includes the name of the interface from which to pick the IP source address.
prefer	(Optional) Make this peer the preferred peer that provides synchronization.

Defaults

No IP address is defined.

NTP version 3 is the default.

No NTP authentication key is defined.

No source interface is defined.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

Using the **prefer** keyword will reduce switching between peers.

If you are using the default NTP version of 3 and NTP synchronization does not occur, try using NTP version 2. Many NTP servers on the Internet run version 2.

Examples

The following example shows how to configure the router to allow its system clock to be synchronized with the clock of the peer (or vice versa) at IP address 131.108.22.33 using NTP version 2. The source IP address will be the address of Ethernet 0.

```
Switch(config)# ntp peer 131.108.22.33 version 2 source Ethernet 0
```

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

Related Commands

Command	Description
ntp authentication-key	Defines an authentication key for NTP.
ntp server	Allows the switch system clock to be synchronized by a time server.
ntp source	Uses a particular source address in NTP packets.
show running-config	Displays the running configuration on the switch.

ntp server

Use the **ntp server** global configuration command to allow the switch system clock to be synchronized by a time server. Use the **no** form of the command to disable this capability.

ntp server *ip-address* [**version** *number*] [**key** *keyid*] [**source** *interface*] [**prefer**]

no ntp server *ip-address*

Syntax Description

ip-address	IP address of the time server providing the clock synchronization.
version *number*	(Optional) Define the Network Time Protocol (NTP) version number (1 to 3).
key *keyid*	(Optional) Define the authentication key. Authentication key to use when sending packets to this peer. The range is from 0 to 4294967295.
source *interface*	(Optional) Identify the interface from which to pick the IP source address.
prefer	(Optional) Make this server the preferred server that provides synchronization.

Defaults

No IP address is defined.

NTP version 3 is the default.

No NTP authentication key is defined.

No source interface is defined.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

Use this command if you want to allow this machine to synchronize with the specified server. The server will not synchronize to this machine.

Using the **prefer** keyword will reduce switching between servers.

If you are using the default NTP version of 3 and NTP synchronization does not occur, try using NTP version 2. Many NTP servers on the Internet run version 2.

Examples

The following example shows how to configure the router to allow its system clock to be synchronized with the clock of the peer at IP address 128.108.22.44 using NTP version 2:

```
Switch(config)# ntp server 128.108.22.44 version 2
```

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

Related Commands

Command	Description
ntp authentication-key	Defines an authentication key for NTP.
ntp server	Allows the switch system clock to be synchronized by a time server.
ntp source	Uses a particular source address in NTP packets.
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

interface	Any valid system interface name.

Defaults

No source address is defined.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)WC(1)	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

The following example shows how to configure the router to use the IP address of VLAN 1 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** command in privileged EXEC mode.

Related Commands

Command	Description
ntp peer	Configures the switch system clock to synchronize a peer or to be synchronized by a peer.
ntp server	Allows the switch system clock to be synchronized by a time server.
show running-config	Displays the running configuration on the switch.

ntp trusted-key

Use the **ntp trusted-key** global configuration command if you want to authenticate the identity of a system to which the Network Time Protocol (NTP) will synchronize. Use the **no** form of this command to disable authentication of the identity of the system.

ntp trusted-key *key-number*

no ntp trusted-key *key-number*

Syntax Description

key-number	Authentication key to be used for time authentication. The range is from 1 to 4294967295.

Defaults

No key number is defined.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

If authentication is enabled, use this command to define one or more key numbers that a peer NTP system must provide in its NTP packets in order for this system to synchronize to it. The key numbers must correspond to the keys defined with the **ntp authentication-key** command. This provides protection against accidentally synchronizing the system to a system that is not allowed because the other system must know the correct authentication key.

Examples

The following example shows how to configure the system to synchronize only to systems providing authentication key 42 in its NTP packets:

```
Switch(config)# ntp authenticate
Switch(config)# ntp authentication-key 42 md5 aNiceKey
Switch(config)# ntp trusted-key 42
```

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

Related Commands

Command	Description
ntp authenticate	Enables NTP authentication.
ntp authentication-key	Defines an authentication key for NTP.
show running-config	Displays the running configuration on the switch.

port group

Use the **port group** interface configuration command to assign a port to a Fast EtherChannel or Gigabit EtherChannel port group. Up to six port groups can be created on a switch. Up to eight ports can belong to a source-based or destination-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

group-number	Port group number to which the port belongs. The range is from 1 to 6.
distribution {**source** | **destination**}	(Optional) Forwarding method for the port group. • **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
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

The following restrictions apply for all ports:

- 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 six port groups of all source-based, all destination-based, or a combination of source-based and destination-based port groups. A source-based port group can have up to eight ports in its group. A destination-based port group can also have only eight ports in its group. You cannot mix source-based and destination-based ports in the same group.
- Port group members must belong to the same set of VLANs and must be all static-access or all trunk ports.

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

- VLAN membership of ports in the group
- VLAN mode (static or 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
- 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.

Examples

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

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

The following 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** command in privileged EXEC mode.

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

interface	(Optional) Port number for the SPAN to be enabled. The interface specified is the port to be monitored.
vlan *vlan-id*	(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
12.0(5)WC(1)	This command was first introduced.

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.

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 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 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

The following 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** command in privileged EXEC mode.

Related Commands

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

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 monitor port can not be configured as a protected port. However, it is possible to monitor or a protected port.

A protected port continues to forward unicast, multicast, and broadcast traffic to unprotected ports and vice versa.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)WC(1)	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.

Port monitoring does not work if both the monitor and the monitored ports are protected ports. A monitor port cannot be configured as a protected port. However, you can monitor a protected port by a non protected port.

A protected port is different from a secure port.

Examples

The following 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** command in privileged EXEC mode.

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. • **shutdown**—Disable the port when a security violation occurs. • **trap**—Generate an SNMP trap when a security violation occurs
max-mac-count *addresses*	(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
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

If you specify **trap**, use the **snmp-server host** 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 dynamic-access port or a trunk port.

Examples

The following 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
```

The following 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** command in privileged EXEC mode.

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

{**broadcast** | **multicast** | **unicast**}	Determine the type of packet-storm suppression. • **broadcast**—Enable broadcast storm control on the port. • **multicast**—Enable multicast storm control on the port. • **unicast**—Enable unicast storm control on the port.
{**action** {**filter** | **shutdown**}	(Optional) Determines the type of action to perform. • **filter**—Filter traffic during a storm. • **shutdown**—Disable the port during a storm.
threshold {**rising** *rising-number* **falling** *falling-number*}	Defines the rising and falling thresholds • **rising** *rising-number*—Block the flooding of storm packets when the value specified for *rising-number* is reached. The *rising-number* is 0 to 4294967295 packets per second. • **falling** *falling-number*—Restart the normal transmission of broadcast packets when the value specified for *falling-number* is reached. The *falling-number* is 0 to 4294967295 packets per second.
trap	(Optional) Generate an 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.

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
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

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

Examples

The following 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** command in privileged EXEC mode.

Related Commands

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

rcommand

Use the **rcommand** user EXEC command to start a Telnet session and to execute 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

n	Provide the number that identifies a cluster member. The range is from 0 to 15.
commander	Provide access to the command switch from a member switch.
mac-address *hw-addr*	MAC address of the member switch.

Command Modes

User EXEC

Command History

Release	Modification
12.0(5)WC(1)	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 EXEC mode **show cluster members** command on the command switch.

You can use this command to access a member switch from the command-switch prompt or to access a command switch from the member-switch prompt.

For 2950 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 execute 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.

Examples

The following 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 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
12.0(5)WC(1)	This command was first introduced.

Examples

The following example shows how to abandon the proposed VLAN database and reset to the current VLAN database:

```
Switch(vlan)# reset
Switch(vlan)#
```

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

Related Commands

Command	Description
abort	Abandons the proposed new VLAN database, exits VLAN database mode, and returns to privileged EXEC mode.
apply	Implements the proposed new VLAN database, increments the database configuration revision number, propagates it throughout the administrative domain, and remains in VLAN database mode.
exit	Implements the proposed new 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

index	Remote Network Monitoring (RMON) collection control index. The range is 1 to 65535.
owner *name*	(Optional) Owner of the RMON collection.

Defaults

The RMON statistics collection is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

The RMON statistics collection command is based on hardware counters.

Examples

The following example shows how to collect rmon statistics for the owner root on interface fa0/1:

```
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. For more information on this command, refer to the complete IOS Release 12.0 documentation set available on Cisco.com.

show changes

Use the **show changes** VLAN database command to display the differences between the VLAN database currently 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*] **|** [{**begin** | **exclude** | **include**} *expression*]

Syntax Description

vlan-id	(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 1001; do not enter leading zeroes.
| begin	(Optional) Display begins with the line that matches the specified *expression*.
| exclude	(Optional) Display excludes lines that match the specified *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

VLAN database

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

The following is sample output from the **show changes** command. It displays the differences between the current and proposed databases.

```
Switch(vlan)# show changes
ADDED:
    Name:VLAN0003
    Media Type:Ethernet
    VLAN 802.10 Id:100003
    State:Operational
    MTU:1500

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

The following is sample output from the **show changes 4** command. It displays the differences between VLAN 4 in the current database and the proposed database.

```
Switch(vlan)# show changes 4

ADDED:
    Name:VLAN0004
    Media Type:Ethernet
    VLAN 802.10 Id:100004
    State:Operational
```

Related Commands

Command	Description
show current	Displays the current VLAN database on the switch or a selected VLAN.
show proposed	Displays the proposed VLAN database or a selected VLAN.

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 | [{**begin** | **exclude** | **include**} *expression*]

Syntax Descriptions

| begin	(Optional) Display begins with the line that matches the specified *expression*.
| exclude	(Optional) Display excludes lines that match the specified *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.0(5)WC(1)	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 total number of members. It also shows the cluster status and time since the status changed. If redundancy is enabled, it displays the primary and secondary command-switch information.

If you enter this command on a switch that is not a cluster member, the error message `Not a management cluster member` is displayed.

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

The following is sample output when this command is executed 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
```

The following is sample output when this command is executed on a member switch:

```
Switch1# show cluster
Member switch for cluster "commander"
        Member number:                  3
        Management IP address:          192.192.192.192
        Command switch mac address:     0000.0c07.ac14
        Heartbeat interval:             8
        Heartbeat hold-time:            80
```

The following is sample output when this command is executed on a member switch that is configured as the standby command switch:

```
Switch# show cluster
Member switch for cluster "commander"
        Member number:                  3 (Standby command switch)
        Management IP address:          192.192.192.192
        Command switch mac address:     0000.0c07.ac14
        Heartbeat interval:             8
        Heartbeat hold-time:            80
```

The following is sample output when this command is executed on the command switch that is separated from member 1:

```
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, 5 minutes
        Redundancy:                     Disabled
        Heartbeat interval:             8
        Heartbeat hold-time:            80
        Extended discovery hop count:   3
```

The following is sample output when this command is executed on a member switch that is separated from the command switch:

```
Switch> show cluster
Member switch for cluster "commander"
        Member number:                  <UNKNOWN>
        Management IP address:          192.192.192.192
        Command switch mac address:     0000.0c07.ac14
        Heartbeat interval:             8
        Heartbeat hold-time:            80
```

Related Commands

Command	Description
cluster enable	Enables a command-capable switch as the cluster command switch, assigns a cluster name, and optionally assigns a member number to it.
show cluster candidates	Displays a list of candidate switches.
show cluster members	Displays information about the cluster members.

show cluster candidates

Use the **show cluster candidates** user EXEC command on the command switch to display a list of candidate switches.

show cluster candidates [**mac-address** *H.H.H.* | **detail**] | [{**begin** | **exclude** | **include**} *expression*]

Syntax Description

mac-address *H.H.H.*	(Optional) Hexadecimal MAC address of the cluster candidate.
detail	(Optional) Display detailed information for all candidates.
| begin	(Optional) Display begins with the line that matches the specified *expression*.
| exclude	(Optional) Display excludes lines that match the specified *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

You should enter this command only on a command switch.

If the switch is not a command switch, the command displays an empty line at the prompt.

The SN in the display means "switch member number." If E is displayed in the SN column, it means that the switch is discovered through extended discovery. The hop count is the number of devices the candidate is from the command switch.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

The following is sample output from the **show cluster candidates** command.

```
Switch# show cluster candidates
                                                                    |---Upstream---|
MAC Address    Name         Device Type      PortIf  FEC Hops SN PortIf  FEC
00d0.7961.c4c0 c2950-012    WS-C2950-12      Fa0/5        1   0  Fa0/3
00d0.bbf5.e900 ldf-dist-128 WS-C3524-XL      Fa0/7        1   0  Fa0/24
00e0.1e7e.be80 1900_Switch  1900             3       0    1   0  Fa0/11
00e0.1e9f.7a00 c2924XL-24   WS-C2924-XL      Fa0/5        1   0  Fa0/3
00e0.1e9f.8c00 c2912XL-12-2 WS-C2912-XL      Fa0/4        1   0  Fa0/7
00e0.1e9f.8c40 c2912XL-12-1 WS-C2912-XL      Fa0/1        1   0  Fa0/9
0050.2e4a.9fb0 C3508XL-0032 WS-C3508-XL E
0050.354e.7cd0 C2924XL-0034 WS-C2924-XL E
```

The following is sample output from the **show cluster candidates** command that uses the MAC address of a member switch directly connected to the command switch:

```
Switch# show cluster candidates mac-address 00d0.7961.c4c0
Device 'c2950-12' with mac address number 00d0.7961.c4c0
        Device type:            cisco WS-C2950-12
        Upstream MAC address:   00d0.796d.2f00 (Cluster Member 0)
        Local port:             Fa0/3   FEC number:
        Upstream port:          Fa0/13  FEC Number:
        Hops from cluster edge: 1
        Hops from command device: 1
```

The following is sample output from the **show cluster candidates** command that uses the MAC address of a member switch three hops from the cluster edge:

```
Switch# show cluster candidates mac-address 0010.7bb6.1cc0
Device 'c2950-24' with mac address number 0010.7bb6.1cc0
        Device type:            cisco WS-C2950-24
        Upstream MAC address:   0010.7bb6.1cd4
        Local port:             Fa2/1   FEC number:
        Upstream port:          Fa0/24  FEC Number:
        Hops from cluster edge: 3
        Hops from command device: -
```

The following is sample output from the **show cluster candidates detail** command:

```
Switch# show cluster candidates detail
Device 'c2950-12' with mac address number 00d0.7961.c4c0
        Device type:            cisco WS-C2950-12
        Upstream MAC address:   00d0.796d.2f00 (Cluster Member 1)
        Local port:             Fa0/3   FEC number:
        Upstream port:          Fa0/13  FEC Number:
        Hops from cluster edge: 1
        Hops from command device: 2
Device '1900_Switch' with mac address number 00e0.1e7e.be80
        Device type:            cisco 1900
        Upstream MAC address:   00d0.796d.2f00 (Cluster Member 2)
        Local port:             3       FEC number: 0
        Upstream port:          Fa0/11  FEC Number:
        Hops from cluster edge: 1
        Hops from command device: 2
Device 'c2924-XL' with mac address number 00e0.1e9f.7a00
        Device type:            cisco WS-C2924-XL
        Upstream MAC address:   00d0.796d.2f00 (Cluster Member 3)
        Local port:             Fa0/5   FEC number:
        Upstream port:          Fa0/3   FEC Number:
        Hops from cluster edge: 1
        Hops from command device: 2
```

Related Commands

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

show cluster members

Use the **show cluster members** user EXEC command on the command switch to display information about the cluster members.

show cluster members [*n* | **detail**] | [{**begin** | **exclude** | **include**} *expression*]

Syntax Description

n	(Optional) Number that identifies a cluster member. The range is from 0 to 15.
detail	(Optional) Display detailed information for all cluster members.
| begin	(Optional) Display begins with the line that matches the specified *expression*.
| exclude	(Optional) Display excludes lines that match the specified *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

You should enter this command only on a command switch.

If the cluster has no members, this command displays an empty line at the prompt.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

The following is sample output from the **show cluster members** command. The SN in the display means *switch number.*

```
Switch# show cluster members
|---Upstream---|
SN MAC Address    Name         PortIf FEC Hops   SN PortIf  FEC  State
0  0030.0002.0240 c2950-001               0                    Up   (Cmdr)
4  0050.2ae6.2e00 2900XL-1     Fa0/1       1     0  Fa0/1       Up
```

The following is sample output from the **show cluster members** for cluster member 4:

```
Switch# show cluster members 4
Device '2900XL-1' with member number 4
        Device type:           cisco WS-C2924M-XL
        MAC address:           0050.2ae6.2e00
        Upstream MAC address:  0030.0002.0240 (Cluster member 0)
        Local port:            Fa0/1   FEC number:
        Upstream port:         Fa0/1   FEC Number:
        Hops from command device:1
```

The following is sample output from the **show cluster members detail** command:

```
Switch# show cluster members detail
Device 'c2950-001' with member number 0 (Command Switch)
        Device type:           cisco WS-C2950-24
        MAC address:           0030.0002.0240
        Upstream MAC address:
        Local port:                    FEC number:
        Upstream port:                 FEC Number:
        Hops from command device:0
Device '2900XL-1' with member number 4
        Device type:           cisco WS-C2924M-XL
        MAC address:           0050.2ae6.2e00
        Upstream MAC address:  0030.0002.0240 (Cluster member 0)
        Local port:            Fa0/1   FEC number:
        Upstream port:         Fa0/1   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 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*] **|** [{**begin** | **exclude** | **include**} *expression*]

Syntax Description

vlan-id	(Optional) ID of the VLAN in the current 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 1001; do not enter leading zeroes.
| begin	(Optional) Display begins with the line that matches the specified *expression*.
| exclude	(Optional) Display excludes lines that match the specified *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

VLAN database

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

The following is sample output from the **show current** command. It displays the current VLAN database.

```
Switch(vlan)# show current
    Name: default
    Media Type: Ethernet
    VLAN 802.10 Id: 100001
    State: Operational
    MTU: 1500
    Translational Bridged VLAN: 1002
    Translational Bridged VLAN: 1003

    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

    Name: token-ring-default
    Media Type: Token Ring
    VLAN 802.10 Id: 101003
    State: Operational
```

```
MTU: 1500
Bridge Type: SRB
Ring Number: 0
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

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

Name: trnet-default
Media Type: Token Ring Net
VLAN 802.10 Id: 101005
State: Operational
MTU: 1500
Bridge Type: SRB
Bridge Type: SRB
Bridge Number: 1
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 proposed	Displays the proposed VLAN database or a selected VLAN.

show env

Use the **show env** privileged EXEC command to display fan information for the Catalyst 2950 switch.

show env {**all** | **fan**} | [{**begin** | **exclude** | **include**} *expression*]

Syntax Description

all	Display both fan and temperature environmental status.
fan	Display the switch fan status.
| begin	(Optional) Display begins with the line that matches the specified *expression*.
| exclude	(Optional) Display excludes lines that match the specified *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

The following is sample output from the **show env all** command:

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

The following is sample output from the **show env fans** command:

```
FAN 1 is OK
```

or

```
FAN 1 is FAULTY
```

show file systems

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

show file systems | [{**begin** | **exclude** | **include**} *expression*]

Syntax Description

	begin	(Optional) Display begins with the line that matches the specified *expression*.
	exclude	(Optional) Display excludes lines that match the specified *expression*.
	include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Privileged EXEC

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter | **exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

The following is sample 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** | **status** | **switchport** [**allowed-vlan** | **native-vlan**]] | [{**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface-id	ID of the port number.
vlan *number*	VLAN number of the management VLAN. Valid IDs are from 1 to 1001. Do not enter leading zeroes.
flow-control	Displays flowcontrol information for the specified port.
status	(Optional) Display the status of the interface.
switchport	(Optional) Display the administrative and operational status of a switching (nonrouting) port. • **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. • **native-vlan**—Display the native VLAN ID for untagged traffic when the port is in 802.1Q trunking mode.
| begin	(Optional) Display begins with the line that matches the specified *expression*.
| exclude	(Optional) Display excludes lines that match the specified *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

The following is sample 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 you configured by using the **flowcontrol** command or through the Cluster Management Suite (or the default value if you did not configure it). The first value displayed can be one of the following 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 in the display represents the flow control value that is autonegotiated with the link partner and can be one of the following settings:

- None—Flow control with the link partner did 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.

The following is sample output from the **show interface status** command:

```
Switch# show interface status
Port    Name               Status       Vlan     Duplex Speed   Type
------- ------------------ ------------ -------- ------ ------- ----
Fa0/1                      connected    1        A-Full   A-100 100BaseTX/FX
Fa0/2                      connected    1        A-Full   A-100 100BaseTX/FX
Fa0/3                      connected    1        A-Full   A-100 100BaseTX/FX
Fa0/4                      connected    1        A-Full   A-100 100BaseTX/FX
Fa0/5                      connected    1        A-Full   A-100 100BaseTX/FX
Fa0/6                      connected    1        A-Full   A-100 100BaseTX/FX
Fa0/7                      connected    1        A-Full   A-100 100BaseTX/FX
Fa0/8                      connected    1        A-Full   A-100 100BaseTX/FX
Fa0/9                      connected    1        A-Full   A-100 100BaseTX/FX
Fa0/10                     connected    1        A-Full   A-100 100BaseTX/FX
Fa0/11                     connected    1        A-Full   A-100 100BaseTX/FX
Fa0/12                     connected    1        A-Full   A-100 100BaseTX/FX
Fa0/13                     connected    1        A-Full   A-100 100BaseTX/FX
Fa0/14                     connected    1        A-Full   A-100 100BaseTX/FX
Fa0/15                     connected    1        A-Full   A-100 100BaseTX/FX
Fa0/16                     connected    1        A-Full   A-100 100BaseTX/FX
Fa0/17                     connected    1        A-Full   A-100 100BaseTX/FX
Fa0/18                     connected    1        A-Full   A-100 100BaseTX/FX
Fa0/19                     connected    1        A-Full   A-100 100BaseTX/FX
Fa0/20                     connected    1        A-Full   A-100 100BaseTX/FX

Port    Name               Status       Vlan     Duplex Speed   Type
------- ------------------ ------------ -------- ------ ------- ----
Fa0/21                     connected    1        A-Full   A-100 100BaseTX/FX
Fa0/22                     connected    1        A-Full   A-100 100BaseTX/FX
Fa0/23                     connected    1        A-Full   A-100 100BaseTX/FX
Fa0/24                     connected    1        A-Full   A-100 100BaseTX/FX
Gi0/1                      connected    1          Full    1000 1000BaseT
Gi0/2                      connected    1          Full    1000 1000BaseT
```

The following is sample 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: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Disabled
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: NONE
Pruning VLANs Enabled: NONE

Priority for untagged frames: 0
Override vlan tag priority: FALSE
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 switchport 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.
Priority for untagged frames	Displays the port priority on incoming untagged frames.

Related Commands

Command	Description
switchport access	Configures a port as static access.
switchport mode	Configures the VLAN membership mode of a port.
switchport priority default	Provides a default port priority for the incoming untagged frames.

show ip igmp snooping

Use the **show ip igmp snooping** privileged EXEC command to display the Internet Group Management Protocol (IGMP) snooping configuration of the switch or the VLAN.

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

show ip igmp snooping vlan *vlan-id* **|** [{**begin** | **exclude** | **include**} *expression*]

Syntax Description

vlan *vlan-id*	(Optional) Keyword and variable to specify a VLAN; valid values are 1 to 1001.
| begin	(Optional) Display begins with the line that matches the specified *expression*.
| exclude	(Optional) Display excludes lines that match the specified *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	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)WC(1)	This command was first introduced.

Usage Guidelines

Use this command to display snooping characteristics for the switch or for a specific VLAN.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

The following example shows how to display snooping information for the switch:

```
Switch# show ip igmp snooping

vlan 1
----------
  IGMP snooping is globally enabled
  IGMP snooping is enabled on this Vlan
  IGMP snooping immediate-leave is enabled on this Vlan
  IGMP snooping mrouter learn mode is pim-dvmrp on this Vlan
vlan 2
----------
  IGMP snooping is globally enabled
  IGMP snooping is enabled on this Vlan
  IGMP snooping immediate-leave is enabled on this Vlan
  IGMP snooping mrouter learn mode is cgmp on this Vlan
```

```
vlan 3
----------
  IGMP snooping is globally enabled
  IGMP snooping is enabled on this Vlan
  IGMP snooping immediate-leave is disabled on this Vlan
  IGMP snooping mrouter learn mode is cgmp on this Vlan
vlan 4
----------
  IGMP snooping is globally enabled
  IGMP snooping is enabled on this Vlan
  IGMP snooping immediate-leave is disabled on this Vlan
  IGMP snooping mrouter learn mode is cgmp on this Vlan
vlan 5
----------
  IGMP snooping is globally enabled
  IGMP snooping is enabled on this Vlan
  IGMP snooping immediate-leave is disabled on this Vlan
  IGMP snooping mrouter learn mode is pim-dvmrp on this Vlan
vlan 33
----------
  IGMP snooping is globally enabled
  IGMP snooping is enabled on this Vlan
  IGMP snooping immediate-leave is disabled on this Vlan
  IGMP snooping mrouter learn mode is pim-dvmrp on this Vlan
```

The following example shows how to display snooping information for a specific VLAN:

```
Switch# show ip igmp snooping vlan 1

vlan 1
----------
  IGMP snooping is globally enabled
  IGMP snooping is enabled on this Vlan
  IGMP snooping immediate-leave is enabled on this Vlan
  IGMP snooping mrouter learn mode is pim-dvmrp on this Vlan
```

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping.
ip igmp snooping vlan vlan_id	Enables IGMP snooping on the VLAN interface.
ip igmp snooping vlan immediate-leave	Configures IGMP Immediate-Leave processing.
ip igmp snooping vlan mrouter	Configures a Layer 2 port as a multicast router port.
show mac-address-table multicast	Displays the Layer 2 multicast entries for a VLAN.

show ip igmp snooping mrouter

Use the **show ip igmp snooping mrouter** privileged EXEC command to display information on dynamically learned and manually configured multicast router ports.

show ip igmp snooping mrouter vlan *vlan-id* **|** [{**begin** | **exclude** | **include**} *expression*]

Syntax Description

vlan *vlan-id*	(Optional) Keyword and variable to specify a VLAN; valid values are 1 to 1001.
| begin	(Optional) Display begins with the line that matches the specified *expression*.
| exclude	(Optional) Display excludes lines that match the specified *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	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)WC(1)	This command was first introduced.

Usage Guidelines

You can also use the **show mac-address-table multicast** command to display entries in the MAC address table for a VLAN that has Internet Group Management Protocol (IGMP) snooping enabled.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

The following example shows how to display snooping information for VLAN 1.

Note In this example, `Fa0/3` is a dynamically learned router port, and `Fa0/2` is a configured static router port.

```
Switch# show ip igmp snooping mrouter vlan 1

Vlan    ports
----    -----
   1    Fa0/2(static), Fa0/3(dynamic)
```

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping.
ip igmp snooping vlan	Enables IGMP snooping on the VLAN interface.
ip igmp snooping vlan immediate-leave	Configures IGMP Immediate-Leave processing.
ip igmp snooping vlan mrouter	Configures a Layer 2 port as a multicast router port.
show mac-address-table multicast	Displays the Layer 2 multicast entries for a VLAN.

show mac-address-table

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

show mac-address-table [**static** | **dynamic** | **secure** | **self** | **aging-time** | **count**] [**address** *hw-addr*] [**interface** *interface*] [**vlan** *vlan-id*] | [{**begin** | **exclude** | **include**} *expression*]

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 *hw-addr*	(Optional) Display information for a specific address.
interface *interface*	(Optional) Display addresses for a specific port.
vlan *vlan-id*	(Optional) Display addresses for a specific VLAN. Valid IDs are from 1 to 1001; do not enter leading zeroes.
| **begin**	(Optional) Display begins with the line that matches the specified *expression*.
| **exclude**	(Optional) Display excludes lines that match the specified *expression*.
| **include**	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

This command displays the MAC address table for the switch. Specific views can be defined by using the optional keywords and values. If more than one optional keyword is used, all of the conditions must be true in order for that entry to be displayed.

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

The following is sample 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 multicast

Use the **show mac-address-table multicast** privileged EXEC command to display the Layer 2 multicast entries for the switch or for the VLAN.

show mac-address-table multicast vlan *vlan-id* **[user|igmp-snooping] [count]** | [{**begin** | **exclude** | **include**} *expression*]

Syntax Description

vlan *vlan-id*	(Optional) Specify a VLAN; valid values are 0 to 1001.
user	(Optional) Display only the user-configured multicast entries.
igmp_snooping	(Optional) Display only entries learned through Internet Group Management Protocol (IGMP) snooping.
count	(Optional) Display total number of entries for the specified criteria instead of the actual entries.
| begin	(Optional) Display begins with the line that matches the specified *expression*.
| exclude	(Optional) Display excludes lines that match the specified *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Defaults

This command has no default setting.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

Displays the multicast MAC address for the switch.

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

The following example shows how to display the multicast MAC address for the switch:

```
Switch#show mac-address-table multicast

Vlan    Mac Address     Type    Ports
----    -----------     ----    -----
   1    0100.5e00.0128  IGMP    Fa0/11
   1    0100.5e01.1111  USER    Fa0/5, Fa0/6, Fa0/7, Fa0/11
```

show ntp associations

Use the **show ntp associations** privileged EXEC command to display the status of Network Time Protocol (NTP) associations.

show ntp associations [**detail**] **|** [{**begin** | **exclude** | **include**} *expression*]

Syntax Description

detail	(Optional) Show detailed information about each NTP association.
| begin	(Optional) Display begins with the line that matches the specified *expression*.
| exclude	(Optional) Display excludes lines that match the specified *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

Detailed descriptions of the information displayed by this command can be found in the NTP specification RFC 1305.

The following is sample output from the **show ntp associations** command:

```
Switch# show ntp associations
     address         ref clock     st  when  poll reach  delay  offset    disp
 ~160.89.32.2      160.89.32.1       5    29  1024  377     4.2   -8.59     1.6
+~131.108.13.33    131.108.1.111     3    69   128  377     4.1    3.48     2.3
*~131.108.13.57    131.108.1.111     3    32   128  377     7.9   11.18     3.6
* master (synced), # master (unsynced), + selected, - candidate, ~ configured
```

show ntp status

Use the **show ntp status** privileged EXEC command to display the status of the Network Time Protocol (NTP).

show ntp status | [{**begin** | **exclude** | **include**} *expression*]

Syntax Description

| begin	(Optional) Display begins with the line that matches the specified *expression*.
| exclude	(Optional) Display excludes lines that match the specified *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

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.

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

The following is sample output from the **show ntp status** command:

```
Switch# show ntp status
Clock is synchronized, stratum 4, reference is 131.108.13.57
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**19
reference time is AFE2525E.70597B34 (00:10:22.438 PDT Mon Jul 5 1993)
clock offset is 7.33 msec, root delay is 133.36 msec
root dispersion is 126.28 msec, peer dispersion is 5.98 msec
```

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*] **|** [{**begin** | **exclude** | **include**} *expression*]

Syntax Description

group-number	(Optional) Port group to which the port is assigned.
| begin	(Optional) Display begins with the line that matches the specified *expression*.
| exclude	(Optional) Display excludes lines that match the specified *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

If the variable *group-number* is omitted, the **show port group** command displays all port groups on the switch.

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

The following is sample output from the **show port group** command:

```
Switch# show port group 1

Group  Interface
-----  --------------
    1  FastEthernet0/1
    1  FastEthernet0/4
```

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*] | [{**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface-id	(Optional) ID of the port number enabled for SPAN.
vlan *number*	(Optional) VLAN number from 1 to 1001. Do not enter leading zeroes.
| begin	(Optional) Display begins with the line that matches the specified *expression*.
| exclude	(Optional) Display excludes lines that match the specified *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

If the variable *interface* is omitted, the **show port monitor** command displays all monitor ports on the switch.

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

The following is sample 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 protected

Use the **show port protected** privileged EXEC command to display the port protected mode for all ports.

show port protected | [{**begin** | **exclude** | **include**} *expression*]

Syntax Description

| begin	(Optional) Display begins with the line that matches the specified *expression*.
| exclude	(Optional) Display excludes lines that match the specified *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

The following is sample 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*] | [{**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface-id	(Optional) ID of the port number.
vlan *number*	(Optional) VLAN number from 1 to 1001. Do not enter leading zeroes.
| begin	(Optional) Display begins with the line that matches the specified *expression*.
| exclude	(Optional) Display excludes lines that match the specified *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

If the variable *interface* is omitted, the **show port security** command displays all secure ports on the switch.

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

The following is sample output from the **show port security** command for fixed port 07:

```
Switch# show port security fa0/7

Secure Port      Secure Addr    Secure Addr  Security   Security Action
                 Cnt (Current)  Cnt (Max)    Reject Cnt
---------------  -------------  -----------  ---------- ----------------
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**}] | [{**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface	(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.
| begin	(Optional) Display begins with the line that matches the specified *expression*.
| exclude	(Optional) Display excludes lines that match the specified *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

If the variable *interface* 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.

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

The following is sample 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 proposed

Use the **show proposed** VLAN database command to display the proposed VLAN database or a selected VLAN from it.

show proposed [*vlan-id*] **|** [{**begin** | **exclude** | **include**} *expression*]

Syntax Description

vlan-id	(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 1001; do not enter leading zeroes.
| begin	(Optional) Display begins with the line that matches thespecified *expression*.
| exclude	(Optional) Display excludes lines that match the specified *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

VLAN database

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

If the variable *vlan-id* is omitted, the **show proposed** command displays the entire proposed VLAN database.

The proposed VLAN database is not the running configuration until you use the **exit** or **apply** command.

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

The following is sample output from the **show proposed** command:

```
Switch(vlan)# show proposed
    Name: default
    Media Type: Ethernet
    VLAN 802.10 Id: 100001
    State: Operational
    MTU: 1500
    Translational Bridged VLAN: 1002
    Translational Bridged VLAN: 1003

    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
```

```
Name: token-ring-default
Media Type: Token Ring
VLAN 802.10 Id: 101003
State: Operational
MTU: 1500
Bridge Type: SRB
Ring Number: 0
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

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

Name: trnet-default
Media Type: Token Ring Net
VLAN 802.10 Id: 101005
State: Operational
MTU: 1500
Maximum ARE Hop Count: 7
Maximum STE Hop Count: 7
Backup CRF Mode: Disabled
Translational Bridged VLAN: 1
Translational Bridged VLAN: 1002

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
Name: trnet-default
Media Type: Token Ring Net
VLAN 802.10 Id: 101005
State: Operational
MTU: 1500
Bridge Type: SRB
Bridge Number: 1
STP Type: IBM
```

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

show rps

Use the **show rps** privileged EXEC command to display the status of the Cisco Redundant Power System (RPS).

show rps | [{**begin** | **exclude** | **include**} *expression*]

Syntax Description

| begin	(Optional) Display begins with the line that matches the specified *expression*.
| exclude	(Optional) Display excludes lines that match the specified *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

The following is sample 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
DEACTIVATED	The RPS is connected, operational, and in active mode. The switch is operating from its own internal power supply.	Solid green

Table 2-2 Show RPS Display Output Description (continued)

Display	Description	Switch RPS LED Color
FAULTY	The RPS is connected but not functioning. One of the power supplies in the RPS could be powered down, or a fan on the RPS could have failed, or RPS temperature is too high, or RPS is in standby mode.	Solid amber (all switch and RPS models)
NOT AVAILABLE	The RPS is backing up another switch; power redundancy is lost.	Blinking green

show spanning-tree

Use the **show spanning-tree** privileged EXEC command to display spanning-tree information for the specified spanning-tree instances.

show spanning-tree [**brief**] | [**summary**] | [**vlan** *stp-list*] [**interface** *interface-list*] | [{**begin** | **exclude** | **include**} *expression*]

Syntax Description

brief	Display a brief status of the spanning tree.
summary	Display a summary of the spanning-tree states.
vlan *stp-list*	(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 1001; do not enter leading zeroes. Ranges are not supported.
interface *interface-list*	List of ports for which spanning-tree information is displayed. Enter each port separated by a space. Ranges are not supported.
| begin	(Optional) Display begins with the line that matches the specified *expression*.
| exclude	(Optional) Display excludes lines that match the specified *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

If the variable *stp-list* is omitted, the command applies to the Spanning Tree Protocol (STP) instance associated with VLAN 1.

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

The following is sample output from the **show spanning-tree summary** command:

```
Switch# show spanning-tree summary

UplinkFast is disabled

Name                 Blocking Listening Learning Forwarding STP Active
-------------------- -------- --------- -------- ---------- ----------
VLAN1                23       0         0        1          24
-------------------- -------- --------- -------- ---------- ----------
              1 VLAN 23       0         0        1          24
```

```
Switch# show spanning-tree brief
VLAN1
  Spanning tree enabled protocol IEEE
  ROOT ID    Priority 32768
             Address 0030.7172.66c4
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
VLAN1
  Spanning tree enabled protocol IEEE
  ROOT ID    Priority 32768
             Address 0030.7172.66c4
Port                            Designated
Name    Port ID Prio Cost Sts  Cost  Bridge ID      Port ID
------- ------- ---- ---- ---  ----  -------------- -------
Fa0/11  128.17  128  100  BLK  38    0404.0400.0001 128.17
Fa0/12  128.18  128  100  BLK  38    0404.0400.0001 128.18
Fa0/13  128.19  128  100  BLK  38    0404.0400.0001 128.19
Fa0/14  128.20  128  100  BLK  38    0404.0400.0001 128.20
Fa0/15  128.21  128  100  BLK  38    0404.0400.0001 128.21
Fa0/16  128.22  128  100  BLK  38    0404.0400.0001 128.22
Fa0/17  128.23  128  100  BLK  38    0404.0400.0001 128.23
Fa0/18  128.24  128  100  BLK  38    0404.0400.0001 128.24
Fa0/19  128.25  128  100  BLK  38    0404.0400.0001 128.25
Fa0/20  128.26  128  100  BLK  38    0404.0400.0001 128.26
Fa0/21  128.27  128  100  BLK  38    0404.0400.0001 128.27

Port                            Designated
Name    Port ID Prio Cost Sts  Cost  Bridge ID      Port ID
------- ------- ---- ---- ---  ----  -------------- -------
Fa0/22  128.28  128  100  BLK  38    0404.0400.0001 128.28
Fa0/23  128.29  128  100  BLK  38    0404.0400.0001 128.29
Fa0/24  128.30  128  100  BLK  38    0404.0400.0001 128.30 Hello Time   2 sec  Max Age 20
sec  Forward Delay 15 sec
```

The following is sample 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 32768, address 00e0.1eb2.ddc0
  Configured hello time 2, max age 20, forward delay 15
  Current root has priority 32768, address 0010.0b3f.ac80
  Root port is 5, cost of root path is 10
  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

Interface Fa0/1  in Spanning tree 1 is down
   Port path cost 100, Port priority 128
   Designated root has priority 32768, address 0010.0b3f.ac80
   Designated bridge has priority 32768, address 00e0.1eb2.ddc0
   Designated port is 1, path cost 10
   Timers: message age 0, forward delay 0, hold 0
   BPDU: sent 0, received 0
...
```

The following is sample 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
```

Related Commands

Command	Description
spanning-tree	Enables STP on a VLAN.
spanning-tree forward-time	Sets 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 to be used for specified spanning-tree instances.

show tacacs

Use the **show tacacs** privileged EXEC command to display various Terminal Access Controller Access Control System Plus (TACACS+) server statistics.

show tacacs | [{**begin** | **exclude** | **include**} *expression*]

Syntax Description

| begin	(Optional) Display begins with the line that matches the specified *expression*.
| exclude	(Optional) Display excludes lines that match the specified *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

The following is sample 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*] | [{**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface-id	(Optional) ID of the port number or a VLAN ID. Valid IDs are from 1 to 1001.
| begin	(Optional) Display begins with the line that matches the specified *expression*.
| exclude	(Optional) Display excludes lines that match the specified *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

The following is sample output from the **show udld fa0/11** command. For 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 is displayed if the link is down or if it is connected to an UDLD-incapable device. A bidirectional state is displayed if the link is a normal two-way connection to a UDLD-capable device. All other values indicate 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 most often 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 current 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.

Table 2-3 Show Udld Field Descriptions (continued)

Field	Description
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	Indicates that there are no outstanding requests from neighbors to resynchronize cache data.
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 number 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** privileged EXEC command to display version information for the hardware and firmware.

show version | [{**begin** | **exclude** | **include**} *expression*]

Syntax Description

| begin	(Optional) Display begins with the line that matches the specified *expression*.
| exclude	(Optional) Display excludes lines that match the specified *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

The following is sample output from the **show version** command:

```
Switch# show version

Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-C3H2S-M), Experimental Version 12.0(5)WC(1)
[cchang-switch2_12_0t 845]
Copyright (c) 1986-2000 by cisco Systems, Inc.
Compiled Tue 29-Aug-00 11:27 by cchang
Image text-base: 0x80010000, data-base: 0x802F2000

ROM: Bootstrap program is Commander boot loader

switch uptime is 14 hours, 57 minutes
System returned to ROM by power-on
System image file is "flash:c2950-c3h2s-mz.120.bin"


cisco WS-C2950-12 (RC32300) processor with 22383K bytes of memory.
Last reset from system-reset

Processor is running Enterprise Edition Software
Cluster command switch capable
Cluster member switch capable
12 FastEthernet/IEEE 802.3 interface(s)
```

```
32K bytes of flash-simulated non-volatile configuration memory.
32K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: 00:01:02:03:04:00
Configuration register is 0xF
```

show vlan

Use the **show vlan** privileged 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*] | [{**begin** | **exclude** | **include**} *expression*]

Syntax Description

brief	(Optional) Display one line for each VLAN with the VLAN name, status, and its ports.
id *vlan-id*	(Optional) ID of the VLAN displayed. Valid IDs are from 1 to 1001; do not enter leading zeroes.
name *vlan-name*	(Optional) Name of the VLAN displayed. The VLAN name is an ASCII string from 1 to 32 characters.
| begin	(Optional) Display begins with the line that matches the specified *expression*.
| exclude	(Optional) Display excludes lines that match the specified *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

The following is sample 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
```

The following is sample 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
```

The following is sample 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 vtp

Use the **show vtp** privileged EXEC command to display general information about the VLAN Trunk Protocol (VTP) management domain, status, and counters.

show vtp {**counters** | **status**} | [{**begin** | **exclude** | **include**} *expression*]

Syntax Description

counters	Display the VTP counters for the switch.
status	Display general information about the VTP management domain.
| **begin**	(Optional) Display begins with the line that matches the specified *expression*.
| **exclude**	(Optional) Display excludes lines that match the specified *expression*.
| **include**	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter | **exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

The following is sample output from the **show vtp counters** command. Table 2-4 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 2-4 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	Number of revision errors. 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. 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 indicates that the VTP password in the two switches is different, or the switches have different configurations. These errors indicate that the switch is filtering incoming advertisements, which causes the VTP database to become unsynchronized across the network.

Table 2-4 Show VTP Counters Field Descriptions (continued)

Field	Description
No. of Configuration Digest Errors	Number of MD5 digest errors. Digest errors increment whenever the MD5 digest in the summary packet and the MD5 digest of the received advertisement calculated by the switch do not match. This error usually indicates that the VTP password in the two switches is different. To solve this problem, make sure the VTP password on all switches is the same. These errors indicate that the switch is filtering incoming advertisements, which causes the VTP database to become unsynchronized across the network.
No. of V1 Summary Errors	Number of version 1 errors. Version 1 summary errors increment whenever a switch in VTP V2 mode receives a VTP version 1 frame. These errors indicate 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.
Summary Advts Received from non-pruning-capable device	Number of VTP summary messages received on the trunk from devices that do not support pruning.

The following is sample output from the **show vtp status** command. Table 2-5 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 2-5 Show VTP Status Field Descriptions

Field	Description
VTP Version	Displays the VTP version operating on the switch. By default, 2950 switches implement version 1 but can be set to version 2.
Configuration Revision	Current configuration revision number on this switch.
Maximum VLANs Supported Locally	Maximum number of VLANs supported locally.
Number of Existing VLANs	Number of existing VLANs.

Table 2-5 Show VTP Status Field Descriptions (continued)

Field	Description
VTP Operating Mode	Displays the VTP operating mode, which can be server, client, or transparent. Server: a switch in VTP server mode is enabled for VTP and sends advertisements. You can configure VLANs on it. The switch guarantees that it can recover all the VLAN information in the current VTP database from nonvolatile storage after reboot. By default, every switch is a VTP server. 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. 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.
VTP Domain Name	Name that identifies the administrative domain for the switch.
VTP V2 Mode	Displays if VTP version 2 mode is enabled. All VTP version 2 switches operate in version 1 mode by default. Each VTP switch automatically detects the capabilities of all the other VTP devices. A network of VTP devices should be configured to version 2 only if all VTP switches in the network can operate in version 2 mode.
VTP Traps Generation	Displays whether VTP traps are 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 counters.
vtp	Configures the VTP mode.

show wrr-queue bandwidth

Use the **show wrr-queue bandwidth** user EXEC command to display the weighted round-robin (WRR) bandwidth allocation for the four class of service (CoS) priority queues.

show wrr-queue bandwidth | [{**begin** | **exclude** | **include**} *expression*]

Syntax Description

| begin	(Optional) Display begins with the line that matches the specified *expression*.
| exclude	(Optional) Display excludes lines that match the specified *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

The following is sample output from the **show wrr-queue bandwidth** command.

```
Switch# show wrr-queue bandwidth

WRR Queue  :   1   2   3   4

Bandwidth  :  10  20  30  40
```

Related Commands

Command	Description
wrr-queue cos-map	Assigns CoS values to the CoS priority queues.
wrr-queue bandwidth	Assigns WRR weights to the four CoS priority queues.
show wrr-queue cos-map	Displays the mapping of the CoS to the priority queues.

show wrr-queue cos-map

Use the **show wrr-queue cos-map** user EXEC command to display the mapping of the class of service (CoS) priority queues.

show wrr-queue cos-map | [{**begin** | **exclude** | **include**} *expression*]

Syntax Description

| begin	(Optional) Display begins with the line that matches the specified *expression*.
| exclude	(Optional) Display excludes lines that match the specified *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

The following is sample output from the **show wrr-queue cos-map** command.

```
Switch# show wrr-queue cos-map

CoS Value      :  0  1  2  3  4  5  6  7

Priority Queue :  1  1  2  2  3  3  4  4
```

Related Commands

Command	Description
wrr-queue cos-map	Assigns CoS values to the CoS priority queues.
wrr-queue bandwidth	Assigns weighted round-robin (WRR) weights to the four CoS priority queues.
show wrr-queue bandwidth	Displays the WRR bandwidth allocation for the four CoS priority queues.

shutdown

Use the **shutdown** interface configuration command to disable a port and to shutdown 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
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

The **shutdown** command for a port causes it to stop forwarding. You can enable the port with the **no shutdown** command.

The **no shutdown** command has no effect if the port is a static-access port assigned to a VLAN that has been deleted, suspended, or shut down. The port must first be a member of an active VLAN before it can be reenabled.

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

The following examples show how to disable fixed port fa0/8 and how to reenable 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** command in privileged EXEC mode.

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

vlan-id	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 Trunk Protocol (VTP). The default VLANs are 1 and 1002–1005. Do not enter leading zeroes.

Defaults

No default is defined.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)WC(1)	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

The following example shows how to shutdown traffic on VLAN 2:

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

You can verify the previous command by entering the **show vlan** command in privileged EXEC mode.

Related Commands

Command	Description
abort	Abandons the proposed new VLAN database, exits VLAN database mode, and returns to privileged EXEC mode.
apply	Implements the proposed new VLAN database, increments the database configuration revision number, propagates it throughout the administrative domain, and remains in VLAN database mode.
exit	Implements the proposed new 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 vlan-membership

Use the **snmp-server enable traps vlan-membership** global configuration command to enable 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
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

Specify the host that receives the traps by using the **snmp-server host** command.

Examples

The following 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** command in privileged EXEC mode.

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 SNMP notification for VLAN Trunk 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
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

Specify the host that receives the traps by using the **snmp-server host** command.

Examples

The following 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** or **show running-config** command in privileged EXEC mode.

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 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

host-address	IP address or name of the SNMP trap host.
community-string	Password-like community string sent with the trap operation
c2900	(Optional) Send SNMP 2950 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 *port-number*	(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 Trunk 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
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

Use the **snmp-server host** command with the **snmp-server enable traps** commands to generate traps.

Examples

The following 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** command in privileged EXEC mode.

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.

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 *stp-list*	(Optional) List of spanning-tree instances. Each spanning-tree instance is associated with a VLAN ID. Valid IDs are from 1 to 1001. 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

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

Disabling STP causes the VLAN or 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.

You can disable STP on a VLAN that is not currently active, and verify the change by using the privileged EXEC **show running-config** or the **show spanning-tree vlan** *stp-lis*t command. The setting takes effect when the VLAN is activated.

If the variable *stp-list* is omitted, the command applies to the STP instance associated with VLAN 1.

You can enable STP on a VLAN that has no ports assigned to it.

Examples

The following example shows how to disable STP on VLAN 5:

```
Switch(config)# no spanning-tree vlan 5
```

You can verify the previous command by entering the **show spanning-tree** command in privileged EXEC mode. In this instance, VLAN 5 does not appear in the list.

Related Commands

Command	Description
show spanning-tree	Displays spanning-tree information for the specified spanning-tree instances.
spanning-tree forward-time	Sets the forwarding-time for the specified spanning-tree instances.

Command	Description
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 protocol 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 *stp-list*	(Optional) List of spanning-tree instances. Each spanning-tree instance is associated with a VLAN ID. Valid IDs are from 1 to 1001. 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

The default path cost is computed from the interface bandwidth setting. The following are IEEE default path cost values:

- 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
12.0(5)WC(1)	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 a cost for a port or on a VLAN that does not exist. The setting takes effect when the VLAN exists.

Examples

The following example shows how to set a path cost value of 64 for VLAN 1:

```
Switch(config-if)# spanning-tree vlan 1 cost 64
```

You can verify the previous command by entering the **show spanning-tree** command in privileged EXEC mode.

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 *stp-list*	(Optional) List of spanning-tree instances. Each spanning-tree instance is associated with a VLAN ID. Valid IDs are from 1 to 1001. Enter each VLAN ID separated by a space. Do not enter leading zeroes. Ranges are not supported.
seconds	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
12.0(5)WC(1)	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 forwarding-time on a VLAN that has no ports assigned to it. The setting takes effect when you assign ports to it.

Examples

The following example shows how to set the spanning-tree forwarding time to 18 seconds for VLAN 20:

```
Switch(config)# spanning-tree vlan 20 forward-time 18
```

You can verify the previous command by entering the **show spanning-tree** command in privileged EXEC mode.

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.

Command	Description
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 protocol 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 *stp-list*	(Optional) List of spanning-tree instances. Each spanning-tree instance is associated with a VLAN ID. Valid IDs are from 1 to 1001. Enter each VLAN ID separated by a space. Do not enter leading zeroes. Ranges are not supported.
seconds	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
12.0(5)WC(1)	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

The following 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** command in privileged EXEC mode.

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 protocol 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 1001. Enter each VLAN ID separated by a space. Do not enter leading zeroes. Ranges are not supported.
seconds	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
12.0(5)WC(1)	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

The following example shows how to set **spanning-tree max-age** to 30 seconds for VLAN 20:

```
Switch(config)# spanning-tree vlan 20 max-age 30
```

The following 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** command in privileged EXEC mode.

Related Commands

Command	Description
show spanning-tree	Displays spanning-tree information for the specified spanning-tree instances.
spanning-tree forward-time	Sets 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 protocol 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
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

Use this feature only on ports that connect to end stations.

This feature affects all VLANs on the port.

A port with the Port Fast feature enabled is moved directly to the spanning-tree forwarding state.

Examples

The following example shows how to enable the Port Fast feature on fixed port 2.

```
Switch(config-if)# spanning-tree portfast fa0/2
```

You can verify the previous commands by entering the **show running-config** in privilege EXEC mode.

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, which 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 *stp-list*	(Optional) List of spanning-tree instances. Each spanning-tree instance is associated with a VLAN ID. Valid IDs are from 1 to 1001. Enter each VLAN ID separated by a space. Do not enter leading zeroes. Ranges are not supported.
port-priority	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
12.0(5)WC(1)	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

The following 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** command in privileged EXEC mode.

Related Commands

Command	Description
show spanning-tree	Displays spanning-tree information for the specified spanning-tree instances.
spanning-tree protocol	Specifies the STP protocol 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 *stp-list*	(Optional) List of spanning-tree instances. Each spanning-tree instance is associated with a VLAN ID. Valid IDs are from 1 to 1001. Enter each VLAN ID separated by a space. Do not enter leading zeroes. Ranges are not supported.
bridge-priority	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
12.0(5)WC(1)	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

The following 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** command in privileged EXEC mode.

Related Commands

Command	Description
show spanning-tree	Displays spanning-tree information for the specified spanning-tree instances.
spanning-tree forward-time	Sets the forwarding-time for the specified spanning-tree instances.
spanning-tree hello-time	Specifies the interval between hello Bridge Protocol Data Units (BPDUs).

Command	Description
spanning-tree max-age	Changes the interval between messages the spanning tree receives from the root switch.
spanning-tree protocol	Specifies the STP protocol 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 1001. 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
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

Changing the **spanning-tree protocol** command causes STP parameters to change to default values of the new protocol.

If the variable *stp-list* is omitted, this command applies to the STP 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

The following example shows how to change the STP protocol 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** command in privileged EXEC mode.

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	Sets 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 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)WC(1)	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 executed, 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

The following 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** command in privileged EXEC mode.

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	Sets 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, which 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 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 *pkts-per-second*	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
12.0(5)WC(1)	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** command in privileged EXEC mode.

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** | **1000** | **auto**}

no speed

Syntax Description

10	Port runs at 10 Mbps.
100	Port runs at 100 Mbps.
1000	Port runs at 1000 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**.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)WC(1)	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.

For Gigabit Ethernet ports, the speed can be configured at 10, 100, or 1000 Mbps.

Note The Gigabit Ethernet ports can operate in either half- or full-duplex mode when they are set to 10 or 100 Mbps, but when they are set to 1000 Mbps, they can only operate in the full-duplex mode.

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 2950 Desktop Switch Software Configuration Guide.*

Examples

The following example shows how to set port 1 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 privilege 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*

no switchport access vlan *vlan-id*

Syntax Description

vlan *vlan-id*	ID of the VLAN. Valid IDs are from 1 to 1001. Do not enter leading zeroes.

Defaults

All ports are in static-access mode in VLAN 1.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

The port must be in access mode before the **switchport access vlan** *vlan-id* or **switchport access vlan** command can take effect. For more information, see the switchport mode, page 2-163.

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.

Examples

The following example shows how to assign a port already in access mode to VLAN 2 (instead of the default VLAN 1):

```
Switch(config-if)# switchport access vlan 2
```

You can verify 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 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** | **trunk**}

no switchport mode {**access** | **trunk**}

Syntax Description

access	Set the port to access mode (static-access). 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.
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
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

Configuration by using the **access** or **trunk** keywords takes affect only when the port is changed to the corresponding mode by using the **switchport mode** command. The static-access 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.

Trunk ports cannot coexist on the same switch.

The following example shows how to configure a port for access mode:

```
Switch(config-if)# switchport mode access
```

The following 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 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

default-priority-id	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 appliance. • **cos** *value*—Override the 802.1p priority of devices connected to the appliance. The cos value is a number from 0 to 7. Seven is the highest priority. • **none**—The appliance is not instructed what to do with the priority. • **trust**—Specify that the appliance 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)WC(1)	This command was first introduced.

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 IEEE 802.1Q VLAN tagged frames. If the incoming frame is an IEEE 802.1Q VLAN tagged frame, IEEE 802.1p User Priority bits is used.

Examples

The following 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** command in privileged EXEC mode.

The following 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** command in privileged EXEC mode.

Related Commands

Command	Description
show interface	Displays the administrative and operational status of a switching (nonrouting) port.
switchport access	Configures a port as a static-access port.
switchport mode	Configures the VLAN membership mode of a 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 *vlan-list*	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 *vlan-list*	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 *vlan-list*	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
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

When the **no switchport trunk allowed vlan** form is used, the allowed list is reset 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 VLAN 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.

Examples

The following 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** command in privileged EXEC mode.

Related Commands

Command	Description
switchport mode	Configures the VLAN membership mode of a port.
switchport trunk encapsulation	Sets the encapsulation format on the trunk port.
switchport trunk native	Sets 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 *vlan-id*	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
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

All untagged traffic received on the 802.1Q trunk port is forwarded with the native VLAN configured for the port.

If a packet has a VLAN ID that is the same as the sending port native VLAN ID, the packet is transmitted untagged; otherwise, the switch transmits the packet with a tag.

Examples

The following example shows how to configure VLAN 3 as the default port to send all untagged traffic:

```
Switch(config-if)# switchport trunk native vlan 3
```

You can verify the previous command by entering the **show interface** *interface-id* **switchport** command in privileged EXEC mode.

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	Sets the encapsulation format on the trunk 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 restore the default.

tacacs-server attempts *count*

no tacacs-server attempts

Syntax Description

count	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
12.0(5)WC(1)	This command was first introduced.

Examples

The following example shows how to change the login attempt to just one:

```
Switch(config)# tacacs-server attempts 1
```

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

Related Commands

Command	Description
enable use-tacacs	Enables the use of TACACS to determine whether a user can access the privileged command level.
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	Sets the authentication encryption key used for all TACACS+ communications between the access server and the TACACS+ daemon.

Command	Description
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.
tacacs-server timeout	Sets the interval that the server waits for a TACACS, Extended TACACS, or TACACS+ server to reply.

tacacs-server directed-request

Use the **tacacs-server directed-request** global configuration command to send only a username to a specified server when a direct request is issued in association with Terminal Access Controller Access Control System (TACACS), Extended TACACS, and TACACS+. Use the **no** form of this command to send the whole string, both before and after the @ symbol.

tacacs-server directed-request

no tacacs-server directed-request

Syntax Description

This command has no arguments or keywords.

Defaults

The directed-request feature is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

This command sends only the portion of the username before the @ symbol to the host specified after the @ symbol. In other words, with the directed-request feature enabled, you can direct a request to any of the configured servers, and only the username is sent to the specified server.

Using **no tacacs-server directed-request** causes the whole string, both before and after the @ symbol, to be sent to the default TACACS server. When the directed-request feature is disabled, the router queries the list of servers, starting with the first one in the list. It sends the whole string and accepts the first response it gets from the server. The **tacacs-server directed-request** command is useful for sites that have developed their own TACACS server software that parses the whole string and makes decisions based on it.

With **tacacs-server directed-request** enabled, only configured TACACS servers can be specified by the user after the @ symbol. If the host name specified by the user does not match the IP address of a TACACS server configured by the administrator, the user input is rejected.

Use **no tacacs-server directed-request** to disable the ability of the user to choose between configured TACACS servers and to cause the entire string to be passed to the default server.

Examples

The following example shows how to pass the entire user input to the default TACACS server:

```
Switch(config)# no tacacs-server directed-request
```

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

Related Commands

Command	Description
enable use-tacacs	Enables the use of TACACS to determine whether a user can access the privileged command level.
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	Sets 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.
tacacs-server timeout	Sets 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
12.0(5)WC(1)	This command was first introduced.

Examples

The following 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** command in privileged EXEC mode.

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.

tacacs-server extended

Use the **tacacs-server extended** global configuration command to enable an Extended Terminal Access Controller Access Control System (TACACS) mode. Use the **no** form of this command to disable the mode.

tacacs-server extended

no tacacs-server extended

Syntax Description

This command has no arguments or keywords.

Defaults

The Extended TACACS mode is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

This command initializes Extended TACACS. To initialize authentication, authorization, and accounting (AAA) and TACACS+, use the **aaa new-model** command.

Examples

The following example shows how to enable Extended TACACS mode:

```
Switch(config)# tacacs-server extended
```

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

tacacs-server host

Use the **tacacs-server host** global configuration command to specify a Terminal Access Controller Access Control System (TACACS), Extended TACACS, or TACACS+ host. Use the **no** form of this command to delete the specified name or address.

tacacs-server host *hostname* [**single-connection**] [**port** *integer*] [**timeout** *integer*] [**key** *string*]

no tacacs-server host *hostname*

Syntax Description

hostname	Name or IP address of the host.
single-connection	(Optional) Specify that the switch maintain a single open connection for confirmation from an authentication, authorization, and accounting (AAA) and TACACS+ server (CiscoSecure Release 1.0.1 or later). This command contains no autodetect and fails if the specified host is not running a CiscoSecure daemon.
port *integer*	(Optional) Specify a server port number. The range is from 1 to 65535.
timeout *integer*	(Optional) Specify a timeout value. This overrides the global timeout value set with the **tacacs-server timeout** command for this server only. The timeout is an integer in seconds.The range is from 1 to 300 seconds.
key *string*	(Optional) Specify an authentication and encryption key. This key must match the key used by the TACACS+ daemon. Specifying this key overrides the key set by the global configuration **tacacs-server key** command for this server only. The key string is a character string specifying the authentication and encryption key.

Defaults

No host is specified.

The default port number is 49.

The default timeout is 5 seconds.

No key string is specified.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

You can use multiple **tacacs-server host** commands to specify additional hosts. The Cisco IOS software searches for hosts in the order in which you specify them. Use the **single-connection**, **port**, **timeout**, and **key** options only when running an AAA/TACACS+ server.

Because some of the parameters of the **tacacs-server host** command override global settings made by the **tacacs-server timeout** and **tacacs-server key** commands, you can use this command to enhance security on your network by uniquely configuring individual switches.

Examples

The following example shows how to specify a TACACS host named Sea_Change:

```
Switch(config)# tacacs-server host Sea_Change
```

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

The following example shows how to specify that the switch consult the CiscoSecure TACACS+ host named Sea_Cure on port number 51 for AAA confirmation. The timeout value for requests on this connection is 3 seconds; the encryption key is a_secret.

```
Switch(config)# tacacs-server host Sea_Cure single-connection port 51 timeout 3 key
a_secret
```

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

Related Commands

Command	Description
login tacacs	Configures the switch to use TACACS user authentication.
tacacs-server key	Sets the authentication encryption key used for all TACACS+ communications between the access server and the TACACS+ daemon.
tacacs-server timeout	Sets the interval that the server waits for a TACACS, Extended TACACS, or TACACS+ server to reply.

tacacs-server key

Use the **tacacs-server key** global configuration command to set the authentication encryption key used for all Terminal Access Controller Access Control System Plus (TACACS+) communications between the access server and the TACACS+ daemon. Use the **no** form of the command to disable the key.

tacacs-server key *key*

no tacacs-server key [*key*]

Syntax Description

key	Key used to set authentication and encryption. This key must match the key used on the TACACS+ daemon.

Defaults

No key is specified.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

After enabling authentication, authorization, and accounting (AAA) with the **aaa new-model** command, you must set the authentication and encryption key by using the **tacacs-server key** command.

The key entered must match the key used on the TACACS+ daemon. All leading spaces are ignored; spaces within and at the end of the key are not. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.

Examples

The following example shows how to set the authentication and encryption key to *dare to go*:

```
Switch(config)# tacacs-server key dare to go
```

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

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
tacacs-server host	Specifies a TACACS, Extended TACACS, or TACACS+ host.

tacacs-server last-resort

Use the **tacacs-server last-resort** global configuration command to cause the network access server to request the privileged password as verification for Terminal Access Controller Access Control System (TACACS) or Extended TACACS or to allow successful log in without further user input. Use the **no** form of the command to restore the system to the default behavior.

tacacs-server last-resort {**password** | **succeed**}

no tacacs-server last-resort {**password** | **succeed**}

Syntax Description

password	Provide the user access to the privileged EXEC command mode by entering the password set by the **enable** command.
succeed	Provide the user access to the privileged EXEC command mode without further question.

Defaults

The last-resort feature is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

Use the **tacacs-server last-resort** command to be sure that you can log in; for example, a systems administrator would use this command to log in to troubleshoot TACACS servers that might be down.

Note This command is not used in authentication, authorization, and accounting (AAA) and TACACS+.

Examples

The following example shows how to force successful log in:

```
Switch(config)# tacacs-server last-resort succeed
```

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

Related Commands

Command	Description
enable password	Sets a local password to control access to various privilege levels.
login (EXEC)	Changes a login username.

tacacs-server login-timeout

Use the **tacacs-server login-timeout** global configuration command to cause the network access server to request the privileged password as verification for Terminal Access Controller Access Control System (TACACS) or Extended TACACS or to allow successful log in without further user input. Use the **no** form of the command to restore the system to the default behavior.

tacacs-server login-timeout {**password** | **succeed**}

no tacacs-server login-timeout {**password** | **succeed**}

Syntax Descriptions

password	Provide the user access to the privileged EXEC command mode by entering the password set by the enable command.
succeed	Provide the user access to the privileged EXEC command mode without further question.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

Use the **tacacs-server login-timeout** command to be sure that you can log in; for example, a system administrator would use this command to log in to troubleshoot TACACS servers that might be down.

Note This command is not used in authentication, authorization, and accounting (AAA)/TACACS+.

Examples

The following example shows how to force successful log in:

```
Switch(config)# tacacs-server login-timeout succeed
```

Related Commands

Command	Description
enable password	Sets a local password to control access to various privilege levels.
login (EXEC)	Changes a login username.

tacacs-server optional-passwords

Use the **tacacs-server optional-passwords** global configuration command to specify that the first Terminal Access Controller Access Control System (TACACS) request to a TACACS or Extended TACACS server be made without password verification. Use the **no** form of this command to restore the default.

tacacs-server optional-passwords

no tacacs-server optional-passwords

Syntax Description

This command has no arguments or keywords.

Defaults

Password verification is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

When the user enters the login name, the login request is transmitted with the name and a zero-length password. If accepted, the login procedure completes. If the TACACS server refuses this request, the server software prompts for a password and tries again when the user supplies a password. The TACACS server must support authentication for users without passwords to make use of this feature. This feature supports all TACACS request—login, Serial Line Internet Protocol (SLIP), enable, and so on.

Note This command is not used in authentication, authorization, and accounting (AAA)/TACACS+.

Examples

The following example shows how to configure the first login to bypass TACACS verification:

```
Switch(config)# tacacs-server optional-passwords
```

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

tacacs-server retransmit

Use the **tacacs-server retransmit** global configuration command to specify the number of times the Cisco IOS software searches the list of Terminal Access Controller Access Control System (TACACS) or Extended TACACS server hosts. Use the **no** form of this command to disable retransmission.

tacacs-server retransmit *retries*

no tacacs-server retransmit

Syntax Description

retries	Integer that specifies the retransmit count. The range is from 0 to 100.

Defaults

The default is two retries.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

The Cisco IOS software tries all servers, allowing each one to time out before increasing the retransmit count.

Examples

The following example shows how to specify a retransmit counter value of 5:

```
Switch(config)# tacacs-server retransmit 5
```

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

tacacs-server timeout

Use the **tacacs-server timeout** global configuration command to set the interval that the server waits for a Terminal Access Controller Access Control System (TACACS), Extended TACACS, or TACACS+ server to reply. Use the **no** form of this command to restore the default.

tacacs-server timeout *seconds*

no tacacs-server timeout

Syntax Description

seconds	Integer that specifies the timeout interval in seconds. The range is from 1 to 1000.

Defaults

The timeout interval is 5 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Examples

The following example shows how to change the interval timer to 10 seconds:

```
Switch(config)# tacacs-server timeout 10
```

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

Related Commands

Command	Description
tacacs-server host	Specifies a TACACS, Extended TACACS, or TACACS+ host.

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)WC(1)	This command was first introduced.

Usage Guidelines

UDLD is supported on fiber- and copper-based Ethernet ports.

A UDLD-capable port cannot detect a unidirectional link if it is connected to a UDLD-incapable port of another switch.

This setting overrides the global UDLD configuration on the switch.

Examples

The following example shows how to enable UDLD on port 2:

```
Switch(config)# interface fastethernet 0/2
Switch(config-if)# udld enable
```

You can verify the previous command by entering the **show running-config** or the **show udld** *interface* command in privilege EXEC mode.

Related Commands

Command	Description
show running-config	Displays the running configuration on the switch.
show udld	Displays UDLD status for all ports or the specified port.
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)WC(1)	This command was first introduced.

Usage Guidelines

UDLD is supported on fiber- and copper-based Ethernet ports.

A UDLD-capable port cannot detect a unidirectional link if it is connected to a UDLD-incapable port of another switch.

This setting is overridden by each specific port UDLD configuration.

Examples

The following 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 privilege EXEC mode.

Related Commands

Command	Description
show running-config	Displays the running configuration on the switch.
show udld	Displays UDLD status for all ports or the specified port.
udld	Enables UDLD on a port.
udld reset	Resets any interface that has been shut down by UDLD.

udld reset

Use the **udld reset** privileged EXEC command to reset all interfaces that have been shut down by UniDirectional Link Detection (UDLD).

udld reset

Syntax Description

This command has no keywords or arguments.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Examples

The following example shows how to reset all interfaces that have been shut down by UDLD:

```
Switch# udld reset
1 ports shutdown by UDLD were reset.
```

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

Related Commands

Command	Description
show running-config	Displays the running configuration on the switch.
show udld	Displays UDLD status for all ports or the specified port.
udld	Enables UDLD on a port.
udld 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 2950 switches support only Ethernet ports. You can configure only FDDI and Token Ring media-specific characteristics for VLAN Trunk Protocol (VTP) global advertisements to other switches. These VLANs are locally suspended.

Table 2-6 lists the valid syntax for each media type.

Table 2-6 Valid Syntax for Different Media Types

Media Type	Valid Syntax
Ethernet	**vlan** *vlan-id* [**name** *vlan-name*] **media ethernet** [**state** {**suspend** | **active**}] [**said** *said-value*] [**mtu** *mtu-size*] [**tb-vlan1** *tb-vlan1-id*] [**tb-vlan2** *tb-vlan2-id*]
FDDI	**vlan** *vlan-id* [**name** *vlan-name*] **media fddi** [**state** {**suspend** | **active**}] [**said** *said-value*] [**mtu** *mtu-size*] [**ring** *ring-number*] [**parent** *parent-vlan-id*] [**tb-vlan1** *tb-vlan1-id*] [**tb-vlan2** *tb-vlan2-id*]
FDDI-NET	**vlan** *vlan-id* [**name** *vlan-name*] **media fdi-net** [**state** {**suspend** | **active**}] [**said** *said-value*] [**mtu** *mtu-size*] [**bridge** *bridge-number*] [**stp type** {**ieee** | **ibm** | **auto**}] [**tb-vlan1** *tb-vlan1-id*] [**tb-vlan2** *tb-vlan2-id*] If VTP V2 mode is disabled, do not set the **stp type** to **auto**.
Token Ring	VTP V2 mode is disabled. **vlan** *vlan-id* [**name** *vlan-name*] **media tokenring** [**state** {**suspend** | **active**}] [**said** *said-value*] [**mtu** *mtu-size*] [**ring** *ring-number*] [**parent** *parent-vlan-id*] [**tb-vlan1** *tb-vlan1-id*] [**tb-vlan2** *tb-vlan2-id*]
Token Ring concentrator relay function (TRCRF)	VTP V2 mode is enabled. **vlan** *vlan-id* [**name** *vlan-name*] **media tokenring** [**state** {**suspend** | **active**}] [**said** *said-value*] [**mtu** *mtu-size*] [**ring** *ring-number*] [**parent** *parent-vlan-id*] [**bridge type** {**srb** | **srt**}] [**are** *are-number*] [**ste** *ste-number*] [**backupcrf** {**enable** | **disable**}] [**tb-vlan1** *tb-vlan1-id*] [**tb-vlan2** *tb-vlan2-id*]

Table 2-6 Valid Syntax for Different Media Types (continued)

Media Type	Valid Syntax
Token Ring-NET	VTP V2 mode is disabled. **vlan** *vlan-id* [**name** *vlan-name*] **media tr-net** [**state** {**suspend** | **active**}] [**said** *said-value*] [**mtu** *mtu-size*] [**bridge** *bridge-number*] [**stp type** {**ieee** | **ibm**}] [**tb-vlan1** *tb-vlan1-id*] [**tb-vlan2** *tb-vlan2-id*]
Token Ring bridge relay function (TRBRF)	VTP V2 mode is enabled. **vlan** *vlan-id* [**name** *vlan-name*] **media tr-net** [**state** {**suspend** | **active**}] [**said** *said-value*] [**mtu** *mtu-size*] [**bridge** *bridge-number*] [**stp type** {**ieee** | **ibm** | **auto**}] [**tb-vlan1** *tb-vlan1-id*] [**tb-vlan2** *tb-vlan2-id*]

VLAN Configuration Rules

Table 2-7 describes the rules for configuring VLANs.

Table 2-7 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 2-7 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

vlan-id	ID of the configured VLAN. Valid IDs are from 1 to 1001 and must be unique within the administrative domain. Do not enter leading zeroes.
name	(Optional) Keyword to be followed by the VLAN name.
vlan-name	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.
fdi-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.
said-value	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).
mtu-size	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.

ring-number	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.
bridge-number	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.
parent-vlan-id	Integer 0 to 1001.
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.
are-number	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.
ste-number	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.
tb-vlan1-id and *tb-vlan2-id*	Integer from 0 to 1001.

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
12.0(5)WC(1)	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/or **tb-vlan2** 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 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

The following 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
```

The following 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** command in privileged EXEC mode.

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 Trunk 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
12.0(5)WC(1)	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

The following 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 new VLAN database, exits VLAN database mode, and returns to privileged EXEC mode.
apply	Implements the proposed new 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.

vtp

Use the **vtp** VLAN database command to configure the VLAN Trunk 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 current 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 Catalyst 2950 switches support up to 64 VLANs.

Defaults

Server mode is the default mode.

Command Modes

VLAN database

Command History

Release	Modification
12.0(5)WC(1)	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

The following 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** command in privileged EXEC mode.

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 Trunk Protocol (VTP) administrative domain.

vtp domain *domain-name*

Syntax Description

domain-name	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
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

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 currently trunking or after configuring a domain name using the **vtp domain** command. If the switch receives its domain from a summary packet, it resets its configuration revision number to zero. After the switch leaves the no-management-domain state, it can never be configured to reenter it until you clear the nonvolatile RAM (NVRAM) and reload the software.

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

The following 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** command in privileged EXEC mode.

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 Trunk 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

ifsfilename	The IOS IFS filename where the VTP VLAN configuration is stored.

Defaults

The default filename is *flash:vlan.dat*.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)WC(1)	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

The following example shows how to rename the filename for VTP configuration storage to *vtpfilename*:

```
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 Trunk 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.
password-value	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
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

Passwords are case sensitive. Passwords should match on all switches in the same domain.

When the **no vtp password** form of the command is used, the switch returns to the no-password state.

Examples

The following example shows how to configure the VTP domain password:

```
Switch(vlan)# vtp password ThisIsOurDomain'sPassword
```

Related Commands

Command	Description
vtp domain	Configures the VTP administrative domain.

vtp v2-mode

Use the **vtp v2-mode** VLAN database command to enable VLAN Trunk 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
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

Toggling the V2 mode state modifies certain parameters of certain default VLANs.

Each VTP switch automatically detects the capabilities of all the other VTP devices. To use 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).

If you are using VTP in a Token Ring environment, VTP V2 mode must be enabled.

If you are configuring a Token Ring bridge relay function (TRBRF) or Token Ring concentrator relay function (TRCRF) VLAN media type, you must use version 2.

If you are configuring a Token Ring or Token Ring-NET VLAN media type, you must use version 1.

Examples

The following example shows how to enable V2 mode in the proposed new VLAN database:

```
Switch(vlan)# vtp v2-mode
```

You can verify the previous commands by entering the **show vtp status** command in privileged EXEC mode.

Related Commands

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

wrr-queue bandwidth

Use the **wrr-queue bandwidth** global configuration command to assign weighted round-robin (WRR) weights to the four class of service (CoS) priority queues. Use the **no** form to disable the WRR scheduler and enable the strict priority scheduler.

wrr-queue bandwidth *weight1...weight4*

no wrr-queue bandwidth

Syntax Description

weight1...weight4	The ratio of weight1, weight2, weight3, and weight4 determines the weights of the WRR scheduler. Ranges are 1 to 255.

Defaults

WRR is disabled. The strict priority is the default scheduler.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

WRR allows bandwidth sharing at the egress port. This command defines the bandwidths for egress WRR through scheduling weights.

Examples

The following example shows how to assign WRR weights of 10, 20, 30, and 40 to the CoS priority queues 1, 2, 3 and 4:

```
Switch(config)# wrr-queue bandwidth 10 20 30 40
```

The following example shows how to disable the WRR scheduler and enable the strict priority scheduler.

```
Switch(config)# no wrr-queue bandwidth
```

You can verify the previous command by entering the **show wrr-queue bandwidth** command in the privileged EXEC mode.

Related Commands

Command	Description
wrr-queue cos-map	Assigns CoS values to the CoS priority queues.
show wrr-queue bandwidth	Displays the WRR bandwidth allocation for the four CoS priority queues.
show wrr-queue cos-map	Displays the mapping of the CoS to the CoS priority queues.

wrr-queue cos-map

Use the **wrr-queue cos-map** global configuration command to assign class of service (CoS) values to the CoS priority queues. Use the **no** form set the CoS map to default setting.

wrr-queue cos-map *quid cos1...cos 4*

no wrr-queue cos-map

Syntax Description

quid	The queue id of the CoS priority queue. Ranges are 1 to 4 where 1 is the lowest CoS priority queue.
cos1...cosn	The CoS values that are mapped to the queue id.

Defaults

The default CoS values are as follows:

CoS Value	CoS Priority Queues
0, 1	1
2, 3	2
4, 5	3
6, 7	4

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)WC(1)	This command was first introduced.

Usage Guidelines

CoS assigned at the ingress port is used to select a CoS priority at the egress port.

Examples

The following example shows how to map CoS values 0, 1 and 2 to CoS priority queue 1, value 3 to CoS priority queue 2, values 4 and 5 to CoS priority 3, and values 6 and 7 to CoS priority queue 4:

```
Switch(config)# wrr-queue cos-map 1 0 1 2
Switch(config)# wrr-queue cos-map 2 3
Switch(config)# wrr-queue cos-map 3 4 5
Switch(config)# wrr-queue cos-map 4 6 7
```

The following example shows how to map CoS values 0, 1, 2 and 3 to CoS priority queue 2.

```
Switch(config)# wrr-queue cos-map 2 0 1 2 3
```

If all other priority queues use their default setting, the new mapping is as follows:

CoS Value	CoS Priority Queue
Not applied	1
0, 1, 2, 3	2
4, 5	3
6, 7	4

Note CoS priority queue 1 is no longer used because no CoS value is assigned to the queue.

You can set the CoS values to the default values by entering the **no wrr-queue bandwidth** in the global configuration mode.

You can verify the previous command by entering the **show wrr-queue cos-map** command in the privileged EXEC mode.

Related Commands

Command	Description
wrr-queue bandwidth	Assigns weighted round-robin (WRR) weights to the four CoS priority queues.
show wrr-queue bandwidth	Displays the WRR bandwidth allocation for the four CoS priority queues.
show wrr-queue cos-map	Displays the mapping of the CoS to the priority queues.