

service password-recovery

Use the **service password-recovery** global configuration command to enable the password-recovery mechanism (the default). This mechanism allows an end user with physical access to the switch to hold down the **Mode** button and interrupt the boot process while the switch is powering up and to assign a new password. Use the **no** form of this command to disable part of the password-recovery functionality. When the password-recovery mechanism is disabled, interrupting the boot process is allowed only if the user agrees to set the system back to the default configuration.

service password-recovery

no service password-recovery

This command is available only on Catalyst 2950 Long-Reach Ethernet (LRE) switches.

Syntax Description This command has no arguments or keywords.

Defaults The password-recovery mechanism is enabled.

Command Modes Global configuration

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

Usage Guidelines This command is valid only on Catalyst 2950 LRE switches.

As a system administrator, you can use the **no service password-recovery** command to disable some of the functionality of the password recovery feature by allowing an end user to reset a password only by agreeing to return to the default configuration.

To use the password-recovery procedure, a user with physical access to the switch holds down the **Mode** button while the unit powers up and for a second or two after the LED above port 1X goes off. When the button is released, the system continues with initialization. If the password-recovery mechanism is disabled, this message appears:

```
The password-recovery mechanism has been triggered, but
is currently disabled. Access to the boot loader prompt
through the password-recovery mechanism is disallowed at
this point. However, if you agree to let the system be
reset back to the default system configuration, access
to the boot loader prompt can still be allowed.
```

```
Would you like to reset the system back to the default configuration (y/n)?
```

If the user chooses not to reset the system back to the default configuration, the normal boot process continues, as if the **Mode** button had not been pressed. If you choose to reset the system back to the default configuration, the configuration file in flash memory is deleted and the VLAN database file, *flash:vlan.dat* (if present) is deleted.

**Note**

If you use the **no service password-recovery** command to control end user access to passwords, we recommend that you save a copy of the config file in a location away from the switch in case the end user uses the password recovery procedure and sets the system back to default values. Do not keep a backup copy of the config file on the switch.

If the switch is operating in VTP transparent mode, we recommend that you also save a copy of the vlan.dat file in a location away from the switch.

You can verify if password recovery is enabled or disabled by entering the **show version** privileged EXEC command.

Examples

This example shows how to disable password recovery on a switch so that a user can only reset a password by agreeing to return to the default configuration.

```
Switch(config)# no service-password recovery
Switch(config)# exit
```

Related Commands

Command	Description
show version	Displays version information for the hardware and firmware.

service-policy

Use the **service-policy** interface configuration command to apply a policy map defined by the **policy-map** command to the input of a particular interface. Use the **no** form of this command to remove the policy map and interface association.

service-policy input *policy-map-name*

no service-policy input *policy-map-name*

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

Syntax Description	<i>policy-map-name</i>	Apply the specified policy map to the input of an interface.
---------------------------	------------------------	--

Defaults	No policy maps are attached to the interface.
-----------------	---

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

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

Usage Guidelines	Only one policy map per ingress interface is supported. Service policy maps cannot be defined on egress interfaces.
-------------------------	--



Note

For more information about configuring access control lists (ACLs), refer to the “Configuring Network Security with ACLs” chapter in the software configuration guide for this release.

Examples	This example shows how to apply <i>plcmap1</i> to an ingress interface:
-----------------	---

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# service-policy input plcmap1
```

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

Related Commands	Command	Description
	policy-map	Creates or modifies a policy map that can be attached to multiple interfaces to specify a service policy.
	show policy-map	Displays quality of service (QoS) policy maps.

set

Use the **set** policy-map class configuration command to classify IP traffic by setting a Differentiated Services Code Point (DSCP) value. Use the **no** form of this command to remove traffic classification.

set ip dscp *new-dscp*

no set ip dscp *new-dscp*

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

Syntax Description	<i>new-dscp</i>	New DSCP value assigned to the classified traffic. The supported DSCP values are 0, 8, 10, 16, 18, 24, 26, 32, 34, 40, 46, 48, and 56.
---------------------------	-----------------	---

Defaults	No traffic classification is defined.
-----------------	---------------------------------------

Command Modes	Policy-map class configuration
----------------------	--------------------------------

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

Usage Guidelines	The set command can be used in a policy with a match command. The set command sets the DSCP value for in-profile packets.
-------------------------	---



Note

This command does not support IP precedence.

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



Note

For more information about configuring access control lists (ACLs), refer to the “Configuring Network Security with ACLs” chapter in the software configuration guide for this release.

Examples

This example shows how to assign a DSCP value of 10 to all FTP traffic without any policers:

```
Switch(config)# policy-map policy_ftp  
Switch(config-pmap)# class ftp_class  
Switch(config-pmap-c)# set ip dscp 10  
Switch(config-pmap)# exit
```

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

Related Commands

Command	Description
police	Defines a policer for classified traffic.
policy-map	Creates or modifies a policy map that can be attached to multiple interfaces to specify a service policy.
show policy-map	Displays quality of service (QoS) policy maps.

setup express

Use the **setup express** global configuration command to enable Express Setup mode on the switch. This is the default setting. Use the **no** form of this command to disable Express Setup mode.

setup express

no setup express

This command is available only on Catalyst 2950 switches.

Syntax Description This command has no arguments or keywords.

Defaults Express Setup is enabled.

Command Modes Global configuration

Command History	Release	Modification
	12.1(14)EA1	This command was introduced.

Usage Guidelines When Express Setup is enabled on a new (unconfigured) switch, pressing the Mode button for 2 seconds activates Express Setup. You can access the switch through an Ethernet port by using the IP address 10.0.0.1 and then can configure the switch with the web-based Express Setup program or the command-line interface (CLI)-based setup program.

When you press the Mode button for 2 seconds on a configured switch, the mode LEDs start blinking. If you press the Mode button for a total of 10 seconds, the switch configuration is deleted, and the switch reboots. The switch can then be configured like a new switch, either through the web-based Express Setup program or the CLI-based setup program.



Note

As soon as you make any change to the switch configuration (including entering *no* at the beginning of the CLI-based setup program), configuration by Express Setup is no longer available. You can only run Express Setup again by pressing the Mode button for 10 seconds. This deletes the switch configuration and reboots the switch.

If Express Setup is active on the switch, entering the **write memory** or **copy running-configuration startup-configuration** privileged EXEC commands deactivates Express Setup. The IP address 10.0.0.1 is no longer valid on the switch, and your connection using this IP address ends.

The primary purpose of the **no setup express** command is to prevent someone from deleting the switch configuration by pressing the Mode button for 10 seconds.

Examples

This example shows how to enable Express Setup mode:

```
Switch(config)# setup express
```

You can verify that Express Setup mode is enabled by pressing the Mode button:

- On an unconfigured switch, the mode LEDs begin blinking green after 2 seconds.
- On a configured switch, the mode LEDs turn solid green after a total of 10 seconds.

**Caution**

If you *hold* the Mode button down for a total of 10 seconds, the configuration is deleted, and the switch reboots.

This example shows how to disable Express Setup mode:

```
Switch(config)# no setup express
```

You can verify that Express Setup mode is disabled by pressing the Mode button. The mode LEDs only turn solid green *or* begin blinking green if Express Setup mode is enabled on the switch.

Related Commands

Command	Description
clear setup express	Exits Express Setup mode without saving the configuration.
show setup express	Displays if Express Setup mode is active on the switch.

show access-lists

Use the **show access-lists** privileged EXEC command to display access control lists (ACLs) configured on the switch.

```
show access-lists [name | number] [ | { begin | exclude | include } expression]
```

Syntax Description	
<i>name</i>	(Optional) Name of the ACL.
<i>number</i>	(Optional) ACL number. The range is from 1 to 2699.
 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes	
	Privileged EXEC

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

Usage Guidelines	
	Expressions are case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> do not appear, but the lines that contain <i>Output</i> appear.

Examples	
	This is an example of output from the show access-lists command:

```
Switch# show access-lists
Standard IP access list testingacl
  permit 10.10.10.2
Standard IP access list wizard_1-1-1-2
  permit 1.1.1.2
Extended IP access list 103
  permit tcp any any eq www
Extended IP access list CMP-NAT-ACL
  Dynamic Cluster-HSRP deny ip any any
  Dynamic Cluster-NAT permit ip any any
  permit ip host 10.123.222.192 any
  permit ip host 10.228.215.0 any
  permit ip host 10.245.137.0 any
  permit ip host 10.245.155.128 any
  permit ip host 10.221.111.64 any
  permit ip host 10.216.25.128 any
  permit ip host 10.186.122.64 any
  permit ip host 10.169.110.128 any
  permit ip host 10.146.106.192 any
```

Related Commands	Command	Description
	access-list (IP extended)	Configures an extended IP ACL on the switch.
	access-list (IP standard)	Configures a standard IP ACL on the switch.
	ip access-list	Configures an IP ACL on the switch.
	mac access-list extended	Creates an ACL based on MAC addresses.
	show ip access-lists	Displays the IP ACLs configured on a switch.

show auto qos

Use the **show auto qos** user EXEC command to display the automatic quality of service (auto-QoS) configuration that is applied.

```
show auto qos [interface interface-id] [ | { begin | exclude | include } expression]
```

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

Syntax Description

interface <i>interface-id</i>	(Optional) Display auto-QoS information for the specified interface or for all interfaces. Valid interfaces include physical ports.
begin	(Optional) Display begins with the line that matches the <i>expression</i> .
exclude	(Optional) Display excludes lines that match the <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(12c)EA1	This command was first introduced.

Usage Guidelines

The **show auto qos [interface *interface-id*]** command displays the auto-QoS configuration; it does not display any user changes to the configuration that might be in effect.

To display information about the QoS configuration that might be affected by auto-QoS, use one of these commands:

- **show mls qos**
- **show mls qos map cos-dscp**
- **show mls qos interface**
- **show running-config**
- **show wrr-queue bandwidth**
- **show wrr-queue cos-map**

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

Examples

This is an example of output from the **show auto qos** command when auto-QoS is enabled:

```
Switch> show auto qos
Initial configuration applied by AutoQoS:
wrr-queue bandwidth 20 1 80 0
no wrr-queue cos-map
wrr-queue cos 1 0 1 2 4
wrr-queue cos 3 3 6 7
wrr-queue cos 4 5
mls qos map cos-dscp 0 8 16 26 32 46 48 56
!
interface FastEthernet0/3
 mls qos trust device cisco-phone
 mls qos trust cos
```

This is an example of output from the **show auto qos interface** command when the **auto qos voip cisco-phone** interface configuration command is entered:

```
Switch> show auto qos interface
Initial configuration applied by AutoQoS:
!
interface FastEthernet0/3
 mls qos trust device cisco-phone
 mls qos trust cos
```

This is an example of output from the **show auto qos interface fastethernet0/3** command when the **auto qos voip cisco-phone** interface configuration command is entered:

```
Switch> show auto qos interface fastethernet0/3
Initial configuration applied by AutoQoS:
!
interface FastEthernet0/3
 mls qos trust device cisco-phone
 mls qos trust cos
```

This is an example of output from the **show auto qos** command when auto-QoS is disabled:

```
Switch> show auto qos
AutoQoS is disabled
```

Related Commands

Command	Description
auto qos voip	Automatically configures QoS for VoIP within a QoS domain.

show boot

Use the **show boot** privileged EXEC command to display the settings of the boot environment variables.

```
show boot [ | {begin | exclude | include} expression]
```

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

Command Modes Privileged EXEC

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

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



Note

Only the software can read and write a copy of the private configuration file. You cannot read, write, delete, or display a copy of this file.

Examples This is an example of output from the **show boot** command. [Table 2-8](#) describes each field in the output.

```
Switch# show boot
BOOT path-list:      flash:boot
Config file:        flash:config.text
Private Config file: flash:private-config.text
Enable Break:       no
Manual Boot:        yes
HELPER path-list:
NVRAM/Config file
    buffer size:    32768
```

Table 2-8 show boot Field Descriptions

Field	Description
BOOT path-list	<p>Displays a semicolon-separated list of executable files to load and to execute when automatically booting.</p> <p>If the BOOT environment variable is not set, the system attempts to load and execute the first executable image it can find by using a recursive, depth-first search through the Flash file system. In a depth-first search of a directory, each encountered subdirectory is completely searched before continuing the search in the original directory.</p> <p>If the BOOT variable is set but the specified images cannot be loaded, the system attempts to boot the first bootable file that it can find in the Flash file system.</p>
Config file	Displays the filename that the software uses to read and write a nonvolatile copy of the system configuration.
Private Config file	Displays the filename that the software uses to read and write a nonvolatile copy of the private configuration.
Enable Break	Displays whether a break during booting is enabled or disabled. If it is set to <i>yes</i> , <i>on</i> , or <i>1</i> , you can interrupt the automatic boot process by pressing the Break key on the console after the Flash file system is initialized.
Manual Boot	Displays whether the switch automatically or manually boots. If it is set to <i>no</i> or <i>0</i> , the boot loader attempts to automatically boot the system. If it is set to anything else, you must manually boot the switch from the boot loader mode.
Helper path-list	Displays a semicolon-separated list of loadable files to dynamically load during the boot loader initialization. Helper files extend or patch the functionality of the boot loader.
NVRAM/Config file buffer size	Displays the buffer size that the software uses to hold a copy of the configuration file in memory. The configuration file cannot be larger than the buffer size allocation.

Related Commands

Command	Description
boot private-config-file	Specifies the filename that the software uses to read and write a nonvolatile copy of the private configuration.

show class-map

Use the **show class-map** user EXEC command to display quality of service (QoS) class maps, which define the match criteria to classify traffic.

```
show class-map [class-map-name] [ | { begin | exclude | include } expression]
```

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

Syntax Description

<i>class-map-name</i>	(Optional) Display the contents of the specified class map.
begin	(Optional) Display begins with the line that matches the <i>expression</i> .
exclude	(Optional) Display excludes lines that match the <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

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

Usage Guidelines

If you do not specify a *class-map-name*, all class maps appear.

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

Examples

This is an example of output from the **show class-map test** command:

```
Switch> show class-map test
Class Map match-all test (id 2)
  Match access-group name testingacl
```

This is an example of output from the **show class-map** command:

```
Switch> show class-map
Class Map match-all wizard_1-1-1-2 (id 3)
  Match access-group name videowizard_1-1-1-2

Class Map match-all test (id 2)
  Match access-group name testingacl

Class Map match-any class-default (id 0)
  Match any

Class Map match-all class1 (id 5)
  Match access-group 103

Class Map match-all classtest (id 4)
  Description: This is a test.
  Match access-group name testingacl
```

Related Commands	Command	Description
	class-map	Creates a class map to be used for matching packets to the class whose name you specify.
	match	Defines the match criteria to classify traffic.

show cluster

Use the **show cluster** privileged EXEC command to display the cluster status and a summary of the cluster to which the switch belongs. This command can be entered on command and member switches.

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

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

Command Modes Privileged EXEC

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

Usage Guidelines

On a member switch, this command displays the identity of the command switch, the switch member number, and the state of its connectivity with the command switch.

On a command switch, this command displays the cluster name and the total number of members. It also shows the cluster status and time since the status changed. If redundancy is enabled, it displays the primary and secondary command-switch information.

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

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

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

```
Switch# show cluster
Command switch for cluster "Switch1"
  Total number of members:      7
  Status:                      1 members are unreachable
  Time since last status change: 0 days, 0 hours, 2 minutes
  Redundancy:                  Enabled
    Standby command switch: Member 1
    Standby Group:             Switch1_standby
    Standby Group Number:     110
  Heartbeat interval:          8
  Heartbeat hold-time:         80
  Extended discovery hop count: 3
```

This is an example of output when this command is entered on a member switch:

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

This is an example of output when this command is entered on a member switch that is configured as the standby command switch:

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

This is an example of output when this command is entered on the command switch that has lost connectivity from member 1:

```
Switch# show cluster
Command switch for cluster "Switch1"
  Total number of members: 7
  Status:                  1 members are unreachable
  Time since last status change: 0 days, 0 hours, 5 minutes
  Redundancy:              Disabled
  Heartbeat interval:      8
  Heartbeat hold-time:     80
  Extended discovery hop count: 3
```

This is an example of output when this command is entered on a member switch that has lost connectivity with the command switch:

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

Related Commands

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

show cluster candidates

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

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

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

Command Modes Privileged EXEC

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

Usage Guidelines

You should only enter this command on a command switch.

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

The SN in the output means *switch member number*. If *E* is in the SN column, it means that the switch is discovered through extended discovery. If *E* does not appear in the SN column, it means that the *switch member number* is the upstream neighbor of the candidate switch. The hop count is the number of devices the candidate is from the command switch.

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

Examples

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

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

This is an example of output from the **show cluster candidates** command that uses the MAC address of a member switch directly connected to the command switch:

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

This is an example of output from the **show cluster candidates** command that uses the MAC address of a member switch three hops from the cluster edge:

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

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

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

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

show cluster members

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

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

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

Command Modes Privileged EXEC

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

Usage Guidelines You should only enter this command on a command switch.

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

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

Examples This is an example of output from the **show cluster members** command. The SN in the display means *switch number*.

```
Switch# show cluster members
SN MAC Address      Name          PortIf FEC Hops  |---Upstream---|
0  0002.4b29.2e00 StLouis1      0
1  0030.946c.d740 tal-switch-1 Fa0/13      1  0 Gi0/1      Up (Cmdr)
2  0002.b922.7180 nms-2820     10      0  2  1 Fa0/18     Up
3  0002.4b29.4400 SanJuan2     Gi0/1      2  1 Fa0/11     Up
4  0002.4b28.c480 GenieTest    Gi0/2      2  1 Fa0/9      Up
```

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

```
Switch# show cluster members 3
Device 'SanJuan2' with member number 3
Device type:          cisco WS-C3550-12T
MAC address:          0002.4b29.4400
Upstream MAC address: 0030.946c.d740 (Cluster member 1)
Local port:           Gi0/1   FEC number:
Upstream port:        Fa0/11  FEC Number:
Hops from command device: 2
```

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

```
Switch# show cluster members detail
Device 'StLouis1' with member number 0 (Command Switch)
Device type:          cisco WS-C3550-12T
MAC address:          0002.4b29.2e00
Upstream MAC address:
Local port:           FEC number:
Upstream port:        FEC Number:
Hops from command device: 0
Device 'tal-switch-14' with member number 1
Device type:          cisco WS-C3548-XL
MAC address:          0030.946c.d740
Upstream MAC address: 0002.4b29.2e00 (Cluster member 0)
Local port:           Fa0/13  FEC number:
Upstream port:        Gi0/1   FEC Number:
Hops from command device: 1
Device 'nms-2820' with member number 2
Device type:          cisco 2820
MAC address:          0002.b922.7180
Upstream MAC address: 0030.946c.d740 (Cluster member 1)
Local port:           10      FEC number: 0
Upstream port:        Fa0/18  FEC Number:
Hops from command device: 2
Device 'SanJuan2' with member number 3
Device type:          cisco WS-C3550-12T
MAC address:          0002.4b29.4400
Upstream MAC address: 0030.946c.d740 (Cluster member 1)
Local port:           Gi0/1   FEC number:
Upstream port:        Fa0/11  FEC Number:
Hops from command device: 2
Device 'Test' with member number 4
Device type:          cisco SeaHorse
MAC address:          0002.4b28.c480
Upstream MAC address: 0030.946c.d740 (Cluster member 1)
Local port:           Gi0/2   FEC number:
Upstream port:        Fa0/9   FEC Number:
Hops from command device: 2
Device 'Palpatine' with member number 5
Device type:          cisco WS-C2924M-XL
MAC address:          00b0.6404.f8c0
Upstream MAC address: 0002.4b29.2e00 (Cluster member 0)
Local port:           Gi2/1   FEC number:
Upstream port:        Gi0/7   FEC Number:
Hops from command device: 1
```

Related Commands

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

show controllers ethernet-controller

Use the **show controllers ethernet-controller** privileged EXEC command without keywords to display per-interface transmit and receive statistics read from the hardware. Use this command with keywords to display the interface internal registers or to display the statistics read from Long-Reach Ethernet (LRE) and customer premises equipment (CPE) ports.

```
show controllers ethernet-controller interface-id [asic | cpe [port port-id] | phy 32] [ | {begin | exclude | include} expression]
```

Syntax Description

<i>interface-id</i>	ID of the switch interface.
asic	(Optional) Display the state of the internal registers on the forwarding application-specific integrated circuit (ASIC) for the interface. This keyword is available only on non-LRE switches.
cpe	(Optional) Display statistics from the LRE and Fast Ethernet ports on connected devices. This keyword is available only on LRE switches.
port <i>port-id</i>	(Optional) Display the Ethernet statistics of the designated CPE Ethernet port. Valid values vary from 1 to 4, depending on the CPE device. This keyword is available only on LRE switches.
phy 32	(Optional) Display the status of the internal registers on the switch physical layer device (PHY) for the interface. This keyword is available only on non-LRE switches.
begin	(Optional) Display begins with the line that matches the <i>expression</i> .
exclude	(Optional) Display excludes lines that match the <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC (only supported with the *interface-id* keywords in user EXEC mode)

Command History

Release	Modification
12.1(6)EA2	This command was introduced.
12.1(11)YJ	The cpe and port <i>port-id</i> keywords were added.
12.1(19)EA1	The phy keyword was changed to phy 32 .

Usage Guidelines

Use this command without keywords to display traffic statistics, basically the RMON statistics for the interface. If this command is entered on a Catalyst 2950 LRE switch, the command output also shows the statistics for the LRE switch interfaces.

When you enter the **asic** or **phy 32** keyword, the displayed information is primarily useful for Cisco technical support representatives troubleshooting the switch.

When you enter the **cpe** keyword, the displayed information shows the traffic statistics for the connected CPE devices. The CPE Ethernet link on an LRE switch port is the connection between the Cisco LRE CPE and the remote Ethernet device (such as a PC) connected to it. It is not the link between the LRE switch port and the LRE CPE device.

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

Examples

This is an example of output from the **show controllers ethernet-controller** command on a non-LRE switch. For this example, [Table 2-9](#) describes the *Transmit* fields, [Table 2-10](#) describes the *Receive* fields, and [Table 2-11](#) describes the *Transmit and Receive* fields.

```
Switch# show controllers ethernet-controller fastethernet0/2
Transmit
19555003 Bytes
222479 Frames
161490 Multicast frames
  256 Broadcast frames
  0 Pause frames
  0 Single defer frames
  0 Multiple defer frames
  0 1 collision frames
  0 2-15 collisions
  0 Late collisions
  0 Excessive collisions
  0 Total collisions
  0 Control frames
  0 VLAN discard frames
  0 Too old frames
  0 Tagged frames
  0 Aborted Tx frames

Receive
23485398 Bytes
313530 Frames
0 FCS errors
313467 Multicast frames
  1 Broadcast frames
  0 Control frames
  0 Pause frames
  0 Unknown opcode frames
  0 Alignment errors
  0 Length out of range
  0 Symbol error frames
  0 False carrier errors
  0 Valid frames, too small
  0 Valid frames, too large
  0 Invalid frames, too small
  0 Invalid frames, too large
  0 Discarded frames

Transmit and Receive
384595 Minimum size frames
131178 65 to 127 byte frames
  6 128 to 255 byte frames
20229 256 to 511 byte frames
  1 512 to 1023 byte frames
  0 1024 to 1518 byte frames
  0 1519 to 1522 byte frames
```

Table 2-9 Transmit Field Descriptions

Field	Description
Bytes	The total number of bytes sent on an interface.
Frames	The total number of frames sent on an interface.
Multicast frames	The total number of frames sent to multicast addresses.
Broadcast frames	The total number of frames sent to broadcast addresses.
Pause frames	The number of pause frames sent on an interface.
Single defer frames	The number of frames for which the first transmission attempt on an interface is not successful. This value excludes frames in collisions.
Multiple defer frames	The number of frames that are not sent after the time exceeds 2*maximum-packet time.
1 collision frames	The number of frames that are successfully sent on an interface after one collision occurs.

Table 2-9 Transmit Field Descriptions (continued)

Field	Description
2-15 collisions	The number of frames that are successfully sent on an interface after more than one collision occurs.
Late collisions	After a frame is sent, the number of times that a collision is detected on an interface later than 512 bit times.
Excessive collisions	The number of frames that could not be sent on an interface because more than 16 collisions occurred.
Total collisions	The total number of collisions on an interface.
Control frames	The number of control frames sent on an interface, such as STP ¹ BPDUs ² .
VLAN discard frames	The number of frames dropped on an interface because the CFI ³ bit is set.
Too old frames	The number of frames dropped on the egress port because the packet aged out.
Tagged frames	The number of tagged frames sent on an interface.
Aborted Tx frames	The number of aborted transmission attempts on the interface.

1. STP = Spanning Tree Protocol
2. BPDU = bridge protocol data unit
3. CFI = Canonical Format Indicator

Table 2-10 Receive Field Descriptions

Field	Description
Bytes	The total amount of memory (in bytes) used by frames received on an interface, including the FCS ¹ value and the incorrectly formed frames. This value excludes the frame header bits.
Frames	The total number of frames received on an interface, including multicast frames, broadcast frames, and incorrectly formed frames.
FCS errors	The total number of frames received on an interface that have a valid length (in bytes) but do not have the correct FCS values.
Multicast frames	The total number of frames successfully received on the interface that are directed to multicast addresses.
Broadcast frames	The total number of frames successfully received on an interface that are directed to broadcast addresses.
Control frames	The number of control frames received on an interface, such as STP BPDUs.
Pause frames	The number of pause frames received on an interface.
Unknown opcode frames	The number of frames received with an unknown operation code.
Alignment errors	The total number of frames received on an interface that have alignment errors.
Length out of range	The number of frames received on an interface that have an out-of-range length.
Symbol error frames	The number of frames received on an interface that have symbol errors.
False carrier errors	The number of occurrences in which the interface detects a false carrier when frames are not sent or received.
Valid frames, too small	The number of frames received on an interface that are smaller than 64 bytes (or 68 bytes for VLAN-tagged frames) and have valid FCS values. The frame size includes the FCS bits but excludes the frame header bits.

Table 2-10 Receive Field Descriptions (continued)

Field	Description
Valid frames, too large	The number of frames received on an interface that are larger than the maximum allowed frame size.
Invalid frames, too small	The number of frames received that are smaller than 64 bytes (including the FCS bits and excluding the frame header) and that have either an FCS error or an alignment error.
Invalid frames, too large	The number of frames received that were larger than maximum allowed MTU ² size (including the FCS bits and excluding the frame header) and that have either an FCS error or an alignment error. Note For information about the maximum allowed MTU size on the Catalyst 2950 switches, see the system mtu global configuration command.
Discarded frames	The number of frames discarded because of lack of receive buffer memory.

1. FCS = frame check sequence

2. MTU = maximum transmission unit

Table 2-11 Transmit and Receive Field Descriptions

Field	Description
Minimum size frames	The total number of frames that are the minimum frame size.
65 to 127 byte frames	The total number of frames that are from 65 to 127 bytes.
128 to 255 byte frames	The total number of frames that are from 128 to 255 bytes.
256 to 511 byte frames	The total number of frames that are from 256 to 511 bytes.
512 to 1023 byte frames	The total number of frames that are from 512 to 1023 bytes.
1024 to 1518 byte frames	The total number of frames that are from 1024 to 1518 bytes.
1519 to 1522 byte frames	The total number of frames that are from 1519 to 1522 bytes.

This is an example of output from the **show controllers ethernet-controller** command on an LRE switch. For this example, [Table 2-9](#) describes the *Transmit* fields, [Table 2-10](#) describes the *Receive* fields, [Table 2-11](#) describes the *Transmit and Receive* fields, and [Table 2-12](#) describes the *LRE Enet Stats on Switch* fields.

```
Switch# show controllers ethernet-controller longreachethernet0/4
Transmit                                Receive
  64 Bytes                               64 Bytes
    1 Frames                             1 Frames
    0 Multicast frames                   0 FCS errors
    0 Broadcast frames                   0 Multicast frames
    0 Pause frames                       0 Broadcast frames
    0 Single defer frames                 0 Control frames
    0 Multiple defer frames               0 Pause frames
    0 1 collision frames                  0 Unknown opcode frames
    0 2-15 collisions                    0 Alignment errors
    0 Late collisions                    0 Length out of range
    0 Excessive collisions                0 Symbol error frames
    0 Total collisions                    0 False carrier errors
    0 Control frames                      0 Valid frames, too small
    0 VLAN discard frames                 0 Valid frames, too large
    0 Too old frames                      0 Invalid frames, too small
```

```
show controllers ethernet-controller
```

```

0 Tagged frames
0 Aborted Tx frames

0 Invalid frames, too large
0 Discarded frames

Transmit and Receive
2 Minimum size frames
0 65 to 127 byte frames
0 128 to 255 byte frames
0 256 to 511 byte frames
0 512 to 1023 byte frames
0 1024 to 1518 byte frames
0 1519 to 1522 byte frames

```

```
LRE Enet Stats on Switch:
```

```

Transmit
0 Bytes
0 Frames

0 Pause frames
0 1 collision frames
0 Multiple collisions
0 Late collisions
0 Excessive collisions
0 Deferred frames
0 Carrier sense errors

Receive
0 Bytes
0 Frames
0 Broadcast frames
0 Pause frames
0 Alignment errors
0 Collisions and Runts
0 Oversize frames
0 FCS errors

```

Table 2-12 LRE Enet Stats on Switch Field Descriptions

Field	Description
Transmit	
Bytes	The total number of bytes sent on an interface.
Frames	The total number of frames sent on an interface.
Pause frames	The number of pause frames sent on an interface.
1 collision frames	The number of frames that are successfully sent on an interface after one collision occurs.
Multiple collisions	The number of frames that are sent after more than one collision occurs.
Late collisions	After a frame is sent, the number of times that a collision is detected on an interface later than 512 bit times.
Excessive collisions	The number of frames that could not be sent on an interface because more than 16 collisions occurs.
Deferred frames	The number of frames that are not sent on an interface.
Carrier sense errors	The number of frames with carrier sense errors.
Receive	
Bytes	The total amount of memory (in bytes) used by frames received on an interface, including the FCS value and the incorrectly formed frames. This value excludes the frame header bits.
Frames	The total number of frames received on an interface, including broadcast frames and incorrectly formed frames.
Broadcast frames	The total number of frames successfully received on an interface that are directed to broadcast addresses.
Pause frames	The number of pause frames received on an interface.
Alignment errors	The total number of frames received on an interface that have alignment errors.

Table 2-12 LRE Enet Stats on Switch Field Descriptions (continued)

Field	Description
Collisions and Runts	The number of frames that could not be received on an interface because of collisions because the frame length (in bytes) is too small.
Receive	
Oversize frames	The total number of frames that are the larger than the maximum allowed frame size.
FCS errors	The total number of frames received on an interface that have a valid length (in bytes) but do not have the correct FCS values.

This is an example of output from the **show controllers ethernet-controller longreachethernet0/4 cpe** command. It shows the statistics of the LRE chipset and the all the LRE ports on the CPE. For this example, [Table 2-13](#) describes the *LRE Enet Stats on CPE* fields, and [Table 2-14](#) describes the *CPE Fast Ethernet Port* fields.

```
Switch# show controllers ethernet-controller longreachethernet0/4 cpe
LRE Enet Stats on CPE:
```

```

Transmit                                Receive
  0 Bytes                                0 Bytes
  0 Frames                                0 Frames
                                           0 Broadcast frames
  0 Pause frames                          0 Pause frames
  0 1 collision frames                     0 Alignment errors
  0 Multiple collisions                    0 Collisions and Runts
  0 Late collisions                        0 Oversize frames
  0 Excessive collisions                   0 FCS errors
  0 Deferred frames
  0 Carrier sense errors
```

```
CPE Fast Ethernet Port: 1
```

```

Transmit                                Receive
  0 Bytes                                0 Bytes
                                           0 Good Bytes
  0 Unicast Frames                         0 Unicast Frames
  0 Multicast Frames                       0 Multicast Frames
  0 Broadcast Frames                       0 Broadcast Frames
  0 Dropped Frames                         0 Dropped Frames
  0 Pause Frames                           0 Pause Frames
  0 Collision Frames                       0 Alignment Errors
  0 One Collision Frames                   0 Fragments
  0 Multiple Collisions                    0 Undersize Frames
  0 Late Collisions                        0 Oversize Frames
  0 Excess Collisions                      0 FCS errors
  0 Frame Discard                          0 Excess Size Discards
  0 Deferred Frames                        0 Jabbers
                                           0 Source Address Chang
                                           0 Symbol Errors
  0 64 Byte Frames                         0 64 Byte Frames
  0 65-127 Byte Frames                     0 65-127 Byte Frames
  0 128-255 Byte Frames                     0 128-255 Byte Frames
  0 256-511 Byte Frames                     0 256-511 Byte Frames
  0 512-1023 Byte Frames                     0 512-1023 Byte Frames
  0 1024-1522 Byte Frame                     0 1024-1522 Byte Frame
```

This is an example of output from the **show controllers ethernet-controller longreachethernet0/4 cpe port 1** command. It shows the statistics for a specific LRE port on the CPE. For this example, [Table 2-14](#) describes the *CPE Fast Ethernet Port* fields.

```
Switch# show controllers ethernet-controller longreachethernet0/4 cpe port 1
CPE Fast Ethernet Port: 1
```

```
Transmit                               Receive
42308326 Bytes                          8264733 Bytes
                                         8264733 Good Bytes
      193 Unicast Frames                  68745 Unicast Frames
    511408 Multicast Frames              11469 Multicast Frames
      1886 Broadcast Frames              0 Broadcast Frames
        0 Dropped Frames                 0 Dropped Frames
        0 Pause Frames                   0 Pause Frames
        0 Collision Frames                0 Alignment Errors
        0 One Collision Frames            0 Fragments
        0 Multiple Collisions             0 Undersize Frames
        0 Late Collisions                 0 Oversize Frames
        0 Excess Collisions               0 FCS errors
        0 Frame Discard                   0 Excess Size Discards
        2 Deferred Frames                 0 Jabbers
                                         1 Source Address Change
                                         0 Symbol Errors

                                         68745 64 Byte Frames
                                         0 65-127 Byte Frames
                                         0 128-255 Byte Frames
    11469 256-511 Byte Frames
                                         0 512-1023 Byte Frames
                                         0 1024-1522 Byte Frame
```

Table 2-13 LRE Enet Stats on CPE Field Descriptions for LRE and CPE Interfaces

Field	Description
Transmit	
Bytes	The total number of bytes sent on an interface.
Frames	The total number of frames sent on an interface.
Pause frames	The number of pause frames sent on an interface.
1 collision frames	The number of frames that are successfully sent on an interface after one collision occurs.
Multiple collisions	The number of frames that are sent after more than one collision occurs.
Late collisions	After a frame is sent, the number of times that a collision is detected on an interface later than 512 bit times.
Excessive collisions	The number of frames that could not be sent on an interface because more than 16 collisions occurs.
Deferred frames	The number of frames for which the first transmission attempt on an interface is not successful. This value excludes frames in collisions.
Carrier sense errors	The number of frames with carrier sense errors.
Receive	
Bytes	The total amount of memory (in bytes) used by frames received on an interface, including the FCS value and the incorrectly formed frames. This value excludes the frame header bits.
Frames	The total number of frames received on an interface, including multicast frames, broadcast frames, and incorrectly formed frames.

Table 2-13 LRE Enet Stats on CPE Field Descriptions for LRE and CPE Interfaces (continued)

Field	Description
Receive	
Broadcast frames	The total number of frames successfully received on an interface that are directed to broadcast addresses.
Pause frames	The number of pause frames received on an interface.
Alignment errors	The total number of frames received on an interface that have alignment errors.
Collisions and Runts	The number of frames that could not be received on an interface because of collisions because the frame length (in bytes) is too small.
Oversize frames	The total number of frames that are the larger than the maximum frame size.
FCS errors	The total number of frames received on an interface that have a valid length (in bytes) but do not have the correct FCS values.

Table 2-14 CPE Fast Ethernet Port Field Descriptions for LRE and CPE Interfaces

Field	Description
Transmit	
Bytes	The total number of bytes sent on an interface.
Unicast Frames	The total number of frames sent to unicast addresses.
Multicast Frames	The total number of frames sent to multicast addresses.
Broadcast Frames	The total number of frames sent to broadcast addresses.
Dropped Frames	The total number of frames that are not sent.
Pause Frames	The number of pause frames sent on an interface.
Collisions Frames	The total number of frames that are not sent on an interface because of collisions.
One Collision Frames	The number of frames that are successfully sent on an interface after one collision occurs.
Multiple Collisions	The number of frames that are sent after more than one collision occurs.
Late Collisions	After a frame is sent, the number of times that a collision is detected on an interface later than 512 bit times.
Excessive Collisions	The number of frames that could not be sent on an interface because more than 16 collisions occurs.
Deferred Frames	The number of frames for which the first transmission attempt on an interface is not successful. This value excludes frames in collisions.
Receive	
Bytes	The total amount of memory (in bytes) used by frames received on an interface, including the FCS value and the incorrectly formed frames. This value excludes the frame header bits.
Good Bytes	The total amount of memory (in bytes) used by frames received on an interface, including the FCS value and the correctly formed frames. This value excludes the frame header bits.
Unicast Frames	The total number of frames successfully received on an interface that are directed to unicast addresses.
Multicast Frames	The total number of frames successfully received on an interface that are directed to multicast addresses.

Table 2-14 CPE Fast Ethernet Port Field Descriptions for LRE and CPE Interfaces (continued)

Field	Description
Broadcast Frames	The total number of frames successfully received on an interface that are directed to broadcast addresses.
Dropped Frames	The total number of frames successfully received on an interface that are dropped.
Pause Frames	The number of pause frames received on an interface.
Alignment Errors	The total number of frames received on an interface that have alignment errors.
Fragments	The number of frames received on the interface that are smaller than 64 bytes and an invalid FCS value.
Undersize Frames	The total number of frames received on an interface that are smaller than 64 bytes.
Oversize Frames	The total number of frames received on an interface that are the larger than 1518 bytes.
FCS Errors	The total number of frames received on an interface that have a valid length (in bytes) but do not have the correct FCS values.
Excess Size Discards	The total number of frames received on an interface that are dropped because they are larger than 1518 bytes.
Jabbers	The total number of frames received on an interface that are larger than 1522 bytes and have either an FCS or alignment error.
Source Address Chang	The total number of frames received on an interface for which the source address changed.
Symbol Errors	The total number of frames received on an interface that have a valid length (in bytes) but have the symbol errors.
65 to 127 byte Frames	The total number of frames that are from 65 to 127 bytes.
128 to 255 byte Frames	The total number of frames that are from 128 to 255 bytes.
256 to 511 byte Frames	The total number of frames that are from 256 to 511 bytes.
512 to 1023 byte Frames	The total number of frames that are from 512 to 1023 bytes.
1024 to 1518 byte Frames	The total number of frames that are from 1024 to 1518 bytes.
1519 to 1522 byte Frames	The total number of frames that are from 1519 to 1522 bytes.

Related Commands	Command	Description
	clear controllers ethernet-controller	Deletes the Ethernet link send and receive statistics on a Fast Ethernet or an LRE switch port on an LRE switch.
	show interfaces	Displays the administrative and operational status of all interfaces or a specified interface.

show controllers lre cpe

Use the **show controllers lre cpe** privileged EXEC command to display information about the Cisco Long-Reach Ethernet (LRE) customer premises equipment (CPE) devices connected to an LRE switch.

```
show controllers lre cpe {identity | mfg | protected | version} [interface-id] [ | {begin | exclude | include} expression]
```

This command is available only on Catalyst 2950 LRE switches.

Syntax Description

identity	Display the model numbers of the LRE CPE devices connected to an LRE switch and whether or not the connected CPE devices meet the minimum requirements for management by the LRE switch.
mfg	Display the revision and serial numbers of the connected LRE CPE board, assembly, and system.
protected	Display Cisco 585 LRE CPE Ethernet ports that are configured as protected.
version	Display the version numbers of the various components (hardware, firmware, patch software, and bootloader firmware and application firmware) of the LRE CPE interfaces.
<i>interface-id</i>	(Optional) ID of the LRE switch port.
 begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

The **show controllers lre cpe identity** privileged EXEC command output shows the type of CPE device attached to each LRE interface. For all Cisco supported CPE devices, the status can be *certified*, *non-certified*, or *NA*:

- A certified status means that the CPE device meets the minimum requirements (such as having a certain CPE device patch version) for management by the LRE switch.
- A non-certified status means that the CPE device did not meet the minimum requirements. If a CPE device shows a status of non-certified or if the family is not a Cisco 585 LRE CPE, Cisco 576 LRE 997 CPE, or a Cisco 575 LRE CPE, use the **show controllers lre cpe mfg** privileged EXEC command to verify the CPE manufacturing fields.
- An NA status means that there is not a link or there is not any information about that port.

Use the **show controllers lre cpe identity** privileged EXEC command without specifying an LRE switch port to display the model numbers and status of all connected CPE devices.

Use the **show controllers lre cpe mfg** privileged EXEC command output to display fields specific to each CPE device unit. The software uses the model number field to identify the kind of CPE device attached to an LRE interface. The *System Serial Number* is also unique to each CPE device unit.

Use the **show controllers lre cpe protected** privileged EXEC command without specifying an LRE interface to display the protected port setting for all CPE ports. The Cisco 575 LRE CPE or Cisco 576 LRE 997 CPE devices display a protected field output of *NA*.

Use the **show controllers lre cpe version** privileged EXEC command without specifying an LRE switch port to display the version numbers of all CPE interfaces.

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

Examples

This is an example of output from the **show controllers lre cpe identity** command for the Cisco 575 LRE and Cisco 585 LRE CPE devices:

```
Switch# show controllers lre cpe identity

Port      CPE Model      Status      Family
-----
Lo0/1     CISCO585-LRE   CERTIFIED   CISCO585-LRE
Lo0/2     CISCO585-LRE   CERTIFIED   CISCO585-LRE
Lo0/3     CISCO585-LRE   CERTIFIED   CISCO585-LRE
Lo0/4     NA              NA          NA
Lo0/5     NA              NA          NA
Lo0/6     Cisco575-LRE   CERTIFIED   CISCO575-LRE
Lo0/7     NA              NA          NA
Lo0/8     Cisco575-LRE   CERTIFIED   CISCO575-LRE
Lo0/9     NA              NA          NA
Lo0/10    NA              NA          NA
Lo0/11    CISCO585-LRE   CERTIFIED   CISCO585-LRE
Lo0/12    CISCO585-LRE   CERTIFIED   CISCO585-LRE
Lo0/13    CISCO585-LRE   CERTIFIED   CISCO585-LRE
Lo0/14    NA              NA          NA
Lo0/15    NA              NA          NA
Lo0/16                                NON-CERTIFIED  UNSUPPORTED-MAC-MODE

<output truncated>
```

This is an example of output from the **show controllers lre cpe mfg** command that shows the manufacturing information for the Cisco 575 LRE and Cisco 585 CPE devices:

```
Switch# show controllers lre cpe mfg

CPE Manufacturer Information:

Lo0/1
Assembly Revision Number:
Model Number      :CISCO585-LRE
Model Revision Number :A0
Board Assembly Number :
Board Serial Number :
System Serial Number :ACT0613004E
```

```

Lo0/2
Assembly Revision Number:
Model Number           :CISCO585-LRE
Model Revision Number  :A0
Board Assembly Number  :
Board Serial Number    :
System Serial Number   :ACT0613005B
<output truncated>

```

This is an example of output from the **show controllers lre cpe protected** command that shows the CPE protected-port information for an LRE interface:

```

Switch# show controllers lre cpe protected longreachethernet0/9
Interface      Port      Protected
-----
Lo0/9          1         true
Lo0/9          2         true
Lo0/9          3         true
Lo0/9          4         true

```

This is an example of output from the **show controllers lre cpe protected** command that shows the CPE protected-port information for all LRE interfaces:

```

Switch# show controllers lre cpe protected
Interface      Port      Protected
-----
Lo0/1          1         NA
Lo0/2          1         NA
Lo0/3          1         NA
Lo0/4          1         NA
Lo0/5          1         NA
Lo0/6          1         NA
Lo0/7          1         NA
Lo0/8          1         false
Lo0/8          2         false

```

<output truncated>

This is an example of output from the **show controllers lre cpe version** command:

```

Switch# show controllers lre cpe version longreachethernet0/5
Interface      Hw  Sw  Patch  Boot  App
-----
Lo0/5          52  B4   51    1.02  1.02

```

Related Commands

Command	Description
cpe protected	Restricts data traffic to individual ports on Cisco 585 LRE CPE ports.
show controllers lre version	Displays the version number of the hardware, software, and patch software components of the switch LRE interface and the CPE LRE interface.

show controllers lre actual

Use the **show controllers lre actual** privileged EXEC command to display the actual values of the Long-Reach Ethernet (LRE) link on a specific LRE switch port.

```
show controllers lre interface-id actual { dsrserrs | link | rxpower | snr | txpower | usrerrs }
[ | { begin | exclude | include } expression]
```

This command is available only on Catalyst 2950 LRE switches.

Syntax Description

<i>interface-id</i>	ID of the switch LRE port.
actual	Display the LRE port current status, which might not be the same as the administratively configured settings.
dsrserrs	Display the downstream Reed-Solomon errors on the LRE port.
usrerrs	Display the upstream Reed-Solomon errors on the LRE port.
txpower	Display the remote transmit power (dBm/Hz) on the LRE port.
rxpower	Display the local receive power (dBm/Hz) on the customer premises equipment (CPE) port.
snr	Display the signal-to-noise ratio (SNR) ratio on the LRE port.
link	Display the LRE link status of the LRE port.
 begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

You can use the SNR and Reed-Solomon error information to measure the quality of the LRE link. The SNR is the amount of increased received signal-power (in decibels) relative to the noise-power level that the switch can tolerate without disconnecting from the CPE device. The higher the ratio, the more resilient is the link.

The Reed-Solomon errors show the number of errors detected and corrected in the data being received on and sent from the switch LRE ports. Reed-Solomon errors are the result of noise exceeding the noise margin. For short bursts of noise (such as motor power on or power surges), the interleave feature prevents the loss of Ethernet data packets. Then the number of Reed-Solomon errors exceeds the number of Ethernet CRC errors.

The remote transmit power-rates from the connected CPE devices might be different from each other, depending on how long the cable is between the switch and the CPE device. A longer cable typically causes the CPE device to send a higher signal to overcome the loss effects of distance.

The local receive-power actually displays the switch's adjustment to the incoming power level. These numbers might be different from LRE port to LRE port, as the length of the cables to the CPE devices might be different.

If the SNR is too low for the environment but the link still establishes, the Reed-Solomon error rate is high, and there might be link instability (as shown by the number of *Fail* events counted). If the network is being used for data only, a high incidence of Ethernet Frame Check Sequence (FCS) errors or micro-interruptions might be tolerable.

For more information about what can affect the LRE link and for the minimum required SNR ratios, refer to the “LRE Links and LRE Profiles” section in the “Configuring LRE” chapter of the switch software configuration guide for this release.

Expressions are case sensitive. For example, if you enter `! exclude output`, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the `show controllers lre interface-id actual dsrserrs` command on LRE port 2:

```
Switch# show controllers lre longreachethernet0/2 actual dsrserrs
0
Switch#
```

This is an example of output from the `show controllers lre interface-id actual link` command on LRE port 2:

```
Switch# show controllers lre longreachethernet0/2 actual link
UP
Switch#
```

This is an example of output from the `show controllers lre interface-id actual rxpower` command on LRE port 2:

```
Switch# show controllers lre longreachethernet0/2 actual rxpower
26.0
Switch#
```

This is an example of output from the `show controllers lre interface-id actual snr` command on LRE port 2:

```
Switch# show controllers lre longreachethernet0/2 actual snr
27
Switch#
```

This is an example of output from the `show controllers lre interface-id actual txpower` command on LRE port 2:

```
Switch# show controllers lre longreachethernet0/2 actual txpower
-89.7
Switch#
```

This is an example of output from the `show controllers lre interface-id actual usrserrs` command on LRE port 2:

```
Switch# show controllers lre longreachethernet0/2 actual usrserrs
0
Switch#
```

show controllers lre actual

This is an example of output from the **show controllers lre *interface-id* actual link** command on LRE port 1:

```
Switch# show controllers lre longreachethernet0/1 actual link
DOWN
Switch#
```

Related Commands

Command	Description
show controllers lre admin	Displays the administrative settings of the LRE link on a specific switch LRE port.

show controllers lre admin

Use the **show controllers lre *interface-id* admin** privileged EXEC command to display the administrative settings of the Long-Reach Ethernet (LRE) link for a specific switch LRE port.

show controllers lre *interface-id* admin {dsrate | usrate} [| {begin | exclude | include} *expression*]

This command is available only on Catalyst 2950 LRE switches.

Syntax Description

<i>interface-id</i>	ID of the switch LRE port.
admin	Display the administrative settings, which might not be the same as the actual values.
dsrate	Display the downstream rate (in Mbps) of the LRE link.
usrate	Display the upstream rate (in Mbps) of the LRE link.
 begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

This command displays the profile settings of an LRE switch port, even though they might not be active if a global profile is configured on the switch.

The upstream and downstream rates are defined by the profile on the switch LRE port. To change these rates, assign a different profile to the switch LRE port. For information about the LRE profiles, refer to the switch software configuration guide for this release.

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

Examples

This is an example of output from the **show controllers lre *interface-id* admin dsrate** and **show controllers lre *interface-id* admin usrate** commands on LRE ports 1 and 2:

```
Switch# show controllers lre longreachethernet0/1 admin usrate
18.750
Switch# show controllers lre longreachethernet0/1 admin dsrate
16.667
Switch# show controllers lre longreachethernet0/2 admin usrate
12.500
Switch# show controllers lre longreachethernet0/2 admin dsrate
12.500
```

Related Commands	Command	Description
	show controllers lre cpe identity	Displays the actual values of the LRE link on a specific switch LRE port.
	lre profile	Assigns a profile to all switch LRE ports.
	profile (interface configuration)	Assigns a profile to a specific switch LRE port.

show controllers lre link monitor

Use the **show controllers lre link monitor** privileged EXEC command to display Long-Reach Ethernet (LRE) link monitor information.

```
show controllers lre monitor { errors | parameters | statistics } { local [interface-id] | remote [interface-id] } [ | { begin | exclude | include } expression ]
```

This command is available only on Catalyst 2950 LRE switches.

Syntax Description

errors	Display the LRE Reed-Solomon (RS) errors and Ethernet errors
parameters	Display the LRE operating parameter data collected by the link monitor.
statistics	Display the LRE link monitor statistics.
local	(Optional) Display data from the LRE switch controller.
remote	(Optional) Display data from the customer premises equipment (CPE) device.
<i>interface-id</i>	(Optional) ID of the switch LRE port.
begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .
exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

The link monitor process collects error information at 1-minute intervals for 15 minutes. After 15 minutes, the data is analyzed and stored before starting a new collection sequence. Up to 2 hours of link monitor data can be shown.

Local monitoring collects data from the LRE switch. Remote monitoring collects data from attached CPE device.

The *Time* heading in the **show controllers lre link monitor errors** command output shows the timestamp for the last collection sequence. The RS error count shows the cumulative error count from the last reading. Alignment errors, frame check sequence (FCS) errors, receive errors, and oversize errors are the Ethernet statistics collected either at the switch or at the CPE device.

The *Time* heading in the **show controllers lre link monitor parameters** command output shows the timestamp for the last collection sequence. The signal-to-noise (SNR) error counter, shown under the SNR Err heading, increments when the SNR value read from the chipset falls below the theoretical SNR added to the threshold.

The *Time* heading in the **show controllers lre link monitor statistics** command output shows the timestamp for the last collection sequence. The RS error count shows the cumulative error count from the last reading. This count is cleared only when the interface is shut down or when the **clear controllers lre link monitor** privileged EXEC command is entered. The RS error alarm shows the number of 1 minute intervals that had RS errors above the configured threshold.

Use the **show controllers lre monitor {errors | parameters | statistics}** privileged EXEC command without specifying a switch interface to display data for all interfaces.

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

Examples

This is an example of output that shows how to display LRE RS and Ethernet errors for the LRE switch on LRE port 0/1:

```
Switch# show controllers lre link monitor errors local longreachethernet0/1
```

```
LongReachEthernet0/1:LRE Link Health Monitor Error counts :
Time      RS Errors  Align Errs  FCS Errs   Rcv Errs   Oversz Errs
-----
14:42:28   41216      0           0          0           0
14:30:28   40960      0           0          0           0
14:15:28   40960      0           0          0           0
14:00:29   40704      0           0          0           0
13:45:28   40704      0           0          0           0
13:30:29   40448      0           0          0           0
13:15:29   40448      0           0          0           0
13:00:28   40448      0           0          0           0
```

This is an example of output that shows Reed-Solomon and Ethernet errors for a CPE device connected to LRE port 0/1:

```
Switch# show controllers lre link monitor errors remote longreachethernet0/1
```

```
LongReachEthernet0/1:LRE Link Health Monitor Error counts :
Time      RS Errors  Align Errs  FCS Errs   Rcv Errs   Oversz Errs
-----
14:42:28   6400      45835      0           0           0
14:30:28   6400      45835      0           0           0
14:15:28   6400      45835      0           0           0
14:00:29   6400      45835      0           0           0
13:45:28   6144      45835      0           0           0
13:30:29   6144      45835      0           0           0
13:15:29   6144      45835      0           0           0
13:00:28   6144      45835      0           0           0
```

This is an example that shows how to display all LRE link monitor parameters for the attached CPE device:

```
Switch# show controllers lre link monitor parameters remote

LongReachEthernet0/1: LRE Link Health Monitor Parameters :
      SNR          Tx Power          SwAGCGain
Time   Samples  Min Max Err   Min   Max   Min   Max
-----
00:32:30    2      0  0  0  - 85.6  - 85.6  - 2.0  - 2.0
00:30:30   15      0  0  0  - 85.6  - 85.6  - 2.0  - 2.0
00:15:30   15      0  0  0  - 85.6  - 85.6  - 2.0  - 2.0
00:00:30   15      0  0  0  - 85.6  - 85.6  - 2.0  - 2.0
23:45:30   15      0  0  0  - 85.6  - 85.6  - 2.0  - 2.0
23:30:30   15      0  0  0  - 85.6  - 85.6  - 2.0  - 2.0
23:15:30   15      0  0  0  - 85.6  - 85.6  - 2.0  - 2.0

<output truncated>
```

This is an example that shows how to display all LRE link monitor statistics for the LRE controller:

```
Switch# show controllers lre link monitor statistics local

LongReachEthernet0/1: LRE Link Health Monitor Stats :
      RS Errors   Link Fail   Freeze
Time   Samples Count     Alarm   Count   Count
-----
06:58:30    13      0  0      2      3
06:45:30    15      0  0      2      3
06:30:30    15      0  0      2      3
06:15:30    15      0  0      2      3
06:00:30    15      0  0      2      3
05:45:30    15      0  0      2      3
05:30:30    15      0  0      2      3
05:15:30    15      0  0      2      3
```

Related Commands

Command	Description
clear controllers lre link monitor	Deletes LRE link monitor data.
link monitor	Enables the LRE link monitor on a port.
link monitor logging	Enables link monitor event logging per port.
link monitor threshold rserr	Sets a Reed-Solomon error threshold for the LRE link monitor.
link monitor threshold snr	Sets an signal-to-noise margin for the LRE link monitor.

show controllers lre log

Use the **show controllers lre log** user EXEC command without keywords to display the history of link, configuration, and timer events for a specific Long-Reach Ethernet (LRE) port or for all switch LRE ports. Use this command with keywords to display information about the LRE event log level.

show controllers lre log [**level**] [*interface-id*] [| {**begin** | **exclude** | **include**} *expression*]

This command is available only on Catalyst 2950 LRE switches.

Syntax Description

level	(Optional) Display information about the LRE event log level.
<i>interface-id</i>	(Optional) ID of the switch LRE port.
begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .
exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

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

Usage Guidelines

Use the **show controllers lre log** command without specifying a switch LRE port to display the events for all LRE switch ports. The time-stamped and sequentially tagged log entries can be helpful in confirming LRE link drops and configuration changes.

Use the **show controllers lre log level** command without specifying an LRE switch port to list the log level for each LRE port on the switch.

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

Examples

This is an example of output from the **show controllers lre log** command that shows events on an LRE interface:

```
Switch> show controllers lre log longreachethernet0/5

LongReachEthernet0/5: Events Log: =====
 1d00h: [0]: State RESTART: Got event:Reset

 1d00h: [1]: State MODEZERO_APPLIED: Got event:Link Up

 1d00h: [2]: State MODEZERO_APPLIED: Got event:Link Down

 1d00h: [3]: State PROFILE_APPLIED: Got event:Link Up
```

```

1d00h: [4]: State PROFILE_LINKUP: Got event:Link Down
1d00h: [5]: State PROFILE_LINKUP: Got event:Link Up
1d00h: [6]: State PROFILE_LINKUP: Got event:Link Down
1d00h: [7]: State PROFILE_LINKUP: Got event:Link Up

```

This is an example of output from the **show controllers lre log level** command that displays the log level on an LRE port:

```

Switch> show controllers lre log level longreachethernet0/1
Port    Log Level
=====
Lo0/1   Logging disabled

```

Related Commands

Command	Description
clear controllers ethernet-controller	Deletes the history of link, configuration, and timer events for a specific switch LRE port or for all LRE ports on the switch.
logging lre	Specifies the logging level on the LRE port.
show controllers lre profile	Displays the log level for a specific switch LRE port or for all LRE ports on the switch.

show controllers lre profile

Use the **show controllers lre profile** privileged EXEC command to display information about the Long-Reach Ethernet (LRE) profiles and sequences available on the switch.

show controllers lre profile {**details** | **names**} [| {**begin** | **exclude** | **include**} *expression*]

This command is available only on Catalyst 2950 LRE switches.

Syntax Description

details	Display information about the LRE profiles and sequences available on the switch.
names	Display information about the Long-Reach Ethernet (LRE) profiles available on the switch.
 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

Use the **show controllers lre profile details** privileged EXEC command to see the profiles and sequences running on each port. This command also shows global profiles and sequences.

For information about LRE profiles supported on your switch and about LRE links, refer to the “LRE Profiles” section in the “Configuring LRE” chapter of the switch software configuration guide for this release.



Note

Use the information in the software configuration guide only as a guideline. Factors such as the type of cable that you use, how it is bundled, and the interference and noise on the LRE link can affect the actual LRE link performance. Contact Cisco Systems for information about limitations and optimization of LRE link performance. The net data rates are slightly less than the gross data rates displayed by the **show controllers lre profile names** command output.

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

Examples

This is an example of output from the **show controllers lre profile details** command on the Catalyst 2950ST-8 LRE and 2950ST-24 LRE switches:

```
Switch# show controllers lre profile details
```

```
Global Profile:LRE-10-3
```

Interface	Configured Profile	Running Profile	Type
Lo0/1	LRE-10-5	LRE-15	Port Sequence
Lo0/2	LRE-10-3	LRE-10-3	Global Profile
Lo0/3	LRE-10-3	LRE-15	Port Sequence
Lo0/4	LRE-10-3	LRE-10-3	Global Profile
Lo0/5	LRE-10-3	LRE-10-3	Global Profile
Lo0/6	LRE-10-3	LRE-10-3	Global Profile
Lo0/7	LRE-10-3	LRE-15	Global Profile
Lo0/8	LRE-10-3	LRE-10-3	Global Profile
Lo0/9	LRE-10-3	LRE-10-3	Global Profile
Lo0/10	LRE-10-3	LRE-10-3	Global Profile
Lo0/11	LRE-10-3	LRE-10-3	Global Profile
Lo0/12	LRE-10-3	LRE-10-3	Global Profile

```
<output truncated>
```

This is an example of output from the **show controllers lre profile details** command on the Catalyst 2950ST-24 LRE 997 switch:

```
Switch# show controllers lre profile details
```

```
Global Profile:LRE-6
```

Interface	Configured Profile	Running Profile	Type
Lo0/1	LRE-6	LRE-6	Global Profile
Lo0/2	LRE-6	LRE-6	Global Profile
Lo0/3	LRE-6	LRE-6	Global Profile
Lo0/4	LRE-6	LRE-6	Global Profile
Lo0/5	LRE-6	LRE-6	Global Profile
Lo0/6	LRE-6	LRE-6	Global Profile
Lo0/7	LRE-6	LRE-6	Global Profile
Lo0/8	LRE-6	LRE-6	Global Profile
Lo0/9	LRE-6	LRE-6	Global Profile
Lo0/10	LRE-6	LRE-6	Global Profile
Lo0/11	LRE-6	LRE-6	Global Profile
Lo0/12	LRE-6	LRE-6	Global Profile

```
<output truncated>
```

show controllers lre profile

This is an example of output from the **show controllers lre profile names** command on the Catalyst 2950ST-8 LRE and 2950ST-24 LRE switches:

Switch# **show controllers lre profile names**

Profile Name	Type	Downstream Rate (Mbps)	Upstream Rate (Mbps)
LRE-15	System-Configured	16.667	18.750
LRE-10	System-Configured	12.500	12.500
LRE-5	System-Configured	6.250	6.250
LRE-998-15-4	System-Configured	16.667	4.688
LRE-997-10-4	System-Configured	12.500	4.688
LRE-15LL	System-Configured	16.667	18.750
LRE-10LL	System-Configured	12.500	12.500
LRE-5LL	System-Configured	6.250	6.250
LRE-10-5	System-Configured	12.500	6.250
LRE-10-3	System-Configured	12.500	3.125
LRE-10-1	System-Configured	12.500	1.563
LRE-8	System-Configured	9.375	9.375
LRE-7	System-Configured	8.333	8.333
LRE-15-5	System-Configured	16.667	6.250
LRE-15-3	System-Configured	16.667	3.125
LRE-15-1	System-Configured	16.667	1.563
LRE-4	System-Configured	4.167	4.167
LRE-3	System-Configured	3.125	3.125
LRE-2	System-Configured	2.083	2.083
LRE-4-1LL	System-Configured	4.167	1.563

This is an example of output from the **show controllers lre profile names** command on the Catalyst 2950ST-24 LRE 997 switch:

Switch# **show controllers lre profile names**

Profile Name	Type	Downstream Rate (Mbps)	Upstream Rate (Mbps)
LRE-12-9	System-Configured	12.500	9.375
LRE-12-3	System-Configured	12.500	3.125
LRE-9	System-Configured	9.375	9.375
LRE-9-6	System-Configured	9.375	6.250
LRE-9-4	System-Configured	9.375	4.688
LRE-9-3	System-Configured	9.375	3.125
LRE-6	System-Configured	6.250	6.250
LRE-6-4	System-Configured	6.250	4.688
LRE-6-3	System-Configured	6.250	3.125
LRE-4	System-Configured	4.688	4.688

Related Commands

Command	Description
lre profile	Assigns an LRE profile to all the LRE ports on the switch.

show controllers lre sequence

Use the **show controllers lre sequence** privileged EXEC command to display the list of sequences, the profiles that are configured in that sequence, and the downstream and upstream rates of the corresponding profiles.

show controllers lre sequence [| { **begin** | **exclude** | **include** } *expression*]

This command is available only on Catalyst 2950 LRE switches.

Syntax Description

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

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

Use the **show controllers lre sequence** command to display the list of sequences supported in the switch. This command displays the system-defined and user-defined sequences.

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

Examples

This is an example of output from the **show controllers lre sequence** command on the Catalyst 2950ST-8 LRE and 2950ST-24 LRE switches:

```
Switch# show controllers lre sequence

Global Sequence:LRE-SEQ-COMPLETE-REACH

Sequence:LRE-SEQ-COMPLETE-REACH      Type: System-Configured

      Profile Name      Downstream      Upstream
      -----      Rate (Mbps)      Rate (Mbps)
      -----
LRE-15                16.667          18.750
LRE-10                12.500          12.500
LRE-15-5              16.667          6.250
LRE-10-5              12.500          6.250
LRE-8                 9.375           9.375
LRE-7                 8.333           8.333
LRE-15-3              16.667          3.125
LRE-10-3              12.500          3.125
LRE-5                 6.250           6.250
LRE-15-1              16.667          1.563
```

show controllers lre sequence

```

LRE-10-1      12.500      1.563
LRE-4         4.167       4.167
LRE-3         3.125       3.125
LRE-2         2.083       2.083
LRE-4-1       4.167       1.563

Sequence:LRE-SEQ-DOWNSTREAM      Type:System-Configured

      Profile Name      Downstream      Upstream
      -----      -Rate (Mbps)      -Rate (Mbps)
      -----
LRE-15         16.667         18.750
LRE-15-5       16.667          6.250
LRE-15-3       16.667          3.125
LRE-15-1       16.667          1.563
LRE-10         12.500         12.500

```

<output truncated>

This is an example of output from the **show controllers lre sequence** command on the Catalyst 2950ST-24 LRE 997 switch:

```
Switch# show controllers lre sequence
```

Global Sequence:N/A

```

Sequence:LRE-SEQ-COMPLETE-REACH  Type:System-Configured

      Profile Name      Downstream      Upstream
      -----      -Rate (Mbps)      -Rate (Mbps)
      -----
LRE-12-9       12.500          9.375
LRE-12-3       12.500          3.125
LRE-9          9.375           9.375
LRE-9-6        9.375           6.250
LRE-9-4        9.375           4.688
LRE-6           6.250           6.250
LRE-6-4        6.250           4.688
LRE-9-3        9.375           3.125
LRE-4           4.688           4.688
LRE-6-3        6.250           3.125
LRE-4-3        4.688           3.125

```

```

Sequence:LRE-SEQ-DOWNSTREAM      Type:System-Configured

      Profile Name      Downstream      Upstream
      -----      -Rate (Mbps)      -Rate (Mbps)
      -----
LRE-12-9       12.500          9.375
LRE-12-3       12.500          3.125
LRE-9          9.375           9.375
LRE-9-6        9.375           6.250
LRE-9-4        9.375           4.688

```

<output truncated>

Related Commands

Command	Description
lre rate selection sequence	Assigns a rate selection sequence to the entire switch.
lre sequence	Defines a user-defined sequence.

show controllers lre status

Use the **show controllers lre status** privileged EXEC command to display the Long-Reach Ethernet (LRE) link statistics and profile information on a switch LRE port, including link state, link duration, profile name, and data rates.

```
show controllers lre status { cpe | interleave | link | profile | psd | sequence [detail] } [interface-id]
[ | { begin | exclude | include } expression]
```

This command is available only on Catalyst 2950 LRE switches.

Syntax	Description
cpe	Display information about the customer premises equipment (CPE) 10/100 Ethernet ports.
interleave	Display the interleave block size values on the LRE interfaces.
link	Display the various parameters and status associated with the LRE link.
profile	Display the various administrative parameters and status associated with the LRE link.
psd	Display the power-related status.
sequence	Display the status of profiles in a sequence. Possible status values are <i>converged</i> , <i>waiting on link</i> , <i>executing</i> , and <i>locked</i> .
detail	(Optional) Display additional information about the sequences, such as margins, locked profiles, and convergence times.
<i>interface-id</i>	(Optional) ID of the switch LRE port.
 exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(11)YJ	This command was introduced.
	12.1(11)YJ4	The interleave keyword was added.
	12.1(14)EA1	The cpe keyword was added.

Usage Guidelines Use the **show controllers lre status** privileged EXEC command to display the status of all switch LRE ports.

Use the signal-to-noise ratio (SNR) and Reed-Solomon error information to measure the quality of the LRE link. The SNR represents the amount of increased received signal power (in decibels) relative to the noise power-level that the switch can tolerate without disconnecting from the CPE device. The higher the ratio, the more resilient is the link.

The Reed-Solomon errors show the number of errors detected and corrected in the data being received on and sent from the switch LRE ports. Reed-Solomon errors are the result of noise exceeding the noise margin. For short bursts of noise (such as motor power on or power surges), the interleaver prevents the loss of Ethernet data packets. The number of Reed-Solomon errors then exceeds the number of Ethernet CRC errors.

**Note**

The Reed-Solomon errors are reset each time that you enter the **show controllers lre status link** command.

The remote transmit power levels from the connected CPE devices might be different from each other, depending on how long the cable is between the switch and the CPE device. A longer cable typically causes the CPE device to send a higher signal to overcome the loss effects of distance.

The local receive-power rates actually displays the switch's adjustment to the incoming power level. These numbers might be different from LRE port to LRE port, as the length of the cables to the CPE devices might be different.

The interleaver columns display the interleaver block size for both directions of data. A higher interleaver setting is less susceptible to certain kinds of impairments but can introduce a very small amount of delay in the data path.

The PMD-S column refers to physical media dependent status and is provided as diagnostic information.

For more information about what can affect the LRE link and for the minimum required SNR ratios, refer to the “LRE Links and LRE Profiles” section in the “Configuring LRE” chapter of the switch software configuration guide for this release.

The **sequence** and **sequence detail** keywords display these status codes of profiles and sequences during rate selection:

- Converged—Rate selection has converged on a profile.
- Locked—Rate selection has converged on a profile, and the port is locked to that profile.
- Executing—Rate selection is running on the port.
- Waiting on Link—No link is established.
- N/A—Sequence is not assigned to the port.

You can adjust the noise level during convergence by using the **margin** interface configuration command.

Use the **show controllers lre status cpe** *[interface-id]* privileged EXEC command to display information about a specific CPE port or all the CPE ports.

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

Examples

This is an example of output that shows link information for an LRE interface:

```
Switch# show controller lre status link longreachethernet0/2

Port   Link SNR   RS Errs   CPE-Tx   Sw-AGC-Gain   Interleaver   PMD-S
      (dB)                (dBm/Hz)      (dB)      Rx-Bsz Tx-Bsz
-----
Lo0/2  UP        41         4829    - 57.7    - 7.6       16    16    0x04
```

This is an example of output from the **show controllers lre status profile** command:

```
Switch# show controllers lre status profile
```

Port	Link	Uptime	Profile	DSRate	USRate	Fail
Lo0/1	UP	2d23h	LRE-10	12.500	12.500	0
Lo0/2	UP	2d23h	LRE-10	4.167	1.563	0
Lo0/3	UP	2d23h	LRE-10	4.167	1.563	0
Lo0/4	UP	2d23h	LRE-10	4.167	1.563	0
Lo0/5	DOWN	00:00:00	LRE-10	0.000	0.000	0
Lo0/6	UP	2d23h	LRE-10	4.167	1.563	0
Lo0/7	UP	2d23h	LRE-10	4.167	1.563	0
Lo0/8	UP	2d23h	LRE-10	4.167	1.563	0
Lo0/9	UP	2d23h	LRE-10	4.167	1.563	0
Lo0/10	DOWN	00:00:00	LRE-10	0.000	0.000	0
Lo0/11	DOWN	00:00:00	LRE-10	0.000	0.000	0
Lo0/12	DOWN	00:00:00	LRE-10	0.000	0.000	0
Lo0/13	UP	2d23h	LRE-10	12.500	12.500	0
Lo0/14	DOWN	00:00:00	LRE-10	0.000	0.000	0
Lo0/15	UP	2d23h	LRE-10	4.167	1.563	0
Lo0/16	DOWN	00:00:00	LRE-10	0.000	0.000	0
Lo0/17	DOWN	00:00:00	LRE-10	0.000	0.000	0
Lo0/18	DOWN	00:00:00	LRE-10	0.000	0.000	0
Lo0/19	DOWN	00:00:00	LRE-10	0.000	0.000	0
Lo0/20	DOWN	00:00:00	LRE-10	0.000	0.000	0
Lo0/21	UP	2d23h	LRE-10	4.167	1.563	0
Lo0/22	DOWN	00:00:00	LRE-10	0.000	0.000	0
Lo0/23	DOWN	00:00:00	LRE-10	0.000	0.000	0
Lo0/24	DOWN	00:00:00	LRE-10	0.000	0.000	0

This is an example of output from the **show controllers lre status psd** command:

```
Switch# show controllers lre status psd
```

Port	Link	Switch				CPE			
		SNR	RSErr	TxPwr	AGCgain	SNR	RSErr	TxPwr	AGCgain
Lo0/1	UP	32		0 - 6.13	13.0	43	0	- 85.6	- 2.0
Lo0/2	UP	32		0 - 6.13	15.1	42	0	- 85.9	- 2.0
Lo0/3	UP	32		0 - 6.13	13.5	42	0	- 85.6	- 2.0
Lo0/4	DOWN	10		0 - 5.85	63.9	0	0	0.0	0.0
Lo0/5	DOWN	10		0 - 5.85	58.9	0	0	0.0	0.0
Lo0/6	UP	33		0 - 6.13	15.1	42	0	- 85.9	- 2.0
Lo0/7	DOWN	10		0 - 5.85	54.2	0	0	0.0	0.0
Lo0/8	UP	33		0 - 6.13	14.6	42	0	- 85.9	- 2.5
Lo0/9	DOWN	10		0 - 5.85	52.9	0	0	0.0	0.0
Lo0/10	DOWN	10		0 - 5.85	61.5	0	0	0.0	0.0
Lo0/11	UP	33		0 - 6.13	15.1	42	0	- 85.9	- 1.6
Lo0/12	UP	33		0 - 6.13	15.1	42	0	- 85.9	- 2.5
Lo0/13	UP	33		0 - 6.13	15.1	42	0	- 85.9	- 2.5
Lo0/14	DOWN	10	268305	- 5.85	57.5	0	0	0.0	0.0
Lo0/15	DOWN	10		0 - 5.85	50.7	0	0	0.0	0.0
Lo0/16	UP	35		38 - 5.85	15.1	41	1238	- 85.9	- 6.4
Lo0/17	DOWN	10	767128	- 5.85	61.8	0	0	0.0	0.0
Lo0/18	DOWN	10		0 - 5.85	54.2	0	0	0.0	0.0
Lo0/19	DOWN	10		0 - 5.85	51.5	0	0	0.0	0.0
Lo0/20	DOWN	10		0 - 5.85	54.7	0	0	0.0	0.0
Lo0/21	DOWN	10		0 - 5.85	67.8	0	0	0.0	0.0
Lo0/22	DOWN	10		0 - 5.85	50.7	0	0	0.0	0.0
Lo0/23	DOWN	10		0 - 5.85	66.5	0	0	0.0	0.0
Lo0/24	DOWN	10		0 - 5.85	53.6	0	0	0.0	0.0

This is an example of output from the **show controllers lre status sequence** command:

```
Switch# show controllers lre status sequence
```

Port	Sequence	Status	Profile
Lo0/1	LRE-SEQ-DOWNSTREAM	Converged	LRE-15
Lo0/2	N/A	N/A	N/A
Lo0/3	LRE-SEQ-SYM	Converged	LRE-15

This is an example of output from the **show controllers lre status interleave** command:

```
Switch# show controllers lre status interleave longreachethernet0/2
```

Port	Link Profile	Line Rate		Block Size		Delay (mSec)	
		DS	US	DS	US	DS	US
Lo0/2	UP LRE-6	6.250	6.250	16	16	20.316	20.316

This is an example of output using the **details** keyword to obtain further information about the sequence:

```
Switch# show controllers lre status sequence detail
```

```
Lo0/1 :
Sequence:LRE-SEQ-DOWNSTREAM      Status:Converged      Attempts:1
Profile:LRE-15                   Convergence Time: 00:01:54
Rate-Selection:Enabled           Locking:Not-Configured
Downstream Margin:2              Upstream Margin:0
```

```
Lo0/2 :
Sequence:N/A                     Status:N/A            Attempts:0
Profile:N/A                      Convergence Time: 00:00:00
Rate-Selection:Disabled          Locking:Not-Configured
Downstream Margin:0              Upstream Margin:0
```

<output truncated>

This is an example of output from the **show controllers lre status cpe** command:

```
Switch# show controllers lre status cpe
```

```
Lo0/1 :                               CPE-TYPE:Cisco575-LRE
Port      Status      Speed  Duplex  Protected
-----  -
  1      notconnected  NA     NA     false

Lo0/2 :                               CPE-TYPE:NA
Port      Status      Speed  Duplex  Protected
-----  -
  1      NA          NA     NA     NA

Lo0/3 :                               CPE-TYPE:CISCO585-LRE
Port      Status      Speed  Duplex  Protected
-----  -
  1      notconnected  auto   NA     false
  2      notconnected  auto   NA     true
  3      notconnected  auto   NA     false
  4      notconnected  auto   NA     false
  5      connected    100   half   false
```

Related Commands	Command	Description
	<code>margin</code>	Specifies the margin value used to determine link quality during LRE rate selection.
	<code>show controllers lre sequence</code>	Displays the sequence running on a specific switch LRE port.
	<code>show controllers lre profile</code>	Displays information about the LRE profiles available on the switch.
	<code>show controllers lre cpe</code>	Displays the actual values of the LRE link on a specific switch LRE port.
	<code>show controllers lre admin</code>	Displays the administrative settings of the LRE link on a specific switch LRE port.
	<code>show controllers lre profile</code>	Displays information about the LRE profiles available on the switch.

show controllers lre version

Use the **show controllers lre version** privileged EXEC command to display the version numbers of the various components (hardware, firmware, and patch software) that make up the Long-Reach Ethernet (LRE) switch interface.

show controllers lre version [*interface-id*] [| { **begin** | **exclude** | **include** } *expression*]

This command is available only on Catalyst 2950 LRE switches.

Syntax Description

<i>interface-id</i>	(Optional) ID of the switch LRE port.
begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .
exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

Use the **show controllers lre version** command without specifying a switch LRE port to display the version numbers of all switch LRE interfaces.

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

Examples

This is an example of output that shows the version information for an LRE interface:

```
Switch# show controllers lre version longreachethernet0/2
Interface Hw Sw Patch
-----
Lo0/2 32 B4 50
```

Related Commands

Command	Description
show controllers lre cpe	Displays the model numbers of the LRE CPE devices connected to the LRE switch and shows whether or not the connected CPE devices meet the minimum requirements for management by the LRE switch.

show dot1x

Use the **show dot1x** privileged EXEC command to display 802.1X statistics, administrative status, and operational status for the switch or for the specified interface.

```
show dot1x [all] | [interface interface-id] | [statistics [interface interface-id]] [ | {begin | exclude | include} expression]
```

Syntax Description	
all	(Optional) Display the 802.1X status for all interfaces.
interface <i>interface-id</i>	(Optional) Display the 802.1X status for the specified interface.
statistics [interface <i>interface-id</i>]	(Optional) Display 802.1X statistics for the switch or the specified interface.
begin	(Optional) Display begins with the line that matches the <i>expression</i> .
exclude	(Optional) Display excludes lines that match the <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(6)EA2	This command was first introduced.
	12.1(14)EA1	The all keyword was added.

Usage Guidelines If you do not specify an interface, global parameters and a summary appear. If you specify an interface, details for that interface appear.

If you specify the **statistics** keyword without the **interface** *interface-id* option, statistics appear for all interfaces. If you specify the **statistics** keyword with the **interface** *interface-id* option, statistics appear for the specified interface.

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

Examples

This is an example of output from the **show dot1x** and the **show dot1x all** privileged EXEC commands:

```
Switch# show dot1x
Sysauthcontrol           = Enabled
Dot1x Protocol Version   = 1
Dot1x Oper Controlled Directions = Both
Dot1x Admin Controlled Directions = Both
```

```
Switch# show dot1x all
Dot1x Info for interface FastEthernet 0/3
```

```
-----
Supplicant MAC 00d0.b71b.35de
  AuthSM State           = CONNECTING
  BendSM State           = IDLE
PortStatus               = UNAUTHORIZED
MaxReq                   = 2
HostMode                 = Single
Port Control             = Auto
QuietPeriod              = 60 Seconds
Re-authentication       = Disabled
ReAuthPeriod             = 3600 Seconds
ServerTimeout            = 30 Seconds
SuppTimeout              = 30 Seconds
TxPeriod                 = 30 Seconds
Guest-Vlan               = 0
```

```
Dot1x Info for interface FastEthernet 0/7
```

```
-----
PortStatus               = UNAUTHORIZED
MaxReq                   = 2
HostMode                 = Multi
Port Control             = Auto
QuietPeriod              = 60 Seconds
Re-authentication       = Disabled
ReAuthPeriod             = 3600 Seconds
ServerTimeout            = 30 Seconds
SuppTimeout              = 30 Seconds
TxPeriod                 = 30 Seconds
Guest-Vlan               = 0
```

This is an example of output from the **show dot1x interface fastethernet 0/3** privileged EXEC command.

```
Switch# show dot1x interface fastethernet 0/3
Supplicant MAC 00d0.b71b.35de
  AuthSM State           = AUTHENTICATED
  BendSM State           = IDLE
PortStatus               = AUTHORIZED
MaxReq                   = 2
HostMode                 = Single
Port Control             = Auto
QuietPeriod              = 60 Seconds
Re-authentication       = Disabled
ReAuthPeriod             = 3600 Seconds
ServerTimeout            = 30 Seconds
SuppTimeout              = 30 Seconds
TxPeriod                 = 30 Seconds
Guest-Vlan               = 0
```

This is an example of output from the **show dot1x statistics interface fastethernet 0/3** command. [Table 2-15](#) describes the fields in the display.

```
Switch# show dot1x statistics interface fastethernet 0/3
PortStatistics Parameters for Dot1x
-----
TxReqId = 15    TxReq = 0        TxTotal = 15
RxStart = 4     RxLogoff = 0     RxRespId = 1    RxResp = 1
RxInvalid = 0  RxLenErr = 0    RxTotal = 6
RxVersion = 1  LastRxSrcMac 00d0.b71b.35de
```

Table 2-15 show dot1x statistics Field Descriptions

Field	Description
TxReqId	Number of Extensible Authentication Protocol (EAP)-request/identity frames that have been sent.
TxReq	Number of EAP-request frames (other than request/identity frames) that have been sent.
TxTotal	Number of Extensible Authentication Protocol over LAN (EAPOL) frames of any type that have been sent.
RxStart	Number of valid EAPOL-start frames that have been received.
RxLogoff	Number of EAPOL-logoff frames that have been received.
RxRespId	Number of EAP-response/identity frames that have been received.
RxResp	Number of valid EAP-response frames (other than response/identity frames) that have been received.
RxInvalid	Number of EAPOL frames that have been received and have an unrecognized frame type.
RxLenErr	Number of EAPOL frames that have been received in which the packet body length field is invalid.
RxTotal	Number of valid EAPOL frames of any type that have been received.
RxVersion	Received packets in the 802.1X version 1 format.
LastRxSrcMac	Source MAC address carried in the most recently received EAPOL frame.

Related Commands

Command	Description
dot1x default	Resets the configurable 802.1X parameters to their default values.

show env

Use the **show env** user EXEC command to display fan information for the switch.

```
show env {all | fan | power | rps} [ | {begin | exclude | include} expression]
```

Syntax Description		
all		Display both fan and temperature environmental status.
fan		Display the switch fan status (only available in privileged EXEC mode).
power		Display the internal power supply status.
rps		Display the Redundant Power System (RPS) status.
 begin		(Optional) Display begins with the line that matches the specified <i>expression</i> .
 exclude		(Optional) Display excludes lines that match the specified <i>expression</i> .
 include		(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>		Expression in the output to use as a reference point.

Command Modes User EXEC

Command History	Release	Modification
	12.0(5.2)WC(1)	This command was first introduced.
	12.1(12c)EA1	The fan and power keywords were added.

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

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

```
Switch> show env all
FAN is OK
Internal POWER supply is FAULTY
RPS is present
RPS is supplying power
```

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

```
Switch# show env fan
FAN 1 is FAULTY
```

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

```
Switch> show env power
Internal POWER supply is FAULTY
```

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

```
Switch> sho env rps
RPS is supplying power
```

show errdisable recovery

Use the **show errdisable recovery** user EXEC command to display the error-disable recovery timer information.

show errdisable recovery [| { **begin** | **exclude** | **include** } *expression*]

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

Command Modes User EXEC

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

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

Examples This is an example of output from the **show errdisable recovery** command:

```
Switch> show errdisable recovery
ErrDisable Reason      Timer Status
-----
udld                   Enabled
bpduguard              Enabled
channel-misconfig     Enabled
pagg-flap              Enabled
dtp-flap               Enabled
link-flap              Enabled
psecure-violation     Enabled
gbic-invalid           Enabled

Timer interval:300 seconds

Interfaces that will be enabled at the next timeout:

Interface      Errdisable reason      Time left(sec)
-----
Gi0/4          link-flap                279
```

■ show errdisable recovery

Related Commands	Command	Description
	errdisable recovery	Configures the recover mechanism variables.
	show interfaces trunk	Displays interface status or a list of interfaces in error-disabled state.

show etherchannel

Use the **show etherchannel** user EXEC command to display EtherChannel information for a channel.

```
show etherchannel [channel-group-number] {detail | load-balance | port | port-channel |
summary} [ | {begin | exclude | include} expression]
```

Syntax Description	
<i>channel-group-number</i>	(Optional) Number of the channel group. Valid numbers range from 1 to 6.
detail	Display detailed EtherChannel information.
load-balance	Display the load-balance or frame-distribution scheme among ports in the port channel.
port	Display EtherChannel port information.
port-channel	Display port-channel information.
summary	Display a one-line summary per channel-group.
begin	(Optional) Display begins with the line that matches the <i>expression</i> .
exclude	(Optional) Display excludes lines that match the <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes User EXEC

Command History	Release	Modification
	12.1(6)EA2	This command was first introduced. It replaced the show port group command.
	12.1(14)EA1	The brief keyword was removed.

Usage Guidelines If you do not specify a *channel-group*, all channel groups appear. Expressions are case sensitive. For example, if you enter | **exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show etherchannel 1 detail** command:

```
Switch> show etherchannel 1 detail
Group state = L2
Ports: 1 Maxports = 8
Port-channels: 1 Max Port-channels = 1
                Ports in the group:
                -----
Port: Fa0/3
-----

Port state      = Down Not-in-Bndl
Channel group = 1          Mode = Automatic-S1      Gcchange = 0
Port-channel = null       GC   = 0x00000000      Pseudo port-channel = Po1
Port index     = 0          Load = 0x00

Flags: S - Device is sending Slow hello.  C - Device is in Consistent state.
      A - Device is in Auto mode.         P - Device learns on physical port.
      d - PAgP is down.

Timers: H - Hello timer is running.       Q - Quit timer is running.
       S - Switching timer is running.    I - Interface timer is running.

Local information:

Port      Flags State      Timers  Hello    Partner  PAgP    Learning  Group
Fa0/3    dA   U1/S1      1s      Interval Count  Priority Method  Ifindex
Age of the port in the current state: 10d:23h:07m:37s
                Port-channels in the group:
                -----

Port-channel: Po1
-----

Age of the Port-channel = 03d:02h:22m:43s
Logical slot/port = 1/0          Number of ports = 0
GC                = 0x00000000    HotStandBy port = null
Port state        = Port-channel Ag-Not-Inuse
```

This is an example of output from the **show etherchannel 1 summary** command:

```
Switch> show etherchannel 1 summary
Flags: D - down          P - in port-channel
      I - stand-alone s - suspended
      R - Layer3        S - Layer2
      u - unsuitable for bundling
      U - port-channel in use
      d - default port

Group Port-channel  Ports
-----+-----+-----
1      Po1(SU)      Fa0/6(Pd) Fa0/15(P)
```

This is an example of output from the **show etherchannel 1 port** command:

```
Switch> show etherchannel 1 port
      Ports in the group:
      -----
Port: Fa0/3
-----

Port state      = Down Not-in-Bndl
Channel group   = 1           Mode = Automatic-S1      Gcchange = 0
Port-channel    = null       GC   = 0x00000000      Pseudo port-channel = Po1
Port index      = 0           Load = 0x00

Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
        A - Device is in Auto mode.        P - Device learns on physical port.
        d - PAgP is down.

Timers: H - Hello timer is running.        Q - Quit timer is running.
        S - Switching timer is running.    I - Interface timer is running.

Local information:

Port      Flags State   Timers  Hello  Partner  PAgP   Learning  Group
Fa0/3    dA   U1/S1    1s      1s     0        200    Any       0

Age of the port in the current state: 10d:23h:13m:21s
```

Related Commands

Command	Description
channel-group	Assigns an Ethernet interface to an EtherChannel group.
interface port-channel	Accesses or creates the port channel.

show file

Use the **show file** privileged EXEC command to display a list of open file descriptors, file information, and file system information.

show file { **descriptors** | **information** { *device:* } *filename* | **systems** } [| { **begin** | **exclude** | **include** } *expression*]

Syntax Description

descriptors	Display a list of open file descriptors.
information	Display file information.
<i>device:</i>	Device containing the file. Valid devices include the switch Flash memory.
<i>filename</i>	Name of file.
systems	Display file system information.
begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .
exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5.2)WC(1)	This command was first introduced.
12.1(6)EA2	The descriptors and information keywords were added.

Usage Guidelines

File descriptors are the internal representations of open files. You can use this command to see if another user has a file open.

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

Examples

This is an example of output from the **show file descriptors** command:

```
Switch# show file descriptors
File Descriptors:
FD  Position  Open  PID  Path
0   187392    0001  2    tftp://temp/hampton/c2950g.a
1   184320    030A  2    flash:c2950-i-m.a
```

Table 2-16 describes the fields in the **show file descriptors** command output.

Table 2-16 show file descriptors Field Descriptions

Field	Description
FD	File descriptor. The file descriptor is a small integer used to specify the file once it has been opened.
Position	Byte offset from the start of the file.
Open	Flags supplied when opening the file.
PID	Process ID of the process that opened the file.
Path	Location of the file.

This is an example of output from the **show file information nvram:startup-config** command:

```
Switch# show file information nvram:startup-config
nvram:startup-config:
  type is ascii text
```

Table 2-17 lists the possible file types for the previous example.

Table 2-17 Possible File Types

Field	Description
ascii text	Configuration file or other text file.
coff	Runnable image in coff format.
ebcdic	Text generated on an IBM mainframe.
image (a.out)	Runnable image in a.out format.
image (elf)	Runnable image in elf format.
lzw compression	Lzw compressed file.
tar	Text archive file used by the CIP.

This is an example of output from the **show file systems** command:

```
Switch# show file systems
File Systems:

      Size(b)   Free(b)   Type  Flags  Prefixes
* 7741440     433152   flash  rw    flash:
  7741440     433152   unknown  rw    zflash:
    32768      25316   nvram   rw    nvram:
      -        -   network  rw    tftp:
      -        -   opaque   rw    null:
      -        -   opaque   rw    system:
      -        -   opaque   ro    xmodem:
      -        -   opaque   ro    ymodem:
      -        -   network  rw    rcp:
      -        -   network  rw    ftp:
```

For this example, [Table 2-18](#) describes the fields in the **show file systems** command output. [Table 2-19](#) lists the file system types. [Table 2-20](#) lists the file system flags.

Table 2-18 *show file systems Field Descriptions*

Field	Description
Size(b)	Amount of memory in the file system, in bytes.
Free(b)	Amount of free memory in the file system, in bytes.
Type	Type of file system.
Flags	Permissions for file system.
Prefixes	Alias for file system.

Table 2-19 *File System Types*

Field	Description
disk	The file system is for a rotating medium.
flash	The file system is for a Flash memory device.
network	The file system is a network file system, such as TFTP, rcp, or FTP.
nvrn	The file system is for an NVRAM device.
opaque	The file system is a locally generated <i>pseudo</i> file system (for example, the <i>system</i>) or a download interface, such as brimux.
rom	The file system is for a ROM or EPROM device.
tty	The file system is for a collection of terminal devices.
unknown	The file system is of unknown type.

Table 2-20 *File System Flags*

Field	Description
ro	The file system is Read Only.
wo	The file system is Write Only
rw	The file system is Read/Write.

show interfaces

Use the **show interfaces** privileged EXEC command to display the administrative and operational status of all interfaces or a specified interface.

```
show interfaces [interface-id | vlan vlan-id] [accounting | capabilities [module
  {module-number}] | cpe [port port-id] | description | etherchannel | flowcontrol | media
  [interface-id] | pruning | stats | status [err-disabled] | switchport | trunk] [ | {begin | exclude
  | include} expression]
```

Syntax Description

<i>interface-id</i>	(Optional) Valid interfaces include physical ports (including type, slot, and port number) and port channels. The valid port-channel range is 1 to 6.
vlan <i>vlan-id</i>	(Optional) VLAN ID. The valid VLAN range is 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1005 when the standard software image (SI) is installed.
accounting	(Optional) Display interface accounting information.
capabilities	(Optional) Display the capabilities of the ports.
cpe	(Optional) Display link status, speed, and duplex of all the customer premises equipment (CPE) Ethernet ports. This keyword is available only on Long-Reach Ethernet (LRE) switches. Note You must enter an interface ID to display this keyword.
port <i>port-id</i>	(Optional) Display only the designated CPE Ethernet port. Valid values are 1 to 4. This keyword is available only on LRE switches.
description	(Optional) Display the administrative status and description set for an interface.
etherchannel	(Optional) Display interface EtherChannel information.
flowcontrol	(Optional) Display interface flowcontrol information.
media [<i>interface-id</i>]	(Optional) Display the type of media connection. This keyword is available only on LRE switches.
pruning	(Optional) Display interface trunk VTP pruning information.
stats	(Optional) Display the input and output packets by switching path for the interface.
status	(Optional) Display the status of the interface.
err-disabled	(Optional) Display interfaces in error-disabled state.
switchport	(Optional) Display the administrative and operational status of a switching (nonrouting) port.
trunk	Display interface trunk information. If you do not specify an interface, information for only active trunking ports appears.
begin	(Optional) Display begins with the line that matches the <i>expression</i> .
exclude	(Optional) Display excludes lines that match the <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
module <i>module-number</i>	(Optional) The module or interface number. If you do not specify a module number, the information appears for all ports.
<i>expression</i>	Expression in the output to use as a reference point.

**Note**

Though visible in the command-line help strings, the **crb**, **fair-queue**, **irb**, **mac-accounting**, **precedence**, **random-detect**, **rate-limit**, and **shape** options are not supported.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5.2)WC(1)	This command was first introduced.
12.1(11)YJ	The cpe , port <i>port-id</i> , and media keywords were added.
12.1(12c)EA1	The capabilities keyword was added.

Usage Guidelines

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

Examples

This is an example of output from the **show interfaces accounting** command:

```
Switch# show interfaces accounting
Vlan1
      Protocol  Pkts In   Chars In   Pkts Out   Chars Out
      IP        17950     2351279    3205       411175
      ARP        8626     552064     62         3720
Interface Vlan5 is disabled

FastEthernet0/1
      Protocol  Pkts In   Chars In   Pkts Out   Chars Out
Spanning Tree 2956958   179218508  34383      2131700
      CDP        14301     5777240    14307      5722418
      VTP         0         0          1408      145908
      DTP        28592     1572560    0          0

<output truncated>
```

This is an example of output from the **show interfaces capabilities** command:

```
Switch# show interfaces fastethernet0/1 capabilities
FastEthernet0/1
  Model:                WS-C2950G-48-EI
  Type:                 10/100BaseTX
  Speed:                10,100,auto
  Duplex:               half,full,auto
  UDLD:                 yes
  Trunk encap. type:    802.1Q
  Trunk mode:           on,off,desirable,nonegotiate
  Channel:              yes
  Broadcast suppression: percentage(0-100)
  Flowcontrol:          rx-(none),tx-(none)
  Fast Start:           yes
  CoS rewrite:          yes
```

```

ToS rewrite:          yes
Inline power:         no
SPAN:                 source/destination
PortSecure:          Yes
Dot1x:                Yes

```

This is an example of output from the **show interfaces gigabitethernet0/1** command:

```

Switch# show interfaces gigabitethernet0/1
FastEthernet0/1 is up, line protocol is down
  Hardware is Fast Ethernet, address is 0005.7428.09c1 (bia 0005.7428.09c1)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, Auto-speed
  input flow-control is off, output flow-control is off
  Last input never, output 4d21h, output hang never
  Last clearing of "show interface" counters never
  Input queue:0/75/0/0 (size/max/drops/flushes); Total output drops:0
  Queueing strategy:fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    1 packets input, 64 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 0 multicast, 0 pause input
    0 input packets with dribble condition detected
    1 packets output, 64 bytes, 0 underruns
    0 output errors, 0 collisions, 2 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier, 0 PAUSE output
    0 output buffer failures, 0 output buffers swapped out

```

This is an example of output from the **show interfaces gigabitethernet0/2 description** command when the interface has been described as *Connects to Marketing* by using the **description** interface configuration command.

```

Switch# show interfaces gigabitethernet0/2 description
Interface Status      Protocol Description
G10/2 up              down      Connects to Marketing

```

This is an example of output from the **show interfaces fastethernet0/1 pruning** command when pruning is enabled in the VTP domain:

```

Switch# show interfaces fastethernet0/1 pruning

Port      Vlans pruned for lack of request by neighbor
Fa0/1     4,196

Port      Vlan traffic requested of neighbor
Fa0/1     1,4

```

This is an example of output from the **show interfaces stats** command:

```
Switch# show interfaces stats
Vlan1
      Switching path  Pkts In   Chars In   Pkts Out   Chars Out
      Processor       3224706   223689126  3277307    280637322
      Route cache     0         0          0          0
      Total           3224706   223689126  3277307    280637322
Interface Vlan5 is disabled

FastEthernet0/1
      Switching path  Pkts In   Chars In   Pkts Out   Chars Out
      Processor       3286423   231672787  179501     17431060
      Route cache     0         0          0          0
      Total           3286423   231672787  179501     17431060
```

This is an example of output from the **show interfaces status** command. It displays the status of all interfaces.

```
Switch# show interfaces status

Port    Name           Status      Vlan      Duplex  Speed  Type
Fa0/1   Fa0/1         notconnect  1         auto    auto   10/100BaseTX
Fa0/2   Fa0/2         notconnect  1         auto    auto   10/100BaseTX
Fa0/3   Fa0/3         disabled    100       auto    auto   10/100BaseTX
Fa0/4   Fa0/4         connected   trunk     a-full  a-100  10/100BaseTX
Fa0/5   Fa0/5         notconnect  1         auto    auto   10/100BaseTX
Fa0/6   Fa0/6         connected   trunk     a-full  a-100  10/100BaseTX
Fa0/7   Fa0/7         notconnect  1         auto    auto   10/100BaseTX
Fa0/8   Fa0/8         connected   1         a-full  a-100  10/100BaseTX
Fa0/9   Fa0/9         disabled    1         auto    auto   10/100BaseTX
Fa0/10  Fa0/10        notconnect  5         auto    100    10/100BaseTX
Fa0/11  Fa0/11        disabled    1         auto    auto   10/100BaseTX
Fa0/12  Fa0/12        disabled    1         auto    auto   10/100BaseTX
Gi0/1   Gi0/1         disabled    1         auto    auto   unknown
Gi0/2   Gi0/2         notconnect  1         auto    auto   unknown
Po1     Po1           notconnect  1         auto    auto
```

This is an example of output from the **show interfaces status err-disabled** command. It displays the status of interfaces in error-disabled state.

```
switch# show interfaces fastethernet0/15 status err-disabled

Port    Name           Status      Reason
Fa0/15  Fa0/15        err-disabled psecure-violation
```

This is an example of output from the **show interfaces etherchannel** command when port channels are configured on the switch:

```
Switch# show interfaces etherchannel
----
FastEthernet0/1:
Port state      = Up Mstr In-Bndl
Channel group   = 1           Mode = On/FEC      Gcchange = 0
Port-channel    = Po1          GC   = 0x00010001  Pseudo port-channel = Po1
Port index      = 0           Load = 0x00
```

```

Age of the port in the current state:00d:00h:06m:54s
----
Port-channel1:
Age of the Port-channel   = 09d:22h:45m:14s
Logical slot/port        = 1/0             Number of ports = 1
GC                       = 0x00010001     HotStandBy port = null
Port state                = Port-channel Ag-Inuse

Ports in the Port-channel:

Index  Load  Port    EC state
-----+-----+-----+-----
  0     00   Fa0/1   on

Time since last port bundled:  00d:00h:06m:54s   Fa0/1

```

This is an example of output from the **show interfaces flowcontrol** command. [Table 2-21](#) lists the fields in this display.

```

Switch# show interfaces flowcontrol
Port      Send FlowControl  Receive FlowControl  RxPause TxPause
         admin   oper    admin   oper
-----
Fa0/1     Unsupp.  Unsupp.  off     off     0       0
Fa0/2     Unsupp.  Unsupp.  off     off     0       0
<output truncated>
Gi0/1     desired  off      off     off     0       0
Gi0/2     desired  off      off     off     0       0
Po1       Unsupp.  Unsupp.  off     off     0       0
Po2       Unsupp.  Unsupp.  off     off     0       0

```

Table 2-21 show interfaces flowcontrol Field Descriptions

Field	Description
Port	Displays the port name.
Send FlowControl	
Admin	Displays the administrative (configured) setting for the flow control send mode.
Oper	Displays the operational (running) setting for the flow control send mode.
Receive FlowControl	
Admin	Displays the administrative (configured) setting for the flow control receive mode.
Oper	Displays the operational (running) setting for the flow control receive mode.
RxPause	Displays the number of pause frames received.
TxPause	Displays the number of pause frames sent.
On	Flow control is enabled.
Off	Flow control is disabled.
Desired	Flow control is enabled if the other end supports it.
Unsupp.	Flow control is not supported.

This is an example of output from the **show interfaces switchport** command for a single interface. [Table 2-22](#) describes the fields in the output.

```
Switch# show interfaces gigabitethernet0/1 switchport
Name: Gi0/1
Switchport:Enabled
Administrative Mode:dynamic desirable
Operational Mode:static access
Administrative Trunking Encapsulation:negotiate
Negotiation of Trunking:On
Access Mode VLAN:1 (default)
Trunking Native Mode VLAN:1 (default)
Voice VLAN:none
Administrative private-vlan host-association:none
Administrative private-vlan mapping:none
Operational private-vlan:none
Trunking VLANs Enabled:ALL
Pruning VLANs Enabled:2-1001
Capture Mode: Disabled
Capture VLANs Allowed:ALL

Protected:true
Unknown unicast blocked:disabled
Unknown multicast blocked:disabled

Voice VLAN:none (Inactive)
Appliance trust:none
```

Table 2-22 *show interfaces switchport Field Descriptions*

Field	Description
Name	Displays the port name.
Switchport	Displays the administrative and operational status of the port. In this output, the port is in switchport mode.
Administrative Mode Operational Mode	Displays the administrative and operational mode.
Administrative Trunking Encapsulation Negotiation of Trunking	Displays the administrative and operational encapsulation method, and whether trunking negotiation is enabled.
Access Mode VLAN	Displays the VLAN ID to which the port is configured.
Trunking Native Mode VLAN Trunking VLANs Enabled Trunking VLANs Active	Lists the VLAN ID of the trunk that is in native mode. Lists the allowed VLANs on the trunk. Lists the active VLANs on the trunk.
Pruning VLANs Enabled	Lists the VLANs that are pruning-eligible.
Administrative private-vlan host-association Administrative private-vlan mapping Operational private-vlan	Displays the administrative and operational status of the private VLAN, and displays the private-VLAN mapping.

Table 2-22 show interfaces switchport Field Descriptions (continued)

Field	Description
Capture Mode Captured VLANs Allowed	Displays the capture mode and the number of captured VLANs allowed. Note Because the switch does not support the capture feature, the values for these fields do not change.
Protected	Displays whether or not protected port is enabled (True) or disabled (False) on the interface.
Voice VLAN	Displays the VLAN ID on which voice VLAN is enabled.
Appliance trust	Displays the class of service (CoS) setting of the data packets of the IP phone.

This is an example of output from the **show interfaces trunk** command:

```
Switch# show interfaces trunk

Port      Mode      Encapsulation  Status      Native vlan
Fa0/4     on        802.1q         trunking    1
Fa0/6     on        802.1q         trunking    1

Port      Vlans allowed on trunk
Fa0/4     1-4094
Fa0/6     1-4094

Port      Vlans allowed and active in management domain
Fa0/4     1-2,51-52
Fa0/6     1-2,51-52

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/4     1
Fa0/6     1-2,51-52
```

This is an example of output from the **show interfaces fastethernet0/1 trunk** command. It displays trunking information for the interface.

```
Switch# show interfaces fastethernet0/1 trunk

Port      Mode      Encapsulation  Status      Native vlan
Fa0/1     desirable 802.1q         trunking    1

Port      Vlans allowed on trunk
Fa0/1     1-4094

Port      Vlans allowed and active in management domain
Fa0/1     1,4,196,306

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     1,306
```

This is an example of output from the **show interfaces** command for LRE port 5 on an LRE switch:

```
Switch# show interfaces longreachethernet0/5
LongReachEthernet0/5 is up, line protocol is up
  Hardware is Ethernet over LRE, address is 0006.2871.5902 (bia 0006.2871.5902)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not set
  Half-duplex, Auto Speed (10), 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:21, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    8272 packets input, 852898 bytes, 0 no buffer
    Received 1182 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 1182 multicast
    0 input packets with dribble condition detected
  61899 packets output, 17981033 bytes, 0 underruns
  0 output errors, 0 collisions, 1 interface resets
  0 babbles, 0 late collision, 0 deferred
  0 lost carrier, 0 no carrier
  0 output buffer failures, 0 output buffers swapped out
```

This is an example of output from the **show interfaces** command for all interfaces on a CPE device:

```
Switch# show interfaces longreachethernet0/2 cpe
```

Port	Status	Speed	Duplex
1	notconnected	auto	NA
2	notconnected	auto	NA
3	notconnected	auto	NA
4	notconnected	auto	NA
5	connected	100	half

```
Switch#
```

This is an example of output from the **show interfaces** command for port 5 on a CPE device:

```
Switch# show interfaces longreachethernet0/2 cpe port 5
```

Port	Status	Speed	Duplex
5	connected	100	half

```
Switch#
```

This is an example of output from the **show interfaces media** command on an interface:

```
Switch# show interfaces gigabitethernet0/1 media
```

Port	Media-configured	Active	Attached
Gi0/1	auto-select	rj45	1000BaseSX-10/100/1000BaseTX

```
Switch#
```

This is an example of output from the **show interfaces media** command:

```
Switch# show interfaces media
```

```
Port      Media-configured  Active      Attached
Gi0/1     auto-select       rj45        1000BaseSX-10/100/1000BaseTX
Gi0/2     prefer-sfp        sfp         1000BaseSX-10/100/1000BaseTX
```

Related Commands

Command	Description
switchport access	Configures a port as a static-access or dynamic-access port.
switchport protected	Isolates Layer 2 unicast, multicast, and broadcast traffic from other protected ports on the same switch.
switchport trunk pruning	Configures the VLAN pruning-eligible list for ports in trunking mode.

show interfaces counters

Use the **show interfaces counters** privileged EXEC command to display various counters for a specific interface or for all interfaces.

```
show interfaces [interface-id | vlan vlan-id] counters [broadcast | errors | multicast | trunk | unicast] [ | {begin | exclude | include} expression]
```

Syntax Description		
<i>interface-id</i>	(Optional) ID of the physical interface, including type and slot and port number.	
vlan <i>vlan-id</i>	(Optional) VLAN number of the management VLAN. Valid IDs are from 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1001 when the standard software image (SI) is installed.	
broadcast	(Optional) Display discarded broadcast traffic.	
errors	(Optional) Display error counters.	
multicast	(Optional) Display discarded multicast traffic.	
trunk	(Optional) Display trunk counters.	
unicast	(Optional) Display discarded unicast traffic.	
begin	(Optional) Display begins with the line that matches the <i>expression</i> .	
exclude	(Optional) Display excludes lines that match the <i>expression</i> .	
include	(Optional) Display includes lines that match the specified <i>expression</i> .	
<i>expression</i>	Expression in the output to use as a reference point.	

Command Modes Privileged EXEC

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

Usage Guidelines If you do not enter any keywords, all counters for all interfaces are included. Expressions are case sensitive. For example, if you enter | **exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show interfaces counters** command. It displays all the counters for the switch. [Table 2-23](#) describes the fields in the output.

```
Switch# show interfaces counters
Port          InOctets    InUcastPkts  InMcastPkts  InBcastPkts
Gi0/1         23324617    10376        185709       126020
Gi0/2         0           0            0            0

Port          OutOctets    OutUcastPkts  OutMcastPkts  OutBcastPkts
Gi0/1         4990607     28079        21122        10
Gi0/2         1621568     25337        0            0
```

Table 2-23 show interfaces counters Field Descriptions

Field	Description
InOctets	Displays the number of bytes received on an interface.
InUcastPkts	Displays the number of unicast packets received on an interface.
InMcastPkts	Displays the number of multicast packets received on an interface.
InBcastPkts	Displays the number of broadcast packets received on the interface.
OutOctets	Displays the number of bytes sent on an interface.
OutUcastPkts	Displays the number of unicast packets sent on an interface.
OutMcastPkts	Displays the number of multicast packets sent on an interface.
OutBcastPkts	Displays the number of broadcast packets sent on an interface.

This is an example of output from the **show interfaces counters broadcast** command. It displays the dropped broadcast traffic for all interfaces. The *BcastSuppDiscards* field displays the number of broadcast packets dropped on the interface because of broadcast suppression.

```
Switch# show interfaces counters broadcast
Port          BcastSuppDiscards
Gi0/1         1
Gi0/2         0
```

This is an example of output from the **show interfaces gigabitethernet0/1 counters broadcast** command. It displays the dropped broadcast traffic for an specific interface.

```
Switch# show interfaces gigabitethernet0/1 counters broadcast

Port          BcastSuppDiscards
Gi0/1         0
```

This is an example of output from the **show interfaces counters errors** command. It displays the interface error counters for all interfaces. [Table 2-24](#) describes the fields in the output.

```
Switch# show interfaces counters errors

Port          Align-Err    FCS-Err    Xmit-Err    Rcv-Err    UnderSize
Gi0/1         0           0          0           0          0
Gi0/2         0           0          0           0          0

Port          Single-Col  Multi-Col  Late-Col  Excess-Col  Carri-Sen  Runts  Giants
Gi0/1         0          0          0         0           0          0      0
Gi0/2         0          0          0         0           0          0      0
```

Table 2-24 *show interfaces counters errors Field Descriptions*

Field	Description
Align-Err	Displays the total number of frames that are received on an interface and have alignment errors.
FCS-Err	Displays the total number of frames that are received on an interface, have a valid length (in bytes), but do not have the correct FCS ¹ values.
Xmit-Err	Displays the total number of frames that have errors during transmission.
Rcv-Err	Displays the total number of frames that are received on an interface and have errors.
Undersize	Displays the total number of frames received that are less than 64 bytes (including the FCS bits and excluding the frame header) and have either an FCS or an alignment error.
Single-col	Displays the total number of frames that are successfully sent on an interface after one collision occurs.
Multi-col	Displays the total number of frames that are successfully sent on an interface after more than one collision occurs.
Late-col	After a frame is sent, displays the number of times that a collision is detected on an interface after 512 bit times.
Excess-col	Display the number of frames that could not be sent on an interface because more than 16 collisions occurs.
Carri-Sen	Displays the number of occurrences in which the interface detects a false carrier when frames are not sent or received.
Runts	Displays the number of frames received on an interface that are smaller than 64 bytes and have an invalid FCS value.
Giants	Displays the number of frames that are larger than the maximum allowed frame size and have a valid FCS value.

1. FCS = frame check sequence

This is an example of output from the **show interfaces counters multicast** command. It displays the dropped multicast traffic for all interfaces. The *McastSuppDiscards* displays the number of multicast packets dropped on the interface because of multicast suppression.

```
Switch# show interfaces counters multicast
```

```
Port      McastSuppDiscards
Gi0/1    0
Gi0/2    0
```

This is an example of output from the **show interfaces counters trunk** command. It displays the trunk counters for all interfaces. [Table 2-25](#) describes the fields in the output.

```
Switch# show interfaces counters trunk

Port          TrunkFramesTx  TrunkFramesRx  WrongEncap
Gi0/1         0              0              0
Gi0/2         0              0              0
```

Table 2-25 *show interfaces counters trunk Field Descriptions*

Field	Description
TrunkFrameTx	Displays the number of frames sent on a trunk interface.
TrunkFrameRx	Displays the number of frames received on a trunk interface.
WrongEncap	Displays the number of frames that are received on an interface and have the incorrect encapsulation type.

This is an example of output from the **show interfaces counters unicast** command. It displays the dropped unicast traffic for all interfaces. The *UcastSuppDiscards* field displays the number of unicast packets dropped on the interface because of unicast suppression.

```
Switch# show interfaces counters unicast

Port          UcastSuppDiscards
Gi0/1         6872
Gi0/2         0
```

Related Commands

Command	Description
show interfaces	Displays interface characteristics.
storm-control	Configures broadcast, multicast, and unicast storm control for an interface.

show ip access-lists

Use the **show ip access-lists** privileged EXEC command to display IP access control lists (ACLs) configured on the switch.

```
show ip access-lists [name | number] [ | {begin | exclude | include} expression]
```

Syntax Description	
<i>name</i>	(Optional) ACL name.
<i>number</i>	(Optional) ACL number. The range is from 1 to 199 and from 1300 to 2699.
 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes Privileged EXEC

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

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

Examples This is an example of output from the **show ip access-lists** command:

```
Switch# show ip access-lists
Standard IP access list testingacl
  permit 10.10.10.2
Standard IP access list wizard_1-1-1-2
  permit 1.1.1.2
Extended IP access list 103
  permit tcp any any eq www
Extended IP access list CMP-NAT-ACL
  Dynamic Cluster-HSRP deny ip any any
  Dynamic Cluster-NAT permit ip any any
  permit ip host 10.245.155.128 any
  permit ip host 10.245.137.0 any
  permit ip host 10.146.106.192 any
  permit ip host 10.216.25.128 any
  permit ip host 10.228.215.0 any
  permit ip host 10.221.111.64 any
  permit ip host 10.123.222.192 any
  permit ip host 10.169.110.128 any
  permit ip host 10.186.122.64 any
```

This is an example of output from the **show ip access-lists 103** command:

```
Switch# show ip access-lists 103
Extended IP access list 103
  permit tcp any any eq www
```

Related Commands

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

show ip dhcp snooping

Use the **show ip dhcp snooping** privileged EXEC command to display the Dynamic Host Configuration Protocol (DHCP) snooping configuration.

show ip dhcp snooping

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(19)EA1	This command was first introduced

Examples This is an example of output from the **show ip dhcp snooping** command.

```
Switch# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
40-42
Insertion of option 82 is enabled
Interface                Trusted      Rate limit (pps)
-----                -
FastEthernet0/5          yes         unlimited
FastEthernet0/7          yes         unlimited
FastEthernet0/3          no          5000
FastEthernet0/5          yes         unlimited
FastEthernet0/7          yes         unlimited
FastEthernet0/5          yes         unlimited
FastEthernet0/7          yes         unlimited
```

Related Commands	Command	Description
	show ip dhcp snooping binding	Displays the DHCP snooping binding information.

show ip dhcp snooping binding

Use the **show ip dhcp snooping binding** privileged EXEC command to display the Dynamic Host Configuration Protocol (DHCP) snooping binding table and configuration information for all interfaces on a switch.

```
show ip dhcp snooping binding [ip-address] [mac-address] [dynamic] [interface interface-id]
[static] [vlan vlan-id] [ | {begin | exclude | include} expression]
```

Syntax Description	
<i>ip-address</i>	(Optional) Specify the binding entry IP address.
<i>mac-address</i>	(Optional) Specify the binding entry MAC address.
dynamic	(Optional) Specify the dynamic binding entry.
interface <i>interface-id</i>	(Optional) Specify the binding input interface.
static	(Optional) Specify the static binding entry.
vlan <i>vlan-id</i>	(Optional) Specify the binding entry VLAN.
begin	Display begins with the line that matches the <i>expression</i> .
exclude	Display excludes lines that match the <i>expression</i> .
include	Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(19)EA1	This command was first introduced

Examples This example shows how to display the DHCP snooping binding entries for a switch.

```
Switch# show ip dhcp snooping binding
MacAddress      IpAddress      Lease(sec)  Type           VLAN  Interface
-----
00:30:94:C2:EF:35  41.0.0.51      286         dynamic        41    FastEthernet0/3
00:D0:B7:1B:35:DE  41.0.0.52      237         dynamic        41    FastEthernet0/3
00:00:00:00:00:01  40.0.0.46      286         dynamic        40    FastEthernet0/9
00:00:00:00:00:03  42.0.0.33      286         dynamic        42    FastEthernet0/9
00:00:00:00:00:02  41.0.0.53      286         dynamic        41    FastEthernet0/9
```

This example shows how to display the DHCP snooping binding entries for a specific IP address.

```
Switch#show ip dhcp snooping binding 41.0.0.51
MacAddress      IpAddress      Lease(sec)  Type           VLAN  Interface
-----
00:30:94:C2:EF:35  41.0.0.51      285         dynamic        41    FastEthernet0/3
```

show ip dhcp snooping binding

This example shows how to display the DHCP snooping binding entries for a specific MAC address.

```
Switch#show ip dhcp snooping binding 0030.94c2.ef35
-----
MacAddress      IPAddress      Lease(sec)    Type          VLAN  Interface
-----
00:30:94:C2:EF:35  41.0.0.51     279           dynamic       41    FastEthernet0/3
```

This example shows how to display the DHCP snooping dynamic binding entries on a switch.

```
Switch#show ip dhcp snooping binding dynamic
-----
MacAddress      IPAddress      Lease(sec)    Type          VLAN  Interface
-----
00:30:94:C2:EF:35  41.0.0.51     286           dynamic       41    FastEthernet0/3
00:D0:B7:1B:35:DE  41.0.0.52     296           dynamic       41    FastEthernet0/3
00:00:00:00:00:01  40.0.0.46     46            dynamic       40    FastEthernet0/9
00:00:00:00:00:03  42.0.0.33     46            dynamic       42    FastEthernet0/9
00:00:00:00:00:02  41.0.0.53     46            dynamic       41    FastEthernet0/9
```

This example shows how to display the DHCP snooping binding entries on Fast Ethernet interface 0/3.

```
Switch#show ip dhcp snooping binding interface f2/0/3
-----
MacAddress      IPAddress      Lease(sec)    Type          VLAN  Interface
-----
00:30:94:C2:EF:35  41.0.0.51     290           dynamic       41    FastEthernet0/3
00:D0:B7:1B:35:DE  41.0.0.52     270           dynamic       41    FastEthernet0/3
```

This example shows how to display the DHCP snooping binding entries on VLAN 41.

```
Switch#show ip dhcp snooping binding vlan 41
-----
MacAddress      IPAddress      Lease(sec)    Type          VLAN  Interface
-----
00:30:94:C2:EF:35  41.0.0.51     274           dynamic       41    FastEthernet0/3
00:D0:B7:1B:35:DE  41.0.0.52     165           dynamic       41    FastEthernet0/3
00:00:00:00:00:02  41.0.0.53     65            dynamic       41    FastEthernet0/9
```

Related Commands

Command	Description
show ip dhcp snooping	Displays the DHCP snooping configuration.

show ip igmp profile

Use the **show ip igmp profile** privileged EXEC command to view all configured Internet Group Management Protocol (IGMP) profiles or a specified IGMP profile.

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

Syntax Description	
<i>profile number</i>	(Optional) The IGMP profile number to be displayed. The range is from 1 to 4294967295. If no profile number is entered, all IGMP profiles appear.
begin	(Optional) Display begins with the line that matches the <i>expression</i> .
exclude	(Optional) Display excludes lines that match the <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes Privileged EXEC

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

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

Examples These are examples of output from the **show ip igmp profile** privileged EXEC command, with and without specifying a profile number. If no profile number is entered, the display includes all profiles configured on the switch.

```
Switch# show ip igmp profile 40
IGMP Profile 40
  permit
  range 233.1.1.1 233.255.255.255

Switch# show ip igmp profile
IGMP Profile 3
  range 230.9.9.0 230.9.9.0
IGMP Profile 4
  permit
  range 229.9.9.0 229.255.255.255
```

Related Commands	Command	Description
	ip igmp profile	Configures the specified IGMP profile number.

show ip igmp snooping

Use the **show ip igmp snooping** user EXEC command to display the Internet Group Management Protocol (IGMP) snooping configuration of the switch or the VLAN. Use the **mrouter** keyword to display the dynamically learned and manually configured multicast router ports.

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

Syntax Description

group	(Optional) Display information about the IGMP multicast groups, the compatibility mode, and the ports that are associated with each group.
mrouter	(Optional) Display multicast router ports.
querier	(Optional) Display information about the IGMP version that an interface supports.
vlan <i>vlan-id</i>	(Optional) Keyword and variable to specify a VLAN; valid values are 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1001 when the standard software image (SI) is installed. This keyword is available only in privileged EXEC mode.
 begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.0(5.2)WC(1)	This command was introduced.
12.1(19)EA1	The group and querier keywords were added.

Usage Guidelines

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

You can also use the **show mac address-table multicast** privileged EXEC command to display entries in the MAC address table for a VLAN that has IGMP snooping enabled.

When multicast VLAN registration (MVR) is enabled, use the **show ip igmp snooping mrouter** command to display MVR multicast router information and IGMP snooping information.

Use the **group** keyword to display the multicast groups, the compatibility mode, and the ports that are associated with each group.

Use the **querier** keyword to display the IGMP version and ports that are associated with a multicast IP address.

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

Examples

This is an example of output from the **show ip igmp snooping** command:

```
Switch> show ip igmp snooping
Global IGMP Snooping configuration:
-----
IGMP snooping           : Enabled
IGMPv3 snooping (minimal) : Enabled
Report suppression      : Enabled
TCN solicit query       : Disabled
TCN flood query count    : 2

Vlan 1:
-----
IGMP snooping           : Enabled
Immediate leave         : Disabled
Multicast router learning mode : pim-dvmrp
Source only learning age timer : 10
CGMP interoperability mode : IGMP_ONLY

Vlan 2:
-----
IGMP snooping           : Enabled
Immediate leave         : Disabled
Multicast router learning mode : pim-dvmrp
Source only learning age timer : 10
CGMP interoperability mode : IGMP_ONLY

<output truncated>
```

This is an example of output from the **show ip igmp snooping vlan 1** command:

```
Switch# show ip igmp snooping vlan 1
Global IGMP Snooping configuration:
-----
IGMP snooping           : Enabled
IGMPv3 snooping (minimal) : Enabled
Report suppression      : Enabled
TCN solicit query       : Disabled
TCN flood query count    : 2

Vlan 1:
-----
IGMP snooping           : Enabled
Immediate leave         : Disabled
Multicast router learning mode : pim-dvmrp
Source only learning age timer : 10
CGMP interoperability mode : IGMP_ONLY
```

This is an example of output from the **show ip igmp snooping mrouter vlan 1** command:

**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)
```

This is an example of output from the **show ip igmp snooping group vlan 1** command:

```
Switch# show ip igmp snooping group vlan 1
Vlan      Group      Version    Port List
-----
1         229.2.3.4   v3         fa0/1 fa0/3
1         224.1.1.1   v2         fa0/8
```

This is an example of output from the **show ip igmp snooping querier** command:

```
Switch> show ip igmp snooping querier
Vlan      IP Address  IGMP Version  Port
-----
1         172.20.50.11 v3            fa0/1
2         172.20.40.20 v2            Router
```

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping.
ip igmp snooping report-suppression	Enables IGMP report suppression.
ip igmp snooping source-only-learning	Enables IP multicast-source-only learning on the switch.
ip igmp snooping source-only-learning age-timer	Enables and configures the aging time of the forwarding-table entries that the switch learns by using the source-only learning method.
ip igmp snooping vlan <i>vlan-id</i>	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 lacp

Use the **show lacp** user EXEC command to display Link Aggregation Control Protocol (LACP) channel-group information.

```
show lacp {channel-group-number {counters | internal | neighbor} | {counters | internal |
neighbor | sys-id}} [ | {begin | exclude | include} expression]
```

Syntax Description

<i>channel-group-number</i>	(Optional) Number of the channel group. Valid numbers range from 1 to 6.
counters	Display traffic information.
internal	Display internal information.
neighbor	Display neighbor information.
sys-id	Display the system identifier that is being used by LACP. The system identifier is made up of the LACP system priority and a MAC address.
 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(12c)EA1	This command was first introduced.

Usage Guidelines

You can enter any **show lacp** command to display the active port-channel information. To display the nonactive information, enter the **show lacp** command with a group number.

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

Examples

This is an example of output from the **show lacp counters** command:

```
Switch> show lacp counters
LACPDUs      Marker      Marker Response      LACPDUs
Port         Sent   Recv   Sent   Recv   Sent   Recv   Pkts Err
-----
Channel group:1
Fa0/5        19     10     0     0     0     0     0
Fa0/6        14     6      0     0     0     0     0
Fa0/7         8     7      0     0     0     0     0
```

This is an example of output from the **show lacp 1 internal** command:

```
Switch> show lacp internal
Flags: S - Device is sending Slow LACPDUs F - Device is sending Fast LACPDUs
       A - Device is in Active mode       P - Device is in Passive mode

Channel group 1

Port      Flags  State  LACP port  Admin  Oper  Port  Port
Fa0/5    SP    indep  32768      0x1    0x1    0x4    0x7C
Fa0/6    SP    indep  32768      0x1    0x1    0x5    0x7C
Fa0/7    SP    down   32768      0x1    0x1    0x6    0xC
```

This is an example of output from the **show lacp neighbor** command:

```
Switch> show lacp neighbor

Flags: S - Device is sending Slow LACPDUs F - Device is sending Fast LACPDUs
       A - Device is in Active mode       P - Device is in Passive mode

Channel group 1 neighbors

Partner's information:

Port      Partner
System ID  System ID  Partner
Port Number  Age  Partner
Fa0/5    00000,0000.0000.0000  0x0  85947s  SP

LACP Partner  Partner
Port Priority  Oper Key  Port State
0              0x0      0x0

Partner's information:

Port      Partner
System ID  System ID  Partner
Port Number  Age  Partner
Fa0/6    00000,0000.0000.0000  0x0  86056s  SP

LACP Partner  Partner
Port Priority  Oper Key  Port State
0              0x0      0x0

Partner's information:

Port      Partner
System ID  System ID  Partner
Port Number  Age  Partner
Fa0/7    00010,0008.a343.b580  0x6  86032s  SA

LACP Partner  Partner
Port Priority  Oper Key  Port State
32768         0x1      0x35
```

This is an example of output from the **show lacp sys-id** command:

```
Switch> show lacp sys-id
32765,0002.4b29.3a00
```

Related Commands

Command	Description
clear lacp	Clears LACP channel-group information.

show lre upgrade

Use the **show lre upgrade binaries** privileged EXEC command to display the upgrade information for the Long-Reach Ethernet (LRE) switch.

```
show lre upgrade {binaries | status | version} [ | {begin | exclude | include} expression]
```

This command is available only on Catalyst 2950 LRE switches.

Syntax Description	Parameter	Description
	binaries	Display the LRE binaries present on the system Flash memory.
	status	Display the upgrade status on all ports in the switch.
	version	Display the version of binaries on local and remote ends of an LRE link.
	 begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .
	 exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .
	 include	(Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.

Command Modes Privileged EXEC

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

Usage Guidelines Use the **show lre upgrade binaries** command to display the LRE binary information for each interface. The command output shows the path to the LRE binaries, which are always in the same directory as the Cisco IOS image. LRE binary file names consist of:

- The device family. A device family could be an LRE switch or a customer premises equipment (CPE) device.
- The function of the firmware, such as an upgrade for an application, the bootloader, or for the LRE chipset.
- The firmware version.

Files marked with an exclamation point (!) are version description files. A version description file is only for informational purposes and is not a candidate for upgrade. Version description files are used to determine whether or not a CPE device on an LRE link is running a supported LRE binary version.

Use the **show lre upgrade status** command during LRE upgrades to display both the local and remote upgrade status levels in progress on an LRE link. Status levels are:

- None—An upgrade is not in progress.
- Pending—An upgrade is initialized, but transfer has not begun.
- Active—Data transfer is in progress.
- Cmplt—An upgrade is complete.

When an upgrade is running on an LRE switch controller, the status for the controller does not change from *active* to *cmplt* until all hardware elements finish upgrading.

Other information displayed includes the local current (lcl curr) and proposed configuration (cfg) for each LRE interface. File names consist of:

- The device family. A device family could be an LRE switch or a CPE device.
- The function of the firmware, such as an upgrade for an application, for the bootloader, or for the LRE or CPE chipsets.
- The firmware version.

During data transfer but before the upgrade completes, the status also shows the time in hours and minutes that the upgrade has been in progress and the number of attempts that were made.

The **show lre upgrade version** command displays the LRE binary version for each interface. It shows local current (lcl curr) and proposed configuration (cfg) for each LRE interface. File names consist of:

- The device family
- The function of the firmware, such as an upgrade for an application, for the bootloader, or for the LRE chipsets of a CPE device
- The firmware version

Examples

This example shows output from the **show lre upgrade binaries** command:

```
Switch# show lre upgrade binaries
Path containing LRE binaries is flash:/c2950lre-i612q4-mz.121-0.18.YJ/lre-bin;
zflash:/c2950lre-i612q4-mz.121-0.18.YJ/lre-bin

LRE Binary: CISCO585-LRE_vdslsngl_51.00.00,
Flash file name: CISCO585-LRE_vdslsngl_51.00.00.bin

LRE Binary: CISCO585-LRE_MC8051boot_01.03.00,
Flash file name: CISCO585-LRE_MC8051boot_01.03.00.bin!

LRE Binary: CISCO585-LRE_MC8051boot_01.02.00,
Flash file name: CISCO585-LRE_MC8051boot_01.02.00.bin!

LRE Binary: CISCO585-LRE_MC8051appl_01.03.00,
Flash file name: CISCO585-LRE_MC8051appl_01.03.00.bin!

LRE Binary: CISCO585-LRE_MC8051appl_01.02.00,
Flash file name: CISCO585-LRE_MC8051appl_01.02.00.bin!

LRE Binary: CISCO575-LRE_vdslsngl_50.00.00,
Flash file name: CISCO575-LRE_vdslsngl_50.00.00.bin

LRE Binary: CISCO2950-LRE_vdslotl_02.60.00,
Flash file name: CISCO2950-LRE_vdslotl_02.60.00.bin

LRE Binary: CISCO2950-LRE_vdslotl_02.51.00,
Flash file name: CISCO2950-LRE_vdslotl_02.51.00.bin

LRE Binary: CISCO2950-LRE_vdslotl_02.50.00,
Flash file name: CISCO2950-LRE_vdslotl_02.50.00.bin
```

This example shows the status of an upgrade after it starts, but before the data transfer begins:

```
Switch# show lre upgrade status
Lo0/1:
  lcl curr:CISCO2950-LRE_vdsloct1_02.60.00 new:CISCO2950-LRE_vdsloct1_02.60.00
  Status:Pending
  rmt curr:CISCO575-LRE_vdslsng1_52.00.00 new:CISCO575-LRE_vdslsng1_52.00.00
  Status:Pending
Lo0/2:
  lcl curr:CISCO2950-LRE_vdsloct1_02.60.00 new:CISCO2950-LRE_vdsloct1_02.60.00
  Status:Pending
  rmt curr:CISCO575-LRE_vdslsng1_52.00.00 new:CISCO575-LRE_vdslsng1_52.00.00
  Status:Pending
Lo0/3:
  lcl curr:CISCO2950-LRE_vdsloct1_02.60.00 new:CISCO2950-LRE_vdsloct1_02.60.00
  Status:Pending
  rmt curr:CISCO575-LRE_vdslsng1_52.00.00 new:CISCO575-LRE_vdslsng1_52.00.00
  Status:Pending
Lo0/4:
  lcl curr:CISCO2950-LRE_vdsloct1_02.60.00 new:CISCO2950-LRE_vdsloct1_02.60.00
  Status:Pending
  rmt curr:CISCO575-LRE_vdslsng1_52.00.00 new:CISCO575-LRE_vdslsng1_52.00.00
  Status:Pending

<output truncated>
```

This example shows the status of an upgrade after data transfer is in progress.

```
Switch# show lre upgrade status
Lo0/1:
  lcl curr:CISCO2950-LRE_vdsloct1_02.60.00 new:CISCO2950-LRE_vdsloct1_02.60.00
  Status:Pending
  rmt curr:CISCO575-LRE_vdslsng1_52.00.00 new:CISCO575-LRE_vdslsng1_52.00.00
  Status:Active
  10 HHMM:0000, Attempt:001
Lo0/2:
  lcl curr:CISCO2950-LRE_vdsloct1_02.60.00 new:CISCO2950-LRE_vdsloct1_02.60.00
  Status:Pending
  rmt curr:CISCO575-LRE_vdslsng1_52.00.00 new:CISCO575-LRE_vdslsng1_52.00.00
  Status:Active
  09 HHMM:0000, Attempt:001
Lo0/3:
  lcl curr:CISCO2950-LRE_vdsloct1_02.60.00 new:CISCO2950-LRE_vdsloct1_02.60.00
  Status:Pending
  rmt curr:CISCO575-LRE_vdslsng1_52.00.00 new:CISCO575-LRE_vdslsng1_52.00.00
  Status:Active
  22 HHMM:0000, Attempt:001
Lo0/4:
  lcl curr:CISCO2950-LRE_vdsloct1_02.60.00 new:CISCO2950-LRE_vdsloct1_02.60.00

<output truncated>
```

This example shows output from the **show lre upgrade version** command:

```
Switch# show lre upgrade version
Lo0/1:
  CPE:Family CISCO575-LRE, Model Cisco575-LRE , Rev A0
  lcl curr:CISCO2950-LRE_vdsloct1_02.60.00 cfg:CISCO2950-LRE_vdsloct1_02.60.00
  rmt curr:CISCO575-LRE_vdslsng1_52.00.00 cfg:CISCO575-LRE_vdslsng1_52.00.00
Lo0/2:
  CPE:Family CISCO575-LRE, Model Cisco575-LRE , Rev A0
  lcl curr:CISCO2950-LRE_vdsloct1_02.60.00 cfg:CISCO2950-LRE_vdsloct1_02.60.00
  rmt curr:CISCO575-LRE_vdslsng1_52.00.00 cfg:CISCO575-LRE_vdslsng1_52.00.00
```

show lre upgrade

```

Lo0/3:
  CPE:Family CISCO575-LRE, Model Cisco575-LRE , Rev A0
  lcl curr:CISCO2950-LRE_vdslotl1_02.60.00 cfg:CISCO2950-LRE_vdslotl1_02.60.00
  rmt curr:CISCO575-LRE_vdslotl1_52.00.00 cfg:CISCO575-LRE_vdslotl1_52.00.00
Lo0/4:
  CPE:Family CISCO575-LRE, Model Cisco575-LRE , Rev A0
  lcl curr:CISCO2950-LRE_vdslotl1_02.60.00 cfg:CISCO2950-LRE_vdslotl1_02.60.00
  rmt curr:CISCO575-LRE_vdslotl1_52.00.00 cfg:CISCO575-LRE_vdslotl1_52.00.00
Lo0/5:
  CPE:Family CISCO575-LRE, Model Cisco575-LRE , Rev A0
  lcl curr:CISCO2950-LRE_vdslotl1_02.60.00 cfg:CISCO2950-LRE_vdslotl1_02.60.00
  rmt curr:CISCO575-LRE_vdslotl1_52.00.00 cfg:CISCO575-LRE_vdslotl1_52.00.00

<output truncated>

```

Related Commands

Command	Description
show lre upgrade	Displays the upgrade status on all ports in the switch or the versions of binaries on local and remote ends on all ports.

show mac access-group

Use the **show mac access-group** user EXEC command to display the MAC access control lists (ACLs) configured for an interface or a switch.

```
show mac access-group [interface interface-id] [ | { begin | exclude | include } expression]
```

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

Syntax Description

interface <i>interface-id</i>	(Optional) Display the ACLs configured on a specific interface (only available in privileged EXEC mode).
begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .
exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

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

Usage Guidelines

Use the **show mac access-group** command without keywords to display MAC ACLs for all interfaces.

Use this command with the **interface** keyword to display ACLs for a specific interface.

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

Examples

This is an example of output from the **show mac access-group** command:

```
Switch> show mac access-group
Interface FastEthernet0/1:
  Inbound access-list is not set
Interface FastEthernet0/2:
  Inbound access-list is not set
Interface FastEthernet0/3:
  Inbound access-list is not set
Interface FastEthernet0/4:
  Inbound access-list is not set
...
Interface FastEthernet0/47:
  Inbound access-list is not set
Interface FastEthernet0/48:
  Inbound access-list is not set
Interface GigabitEthernet0/1:
  Inbound access-list is not set
```

■ show mac access-group

```
Interface GigabitEthernet0/2:
  Inbound access-list is 101
```

This is an example of output from the **show mac access-group interface gigabitethernet 0/2** command:

```
Switch# show mac access-group interface gigabitethernet 0/2
Interface GigabitEthernet0/2:
  Inbound access-list is 101
```

Related Commands

Command	Description
mac access-group	Applies a MAC ACL to an interface.

show mac address-table

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

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



Note

Beginning with Cisco IOS Release 12.1(11)EA1, the **show mac address-table** command replaces the **show mac-address-table** command (with the hyphen).

Syntax Description

aging-time	(Optional) Display aging time for dynamic addresses for all VLANs.
count	(Optional) Display the count for different kinds of MAC addresses (only available in privileged EXEC mode).
dynamic	(Optional) Display only the dynamic addresses.
static	(Optional) Display only the static addresses.
address <i>hw-addr</i>	(Optional) Display information for a specific address (only available in privileged EXEC mode).
interface <i>interface-id</i>	(Optional) Display addresses for a specific interface.
vlan <i>vlan-id</i>	(Optional) Display addresses for a specific VLAN. Valid IDs are from 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1001 when the standard software image (SI) is installed.
 begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

User EXEC

The **address** and **count** keywords are available only in privileged EXEC mode.

Command History

Release	Modification
12.0(5.2)WC(1)	This command was first introduced.
12.1(6)EA2	The show mac-address-table secure command was replaced by the show port-security command. The self keyword is not supported in this release or later.
12.1(11)EA1	The show mac-address-table command was replaced by the show mac address-table command.

Usage Guidelines

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

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

Examples

This is an example of output from the **show mac address-table** command:

```
Switch> show mac address-table

Dynamic Addresses Count:          9
Secure Addresses (User-defined) Count: 0
Static Addresses (User-defined) Count: 0
System Self Addresses Count:     41
Total MAC addresses:             50
Non-static Address Table:
Destination Address  Address Type  VLAN  Destination Port
-----
0010.0de0.e289      Dynamic      1    FastEthernet0/1
0010.7b00.1540      Dynamic      2    FastEthernet0/5
0010.7b00.1545      Dynamic      2    FastEthernet0/5
0060.5cf4.0076      Dynamic      1    FastEthernet0/1
0060.5cf4.0077      Dynamic      1    FastEthernet0/1
0060.5cf4.1315      Dynamic      1    FastEthernet0/1
0060.70cb.f301      Dynamic      1    FastEthernet0/1
00e0.1e42.9978      Dynamic      1    FastEthernet0/1
00e0.1e9f.3900      Dynamic      1    FastEthernet0/1
```

This is an example of output from the **show mac address-table static** command:

```
Switch> show mac address-table static
vlan  mac address      type  ports
-----+-----+-----+-----
  All  0180.c200.0003  STATIC  CPU
  All  0180.c200.0004  STATIC  CPU
  All  0180.c200.0005  STATIC  CPU
    4   0001.0002.0004  STATIC  Drop
    6   0001.0002.0007  STATIC  Drop
```

This is an example of output from the **show mac address-table static interface fastethernet0/2 vlan 1** command:

```
Switch> show mac address-table static interface fastethernet0/2 vlan 1
vlan  mac address      type  ports
-----+-----+-----+-----
    1  abcd.2345.0099  STATIC  Fa0/2
    1  abcd.0070.0070  STATIC  Fa0/2
    1  abcd.2345.0099  STATIC  Fa0/2
    1  abcd.2345.0099  STATIC  Fa0/2
    1  00d0.d333.7f34  STATIC  Fa0/2
    1  abcd.2345.0099  STATIC  Fa0/2
    1  0005.6667.0007  STATIC  Fa0/2
```

This is an example of output from the **show mac address-table count vlan 1** command:

```
Switch# show mac address-table count vlan 1
MAC Entries for Vlan 1 :
Dynamic Address Count: 1
Static Address (User-defined) Count: 41
Total MAC Addresses In Use:42
Remaining MAC addresses: 8150
```

This is an example of output from the **show mac address-table aging-time** command:

```
Switch> show mac address-table aging-time
Vlan Aging Time
-----
1      450
2      300
3      600
300    450
301    450
```

This is an example of output from the **show mac address-table aging-time vlan 1** command:

```
Switch> show mac address-table aging-time vlan 1
Vlan Aging Time
-----
1      450
```

Related Commands

Command	Description
clear mac address-table dynamic	Deletes from the MAC address table a specific dynamic address, all dynamic addresses on a particular interface, or all dynamic addresses on a particular VLAN.

show mac address-table multicast

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

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



Note

Beginning with Cisco IOS Release 12.1(11)EA1, the **show mac address-table multicast** command replaces the **show mac-address-table multicast** command (with the hyphen).

Syntax Description

vlan <i>vlan-id</i>	(Optional) Specify a VLAN; valid values are 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1005 when the standard software image (SI) is installed. (This keyword is only available in privileged EXEC mode.)
count	(Optional) Display total number of entries for the specified criteria instead of the actual entries (only available in privileged EXEC mode).
igmp-snooping	(Optional) Display only entries learned through Internet Group Management Protocol (IGMP) snooping (only available in privileged EXEC mode).
user	(Optional) Display only the user-configured multicast entries (only available in privileged EXEC mode).
 begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Defaults

This command has no default setting.

Command Modes

User EXEC

Command History

Release	Modification
12.0(5.2)WC(1)	This command was first introduced.
12.1(11)EA1	The show mac-address-table multicast command was replaced by the show mac address-table multicast command.

Usage Guidelines

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

Examples

This is an example of output from the **show mac address-table multicast vlan 1** command:

```
Switch# show mac address-table multicast vlan 1

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

This is an example of output from the **show mac address-table multicast count** command:

```
Switch# show mac address-table multicast count
Multicast Mac Entries for all vlans: 10
```

This is an example of output from the **show mac address-table multicast vlan 1 count** command:

```
Switch# show mac address-table multicast vlan 1 count
Multicast Mac Entries for vlan 1: 2
```

This is an example of output from the **show mac address-table multicast vlan 1 user** command:

```
Switch# show mac address-table multicast vlan 1 user
vlan    mac address      type    ports
-----+-----+-----+-----
1       0100.5e02.0203  user    Fa0/1,Fa0/2,Fa0/4
```

This is an example of output from the **show mac address-table multicast vlan 1 igmp-snooping count** command:

```
Switch# show mac address-table multicast vlan 1 igmp-snooping count
Number of igmp-snooping programmed entries : 1
```

show mac address-table notification

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

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



Note

Beginning with Cisco IOS Release 12.1(11)EA1, the **show mac address-table notification** command replaces the **show mac-address-table notification** command (with the hyphen).

Syntax Description

interface <i>interface-id</i>	(Optional) Specify an interface.
 begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Defaults

This command has no default setting.

Command Modes

User EXEC

Command History

Release	Modification
12.1(6)EA2	This command was first introduced.
12.1(11)EA1	The show mac-address-table notification command was replaced by the show mac address-table notification command.

Usage Guidelines

Use the **show mac address-table notification** command without keywords to display parameters for all interfaces.

Use this command with the **interface** keyword to display parameters for a specific interface.

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

Examples

This is an example of output from the **show mac address-table notification** command:

```
Switch> show mac address-table notification
MAC Notification Feature is Disabled on the switch
```

Related Commands	Command	Description
	clear mac address-table notification	Clears the MAC address notification global counters.
	mac address-table notification	Enables the MAC notification feature.
	snmp trap mac-notification	Enables MAC-notification traps on a port.

show mls masks

Use the **show mls masks** user EXEC command to display the details of the access control parameters (ACPs) used for quality of service (QoS) and security access control lists (ACLs).

show mls masks [**qos** | **security**] [| {**begin** | **exclude** | **include**} *expression*]

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

Syntax Description

qos	(Optional) Display ACPs used for QoS ACLs.
security	(Optional) Display ACPs used for security ACLs.
 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.



Note

ACPs are called masks in the command-line interface (CLI) commands and output.

Command Modes

User EXEC

Command History

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

Usage Guidelines

Use the **show mls masks** command without keywords to display all ACPs configured on the switch.
 Use this command with the **qos** keyword to display the ACPs used for QoS ACLs.
 Use this command with the **security** keyword to display the ACPs used for security ACLs.



Note

You can configure up to four ACPs (QoS and security) on a switch.

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

Examples

This is an example of output from the **show mls masks** command:

```
Switch> show mls masks

Mask1
  Type : qos
  Fields : ip-sa(0.0.0.255), ip-da(host), dest-port, ip-dscp
  Policymap: pmap1
    Interfaces: Fa0/9, Gi0/1
  Policymap: pmap2
    Interfaces: Fa0/1, Fa0/5, Fa0/13

Mask2
  Type : security
  Fields : mac-sa (host), ethertype, ip-dscp
  Access-group: 3
    Interfaces: Fa0/2, Fa0/6
  Access-group: macag1
    Interfaces: Fa0/16
```

In this example, *Mask 1* is a QoS ACP consisting an IP source address (with wildcard bits 0.0.0.255), an IP destination address, and Layer 4 destination port fields. This ACP is used by the QoS policy maps *pmap1* and *pmap2*.

Mask 2 is a security ACP consisting of a MAC source address and ethertype fields. This ACP is used by the MAC security access groups *3* and *macag1*.

Related Commands

Command	Description
ip access-group	Applies an IP ACL to an interface.
mac access-group	Applies a named extended MAC ACL to an interface.
policy-map	Creates or modifies a policy map that can be attached to multiple interfaces, and enters policy-map configuration mode.

show mls qos interface

Use the **show mls qos interface** user EXEC command to display quality of service (QoS) information at the interface level.

```
show mls qos interface [interface-id] [policers] [ | {begin | exclude | include} expression]
```

Syntax Description

<i>interface-id</i>	(Optional) Display QoS information for the specified interface.
policers	(Optional) Display all the policers configured on the interface and their settings (available only when the switch is running the enhanced software image [EI]).
 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.



Note

Though visible in the command-line help strings, the **vlan** *vlan-id* option is not supported.

Command Modes

User EXEC

Command History

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

Usage Guidelines

Though visible in the command-line help string, the **policers** keyword is available only when your switch is running the EI.

Use the **show mls qos interface** command without keywords to display parameters for all interfaces.

Use the **show mls qos interface** *interface-id* command to display the parameters for a specific interface.

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

Examples

This is an example of output from the **show mls qos interface** command when the Cisco IP phone is a trusted device:

```
Switch> show mls qos interface fastethernet0/1
FastEthernet0/1
trust state:trust cos
trust mode:trust cos
COS override:dis
default COS:0
pass-through:none
trust device:cisco-phone
```

This is an example of output from the **show mls qos interface** command when pass-through mode is configured on an interface:

```
Switch> show mls qos interface fastethernet0/2
FastEthernet0/2
trust state:not trusted
trust mode:not trusted
COS override:dis
default COS:0
pass-through:dscp
```

This is an example of output from the **show mls qos interface-id policers** command:

```
Switch> show mls qos interface fastethernet0/1 policers
FastEthernet0/1
policymap=pmtimerin
type=Single rate=1000000, burst=4096
type=Single rate=2000000, burst=4096
```

Related Commands

Command	Description
mls qos cos	Defines the default class of service (CoS) value of a port or assigns the default CoS to all incoming packets on the port.
mls qos map	Defines the class of service (CoS)-to-Differentiated Services Code Point (DSCP) map and DSCP-to-CoS map.
mls qos trust	Configures the port trust state. Ingress traffic can be trusted and classification is performed by examining the CoS or DSCP value.

show mls qos maps

Use the **show mls qos maps** user EXEC command to display quality of service (QoS) mapping information. Maps are used to generate an internal Differentiated Services Code Point (DSCP) value, which represents the priority of the traffic.

```
show mls qos maps [cos-dscp | dscp-cos] [ | {begin | exclude | include} expression]
```

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

Syntax Description

cos-dscp	(Optional) Display class of service (CoS)-to-DSCP map.
dscp-cos	(Optional) Display DSCP-to-CoS map.
 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

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

Usage Guidelines

Use the **show mls qos maps** command without keywords to display all maps.

Use this command with the **cos-dscp** keyword to display the CoS-to-DSCP map.

Use this command with the **dscp-cos** keyword to display the DSCP-to-CoS map.

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

Examples

This is an example of output from the **show mls qos maps cos-dscp** command:

```
Switch> show mls qos maps cos-dscp
```

```
Cos-dscp map:
  cos:  0  1  2  3  4  5  6  7
-----
  dscp:  8  8  8  8 24 32 56 56
```

This is an example of output from the **show mls qos maps dscp-cos** command:

```
Switch> show mls qos maps dscp-cos

Dscp-cos map:
  dscp:  0  8 10 16 18 24 26 32 34 40 46 48 56
-----
  cos:   0  1  1  1  2  2  3  3  4  4  5  6  7
```

This is an example of output from the **show mls qos maps** command:

```
Switch> show mls qos maps

Dscp-cos map:
  dscp:  0  8 10 16 18 24 26 32 34 40 46 48 56
-----
  cos:   0  1  1  2  2  3  7  4  4  5  5  7  7

Cos-dscp map:
  cos:   0  1  2  3  4  5  6  7
-----
  dscp:  0  8 16 24 32 40 48 56
```

Related Commands

Command	Description
mls qos map	Defines the CoS-to-DSCP map and DSCP-to-CoS map.

show monitor

Use the **show monitor** user EXEC command to display Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) session information.

show monitor [session {*session_number* | **all** | **local** | **range** | **remote**}] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

session <i>session_number</i>	(Optional) Specify the session number identified with this SPAN or RSPAN session.
all	Specify all sessions.
local	Specify local sessions.
range	Specify a range of sessions.
remote	Specify remote sessions.
begin	(Optional) Display begins with the line that matches the <i>expression</i> .
exclude	(Optional) Display excludes lines that match the <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(6)EA1	This command was first introduced.
12.1(11)EA1	The all , local , and remote keywords were added.
12.1(13)EA1	The range keyword was added.

Usage Guidelines

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

Examples

This is an example of output for the **show monitor** privileged EXEC command for RSPAN source session 1:

```
Switch# show monitor session 1
Session 1
-----
Type: Remote Source Session
Source Ports:
  RX Only: Fa0/3
  TX Only: None
  Both: None
Source VLANs:
  RX Only: None
  TX Only: None
  Both: None
Source RSPAN VLAN: None
Destination Ports: None
  Encapsulation: Native
Reflector Port: Fa0/4
Filter VLANs: None
Dest RSPAN VLAN: 901
```

Related Commands

Command	Description
monitor session	Enables SPAN and RSPAN monitoring on a port and configures a port as a source or destination port.

show mvr

Use the **show mvr** privileged EXEC command without keywords to display the Multicast VLAN Registration (MVR) global parameter values, including whether or not MVR is enabled, the MVR multicast VLAN, the maximum query response time, the number of multicast groups, and the MVR mode (dynamic or compatible).

```
show mvr [ | {begin | exclude | include} expression]
```

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

Command Modes Privileged EXEC

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

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

Examples This is an example of output from the **show mvr** command:

```
Switch# show mvr
MVR Running: TRUE
MVR multicast vlan: 1
MVR Max Multicast Groups: 256
MVR Current multicast groups: 256
MVR Global query response time: 5 (tenths of sec)
MVR Mode: compatible
```

In the previous example, the maximum number of multicast groups is 256. The MVR mode is either compatible (for interoperability with Catalyst 2900 XL and Catalyst 3500 XL switches) or dynamic (where operation is consistent with Internet Group Management Protocol [IGMP] snooping operation, and dynamic MVR membership on source ports is supported).

Related Commands	Command	Description
	mvr	Enables and configures multicast VLAN registration on the switch.
	mvr type	Configures an MVR port as a receiver or a source port.
	show mvr interface	Displays the configured MVR interfaces, status of the specified interface, or all multicast groups to which the interface belongs.
	show mvr members	Displays all ports that are members of an MVR multicast group.

show mvr interface

Use the **show mvr interface** privileged EXEC command without keywords to display the Multicast VLAN Registration (MVR) receiver and source ports. Use the command with keywords to display MVR parameters for a specific receiver port.

```
show mvr interface [interface-id [members [vlan vlan-id]] [| {begin | exclude | include}
                    expression]
```

Syntax Description		
<i>interface-id</i>	(Optional) Display MVR type, status, and Immediate-Leave setting for the interface.	
members	(Optional) Display all MVR groups to which the specified interface belongs.	
vlan <i>vlan-id</i>	(Optional) Display the VLAN to which the receiver port belongs.	
begin	(Optional) Display begins with the line that matches the <i>expression</i> .	
exclude	(Optional) Display excludes lines that match the <i>expression</i> .	
include	(Optional) Display includes lines that match the specified <i>expression</i> .	
<i>expression</i>	Expression in the output to use as a reference point.	

Command Modes Privileged EXEC

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

Usage Guidelines

If the entered port identification is a non-MVR port or a source port, the command returns an error message. For receiver ports, it displays the port type, per port status, and Immediate-Leave setting. Expressions are case sensitive. For example, if you enter | **exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

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

```
Switch# show mvr interface
Port   Type           Status          Immediate Leave
----   -
Gi0/1  SOURCE         ACTIVE/UP       DISABLED
Gi0/2  RECEIVER       ACTIVE/DOWN     DISABLED
```

In the previous example, Status is defined as:

- Active means the port is part of a VLAN.
- Up/Down means that the port is forwarding/nonforwarding.
- Inactive means that the port is not part of any VLAN.

This is an example of output from the **show mvr interface gigabitethernet0/2** command:

```
Switch# show mvr interface gigabitethernet0/2
Type: RECEIVER Status: ACTIVE Immediate Leave: DISABLED
```

This is an example of output from the **show mvr interface fastethernet0/6 member** command:

```
Switch# show mvr interface fastethernet0/6 member
239.255.0.0      DYNAMIC ACTIVE
239.255.0.1      DYNAMIC ACTIVE
239.255.0.2      DYNAMIC ACTIVE
239.255.0.3      DYNAMIC ACTIVE
239.255.0.4      DYNAMIC ACTIVE
239.255.0.5      DYNAMIC ACTIVE
239.255.0.6      DYNAMIC ACTIVE
239.255.0.7      DYNAMIC ACTIVE
239.255.0.8      DYNAMIC ACTIVE
239.255.0.9      DYNAMIC ACTIVE
```

Related Commands

Command	Description
mvr	Enables and configures multicast VLAN registration on the switch.
mvr type	Configures an MVR port as a receiver or a source port.
show mvr	Displays the global MVR configuration on the switch.
show mvr members	Displays all receiver ports that are members of an MVR multicast group.

show mvr members

Use the **show mvr members** privileged EXEC command to display all receiver and source ports that are currently members of an IP multicast group.

```
show mvr members [ip-address] [ | {begin | exclude | include} expression]
```

Syntax Description		
	<i>ip-address</i>	(Optional) The IP multicast address. If the address is entered, all receiver and source ports that are members of the multicast group appear. If no address is entered, all members of all Multicast VLAN Registration (MVR) groups are listed. If a group has no members, the group is listed as <i>Inactive</i> .
	 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	 include	(Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.

Command Modes Privileged EXEC

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

Usage Guidelines The **show mvr members** command applies to receiver and source ports. For MVR compatible mode, all source ports are members of all multicast groups.

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

Examples This is an example of output from the **show mvr members** command:

```
Switch# show mvr members
MVR Group IP      Status      Members
-----
239.255.0.1      ACTIVE     Gi0/1(d), Gi0/2(s)
239.255.0.2      INACTIVE  None
239.255.0.3      INACTIVE  None
239.255.0.4      INACTIVE  None
239.255.0.5      INACTIVE  None
239.255.0.6      INACTIVE  None
239.255.0.7      INACTIVE  None
239.255.0.8      INACTIVE  None
239.255.0.9      INACTIVE  None
239.255.0.10     INACTIVE  None

<output truncated>

239.255.0.255    INACTIVE  None
239.255.1.0      INACTIVE  None
```

This is an example of output from the **show mvr members 239.255.0.2** command. It shows how to view the members of the IP multicast group 239.255.0.2.

```
Switch# show mvr member 239.255.0.2
239.255.0.2      ACTIVE          Gi0/1(d), Gi0/2(d)
```

Related Commands	Command	Description
	mvr	Enables and configures multicast VLAN registration on the switch.
	mvr type	Configures an MVR port as a receiver or a source port.
	show mvr	Displays the global MVR configuration on the switch.
	show mvr interface	Displays the configured MVR interfaces, status of the specified interface, or all multicast groups to which the interface belongs.

show pagp

Use the **show pagp** user EXEC command to display Port Aggregation Protocol (PAgP) channel-group information.

```
show pagp [channel-group-number] { counters | internal | neighbor } [ | { begin | exclude | include } expression]
```

Syntax Description

<i>channel-group-number</i>	(Optional) Number of the channel group. Valid numbers range from 1 to 6.
counters	Display traffic information.
internal	Display internal information.
neighbor	Display neighbor information.
 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

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

Usage Guidelines

You can enter any **show pagp** command to display the active port channel information. To display the nonactive information, enter the **show pagp** command with a group number.

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

Examples

This is an example of output from the **show pagp 1 counters** command:

```
Switch> show pagp 1 counters
          Information      Flush
Port     Sent  Recv   Sent  Recv
-----
Channel group: 1
  Gi0/1   45   42     0    0
  Gi0/2   45   41     0    0
```

This is an example of output from the **show pagp 1 internal** command:

```
Switch> show pagp 1 internal
Flags: S - Device is sending Slow hello. C - Device is in Consistent state.
      A - Device is in Auto mode.
Timers: H - Hello timer is running.      Q - Quit timer is running.
      S - Switching timer is running.    I - Interface timer is running.

Channel group 1

```

Port	Flags	State	Timers	Hello Interval	Partner Count	PAGP Priority	Learning Method	Group Ifindex
Gi0/1	SC	U6/S7	H	30s	1	128	Any	16
Gi0/2	SC	U6/S7	H	30s	1	128	Any	16

This is an example of output from the **show pagp 1 neighbor** command:

```
Switch> show pagp 1 neighbor
Flags: S - Device is sending Slow hello. C - Device is in Consistent state.
      A - Device is in Auto mode.      P - Device learns on physical port.

Channel group 1 neighbors

```

Port	Partner Name	Partner Device ID	Partner Port	Partner Age	Partner Flags	Partner Group Cap.
Gi0/1	device-p2	0002.4b29.4600	Gi0/1	9s	SC	10001
Gi0/2	device-p2	0002.4b29.4600	Gi0/2	24s	SC	10001

Related Commands

Command	Description
clear pagp	Clears PAgP channel-group information.
pagp learn-method	Sets the source-address learning method of incoming packets received from an EtherChannel port.

show parser macro

Use the **show parser macro** user EXEC command to display the parameters for all configured macros or for one macro on the switch.

```
show parser macro [{brief | description [interface interface-id] | name macro-name}] [| {begin
| exclude | include} expression]
```

Syntax	Description
brief	(Optional) Display the name of each macro.
description [interface <i>interface-id</i>]	(Optional) Display all macro descriptions or the description of a specific interface.
name <i>macro-name</i>	(Optional) Display information about a single macro identified by the macro name.
 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes User EXEC

Command History	Release	Modification
	12.1(19)EA1	The command was first introduced.

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

Examples This is an example of output from the **show parser macro** command:

```
Switch# show parser macro
Total number of macros = 2
-----
Macro name : standard-switch10
Macro type : customizable

macro description standard-switch10
# Trust QoS settings on VOIP packets
auto qos voip trust
# Allow port channels to be automatically formed
channel-protocol pagp
-----
Macro name : testm
Macro type : customizable

macro description this is test macro
speed 100
-----
```

This is an example of output from the **show parser macro name** command:

```
Switch# show parser macro name standard-switch10
Macro name : standard-switch10
Macro type : customizable

macro description standard-switch10
# Trust QoS settings on VOIP packets
auto qos voip trust
# Allow port channels to be automatically formed
channel-protocol pagp
```

This is an example of output from the **show parser brief** command:

```
Switch# show parser macro brief
      standard-switch10
      testm
```

This is an example of output from the **show parser description** command:

```
Switch# show parser macro description
Interface      Macro Description
-----
Fa0/9          standard-switch10
Fa0/10         this is test macro
-----
```

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

```
Switch# show parser macro description interface fa0/10
Interface      Macro Description
-----
Fa0/10         this is test macro
-----
```

Related Commands

Command	Description
macro apply	Applies a macro on an interface or applies and traces a macro on an interface.
macro description	Adds a description about the macros that are applied to an interface.
macro name	Creates a macro.

show policy-map

Use the **show policy-map** user EXEC command to display quality of service (QoS) policy maps, which define classification criteria for incoming traffic. Policy maps can include policers that specify the bandwidth limitations and the action to take if the limits are exceeded.

show policy-map [*policy-map-name* [**class** *class-name*]] [| { **begin** | **exclude** | **include** } *expression*]

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

Syntax Description

<i>policy-map-name</i>	(Optional) Display the specified policy-map name.
class <i>class-name</i>	(Optional) Display QoS policy actions for a individual class.
begin	(Optional) Display begins with the line that matches the <i>expression</i> .
exclude	(Optional) Display excludes lines that match the <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

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

Usage Guidelines

Use the **show policy-map** command without keywords to display all policy maps configured on the switch.



Note

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

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

Examples

This is an example of output from the **show policy-map** command:

```
Switch> show policy-map
Policy Map bumbum
  Description: this is a description.

Policy Map wizard_policy3
  class wizard_1-1-1-2
    set ip dscp 34
```

```

Policy Map test

Policy Map policytest
  class classtest
    set ip dscp 20
    police 10000000 8192 exceed-action drop

```

This is an example of output from the **show policy-map pmtimerin** command:

```

Switch> show policy-map pmtimerin
Policy Map pmtimerin
  class cmtimerin
    set ip dscp 10
    police 1000000 4096 exceed-action drop
  class ctimerin1
    police 2000000 4096 exceed-action drop

```

This is an example of output from the **show policy-map policytest class classtest** command:

```

Switch> show policy-map policytest class classtest
  set ip dscp 20
  police 10000000 8192 exceed-action drop

```

Related Commands

Command	Description
policy-map	Creates or modifies a policy map that can be attached to multiple interfaces to specify a service policy.

show port-security

Use the **show port-security** privileged EXEC command to display the port security settings defined for an interface or for the switch.

```
show port-security [interface interface-id] [address] [ | {begin | exclude | include} expression]
```

Syntax Description		
interface	(Optional)	Display the port security settings for the specified interface.
<i>interface-id</i>		
address	(Optional)	Display all the secure addresses on all ports.
begin	(Optional)	Display begins with the line that matches the specified <i>expression</i> .
exclude	(Optional)	Display excludes lines that match the specified <i>expression</i> .
include	(Optional)	Display includes lines that match the specified <i>expression</i> .
<i>expression</i>		Expression in the output to use as a reference point.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(6)EA2	This command was first introduced. It replaced the show port security and show mac-address-table secure commands.

Usage Guidelines

If you enter this command without keywords, the output includes the administrative and the operational status of all secure ports on the switch.

If you enter an *interface-id*, the **show port-security** command displays port security settings for the interface.

If you enter the **address** keyword, the **show port-security address** command displays the secure MAC addresses for all interfaces and the aging information for each secure address.

If you enter an *interface-id* and the **address** keyword, the **show port-security interface *interface-id* address** command displays all the MAC addresses for the interface with aging information for each secure address. You can also use this command to display all the MAC addresses for an interface even if you have not enabled port security on it.

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

Examples

This is an example of output from the **show port-security** command:

```
Switch# show port-security
Secure Port      MaxSecureAddr  CurrentAddr  SecurityViolation  Security
Action
                (Count)          (Count)      (Count)
-----
---
    Fa0/1         11             11           0                 Shutdown
    Fa0/5         15             5            0                 Restrict
    Fa0/11        5              4            0                 Protect
-----
---
Total Addresses in System :21
Max Addresses limit in System :1024
```

This is an example of output from the **show port-security interface fastethernet0/2** command:

```
Switch# show port-security interface fastethernet0/2
Port Security :Enabled
Port status :SecureUp
Violation mode :Shutdown
Maximum MAC Addresses :11
Total MAC Addresses :11
Configured MAC Addresses :3
Aging time :20 mins
Aging type :Inactivity
SecureStatic address aging :Enabled
Security Violation count :0
```

This is an example of output from the **show port-security address** command:

```
Switch# show port-security address

Secure Mac Address Table
-----
Vlan    Mac Address      Type                Ports    Remaining Age
        (mins)
-----
1       0001.0001.0001  SecureDynamic      Fa0/1    15 (I)
1       0001.0001.0002  SecureDynamic      Fa0/1    15 (I)
1       0001.0001.1111  SecureConfigured   Fa0/1    16 (I)
1       0001.0001.1112  SecureConfigured   Fa0/1    -
1       0001.0001.1113  SecureConfigured   Fa0/1    -
1       0005.0005.0001  SecureConfigured   Fa0/5    23
1       0005.0005.0002  SecureConfigured   Fa0/5    23
1       0005.0005.0003  SecureConfigured   Fa0/5    23
1       0011.0011.0001  SecureConfigured   Fa0/11   25 (I)
1       0011.0011.0002  SecureConfigured   Fa0/11   25 (I)
-----
Total Addresses in System :10
Max Addresses limit in System :1024
```

show port-security

This is an example of output from the **show port-security interface fastethernet0/5 address** command:

```
Switch# show port-security interface fastethernet0/5 address
Secure Mac Address Table
-----
Vlan    Mac Address      Type                Ports    Remaining Age
        (mins)
-----
   1     0005.0005.0001  SecureConfigured   Fa0/5    19 (I)
   1     0005.0005.0002  SecureConfigured   Fa0/5    19 (I)
   1     0005.0005.0003  SecureConfigured   Fa0/5    19 (I)
-----
Total Addresses:3
```

Related Commands

Command	Description
switchport port-security	Enables port security on a port, restricts the use of the port to a user-defined group of stations, and configures secure MAC addresses.

show 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 <i>expression</i> .	
exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .	
include	(Optional) Display includes lines that match the specified <i>expression</i> .	
<i>expression</i>	Expression in the output to use as a reference point.	

Command Modes Privileged EXEC

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

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

Examples This is an example of output from the **show rps** command. [Table 2-26](#) describes the possible output.

```
Switch# show rps
GREEN
```

Table 2-26 *show rps Output Description*

Display	Description
BLACK	The RPS is off or not properly connected.
GREEN	The RPS is connected and ready to provide back-up power, if required.
ALT_GREEN_BLACK	The RPS is connected but is unavailable because it is providing power to another device (redundancy has been allocated to a neighboring device).

Table 2-26 show rps Output Description (continued)

Display	Description
ALT_AMBER_BLACK	The internal power supply in the switch has failed, and the RPS is providing power to the switch (redundancy has been allocated to this device).
AMBER	<p>The RPS is in standby mode, or the RPS has detected a failure.</p> <p>Press the Standby/Active button on the RPS to put the RPS in active mode. If the RPS LED on the switch remains amber, the RPS has detected a failure.</p> <p>If the failure is minor, the RPS might be in any of the previously described modes. If the failure is critical, the RPS will be down.</p> <p>RPS failures include these modes:</p> <ul style="list-style-type: none"> • The RPS +12V or -48V voltages exceed the specified thresholds. • The RPS has a fan failure. • The RPS detects excessive temperature. • The RPS has a faulty connection to the switch.

show running-config vlan

Use the **show running-config vlan** privileged EXEC command to display all or a range of VLAN-related configurations on the switch.

```
show running-config vlan [vlan-ids] [ | { begin | exclude | include } expression]
```

Syntax Description

<i>vlan-ids</i>	(Optional) Display configuration information for a single VLAN identified by VLAN ID number or a range of VLANs separated by a hyphen. For <i>vlan-id</i> , the range is 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1005 when the standard software image (SI) is installed.
begin	(Optional) Display begins with the line that matches the <i>expression</i> .
exclude	(Optional) Display excludes lines that match the <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

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

Examples

This is an example of output from the **show running-config vlan** command:

```
Switch# show running-config vlan 900-2005
Building configuration...

Current configuration:
!
vlan 907
!
vlan 920
!
vlan 1025
!
vlan 2000
!
vlan 2001
end
```

Related Commands	Command	Description
	show running-config	Displays the running configuration on the switch. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 > Cisco IOS File Management Commands > Configuration File Commands .
	vlan (global configuration)	Enters config-vlan mode for creating and editing VLANs. When VLAN Trunking Protocol (VTP) mode is transparent, you can use this mode to create extended-range VLANs (VLAN IDs greater than 1005).
	vlan database	Enters VLAN configuration mode for creating and editing normal-range VLANs.

show setup express

Use the **show setup express** privileged EXEC command to show if Express Setup mode is active on the switch.

show setup express

This command is available only on Catalyst 2950 switches.

Syntax Description

This command has no arguments or keywords.

Defaults

No default is defined.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(14)EA1	This command was first introduced.

Examples

This is an example of output from the **show setup express** command:

```
Switch# show setup express
express setup mode is active
```

Related Commands

Command	Description
clear setup express	Exits Express Setup mode without saving the configuration.
setup express	Enables Express Setup mode on the switch.

show spanning-tree

Use the **show spanning-tree** user EXEC command to display spanning-tree state information.

```
show spanning-tree [active [detail] | backbonefast | blockedports | bridge | detail [active] |
inconsistentports | interface interface-id | mst | pathcost method | root | summary [totals] |
uplinkfast | vlan vlan-id] [ | {begin | exclude | include} expression]
```

```
show spanning-tree vlan vlan-id [active [detail] | blockedports | bridge | detail [active] |
inconsistentports | interface interface-id | root | summary] [ | {begin | exclude | include}
expression]
```

```
show spanning-tree {vlan vlan-id} bridge [address | detail | forward-time | hello-time | id |
max-age | priority [system-id] | protocol] [ | {begin | exclude | include} expression]
```

```
show spanning-tree {vlan vlan-id} root [address | cost | detail | forward-time | hello-time | id |
max-age | port | priority [system-id]] [ | {begin | exclude | include} expression]
```

```
show spanning-tree interface interface-id [active [detail] | cost | detail [active] | inconsistency |
portfast | priority | rootcost | state] [ | {begin | exclude | include} expression]
```

```
show spanning-tree mst [configuration | instance-id] [detail | interface interface-id [detail]]
[ | {begin | exclude | include} expression]
```

Syntax Description

active [detail]	(Optional) Display spanning-tree information only on active interfaces (only available in privileged EXEC mode).
backbonefast	(Optional) Display spanning-tree BackboneFast status.
blockedports	(Optional) Display blocked port information (only available in privileged EXEC mode).
bridge [address detail forward-time hello-time id max-age priority [system-id] protocol]	(Optional) Display status and configuration of this switch (optional keywords only available in privileged EXEC mode).
detail [active]	(Optional) Display a detailed summary of interface information (active keyword only available in privileged EXEC mode).
inconsistentports	(Optional) Display inconsistent port information (only available in privileged EXEC mode).
interface <i>interface-id</i> [active [detail] cost detail [active] inconsistency portfast priority rootcost state]	(Optional) Display spanning-tree information for the specified interface (all options except portfast and state only available in privileged EXEC mode). Enter each interface separated by a space. Ranges are not supported. Valid interfaces include physical ports, VLANs, and port channels. The valid VLAN range is 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1005 when the standard software image (SI) is installed. The valid port-channel range is 1 to 6.

mst [configuration <i>instance-id</i>] [detail interface <i>interface-id</i> [detail]]	<p>These keywords and options are available only if your switch is running the EI.</p> <p>(Optional) Display the multiple spanning-tree (MST) region configuration and status (all options only available in privileged EXEC mode).</p> <p>Display MST information for an instance, a range of instances separated by a hyphen, or a series of instances separated by a comma. The range is 0 to 15.</p> <p>Valid interfaces include physical ports, VLANs, and port channels. The valid VLAN range is 1 to 4094. The valid port-channel range is 1 to 6.</p>
pathcost method	(Optional) Display the default path cost method (only available in privileged EXEC mode).
root [address cost detail forward-time hello-time id max-age port priority [system-id]]	(Optional) Display root switch status and configuration (all keywords only available in privileged EXEC mode).
summary [totals]	(Optional) Display a summary of port states or the total lines of the spanning-tree state section.
uplinkfast	(Optional) Display spanning-tree UplinkFast status.
vlan <i>vlan-id</i> [active [detail] backbonefast blockedports bridge [address detail forward-time hello-time id max-age priority [system-id] protocol]	<p>(Optional) Display spanning-tree information for a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma (some keywords only available in privileged EXEC mode).</p> <p>The range is 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1005 when the standard software image (SI) is installed.</p>
begin	(Optional) Display begins with the line that matches the <i>expression</i> .
exclude	(Optional) Display excludes lines that match the <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

User EXEC; indicated keywords available only in privileged EXEC mode

Command History

Release	Modification
12.0(5.2)WC(1)	This command was first introduced.
12.1(6)EA2	The active , backbonefast , blockedports , bridge , inconsistentports , pathcost method , root , total , and uplinkfast keywords were added.
12.1(9)EA1	The mst keyword and options were added. The brief keyword was removed, and the detail keyword was added.
12.1(13)EA1	The values for the <i>instance-id</i> and <i>vlan-id</i> variables were changed.

Usage Guidelines

If the *vlan-id* variable is omitted, the command applies to the spanning-tree instance for all VLANs. Expressions are case sensitive. For example, if you enter **! exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show spanning-tree active** command:

```
Switch# show spanning-tree active
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    20481
            Address    0008.217a.5800
            Cost      38
            Port      1 (FastEthernet0/1)
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
            Address    0008.205e.6600
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
            Aging Time 300

Interface          Role Sts Cost      Prio.Nbr Type
-----
Fa0/1              Root FWD 19        128.1   P2p
```

This is an example of output from the **show spanning-tree detail** command:

```
Switch> show spanning-tree detail

VLAN0001 is executing the ieee compatible Spanning Tree protocol
  Bridge Identifier has priority 32768, sysid 1, address 0008.205e.6600
  Configured hello time 2, max age 20, forward delay 15
  Current root has priority 20481, address 0008.217a.5800
  Root port is 1 (FastEthernet0/1), cost of root path is 38
  Topology change flag not set, detected flag not set
  Number of topology changes 0 last change occurred 3w0d ago
  Times: hold 1, topology change 35, notification 2
         hello 2, max age 20, forward delay 15
  Timers: hello 0, topology change 0, notification 0, aging 300

Port 1 (FastEthernet0/1) of VLAN0001 is forwarding
  Port path cost 19, Port priority 128, Port Identifier 128.1.
  Designated root has priority 20481, address 0008.217a.5800
  Designated bridge has priority 65535, address 0050.2aed.5c80
  Designated port id is 128.26, designated path cost 19
  Timers: message age 3, forward delay 0, hold 0
  Number of transitions to forwarding state: 1
  Link type is point-to-point by default
  BPDU: sent 0, received 947349

<output truncated>
```

This is an example of output from the **show spanning-tree interface fastethernet 0/1** command:

```
Switch> show spanning-tree interface fastethernet0/1
```

Vlan	Role	Sts	Cost	Prio.Nbr	Type
VLAN0001	Root	FWD	19	128.1	P2p

This is an example of output from the **show spanning-tree summary** command:

```
Switch> show spanning-tree summary
Switch is in pvst mode
Root bridge for: none
EtherChannel misconfiguration guard is enabled
Extended system ID is enabled
Portfast is disabled by default
PortFast BPDU Guard is disabled by default
Portfast BPDU Filter is disabled by default
Loopguard is disabled by default
UplinkFast is disabled
BackboneFast is disabled
Pathcost method used is short
```

Name	Blocking	Listening	Learning	Forwarding	STP Active
VLAN0001	0	0	0	1	1
1 vlan	0	0	0	1	1

<output truncated>

This is an example of output from the **show spanning-tree mst configuration** command:

```
Switch# show spanning-tree mst configuration
```

```
Name [region1]
Revision 1
Instance Vlans mapped
```

```
-----
0 101-4094
1 1-100
-----
```

This is an example of output from the **show spanning-tree mst interface fastethernet0/1** command:

```
Switch# show spanning-tree mst interface fastethernet0/1
```

```
FastEthernet0/1 of MST00 is designated forwarding
Edge port:no (default) port guard :none (default)
Link type:point-to-point (auto) bpdu filter:disable (default)
Boundary :internal bpdu guard :disable (default)
Bpdus sent 84122, received 83933
```

Instance	Role	Sts	Cost	Prio.Nbr	Vlans mapped
0	Desg	FWD	200000	128.1	101-4094
1	Root	FWD	200000	128.1	1-100

This is an example of output from the **show spanning-tree mst 0** command:

```
Switch# show spanning-tree mst 0
##### MST00 vlans mapped: 101-4094
Bridge address 0005.7428.1f40 priority 32768 (32768 sysid 0)
Root address 0001.42e2.cdc6 priority 32768 (32768 sysid 0)
port Gi0/2 path cost 200038
IST master this switch
```

show spanning-tree

```
Operational hello time 2, forward delay 15, max age 20
Configured hello time 2, forward delay 15, max age 20, max hops 20
```

Interface	Role	Sts	Cost	Prio.	Nbr	Type
Gi/1	Desg	FWD	200000	128.1		P2p
Gi0/2	Root	FWD	200000	128.2		P2p Bound(PVST)

Related Commands

Command	Description
clear spanning-tree counters	Clears the spanning-tree counters.
clear spanning-tree detected-protocols	Restarts the protocol migration process.
spanning-tree backbonefast	Enables the BackboneFast feature.
spanning-tree bpdudfilter	Prevents a port from sending or receiving bridge protocol data units (BPDUs).
spanning-tree bpduguard	Puts a port in the error-disabled state when it receives a BPDU.
spanning-tree cost	Sets the path cost for spanning-tree calculations.
spanning-tree extend system-id	Enables the extended system ID feature.
spanning-tree guard	Enables the root guard or the loop guard feature for all the VLANs associated with the selected interface.
spanning-tree link-type	Overrides the default link-type setting for rapid spanning-tree transitions to the forwarding state.
spanning-tree loopguard default	Prevents alternate or root ports from becoming the designated port because of a failure that leads to a unidirectional link.
spanning-tree mst configuration	Enters multiple spanning-tree (MST) configuration mode through which the MST region configuration occurs.
spanning-tree mst cost	Sets the path cost for MST calculations.
spanning-tree mst forward-time	Sets the forward-delay time for all MST instances.
spanning-tree mst hello-time	Sets the interval between hello BPDUs sent by root switch configuration messages.
spanning-tree mst max-age	Sets the interval between messages that the spanning tree receives from the root switch.
spanning-tree mst max-hops	Sets the number of hops in an MST region before the BPDU is discarded and the information held for a port is aged.
spanning-tree mst port-priority	Configures an interface priority.
spanning-tree mst priority	Configures the switch priority for the specified spanning-tree instance.
spanning-tree mst root	Configures the MST root switch priority and timers based on the network diameter.
spanning-tree port-priority	Configures an interface priority.
spanning-tree portfast (global configuration)	Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled ports or enables the Port Fast feature on all nontrunking ports.

Command	Description
spanning-tree portfast (interface configuration)	Enables the Port Fast feature on an interface and all its associated VLANs.
spanning-tree uplinkfast	Accelerates the choice of a new root port when a link or switch fails or when the spanning tree reconfigures itself.
spanning-tree vlan	Configures spanning tree on a per-VLAN basis.

show storm-control

Use the **show storm-control** user EXEC command to display the packet-storm control information. This command also displays the action that the switch takes when the thresholds are reached.

```
show storm-control [interface-id] [{broadcast | history | multicast | unicast}] [ | {begin | exclude | include} expression]
```

Syntax Description

<i>interface-id</i>	(Optional) Port for which information is to be displayed.
broadcast	(Optional) Display broadcast storm information.
history	(Optional) Display storm history on a per-port basis.
multicast	(Optional) Display multicast storm information.
unicast	(Optional) Display unicast storm information.
 begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(6)EA2	This command was first introduced. It replaced the show port storm-control command.

Usage Guidelines

If the variable *interface-id* is omitted, the **show storm-control** command displays storm-control settings for all ports on the switch.

You can display broadcast, multicast, or unicast packet-storm information by using the corresponding keyword. When no option is specified, the default is to display broadcast storm-control information.

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

Examples

This is an example of output from the **show storm-control broadcast** command when the rising and falling suppression levels are defined as percentages of the total bandwidth:

```
Switch> show storm-control broadcast

Interface  Filter State  Trap State  Upper  Lower  Current  Traps Sent
-----  -
Fa0/1     <inactive>    <inactive>  100.00%  100.00%  0.00%    0
Fa0/2     <inactive>    <inactive>  100.00%  100.00%  0.00%    0
Fa0/3     <inactive>    <inactive>  100.00%  100.00%  0.00%    0
Fa0/4     Forwarding    Below rising  30.00%  20.00%  20.32%   17
. . . . .
```

Table 2-27 lists the **show storm-control** field descriptions.

Table 2-27 show storm-control Field Descriptions

Field	Description
Interface	Displays the ID of the interface.
Filter State	Displays the status of the filter: <ul style="list-style-type: none"> Blocking—Storm control is enabled, action is filter, and a storm has occurred. Forwarding—Storm control is enabled, and a storm has not occurred. Inactive—Storm control is disabled. Shutdown—Storm control is enabled, the action is to shut down, and a storm has occurred. <p>Note If an interface is disabled by a broadcast, multicast, or unicast storm, the filter state for all traffic types is <i>shutdown</i>.</p>
Trap State	Displays the status of the SNMP trap: <ul style="list-style-type: none"> Above rising—Storm control is enabled, and a storm has occurred. Below rising—Storm control is enabled, and a storm has not occurred. Inactive—The trap option is not enabled.
Upper	Displays the rising suppression level as a percentage of total available bandwidth or as the rate at which packets are received in packets per second.
Lower	Displays the falling suppression level as a percentage of total available bandwidth or as the rate at which packets are received in packets per second.
Current	Displays the bandwidth utilization of a specific traffic type as a percentage of total available bandwidth or the current rate at which packets are received in packets per second. This field is valid only when storm control is enabled.
Traps Sent	Displays the number traps sent on an interface for a specific traffic type.

This is an example of output from the **show storm-control fastethernet0/4 history** command, which displays the ten most recent storm events for an interface.

```
Switch> show storm-control fastethernet0/4 history
```

```
Interface Fa0/4 Storm Event History

Event Type          Event Start Time  Duration (seconds)
-----
Unicast             04:58:18          206
Broadcast           05:01:54          n/a
Multicast           05:01:54          n/a
Unicast             05:01:54          108
Broadcast           05:05:00          n/a
Multicast           05:05:00          n/a
Unicast             05:06:00          n/a
Broadcast           05:09:39          n/a
Multicast           05:09:39          n/a
Broadcast           05:11:32          172
```

**Note**

The duration field could be *n/a* when a storm is still present or when a new storm of a different type occurs before the current storm ends.

Related Commands

Command	Description
storm-control	Enables broadcast, multicast, or unicast storm control on a port.

show system mtu

Use the **show system mtu** privileged EXEC command to display the global maximum packet size or maximum transmission unit (MTU) set for the switch.

```
show system mtu [ | {begin | exclude | include} expression]
```

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

Command Modes Privileged EXEC

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

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

Examples This is an example of output from the **show system mtu** command:

```
Switch# show system mtu
System MTU size is 1500 bytes
```

Related Commands	Command	Description
	system mtu	Sets the MTU size for the switch.

show udld

Use the **show udld** user EXEC command to display UniDirectional Link Detection (UDLD) status for all ports or the specified port.

```
show udld [interface-id] [ | {begin | exclude | include} expression]
```

Syntax Description		
	<i>interface-id</i>	(Optional) ID of the interface and port number. Valid interfaces include physical ports and VLANs. The VLAN range is 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1001 when the standard software image (SI) is installed.
	begin	(Optional) Display begins with the line that matches the specified <i>expression</i> .
	exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .
	include	(Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.

Command Modes User EXEC

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

Usage Guidelines If you do not enter an *interface-id*, the administrative and the operational UDLD status for all interfaces appear.

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

Examples This is an example of output from the **show udld gigabitethernet0/1** command. In this example, UDLD is enabled on both ends of the link, and UDLD detects that the link is bidirectional. [Table 2-28](#) describes the fields in this example.

```
Switch> show udld gigabitethernet0/1
Interface gi0/1
---
Port enable administrative configuration setting: Follows device default
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single Neighbor detected
Message interval: 60
Time out interval: 5
  Entry 1
    Expiration time: 146
    Device ID: 1
    Current neighbor state: Bidirectional
    Device name: Switch-A
    Port ID: Gi0/2
```

```
Neighbor echo 1 device: Switch-B
Neighbor echo 1 port: Gi0/1
Message interval: 5
CDP Device name: Switch-A
```

Table 2-28 show uddld Field Descriptions

Field	Description
Interface	The interface on the local device configured for UDLD.
Port enable administrative configuration setting	How UDLD is configured on the port. If UDLD is enabled or disabled, the port enable configuration setting is the same as the operational enable state. Otherwise, the enable operational setting depends on the global enable setting.
Port enable operational state	Operational state that shows whether UDLD is actually running on this port.
Current bidirectional state	The bidirectional state of the link. An unknown state appears if the link is down or if it is connected to an UDLD-incapable device. A bidirectional state appears if the link is a normal two-way connection to a UDLD-capable device. All other values mean miswiring.
Current operational state	The phase of the UDLD state machine. For a normal bidirectional link, the state machine is usually in the Advertisement phase.
Message interval	How often advertisement messages are sent from the local device. Measured in seconds.
Time out interval	The time period, in seconds, that UDLD waits for echoes from a neighbor device during the detection window.
Entry 1	Information from the first cache entry, which contains a copy of echo information received from the neighbor.
Expiration time	The amount of time in seconds remaining before this cache entry is aged out.
Device ID	The neighbor device identification.
Current neighbor state	The neighbor's state. If both the local and neighbor devices are running UDLD, the neighbor state and the local state is bidirectional. If the link is down or the neighbor is not UDLD-capable, no cache entries appear.
Device name	The device name or the system serial number of the neighbor. The system serial number appears if the device name is not set or is set to the default (Switch).
Port ID	The neighbor port ID enabled for UDLD.
Neighbor echo 1 device	The device name of the neighbors' neighbor from which the echo originated.
Neighbor echo 1 port	The port number ID of the neighbor from which the echo originated.
Message interval	The rate, in seconds, at which the neighbor is sending advertisement messages.
CDP ¹ device name	The CDP device name or the system serial number. The system serial number appears if the device name is not set or is set to the default (Switch).

1. CDP = Cisco Discovery Protocol

This is an example of output from the **show uddl** interface configuration command when the aggressive mode is configured:

```
Switch# show uddl gigabitethernet0/1
Interface Gi0/1
---
Port enable administrative configuration setting:Enabled / in aggressive mode
Port enable operational state:Enabled / in aggressive mode
Current bidirectional state:Unknown
Current operational state:Link down
Message interval:7
Time out interval:5
No neighbor cache information stored
```

Related Commands

Command	Description
uddl	Enables UDLD on all ports on the switch.
uddl port	Enables UDLD on a specific port.
uddl reset	Resets any interface that was shut down by UDLD.

show version

Use the **show version** user EXEC command to display version information for the hardware and firmware.

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

Syntax Description

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

Command Modes

User EXEC

Command History

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

Usage Guidelines

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

Examples

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

```
Switch> show version

Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(9)EA1
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Wed 27-Feb-02 06:51 by antonino
Image text-base:0x80010000, data-base:0x804E2000

ROM:Bootstrap program is C2950 boot loader

Switch uptime is 1 hour, 54 minutes
System returned to ROM by power-on
System image file is "flash:c2950-i6q4l2-mz.121-0.0.9.EA1.bin"

cisco WS-C2950G-12-EI (RC32300) processor with 20830K bytes of memory.
Last reset from system-reset
Running Enhanced Image
12 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)

32K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address:00:05:74:28:09:C0
Configuration register is 0xF
```

show vlan

Use the **show vlan** user EXEC command to display the parameters for all configured VLANs or one VLAN (if the VLAN ID or name is specified) on the switch.

```
show vlan [brief | id vlan-id | name vlan-name | remote-span | summary] [ | {begin | exclude | include} expression]
```

Syntax Description

brief	(Optional) Display one line for each VLAN with the VLAN name, status, and its ports.
id <i>vlan-id</i>	(Optional) Display information about a single VLAN identified by VLAN ID number or a range of VLANs. For <i>vlan-id</i> , the range is 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1005 when the standard software image (SI) is installed.
name <i>vlan-name</i>	(Optional) Display information about a single VLAN identified by VLAN name. The VLAN name is an ASCII string from 1 to 32 characters.
remote-span	(Optional) Display information about Remote SPAN (RSPAN) VLANs.
summary	(Optional) Display VLAN summary information. This keyword is available only if your switch is running the EI.
 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
 include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.



Note

Though visible in the command-line help string when the EI is installed, the **internal usage**, **ifindex**, and **private-vlan** keywords are not supported.

Command Modes

User EXEC

Command History

Release	Modification
12.0(5.2)WC(1)	This command was first introduced.
12.1(9)EA1	The summary keyword was added.
12.1(11)EA1	The remote-span keyword was added.
12.1(13)EA1	The value for <i>vlan-id</i> variable was changed.

Usage Guidelines

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

Examples

This is an example of output from the **show vlan** command. [Table 2-29](#) describes each field in the display.

```
Switch> show vlan
```

```

VLAN Name                Status    Ports
-----
1    default                active   Fa0/1, Fa0/2, Fa0/5, Fa0/7
                                   Fa0/8, Fa0/9, Fa0/11, Fa0/12
                                   Gi0/1, Gi0/2

2    VLAN0002              active
51   VLAN0051              active
52   VLAN0052              active
100  VLAN0100              suspended Fa0/3
400  VLAN0400              suspended
1002 fddi-default          active
1003 token-ring-default  active
1004 fddinet-default    active
1005 trnet-default      active

VLAN Type  SAID      MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
-----
1    enet  100001   1500 -     -     -     -     -     1002  1003
2    enet  100002   1500 -     -     -     -     -     0     0
51   enet  100051   1500 -     -     -     -     -     0     0
52   enet  100052   1500 -     -     -     -     -     0     0
100  enet  100100   1500 -     -     -     -     -     0     0
400  enet  100400   1500 -     -     -     -     -     0     0
1002 fddi  101002   1500 -     -     -     -     -     1     1003
1003 tr    101003   1500 1005  3276 -     -     srb   1     1002
1004 fdnet 101004   1500 -     -     1     -     ieee -     0     0
1005 trnet 101005   1500 -     -     15    -     ibm  -     0     0
Remote SPAN VLANs
-----

Primary Secondary Type          Ports
-----

```

Table 2-29 show vlan Command Output Fields

Field	Description
VLAN	VLAN number.
Name	Name, if configured, of the VLAN.
Status	Status of the VLAN (active or suspend).
Ports	Ports that belong to the VLAN.
Type	Media type of the VLAN.
SAID	Security association ID value for the VLAN.
MTU	Maximum transmission unit size for the VLAN.
Parent	Parent VLAN, if one exists.
RingNo	Ring number for the VLAN, if applicable.

Table 2-29 show vlan Command Output Fields (continued)

Field	Description
BrdgNo	Bridge number for the VLAN, if applicable.
Stp	Spanning Tree Protocol type used on the VLAN.
BrdgMode	Bridging mode for this VLAN—possible values are source-route bridging (SRB) and source-route transparent (SRT); the default is SRB.
Trans1	Translation bridge 1.
Trans2	Translation bridge 2.
AREHops	Maximum number of hops for All-Routes Explorer frames—possible values are 1 through 13; the default is 7.
STEHops	Maximum number of hops for Spanning-Tree Explorer frames—possible values are 1 through 13; the default is 7.
Backup CRF	Status of whether or not the Token Ring concentrator relay function (TrCRF) is a backup path for traffic.

This is an example of output from the **show vlan brief** command:

```
Switch> show vlan brief
VLAN Name                Status    Ports
-----
1    default                active   Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                         Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                         Fa0/9, Fa0/10, Fa0/11, Fa0/12
1002 fddi-default         active
1003 token-ring-default   active
1004 fddinet-default       active
1005 trnet-default         active
```

This is an example of output from the **show vlan id** command. The specified VLAN is in the extended VLAN range.

```
Switch# show vlan id 2005
VLAN Name                Status    Ports
-----
2005 VLAN2005           active   Fa0/2

VLAN Type  SAID      MTU   Parent  RingNo  BridgeNo  Stp   BrdgMode  Trans1  Trans2
-----
2005 enet   102005   1500  -       -       -        -    -         0       0
```

This is an example of output from the **show vlan summary** command:

```
Switch> show vlan summary
Number of existing VLANs      : 7
Number of existing VTP VLANs  : 7
Number of existing extended VLANs : 0
```

Related Commands	Command	Description
	switchport mode	Configures the VLAN membership mode of a port.
	vlan (global configuration)	Enables config-vlan mode where you can configure VLANs 1 to 4094 when the EI is installed and 1 to 1005 when the standard software image (SI) is installed.
	vlan (VLAN configuration)	Configures VLAN characteristics in the VLAN database. Only available for normal-range VLANs (VLAN IDs 1 to 1005). Do not enter leading zeros.

show vmps

Use the **show vmps** user EXEC command without keywords to display the VLAN Query Protocol (VQP) version, reconfirmation interval, retry count, VLAN Membership Policy Server (VMPS) IP addresses, and the current and primary servers, or use the **statistics** keyword to display client-side statistics.

```
show vmps [statistics] [ | { begin | exclude | include } expression]
```

Syntax Description		
	statistics	(Optional) Display VQP client-side statistics and counters.
	 begin	(Optional) Display begins with the line that matches the <i>expression</i> .
	 exclude	(Optional) Display excludes lines that match the <i>expression</i> .
	 include	(Optional) Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>	Expression in the output to use as a reference point.

Command Modes User EXEC

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

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

Examples This is an example of output from the **show vmps** command:

```
Switch> show vmps
VQP Client Status:
-----
VMPS VQP Version: 1
Reconfirm Interval: 60 min
Server Retry Count: 3
VMPS domain server:

Reconfirmation status
-----
VMPS Action:          other
```

This is an example of output from the **show vmps statistics** command. [Table 2-30](#) describes each field in the example.

```
Switch> show vmps statistics
VMPS Client Statistics
-----
VQP Queries:           0
VQP Responses:        0
VMPS Changes:         0
VQP Shutdowns:       0
VQP Denied:           0
VQP Wrong Domain:    0
VQP Wrong Version:   0
VQP Insufficient Resource: 0
```

Table 2-30 *show vmps statistics Field Descriptions*

Field	Description
VQP Queries	Number of queries sent by the client to the VMPS.
VQP Responses	Number of responses sent to the client from the VMPS.
VMPS Changes	Number of times that the VMPS changed from one server to another.
VQP Shutdowns	Number of times the VMPS sent a response to shut down the port. The client disables the port and removes all dynamic addresses on this port from the address table. You must administratively re-enable the port to restore connectivity.
VQP Denied	Number of times the VMPS denied the client request for security reasons. When the VMPS response denies an address, no frame is forwarded to or from the workstation with that address. (Broadcast or multicast frames are delivered to the workstation if the port on the switch has been assigned to a VLAN.) The client keeps the denied address in the address table as a blocked address to prevent further queries from being sent to the VMPS for each new packet received from this workstation. The client ages the address if no new packets are received from this workstation on this port within the aging time period.
VQP Wrong Domain	Number of times the management domain in the request does not match the one for the VMPS. Any previous VLAN assignments of the port are not changed. This response means that the server and the client have not been configured with the same VTP management domain.
VQP Wrong Version	Number of times the version field in the query packet contains a value that is higher than the version supported by the VMPS. The previous VLAN assignment of the port is not changed. The switches send only VMPS version 1 requests.
VQP Insufficient Resource	Number of times the VMPS is unable to answer the request because of a resource availability problem. If the retry limit has not yet been reached, the client repeats the request with the same server or with the next alternate server, depending on whether the per-server retry count has been reached.

Related Commands	Command	Description
	clear vmps statistics	Clears the statistics maintained by the VQP client.
	vmps reconfirm (global configuration)	Sends VQP queries to reconfirm all dynamic VLAN assignments with the VMPS.
	vmps retry	Configures the per-server retry count for the VQP client.
	vmps server	Configures the primary VMPS and up to three secondary servers.

show vtp

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

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

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

Command Modes	
	User EXEC

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

Usage Guidelines	
	Expressions are case sensitive. For example, if you enter exclude output , the lines that contain <i>output</i> do not appear, but the lines that contain <i>Output</i> appear.

Examples	
	This is an example of output from the show vtp counters command. Table 2-31 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 2-31 *show vtp counters Field Descriptions*

Field	Description
Summary advertisements received	Number of summary advertisements received by this switch on its trunk ports. Summary advertisements contain the management domain name, the configuration revision number, the update timestamp and identity, the authentication checksum, and the number of subset advertisements to follow.
Subset advertisements received	Number of subset advertisements received by this switch on its trunk ports. Subset advertisements contain all the information for one or more VLANs.
Request advertisements received	Number of advertisement requests received by this switch on its trunk ports. Advertisement requests normally request information on all VLANs. They can also request information on a subset of VLANs.
Summary advertisements transmitted	Number of summary advertisements sent by this switch on its trunk ports. Summary advertisements contain the management domain name, the configuration revision number, the update timestamp and identity, the authentication checksum, and the number of subset advertisements to follow.
Subset advertisements transmitted	Number of subset advertisements sent by this switch on its trunk ports. Subset advertisements contain all the information for one or more VLANs.
Request advertisements transmitted	Number of advertisement requests sent by this switch on its trunk ports. Advertisement requests normally request information on all VLANs. They can also request information on a subset of VLANs.
Number of configuration revision errors	<p>Number of revision errors.</p> <p>Whenever you define a new VLAN, delete an existing one, suspend or resume an existing VLAN, or modify the parameters on an existing VLAN, the configuration revision number of the switch increments.</p> <p>Revision errors increment whenever the switch receives an advertisement whose revision number matches the revision number of the switch, but the MD5 digest values do not match. This error means that the VTP password in the two switches is different or that the switches have different configurations.</p> <p>These errors means that the switch is filtering incoming advertisements, which causes the VTP database to become unsynchronized across the network.</p>

Table 2-31 show vtp counters Field Descriptions (continued)

Field	Description
Number of configuration digest errors	Number of MD5 digest errors. Digest errors increment whenever the MD5 digest in the summary packet and the MD5 digest of the received advertisement calculated by the switch do not match. This error usually means that the VTP password in the two switches is different. To solve this problem, make sure the VTP password on all switches is the same. These errors mean that the switch is filtering incoming advertisements, which causes the VTP database to become unsynchronized across the network.
Number of V1 summary errors	Number of version 1 errors. Version 1 summary errors increment whenever a switch in VTP V2 mode receives a VTP version 1 frame. These errors mean that at least one neighboring switch is either running VTP version 1 or VTP version 2 with V2-mode disabled. To solve this problem, change the configuration of the switches in VTP V2-mode to disabled.
Join Transmitted	Number of VTP pruning messages sent on the trunk.
Join Received	Number of VTP pruning messages received on the trunk.
Summary Advts Received from non-pruning-capable device	Number of VTP summary messages received on the trunk from devices that do not support pruning.

This is an example of output from the **show vtp status** command. [Table 2-32](#) describes each field in the display.

```
Switch> show vtp status

VTP Version           : 2
Configuration Revision : 0
Maximum VLANs supported locally : 250
Number of existing VLANs : 5
VTP Operating Mode    : Server
VTP Domain Name       :
VTP Pruning Mode      : Disabled
VTP V2 Mode           : Disabled
VTP Traps Generation  : Disabled
MD5 digest            : 0xBF 0x86 0x94 0x45 0xFC 0xDF 0xB5 0x70
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 172.20.135.196 on interface V11 (lowest numbered VLAN interface found)
```

Table 2-32 show vtp status Field Descriptions

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

Table 2-32 show vtp status Field Descriptions (continued)

Field	Description
VTP Operating Mode	<p>Displays the VTP operating mode, which can be server, client, or transparent.</p> <p>Server: a switch in VTP server mode is enabled for VTP and sends advertisements. You can configure VLANs on it. The switch guarantees that it can recover all the VLAN information in the current VTP database from nonvolatile RAM (NVRAM) after reboot. By default, every switch is a VTP server.</p> <p>Note The switch automatically changes from VTP server mode to VTP client mode if it detects a failure while writing the configuration to NVRAM and cannot return to server mode until the NVRAM is functioning.</p> <p>Client: a switch in VTP client mode is enabled for VTP, can send advertisements, but does not have enough nonvolatile storage to store VLAN configurations. You cannot configure VLANs on it. When a VTP client starts up, it does not send VTP advertisements until it receives advertisements to initialize its VLAN database.</p> <p>Transparent: a switch in VTP transparent mode is disabled for VTP, does not send or learn from advertisements sent by other devices, and cannot affect VLAN configurations on other devices in the network. The switch receives VTP advertisements and forwards them on all trunk ports except the one on which the advertisement was received.</p>
VTP Domain Name	Name that identifies the administrative domain for the switch.
VTP Pruning Mode	Displays whether pruning is enabled or disabled. Enabling pruning on a VTP server enables pruning for the entire management domain. Pruning restricts flooded traffic to those trunk links that the traffic must use to access the appropriate network devices.
VTP V2 Mode	Displays if VTP version 2 mode is enabled. By default, all VTP version 2 switches operate in version 1 mode. Each VTP switch automatically detects the capabilities of all the other VTP devices. A network of VTP devices should be configured to version 2 only if all VTP switches in the network can operate in version 2 mode.
VTP Traps Generation	Displays whether VTP traps are sent to a network management station.
MD5 Digest	A 16-byte checksum of the VTP configuration.
Configuration Last Modified	Displays the date and time of the last configuration modification. Displays the IP address of the switch that caused the configuration change to the database.

Related Commands	Command	Description
	clear vtp counters	Clears the VTP and pruning counters.
	vtp (global configuration)	Configures the VTP filename, interface name, domain name, and mode. You can save configuration resulting from this command in the switch configuration file.
	vtp (privileged EXEC)	Configures the VTP password, pruning, and version.
	vtp (VLAN configuration)	Configures the VTP domain name, password, pruning, and mode.

show wrr-queue bandwidth

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 <i>expression</i> .	
exclude	(Optional) Display excludes lines that match the specified <i>expression</i> .	
include	(Optional) Display includes lines that match the specified <i>expression</i> .	
<i>expression</i>	Expression in the output to use as a reference point.	

Command Modes User EXEC

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

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

Examples This is an example of output from the **show wrr-queue bandwidth** command:

```
Switch> show wrr-queue bandwidth
WRR Queue : 1 2 3 4
Bandwidth : 10 20 30 40
```

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

show wrr-queue cos-map

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

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

Syntax Description

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

Command Modes

User EXEC

Command History

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

Usage Guidelines

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

Examples

This is an example of output from the **show wrr-queue 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
show wrr-queue bandwidth	Displays the WRR bandwidth allocation for the four CoS priority queues.
wrr-queue bandwidth	Assigns weighted round-robin (WRR) weights to the four CoS priority queues.
wrr-queue cos-map	Assigns CoS values to the CoS priority queues.

shutdown

Use the **shutdown** interface configuration command to disable a port and to shut down the management VLAN. Use the **no** form of this command to enable a disabled port or to activate the management VLAN.

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

Only one management VLAN interface can be active at a time. The remaining VLANs are shut down. In the **show running-config** command, the active management VLAN interface is the one without the **shutdown** command displayed.

When you enter the **shutdown** command on an LRE switch, the switch disables the interface by de-activating the MAC interface and the LRE chipset transmitter. Under some circumstances, the power emitted by LRE switch ports can affect other LRE switch ports. We recommend that ports that are not connected to CPE devices be shut down by using this command. You can also use this command to disable access to the switch from a particular port.

Examples

This example shows how to disable fixed Fast Ethernet port 0/8 and how to re-enable it:

```
Switch(config)# interface fastethernet0/8
Switch(config-if)# shutdown

Switch(config-if)# no shutdown
```

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

shutdown vlan

Use the **shutdown vlan** global configuration command to shut down (suspend) local traffic on the specified VLAN. Use the **no** form of this command to restart local traffic on the VLAN.

shutdown vlan *vlan-id*

no shutdown vlan *vlan-id*

Syntax Description	<i>vlan-id</i>	ID of the VLAN to be locally shut down. Valid IDs are from 2 to 1001. VLANs defined as default VLANs under the VLAN Trunking Protocol (VTP), as well as extended-range VLANs (greater than 1005) cannot be shut down. The default VLANs are 1 and 1002 to 1005.
Defaults	No default is defined.	
Command Modes	Global configuration	
Command History	Release	Modification
	12.0(5.2)WC(1)	This command was first introduced.
Usage Guidelines	The shutdown vlan command does not change the VLAN information in the VTP database. It shuts down traffic locally, but the switch still advertises VTP information.	
Examples	<p>This example shows how to shutdown traffic on VLAN 2:</p> <pre>Switch(config)# shutdown vlan 2</pre> <p>You can verify your setting by entering the show vlan privileged EXEC command.</p>	
Related Commands	Command	Description
	shutdown (config-vlan mode)	Shuts down local traffic on the VLAN when in config-VLAN mode (accessed by the vlan <i>vlan-id</i> global configuration command).
	vlan (global configuration)	Enables config-vlan mode.
	vlan database	Enters VLAN configuration mode.

snmp-server enable traps

Use the **snmp-server enable traps** global configuration command to enable the switch to send Simple Network Management Protocol (SNMP) notification for various trap types to the network management system (NMS). Use the **no** form of this command to return to the default setting.

snmp-server enable traps [alarms | bridge | c2900 | cluster | config | copy-config | entity | envmon [fan | shutdown | supply | temperature | voltage] | flash | hsrp | mac-notification | port-security [trap-rate *value*] | rtr | snmp [authentication | coldstart | linkdown | linkup | warmstart] | stpx | syslog | vlan-membership | vlancreate | vlandelete | vtp]

no snmp-server enable traps [alarms | bridge | c2900 | cluster | config | copy-config | entity | envmon | flash | hsrp | mac-notification | port-security | rtr | snmp | stpx | syslog | vlan-membership | vlancreate | vlandelete | vtp]

Syntax	Description
alarms	(Optional) Enable SNMP alarm traps. This keyword is only available on a Catalyst 2955 switch.
bridge	(Optional) Enable SNMP Spanning Tree Protocol (STP) bridge management information base (MIB) traps.
c2900	(Optional) Enable SNMP configuration traps.
cluster	(Optional) Enable cluster traps.
config	(Optional) Enable SNMP configuration traps.
copy-config	(Optional) Enable SNMP copy-configuration traps.
entity	(Optional) Enable SNMP entity traps.
envmon	(Optional) Enable environmental monitor (EnvMon) MIB.
fan	(Optional) Enable SNMP EnvMon fan traps.
shutdown	(Optional) Enable SNMP EnvMon monitor shutdown traps.
supply	(Optional) Enable SNMP power supply traps.
temperature	(Optional) Enable SNMP EnvMon temperature traps.
voltage	(Optional) Enable SNMP EnvMon voltage traps.
flash	(Optional) Enable SNMP FLASH notifications.
hsrp	(Optional) Enable Hot Standby Router Protocol (HSRP) traps.
mac-notification	(Optional) Enable MAC address notification traps.
port-security	(Optional) Enable port security traps.
trap-rate <i>value</i>	(Optional) Set the number of traps per second. The range is from 0 to 1000.
rtr	(Optional) Enable SNMP Response Time Reporter traps.
snmp	(Optional) Enable SNMP traps.
authentication	(Optional) Enable SNMP authentication traps.
coldstart	(Optional) Enable SNMP coldstart traps.
linkdown	(Optional) Enable SNMP linkdown traps.
linkup	(Optional) Enable SNMP linkup traps.
warmstart	(Optional) Enable SNMP warmstart traps.
stpx	(Optional) Enable SNMP STPX MIB traps.
syslog	(Optional) Enable SNMP syslog traps.

vlan-membership	(Optional) Enable SNMP VLAN membership traps.
vlancreate	(Optional) Enable SNMP VLAN-created traps.
vlandelete	(Optional) Enable SNMP VLAN-deleted traps.
vtp	(Optional) Enable VLAN Trunking Protocol (VTP) traps.

**Note**

Though visible in the command-line help strings, the **flash insertion** and **flash removal** keywords are not supported. The **snmp-server enable informs** command is not supported. To enable sending of SNMP inform notifications, use the **snmp-server enable traps** command combined with the **snmp-server host *host-addr* informs** command.

Defaults

The sending of SNMP traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(6)EA2	This command was first introduced.
12.1(9)EA1	The vlan-membership keyword was added.
12.1(12c)EA1	The envmon , fan , shutdown , supply , temperature , and voltage keywords were added. The alarm keyword was also added (only available on a Catalyst 2955 switch).
12.1(13)EA1	The port-security and trap-rate keywords were added.
12.1(14)EA1	The authentication , bridge , coldstart , copy-config , flash , linkdown , linkup , stp , stp , vlancreate , vlandelete , and warmstart keywords were added.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Use the **snmp-server enable traps** command to enable sending of traps or informs, when supported.

**Note**

Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to send EnvMon traps to the NMS:

```
Switch(config)# snmp-server enable traps envmon fan
```

This example shows how to send VTP traps to the NMS:

```
Switch(config)# snmp-server enable traps vtp
```

You can verify your setting by entering the **show vtp status** privileged EXEC or the **show running-config** privileged EXEC command.

Related Commands	Command	Description
	show running-config	Displays the running configuration on the switch. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 > Cisco IOS File Management Commands > Configuration File Commands .
	snmp-server host	Specifies the host that receives SNMP traps.

snmp-server host

Use the **snmp-server host** global configuration command to specify the recipient (host) of a Simple Network Management Protocol (SNMP) notification operation. Use the **no** form of this command to remove the specified host.

```
snmp-server host host-addr [informs | traps] [version {1 | 2c | 3 [auth | noauth | priv]]]
  community-string [alarms] [bridge] [c2900] [cluster] [config] [copy-config] [entity]
  [envmon] [flash] [hsrp] [mac-notification] [port-security] [rtr] [snmp] [stpx] [syslog] [tty]
  [udp-port] [vlan-membership] [vlancreate] [vlandelete] [vtp]
```

```
no snmp-server host host-addr [informs | traps] [version {1 | 2c | 3 [auth | noauth | priv]]]
  community-string
```

Syntax Description

<i>host-addr</i>	Name or Internet address of the host (the targeted recipient).
informs traps	(Optional) Send SNMP traps or informs to this host.
version 1 2c 3	(Optional) Version of SNMP used to send the traps. These keywords are supported: 1—SNMPv1. This option is not available with informs. 2c—SNMPv2C. 3—SNMPv3. These optional keywords can follow the version 3 keyword: <ul style="list-style-type: none"> auth (Optional). Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication. noauth (Default). The noAuthNoPriv security level. This is the default if the [auth noauth] keyword choice is not specified. priv (Optional). Enables Data Encryption Standard (DES) packet encryption (also called <i>privacy</i>). <p>Note The priv keyword is available only when the cryptographic (encrypted) software image is installed.</p>
<i>community-string</i>	Password-like community string sent with the notification operation. Though you can set this string by using the snmp-server host command, we recommend that you define this string by using the snmp-server community global configuration command before using the snmp-server host command.
alarms	(Optional) Send SNMP alarm traps. This keyword is only available on a Catalyst 2955 switch.
bridge	(Optional) Send SNMP STP bridge MIB traps.
c2900	(Optional) Send SNMP switch traps.
cluster	(Optional) Send cluster member status traps.
config	(Optional) Send SNMP configuration traps.
copy-config	(Optional) Send SNMP copy-configuration traps.
entity	(Optional) Send SNMP entity traps.
envmon	(Optional) Send enviromental monitor (EnvMon) traps.
flash	(Optional) Send SNMP FLASH notifications.

hsrp	(Optional) Send Hot Standby Router Protocol (HSRP) traps.
mac-notification	(Optional) Send MAC notification traps.
port-security	(Optional) Send port security traps.
rtr	(Optional) Send SNMP Response Time Reporter traps.
snmp	(Optional) Send SNMP-type traps.
stpx	(Optional) Send SNMP STPX MIB traps.
syslog	(Optional) Send SNMP syslog traps.
tty	(Optional) Send Transmission Control Protocol (TCP) connection traps.
udp-port	(Optional) Send notification host's User Datagram Protocol (UDP) port number.
vlan-membership	(Optional) Send SNMP VLAN membership traps.
vlancreate	(Optional) Send SNMP VLAN-created traps.
vlandelete	(Optional) Send SNMP VLAN-deleted traps.
vtp	(Optional) Send VLAN Trunking Protocol (VTP) traps.

Defaults

This command is disabled. No notifications are sent.

If you enter this command with no keywords, the default is to send all trap types to the host. No informs are sent to this host.

If no **version** keyword is present, the default is version 1.

If version 3 is selected and no authentication keyword is entered, the default is the **noauth** (noAuthNoPriv) security level.



Note

If the *community-string* is not defined by using the **snmp-server community** global configuration command before using this command, the default form of the **snmp-server community** command is automatically inserted into the configuration. The password (*community-string*) used for this automatic configuration of the **snmp-server community** will be the same as that specified in the **snmp-server host** command.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5.2)WC(1)	This command was first introduced.
12.1(6)EA2	The cluster , mac-notification , and rtr keywords were added.
12.1(9)EA1	The vlan-membership keyword was added.
12.1(11)EA1	The version 3 option was added, with the auth and noauth keywords.
12.1(12c)EA1	The envmon and priv keywords were added. The alarm keyword was also added (only for the Catalyst 2955 switch).
12.1(13)EA1	The port-security keyword was added.
12.1(14)EA1	The bridge , copy-config , flash , stpx , syslog , vlancreate , and vlandelete keywords were added.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response PDU. If the sender never receives the response, the inform request can be sent again. Thus, informs are more likely to reach their intended destinations.

However, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Traps are also sent only once, but an inform might be retried several times. The retries increase traffic and contribute to a higher overhead on the network.

If you do not enter an **snmp-server host** command, no notifications are sent. To configure the switch to send SNMP notifications, you must enter at least one **snmp-server host** command. If you enter the command with no keywords, all trap types are enabled for the host. To enable multiple hosts, you must enter a separate **snmp-server host** command for each host. You can specify multiple notification types in the command for each host.

When multiple **snmp-server host** commands are given for the same host and kind of notification (trap or inform), each succeeding command overwrites the previous command. Only the last **snmp-server host** command is in effect. For example, if you enter an **snmp-server host inform** command for a host and then enter another **snmp-server host inform** command for the same host, the second command replaces the first.

The **snmp-server host** command is used with the **snmp-server enable traps** global configuration command. Use the **snmp-server enable traps** command to specify which SNMP notifications are sent globally. For a host to receive most notifications, at least one **snmp-server enable traps** command and the **snmp-server host** command for that host must be enabled. Some notification types cannot be controlled with the **snmp-server enable traps** command. For example, some notification types are always enabled. Other notification types are enabled by a different command.

The **no snmp-server host** command with no keywords disables traps, but not informs, to the host. To disable informs, use the **no snmp-server host informs** command.

Examples

This example shows how to configure a unique SNMP community string named *comaccess* for traps and prevent SNMP polling access with this string through access-list 10:

```
Switch(config)# snmp-server community comaccess ro 10
Switch(config)# snmp-server host 172.20.2.160 comaccess
Switch(config)# access-list 10 deny any
```

This example shows how to send the SNMP traps to the host specified by the name *myhost.cisco.com*. The community string is defined as *comaccess*:

```
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server host myhost.cisco.com comaccess snmp
```

This example shows how to enable the switch to send all traps to the host *myhost.cisco.com* using the community string *public*:

```
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server host myhost.cisco.com public
```

This example shows how to enable the switch to send EnvMon traps to the host *myhost.cisco.com* using the community string *public*:

```
Switch(config)# snmp-server host myhost.cisco.com version 2c public envmon
```

Related Commands	Command	Description
	show running-config	Displays the running configuration on the switch. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 > Cisco IOS File Management Commands > Configuration File Commands.
	snmp-server enable traps	Enables SNMP notification for various trap types.

snmp trap mac-notification

Use the **snmp trap mac-notification** interface configuration command to enable the MAC notification traps on a port. Use the **no** form of this command to disable the traps and to return the port to default settings.

snmp trap mac-notification [added | removed]

no snmp trap mac-notification [added | removed]

Syntax Description

added	(Optional) Enable MAC notification traps when a MAC address is added to a port.
removed	(Optional) Enable MAC notification traps when a MAC address is removed from a port.

Defaults

The Simple Network Management Protocol (SNMP) address-addition and address-removal traps are disabled.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Even though you enable the notification trap for a specific interface by using the **snmp trap mac-notification** command, the trap is generated only when you enter the **snmp-server enable traps mac-notification** and the **mac address-table notification** global configuration commands.

Examples

This example shows how to enable an address-addition trap on a port:

```
Switch(config-if)# snmp trap mac-notification added
```

This example shows how to enable an address-removal trap on a port:

```
Switch(config-if)# snmp trap mac-notification removed
```

You can verify your settings by entering the **show mac address-table notification** privileged EXEC command.

Related Commands

Command	Description
clear mac address-table notification	Clears the MAC address notification global counters.
mac address-table notification	Enables the MAC notification feature on a switch.
show mac address-table notification	Displays MAC notification parameters.
snmp-server enable traps	Enables SNMP notification for various trap types.

spanning-tree backbonefast

Use the **spanning-tree backbonefast** global configuration command to enable the BackboneFast feature. Use the **no** form of this command to return to the default setting.

spanning-tree backbonefast

no spanning-tree backbonefast

Syntax Description This command has no arguments or keywords.

Defaults BackboneFast is disabled.

Command Modes Global configuration

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

Usage Guidelines The BackboneFast feature is supported only when the switch is running per-VLAN spanning-tree plus (PVST+). It is not supported when the switch is running rapid PVST+ or multiple spanning-tree (MST).

BackboneFast is started when a root port or blocked port on a switch receives inferior bridge protocol data units (BPDUs) from its designated bridge. An inferior BPDU identifies one switch as both the root bridge and the designated bridge. When a switch receives an inferior BPDU, it means that a link to which the switch is not directly connected (an *indirect* link) has failed (that is, the designated bridge has lost its connection to the root switch). If there are alternate paths to the root switch, BackboneFast causes the maximum aging time on the ports on which it received the inferior BPDU to expire and allows a blocked port to move immediately to the listening state. BackboneFast then transitions the interface to the forwarding state. For more information, refer to the software configuration guide for this release.

Enable BackboneFast on all supported switches to allow the detection of indirect link failures and to start the spanning-tree reconfiguration sooner.

Examples This example shows how to enable BackboneFast on the switch:

```
Switch(config)# spanning-tree backbonefast
```

You can verify your setting by entering the **show spanning-tree summary** privileged EXEC command.

Related Commands	Command	Description
	show spanning-tree summary	Displays a summary of the spanning-tree port states.

spanning-tree bpdudfilter

Use the **spanning-tree bpdudfilter** interface configuration command to prevent a port from sending or receiving bridge protocol data units (BPDUs). Use the **no** form of this command to return to the default setting.

spanning-tree bpdudfilter { disable | enable }

no spanning-tree bpdudfilter

Syntax Description

disable	Disable BPDU filtering on the specified interface.
enable	Enable BPDU filtering on the specified interface.

Defaults

BPDU filtering is disabled.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

You can enable the BPDU filtering feature when the switch is operating in the per-VLAN spanning-tree plus (PVST+), rapid-PVST+, or in the multiple spanning-tree (MST) mode. The rapid-PVST+ and MST modes are available only if you have the enhanced software image (EI) installed on your switch.



Caution

Enabling BPDU filtering on an interface is the same as disabling spanning tree on it and can result in spanning-tree loops.

You can globally enable BPDU filtering on all Port Fast-enabled ports by using the **spanning-tree portfast bpdudfilter default** global configuration command.

You can use the **spanning-tree bpdudfilter** interface configuration command to override the setting of the **spanning-tree portfast bpdudfilter default** global configuration command.

Examples

This example shows how to enable the BPDU filtering feature on a port:

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# spanning-tree bpdudfilter enable
```

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

Related Commands

Command	Description
show running-config	Displays the current operating configuration. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 > Cisco IOS File Management Commands > Configuration File Commands .
spanning-tree portfast (global configuration)	Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled ports or enables the Port Fast feature on all nontrunking ports.
spanning-tree portfast (interface configuration)	Enables the Port Fast feature on an interface and all its associated VLANs.

spanning-tree bpduguard

Use the **spanning-tree bpduguard** interface configuration command to put a port in the error-disabled state when it receives a bridge protocol data unit (BPDU). Use the **no** form of this command to return to the default setting.

```
spanning-tree bpduguard { disable | enable }
```

```
no spanning-tree bpduguard
```

Syntax Description

disable	Disable BPDU guard on the specified interface.
enable	Enable BPDU guard on the specified interface.

Defaults

BPDU guard is disabled.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

The BPDU guard feature provides a secure response to invalid configurations because you must manually put the port back in service. Use the BPDU guard feature in a service-provider network to prevent a port from being included in the spanning-tree topology.

You can enable the BPDU guard feature when the switch is operating in the per-VLAN spanning-tree plus (PVST+), rapid-PVST+, or the multiple spanning-tree (MST) mode. The rapid-PVST+ and MST modes are available only if you have the enhanced software image (EI) installed on your switch.

You can globally enable BPDU guard on all Port Fast-enabled ports by using the **spanning-tree portfast bpduguard default** global configuration command.

You can use the **spanning-tree bpduguard** interface configuration command to override the setting of the **spanning-tree portfast bpduguard default** global configuration command.

Examples

This example shows how to enable the BPDU guard feature on a port:

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# spanning-tree bpduguard enable
```

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

Related Commands	Command	Description
	show running-config	Displays the current operating configuration. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 > Cisco IOS File Management Commands > Configuration File Commands .
	spanning-tree portfast (global configuration)	Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled ports, or enables the Port Fast feature on all nontrunking ports.
	spanning-tree portfast (interface configuration)	Enables the Port Fast feature on an interface and all its associated VLANs.

spanning-tree cost

Use the **spanning-tree cost** interface configuration command to set the path cost for spanning-tree calculations. If a loop occurs, spanning tree considers the path cost when selecting an interface to place in the forwarding state. Use the **no** form of this command to return to the default setting.

spanning-tree [vlan *vlan-id*] cost *cost*

no spanning-tree [vlan *vlan-id*] cost

Syntax Description

vlan <i>vlan-id</i>	(Optional) VLAN range associated with a spanning-tree instance. You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1005 when the standard software image (SI) is installed.
<i>cost</i>	Path cost can range from 1 to 200000000, with higher values meaning higher costs.

Defaults

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

- 10 Mbps—100
- 100 Mbps—19
- 155 Mbps—14
- 1000 Mbps—4
- 1 Gbps—4
- 10 Gbps—2
- Speeds greater than 10 Gbps—1

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5.2)WC(1)	This command was first introduced.
12.1(9)EA1	The range for the <i>cost</i> variable increased.
12.1(13)EA1	The value for the <i>vlan-id</i> variable was changed.

Usage Guidelines

When you configure the cost, higher values represent higher costs.

You can set a cost on a VLAN that does not exist. The setting takes effect when the VLAN exists.

If you configure an interface with both the **spanning-tree vlan *vlan-id* cost *cost*** command and the **spanning-tree cost *cost*** command, the **spanning-tree vlan *vlan-id* cost *cost*** command takes effect.

Examples

This example shows how to set a path cost of 250 on an interface:

```
Switch(config)# interface fastethernet0/4
Switch(config-if)# spanning-tree cost 250
```

This example shows how to set a path cost of 300 for VLANs 10, 12 to 15, and 20:

```
Switch(config-if)# spanning-tree vlan 10,12-15,20 cost 300
```

You can verify your settings by entering the **show spanning-tree interface *interface-id*** privileged EXEC command.

Related Commands

Command	Description
show spanning-tree interface <i>interface-id</i>	Displays spanning-tree information for the specified interface.
spanning-tree port-priority	Configures an interface priority.
spanning-tree vlan priority	Sets the switch priority for the specified spanning-tree instance.

spanning-tree etherchannel guard misconfig

Use the **spanning-tree etherchannel guard misconfig** global configuration command to display an error message when the switch detects a loop that occurred because of an EtherChannel misconfiguration. Use the **no** form of this command to disable the feature.

spanning-tree etherchannel guard misconfig

no spanning-tree etherchannel guard misconfig

Syntax Description

This command has no arguments or keywords.

Defaults

EtherChannel guard is enabled on the switch.

Command Modes

Global configuration

Command History

Release	Modification
12.1(13)EA1	This command was first introduced.

Usage Guidelines

When the switch detects a loop that is caused by an EtherChannel misconfiguration, this error message appears:

```
PM-4-ERR_DISABLE: Channel-misconfig error detected on [chars], putting [chars] in
err-disable state.
```

To determine which switch ports are in the misconfigured EtherChannel, use the **show interfaces status err-disabled** privileged EXEC command. To verify the EtherChannel configuration on a remote device, use the **show etherchannel summary** privileged EXEC command on the remote device.

When a port is in the error-disabled state because of an EtherChannel misconfiguration, you can bring it out of this state by entering the **errdisable recovery cause channel-misconfig** global configuration command, or you can manually re-enable it by entering the **shutdown** and **no shut down** interface configuration commands.

Examples

This example shows how to enable the EtherChannel guard misconfiguration feature:

```
Switch(config)# spanning-tree etherchannel guard misconfig
```

You can verify your settings by entering the **show spanning-tree summary** privileged EXEC command.

Related Commands	Command	Description
	<code>errdisable recovery cause channel-misconfig</code>	Enables the timer to recover from the EtherChannel misconfiguration error-disable state.
	<code>show etherchannel summary</code>	Displays EtherChannel information for a channel as a one-line summary per channel-group.
	<code>show interfaces status err-disabled</code>	Displays the interfaces in the error-disabled state.

spanning-tree extend system-id

Use the **spanning-tree extend system-id** global configuration command to enable the extended system ID feature.

spanning-tree extend system-id



Note

Though visible in the command-line help strings, the **no** version of this command is not supported. You cannot disable the extended system ID feature.

Syntax Description

This command has no arguments or keywords.

Defaults

The extended system ID is enabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

In Cisco IOS Release 12.1(9)EA1 and later, Catalyst 2950 switches support the 802.1T spanning-tree extensions, and some of the bits previously used for the switch priority are now used for the extended system ID (VLAN identifier for the per-VLAN spanning-tree plus [PVST+] and for rapid PVST+ or an instance identifier for the multiple spanning tree [MST]). In earlier releases, the switch priority is a 16-bit value.

The spanning tree uses the extended system ID, the switch priority, and the allocated spanning-tree MAC address to make the bridge ID unique for each VLAN or multiple spanning-tree instance. With earlier releases, spanning tree used one MAC address per VLAN to make the bridge ID unique for each VLAN.

Support for the extended system ID affects how you manually configure the root switch, the secondary root switch, and the switch priority of a VLAN. For more information, see the [“spanning-tree mst root”](#) and the [“spanning-tree vlan”](#) sections.

If your network consists of switches that do not support the extended system ID and switches that do support it, it is unlikely that the switch with the extended system ID support will become the root switch. The extended system ID increases the switch priority value every time the VLAN number is greater than the priority of the connected switches running older software.

Related Commands	Command	Description
	show spanning-tree summary	Displays a summary of spanning-tree port states.
	spanning-tree mst root	Configures the multiple spanning-tree (MST) root switch priority and timers based on the network diameter.
	spanning-tree vlan priority	Sets the switch priority for the specified spanning-tree instance.

spanning-tree guard

Use the **spanning-tree guard** interface configuration command to enable root guard or loop guard on all the VLANs associated with the selected interface. Root guard restricts which interface is allowed to be the spanning-tree root port or the path-to-the root for the switch. Loop guard prevents alternate or root ports from becoming designated ports when a failure creates a unidirectional link. Use the **no** form of this command to return to the default setting.

```
spanning-tree guard {loop | none | root}
```

```
no spanning-tree guard
```

Syntax Description

loop	Enable loop guard.
none	Disable root guard or loop guard.
root	Enable root guard.

Defaults

Root guard is disabled.

Loop guard is configured according to the **spanning-tree loopguard default** global configuration command (globally disabled).

Command Modes

Interface configuration

Command History

Release	Modification
12.1(6)EA2	This command was first introduced. It replaced the spanning-tree rootguard command.
12.1(9)EA1	The loop keyword was added.

Usage Guidelines

You can enable root guard or loop guard when the switch is operating in the per-VLAN spanning-tree plus (PVST+), rapid-PVST+, or the multiple spanning-tree (MST) mode. However, you cannot enable both PVST+ and MST or both rapid PVST+ and MST at the same time. The rapid-PVST+ and MST modes are available only if you have the enhanced software image (EI) installed on your switch.

When root guard is enabled, if spanning-tree calculations cause a port to be selected as the root port, the port transitions to the root-inconsistent (blocked) state to prevent the customer's switch from becoming the root switch or being in the path to the root. The root port provides the best path from the switch to the root switch.

When the **no spanning-tree guard** or the **no spanning-tree guard none** command is entered, root guard is disabled for all VLANs on the selected interface. If this interface is in the root-inconsistent (blocked) state, it automatically transitions to the listening state.

Do not enable root guard on interfaces that will be used by the UplinkFast feature. With UplinkFast, the backup interfaces (in the blocked state) replace the root port in the case of a failure. However, if root guard is also enabled, all the backup interfaces used by the UplinkFast feature are placed in the root-inconsistent state (blocked) and prevented from reaching the forwarding state. The UplinkFast feature is not available when the switch is operating in rapid-PVST+ or MST mode.

Loop guard is most effective when it is configured on the entire switched network. When the switch is operating in PVST+ or rapid-PVST+ mode, loop guard prevents alternate and root ports from becoming designated ports, and spanning tree does not send bridge protocol data units (BPDUs) on root or alternate ports. When the switch is operating in MST mode, BPDUs are not sent on nonboundary ports only if the port is blocked by loop guard in all MST instances. On a boundary port, loop guard blocks the port in all MST instances.

To disable root guard or loop guard, use the **spanning-tree guard none** interface configuration command. You cannot enable both root guard and loop guard at the same time.

You can override the setting of the **spanning-tree loopguard default** global configuration command by using the **spanning-tree guard loop** interface configuration command.

Examples

This example shows how to enable root guard on all the VLANs associated with the specified interface:

```
Switch(config)# interface fastethernet0/3
Switch(config-if)# spanning-tree guard root
```

This example shows how to enable loop guard on all the VLANs associated with the specified interface:

```
Switch(config)# interface fastethernet0/3
Switch(config-if)# spanning-tree guard loop
```

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

Related Commands

Command	Description
show running-config	Displays the current operating configuration. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 > Cisco IOS File Management Commands > Configuration File Commands .
spanning-tree cost	Sets the path cost for spanning-tree calculations.
spanning-tree loopguard default	Prevents alternate or root ports from becoming designated ports because of a failure that leads to a unidirectional link.
spanning-tree mst cost	Configures the path cost for MST calculations.
spanning-tree mst port-priority	Configures an interface priority.
spanning-tree mst root	Configures the MST root switch priority and timers based on the network diameter.
spanning-tree port-priority	Configures an interface priority.
spanning-tree vlan priority	Sets the switch priority for the specified spanning-tree instance.

spanning-tree link-type

Use the **spanning-tree link-type** interface configuration command to override the default link-type setting, which is determined by the duplex mode of the port, and to enable Rapid Spanning-Tree Protocol (RSTP) transitions to the forwarding state. Use the **no** form of this command to return to the default setting.

spanning-tree link-type {point-to-point | shared}

no spanning-tree link-type

Syntax Description	
point-to-point	Specify that the link type of a port is point-to-point.
shared	Specify that the link type of a port is shared.

Defaults The switch derives the link type of a port from the duplex mode. A full-duplex port is considered a point-to-point link, and a half-duplex port is considered a shared link.

Command Modes Interface configuration

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

Usage Guidelines You can override the default setting of the link type by using the **spanning-tree link-type** command; for example, a half-duplex link can be physically connected point-to-point to a single port on a remote switch running the Multiple Spanning Tree Protocol (MSTP) or the rapid per-VLAN spanning-tree plus (rapid-PVST+) protocol and be enabled for rapid transitions.

Examples This example shows how to specify the link type as shared (regardless of the duplex setting) and to prevent RSTP rapid transitions to the forwarding state:

```
Switch(config-if)# spanning-tree link-type shared
```

You can verify your settings by entering the **show spanning-tree mst interface interface-id** privileged EXEC command.

Related Commands	Command	Description
	show spanning-tree mst interface interface-id	Displays multiple spanning-tree (MST) information for the specified interface.

spanning-tree loopguard default

Use the **spanning-tree loopguard default** global configuration command to prevent alternate or root ports from becoming designated ports because of a failure that leads to a unidirectional link. Use the **no** form of this command to return to the default setting.

spanning-tree loopguard default

no spanning-tree loopguard default

Syntax Description This command has no arguments or keywords.

Defaults Loop guard is disabled.

Command Modes Global configuration

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

Usage Guidelines You can enable the loop guard feature when the switch is operating in the per-VLAN spanning-tree plus (PVST+), rapid-PVST+, or the multiple spanning-tree (MST) mode. The rapid-PVST+ and MST modes are available only if you have the enhanced software image (EI) installed on your switch.

Loop guard is most effective when it is configured on the entire switched network. When the switch is operating in PVST+ or rapid-PVST+ mode, loop guard prevents alternate and root ports from becoming designated ports, and spanning tree does not send bridge protocol data units (BPDUs) on root or alternate ports. When the switch is operating in MST mode, BPDUs are not sent on nonboundary ports only if the port is blocked by loop guard in all MST instances. On a boundary port, loop guard blocks the port in all MST instances.

Loop guard operates only on ports that are considered point-to-point by the spanning tree.

You can override the setting of the **spanning-tree loopguard default** global configuration command by using the **spanning-tree guard loop** interface configuration command.

Examples This example shows how to globally enable loop guard:

```
Switch(config)# spanning-tree loopguard default
```

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

Related Commands	Command	Description
	show running-config	Displays the current operating configuration. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 > Cisco IOS File Management Commands > Configuration File Commands .
	spanning-tree guard loop	Enables the loop guard feature on all the VLANs associated with the specified interface.

spanning-tree mode

Use the **spanning-tree mode** global configuration command to enable per-VLAN spanning-tree plus PVST+), rapid PVST+, or multiple spanning tree (MST) on your switch. Use the **no** form of this command to return to the default setting.

spanning-tree mode {mst | pvst | rapid-pvst}

no spanning-tree mode

Syntax Description

mst	Enable MST and Rapid Spanning Tree Protocol (RSTP) (based on IEEE 802.1S and IEEE 802.1W). This keyword is available only if your switch is running the enhanced software image (EI).
pvst	Enable PVST+ (based on IEEE 802.1D).
rapid-pvst	Enable rapid PVST+ (based on IEEE 802.1W). This keyword is available only if your switch is running the EI.

Defaults

The default mode is PVST+.

Command Modes

Global configuration

Command History

Release	Modification
12.1(9)EA1	This command was first introduced.
12.1(13)EA1	The rapid-pvst keyword was added.

Usage Guidelines

The switch supports PVST+, rapid PVST+, and MSTP, but only one version can be active at any time. All VLANs run PVST+, all VLANs run rapid PVST+, or all VLANs run MSTP.



Caution

Changing spanning-tree modes can disrupt traffic because all spanning-tree instances are stopped for the previous mode and restarted in the new mode.

When you enable the MST mode, RSTP is automatically enabled.

Examples

This example shows to enable MST on the switch:

```
Switch(config)# spanning-tree mode mst
```

This example shows to enable rapid PVST+ on the switch:

```
Switch(config)# spanning-tree mode rapid-pvst
```

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

Related Commands	Command	Description
	show running-config	Displays the current operating configuration. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 > Cisco IOS File Management Commands > Configuration File Commands .

spanning-tree mst configuration

Use the **spanning-tree mst configuration** global configuration command to enter multiple spanning-tree (MST) configuration mode through which you configure the MST region. Use the **no** form of this command to return to the default settings.

spanning-tree mst configuration

no spanning-tree mst configuration

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

Syntax Description This command has no arguments or keywords.

Defaults The default mapping is that all VLANs are mapped to the common and internal spanning tree (CIST) instance (instance 0).
The default name is an empty string.
The revision number is 0.

Command Modes Global configuration

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

Usage Guidelines Entering the **spanning-tree mst configuration** command enables the MST configuration mode. These configuration commands are available:

- **abort**: exits the MST region configuration mode without applying configuration changes.
- **exit**: exits the MST region configuration mode and applies all configuration changes.
- **instance** *instance-id* **vlan** *vlan-range*: maps VLANs to an MST instance. The range for the *instance-id* is 1 to 15; the range for *vlan-range* is 1 to 4094. You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma.
- **name** *name*: sets the configuration name. The *name* string has a maximum length of 32 characters and is case sensitive.
- **no**: negates the **instance**, **name**, and **revision** commands or sets them to their defaults.
- **private-vlan**: Though visible in the command-line help strings, this command is not supported.
- **revision** *version*: sets the configuration revision number. The range is 0 to 65535.
- **show** [**current** | **pending**]: displays the current or pending MST region configuration.

In MST mode, the switch supports up to 16 MST instances. The number of VLANs that can be mapped to a particular MST instance is unlimited.

When you map VLANs to an MST instance, the mapping is incremental, and the VLANs specified in the command are added to or removed from the VLANs that were previously mapped. To specify a range, use a hyphen; for example, **instance 1 vlan 1-63** maps VLANs 1 to 63 to MST instance 1. To specify a series, use a comma; for example, **instance 1 vlan 10, 20, 30** maps VLANs 10, 20, and 30 to MST instance 1.

All VLANs that are not explicitly mapped to an MST instance are mapped to the common and internal spanning tree (CIST) instance (instance 0) and cannot be unmapped from the CIST by using the **no** form of the command.

For two or more switches to be in the same MST region, they must have the same VLAN mapping, the same configuration revision number, and the same name.

Examples

This example shows how to enter MST configuration mode, map VLAN 10 to 20 to MST instance 1, name the region *region1*, set the configuration revision to 1, display the pending configuration, apply the changes, and return to global configuration mode:

```
Switch# spanning-tree mst configuration
Switch(config-mst)# instance 1 vlan 10-20
Switch(config-mst)# name region1
Switch(config-mst)# revision 1
Switch(config-mst)# show pending
Pending MST configuration
Name      [region1]
Revision  1
Instance  Vlans Mapped
-----  -
0         1-9,21-4094
1         10-20
-----  -

Switch(config-mst)# exit
Switch(config)#
```

This example shows how to add VLANs 1 to 100 to the ones already mapped (if any) to instance 2, to move VLANs 40 to 60 that were previously mapped to instance 2 to the CIST instance, to add VLAN 10 to instance 10, and to remove all the VLANs mapped to instance 2 and map them to the CIST instance:

```
Switch(config-mst)# instance 2 vlan 1-100
Switch(config-mst)# no instance 2 vlan 40-60
Switch(config-mst)# instance 10 vlan 10
Switch(config-mst)# no instance 2
```

You can verify your settings by entering the **show pending** MST configuration command.

Related Commands

Command	Description
show spanning-tree mst configuration	Displays the MST region configuration.

spanning-tree mst cost

Use the **spanning-tree mst cost** interface configuration command to set the path cost for multiple spanning-tree (MST) calculations. If a loop occurs, spanning tree considers the path cost when selecting an interface to put in the forwarding state. Use the **no** form of this command to return to the default setting.

spanning-tree mst *instance-id* **cost** *cost*

no spanning-tree mst *instance-id* **cost**

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

Syntax Description	<i>instance-id</i>	Range of spanning-tree instances. You can specify a single instance, a range of instances separated by a hyphen, or a series of instances separated by a comma. The range is 0 to 15.
	<i>cost</i>	Path cost is 1 to 200000000, with higher values meaning higher costs.

Defaults	The default path cost is computed from the interface bandwidth setting. These are the IEEE default path cost values: <ul style="list-style-type: none"> • 1000 Mbps—20000 • 100 Mbps—200000 • 10 Mbps—2000000
----------	--

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

Command History	Release	Modification
	12.1(9)EA1	This command was first introduced.
	12.1(13)EA1	The value for the <i>instance-id</i> variable was changed.

Usage Guidelines	When you configure the cost, higher values represent higher costs.
------------------	--

Examples	<p>This example shows how to set a path cost of 250 on an interface associated with instances 2 and 4:</p> <pre>Switch(config)# interface fastethernet0/4 Switch(config-if)# spanning-tree mst 2,4 cost 250</pre> <p>You can verify your settings by entering the show spanning-tree mst interface <i>interface-id</i> privileged EXEC command.</p>
----------	--

Related Commands	Command	Description
	show spanning-tree mst interface <i>interface-id</i>	Displays MST information for the specified interface.
	spanning-tree mst port-priority	Configures an interface priority.
	spanning-tree mst priority	Configures the switch priority for the specified spanning-tree instance.

spanning-tree mst forward-time

Use the **spanning-tree mst forward-time** global configuration command to set the forward-delay time for all multiple spanning-tree (MST) instances. The forwarding time determines how long each of the listening and learning states last before the interface begins forwarding. Use the **no** form of this command to return to the default setting.

spanning-tree mst forward-time *seconds*

no spanning-tree mst forward-time

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

Syntax Description	<i>seconds</i>	Length of the listening and learning states. The range is 4 to 30 seconds.
Defaults	The default is 15 seconds.	
Command Modes	Global configuration	
Command History	Release	Modification
	12.1(9)EA1	This command was first introduced.
Usage Guidelines	Changing the spanning-tree mst forward-time command affects all spanning-tree instances.	
Examples	<p>This example shows how to set the spanning-tree forwarding time to 18 seconds for all MST instances:</p> <pre>Switch(config)# spanning-tree mst forward-time 18</pre> <p>You can verify your settings by entering the show spanning-tree mst privileged EXEC command.</p>	
Related Commands	Command	Description
	show spanning-tree mst	Displays MST information.
	spanning-tree mst hello-time	Sets the interval between hello bridge protocol data units (BPDUs) sent by root switch configuration messages.
	spanning-tree mst max-age	Sets the interval between messages that the spanning tree receives from the root switch.
	spanning-tree mst max-hops	Sets the number of hops in a region before the BPDU is discarded.

spanning-tree mst hello-time

Use the **spanning-tree mst hello-time** global configuration command to set the interval between hello bridge protocol data units (BPDUs) sent by root switch configuration messages. Use the **no** form of this command to return to the default setting.

spanning-tree mst hello-time *seconds*

no spanning-tree mst hello-time

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

Syntax Description	<i>seconds</i>	Interval between hello BPDUs sent by root switch configuration messages. The range is 1 to 10 seconds.
--------------------	----------------	--

Defaults The default is 2 seconds.

Command Modes Global configuration

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

Usage Guidelines After you set the **spanning-tree mst max-age** *seconds* global configuration command, if a switch does not receive BPDUs from the root switch within the specified interval, the switch recomputes the spanning-tree topology. The **max-age** setting must be greater than the **hello-time** setting. Changing the **spanning-tree mst hello-time** command affects all spanning-tree instances.

Examples This example shows how to set the spanning-tree hello time to 3 seconds for all MST instances:

```
Switch(config)# spanning-tree mst hello-time 3
```

You can verify your settings by entering the **show spanning-tree mst** privileged EXEC command.

Related Commands	Command	Description
	show spanning-tree mst	Displays multiple spanning-tree (MST) information.
	spanning-tree mst forward-time	Sets the forward-delay time for all MST instances.
	spanning-tree mst max-age	Sets the interval between messages that the spanning tree receives from the root switch.
	spanning-tree mst max-hops	Sets the number of hops in a region before the BPDU is discarded.

spanning-tree mst max-age

Use the **spanning-tree mst max-age** global configuration command to set the interval between messages that the spanning tree receives from the root switch. If a switch does not receive a bridge protocol data unit (BPDU) message from the root switch within this interval, it recomputes the spanning-tree topology. Use the **no** form of this command to return to the default setting.

spanning-tree mst max-age *seconds*

no spanning-tree mst max-age

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

Syntax Description	<i>seconds</i>	Interval between messages the spanning tree receives from the root switch. If a switch does not receive a BPDU message from the root switch within this interval, it recomputes the spanning-tree topology. The range is 6 to 40 seconds.
---------------------------	----------------	---

Defaults	The default is 20 seconds.
-----------------	----------------------------

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

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

Usage Guidelines	<p>After you set the spanning-tree mst max-age <i>seconds</i> global configuration command, if a switch does not receive BPDUs from the root switch within the specified interval, the switch recomputes the spanning-tree topology. The max-age setting must be greater than the hello-time setting.</p> <p>Changing the spanning-tree mst max-age command affects all spanning-tree instances.</p>
-------------------------	--

Examples	<p>This example shows how to set the spanning-tree max-age to 30 seconds for all MST instances:</p> <pre>Switch(config)# spanning-tree mst max-age 30</pre> <p>You can verify your settings by entering the show spanning-tree mst privileged EXEC command.</p>
-----------------	--

Related Commands	Command	Description
	show spanning-tree mst	Displays multiple spanning-tree (MST) information.
	spanning-tree mst forward-time	Sets the forward-delay time for all MST instances.
	spanning-tree mst hello-time	Sets the interval between hello BPDUs sent by root switch configuration messages.
	spanning-tree mst max-hops	Sets the number of hops in a region before the BPDU is discarded.

spanning-tree mst max-hops

Use the **spanning-tree mst max-hops** global configuration command to set the number of hops in a region before the bridge protocol data unit (BPDU) is discarded and the information held for a port is aged. Use the **no** form of this command to return to the default setting.

spanning-tree mst max-hops *hop-count*

no spanning-tree mst max-hops

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

Syntax Description	<i>hop-count</i>	Number of hops in a region before the BPDU is discarded. The range is 1 to 40 hops.
--------------------	------------------	---

Defaults	The default is 20 hops.
----------	-------------------------

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

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

Usage Guidelines	The root switch of the instance always sends a BPDU (or M-record) with a cost of 0 and the hop count set to the maximum value. When a switch receives this BPDU, it decrements the received remaining hop count by one and propagates the decremented count as the remaining hop count in the generated M-records. A switch discards the BPDU and ages the information held for the port when the count reaches 0.
------------------	--

Changing the **spanning-tree mst max-hops** command affects all spanning-tree instances.

Examples	This example shows how to set the spanning-tree max-hops to 10 for all MST instances:
----------	---

```
Switch(config)# spanning-tree mst max-hops 10
```

You can verify your settings by entering the **show spanning-tree mst** privileged EXEC command.

Related Commands	Command	Description
	show spanning-tree mst	Displays multiple spanning-tree (MST) information.
	spanning-tree mst forward-time	Sets the forward-delay time for all MST instances.
	spanning-tree mst hello-time	Sets the interval between hello BPDU sent by root switch configuration messages.
	spanning-tree mst max-age	Sets the interval between messages that the spanning tree receives from the root switch.

spanning-tree mst port-priority

Use the **spanning-tree mst port-priority** interface configuration command to configure an interface priority. If a loop occurs, the Multiple Spanning Tree Protocol (MSTP) can determine which interface to put in the forwarding state. Use the **no** form of this command to return to the default setting.

spanning-tree mst *instance-id* port-priority *priority*

no spanning-tree mst *instance-id* port-priority

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

Syntax Description

<i>instance-id</i>	Range of spanning-tree instances. You can specify a single instance, a range of instances separated by a hyphen, or a series of instances separated by a comma. The range is 0 to 15.
<i>priority</i>	The range is 0 to 240 in increments of 16. Valid priority values are 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, and 240. All other values are rejected. The lower the number, the higher the priority.

Defaults

The default is 128.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(9)EA1	This command was first introduced.
12.1(13)EA1	The values for the <i>instance-id</i> and the <i>priority</i> variables were changed.

Usage Guidelines

You can assign higher priority values (lower numerical values) to interfaces that you want selected first and lower priority values (higher numerical values) that you want selected last. If all interfaces have the same priority value, the MST puts the interface with the lowest interface number in the forwarding state and blocks other interfaces.

Examples

This example shows how to increase the likelihood that the interface associated with spanning-tree instance 20 is placed into the forwarding state if a loop occurs:

```
Switch(config)# interface fastethernet0/2
Switch(config-if)# spanning-tree mst 20 port-priority 0
```

You can verify your settings by entering the **show spanning-tree mst interface *interface-id*** privileged EXEC command.

Related Commands	Command	Description
	<code>show spanning-tree mst interface <i>interface-id</i></code>	Displays MST information for the specified interface.
	<code>spanning-tree mst cost</code>	Sets the path cost for MST calculations.
	<code>spanning-tree mst priority</code>	Sets the switch priority for the specified spanning-tree instance.

spanning-tree mst priority

Use the **spanning-tree mst priority** global configuration command to set the switch priority for the specified spanning-tree instance. Use the **no** form of this command to return to the default setting.

spanning-tree mst *instance-id* **priority** *priority*

no spanning-tree mst *instance-id* **priority**

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

Syntax Description	
<i>instance-id</i>	Range of spanning-tree instances. You can specify a single instance, a range of instances separated by a hyphen, or a series of instances separated by a comma. The range is 0 to 15.
<i>priority</i>	Set the switch priority for the specified spanning-tree instance. This setting affects the likelihood that the switch is selected as the root switch. A lower value increases the probability that the switch is selected as the root switch. The range is 0 to 61440 in increments of 4096. Valid priority values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected.

Defaults The default is 32768.

Command Modes Global configuration

Command History	Release	Modification
	12.1(9)EA1	This command was first introduced.
	12.1(13)EA1	The value for the <i>instance-id</i> variable was changed.

Examples This example shows how to set the spanning-tree priority to 8192 for multiple spanning-tree (MST) instance 20:

```
Switch(config)# spanning-tree mst 20 priority 8192
```

You can verify your settings by entering the **show spanning-tree mst instance-id** privileged EXEC command.

Related Commands	Command	Description
	show spanning-tree mst <i>instance-id</i>	Displays MST information for the specified interface.
	spanning-tree mst cost	Sets the path cost for MST calculations.
	spanning-tree mst port-priority	Configures an interface priority.

spanning-tree mst root

Use the **spanning-tree mst root** global configuration command to configure the multiple spanning-tree (MST) root switch priority and timers based on the network diameter. Use the **no** form of this command to return to the default setting.

```
spanning-tree mst instance-id root {primary | secondary} [diameter net-diameter
hello-time seconds]
```

```
no spanning-tree mst instance-id root
```

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

Syntax Description

<i>instance-id</i>	Range of spanning-tree instances. You can specify a single instance, a range of instances separated by a hyphen, or a series of instances separated by a comma. The range is 0 to 15.
root primary	Force this switch to be the root switch.
root secondary	Set this switch to be the root switch should the primary root switch fail.
diameter <i>net-diameter</i>	(Optional) Set the maximum number of switches between any two end stations. The range is 2 to 7. This keyword is available only for MST instance 0.
hello-time <i>seconds</i>	(Optional) Set the interval between hello bridge protocol data units (BPDUs) sent by the root switch configuration messages. The range is 1 to 10 seconds. This keyword is available only for MST instance 0.

Defaults

The primary root switch priority is 24576.

The secondary root switch priority is 28672.

The hello time is 2 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.1(9)EA1	This command was first introduced.
12.1(13)EA1	The value for the <i>instance-id</i> variable was changed.

Usage Guidelines

Use the **spanning-tree mst** *instance-id* **root** command used only on backbone switches.

When you enter the **spanning-tree mst** *instance-id* **root** command, the software tries to set a high enough priority to make this switch the root of the spanning-tree instance. Because of the extended system ID support, the switch sets the switch priority for the instance to 24576 if this value will cause this switch to become the root for the specified instance. If any root switch for the specified instance has a switch priority lower than 24576, the switch sets its own priority to 4096 less than the lowest switch priority. (4096 is the value of the least-significant bit of a 4-bit switch priority value.)

When you enter the **spanning-tree mst *instance-id* root secondary** command, because of support for the extended system ID, the software changes the switch priority from the default value (32768) to 28672. If the root switch fails, this switch becomes the next root switch (if the other switches in the network use the default switch priority of 32768 and are therefore unlikely to become the root switch).

Examples

This example shows how to configure the switch as the root switch for instance 10 with a network diameter of 4:

```
Switch(config)# spanning-tree mst 10 root primary diameter 4
```

This example shows how to configure the switch as the secondary root switch for instance 10 with a network diameter of 4:

```
Switch(config)# spanning-tree mst 10 root secondary diameter 4
```

You can verify your settings by entering the **show spanning-tree mst *instance-id*** privileged EXEC command.

Related Commands

Command	Description
show spanning-tree mst <i>instance-id</i>	Displays MST information for the specified instance.
spanning-tree mst forward-time	Sets the forward-delay time for all MST instances.
spanning-tree mst hello-time	Sets the interval between hello BPDUs sent by root switch configuration messages.
spanning-tree mst max-age	Sets the interval between messages that the spanning tree receives from the root switch.
spanning-tree mst max-hops	Sets the number of hops in a region before the BPDU is discarded.

spanning-tree port-priority

Use the **spanning-tree port-priority** interface configuration command to configure an interface priority. If a loop occurs, spanning tree can determine which interface to put in the forwarding state. Use the **no** form of this command to return to the default setting.

spanning-tree [vlan *vlan-id*] port-priority *priority*

no spanning-tree [vlan *vlan-id*] port-priority

Syntax Description

vlan <i>vlan-id</i>	(Optional) VLAN range associated with a spanning-tree instance. You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1005 when the standard software image (SI) is installed.
<i>priority</i>	The range is 0 to 240 in increments of 16. Valid priority values are 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, and 240. All other values are rejected. The lower the number, the higher the priority.

Defaults

The default is 128.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5.2)WC(1)	This command was first introduced.
12.1(13)EA1	The values for the <i>vlan-id</i> and the <i>priority</i> variables were changed.

Usage Guidelines

If the variable *vlan-id* is omitted, the command applies to the spanning-tree instance associated with VLAN 1.

You can set the priority on a VLAN that has no interfaces assigned to it. The setting takes effect when you assign the interface to the VLAN.

If you configure an interface with both the **spanning-tree vlan *vlan-id* port-priority *priority*** command and the **spanning-tree port-priority *priority*** command, the **spanning-tree vlan *vlan-id* port-priority *priority*** command takes effect only on the range of VLANs specified by that command. On the VLANs that are not specified by the **spanning-tree vlan *vlan-id* port-priority *priority*** command, the **spanning-tree port-priority *priority*** command takes effect.

Examples

This example shows how to increase the likelihood that the Fast Ethernet interface 0/2 will be put in the forwarding state if a loop occurs:

```
Switch(config)# interface fastethernet0/2
Switch(config-if)# spanning-tree vlan 20 port-priority 0
```

You can verify your settings by entering the **show spanning-tree interface *interface-id*** privileged EXEC command.

Related Commands

Command	Description
show spanning-tree interface <i>interface-id</i>	Displays spanning-tree information for the specified interface.
spanning-tree cost	Sets the path cost for spanning-tree calculations.
spanning-tree vlan priority	Sets the switch priority for the specified spanning-tree instance.

spanning-tree portfast (global configuration)

Use the **spanning-tree portfast** global configuration command to globally enable bridge protocol data unit (BPDU) filtering on Port Fast-enabled ports, the BPDU guard feature on Port Fast-enabled ports, or the Port Fast feature on all nontrunking ports. The BPDU filtering feature prevents the switch port from sending or receiving BPDUs. The BPDU guard feature puts Port Fast-enabled ports that receive BPDUs in an error-disabled state. Use the **no** form of this command to return to the default setting.

spanning-tree portfast { bpdupfilter default | bpduguard default | default }

no spanning-tree portfast { bpdupfilter default | bpduguard default | default }

Syntax Description

bpdupfilter default	Globally enable BPDU filtering on Port Fast-enabled ports and prevent the switch port connected to end stations from sending or receiving BPDUs.
bpduguard default	Globally enable the BPDU guard feature on Port Fast-enabled ports and place the ports that receive BPDUs in an error-disabled state.
default	Globally enable the Port Fast feature on all nontrunking ports. When the Port Fast feature is enabled, the port changes directly from a blocking state to a forwarding state without making the intermediate spanning-tree state changes.

Defaults

The BPDU filtering, the BPDU guard, and the Port Fast features are disabled on all ports unless they are individually configured.

Command Modes

Global configuration

Command History

Release	Modification
12.1(6)EA2	This command was first introduced.
12.1(9)EA1	The bpdupfilter default and default keywords were added.

Usage Guidelines

You can enable these features when the switch is operating in the per-VLAN spanning-tree plus (PVST+), rapid-PVST+, or the multiple spanning-tree (MST) mode. The rapid-PVST+ and MST modes are available only if you have the enhanced software image (EI) installed on your switch.

Use the **spanning-tree portfast bpdupfilter default** global configuration command to globally enable BPDU filtering on ports that are Port Fast-enabled (the ports are in a Port Fast-operational state). The ports still send a few BPDUs at link-up before the switch begins to filter outbound BPDUs. You should globally enable BPDU filtering on a switch so that hosts connected to switch ports do not receive BPDUs. If a BPDU is received on a Port Fast-enabled port, the port loses its Port Fast-operational status and BPDU filtering is disabled.

You can override the **spanning-tree portfast bpdupfilter default** global configuration command by using the **spanning-tree bpdupfilter** interface configuration command.

**Caution**

Enabling BPDU filtering on an interface is the same as disabling spanning tree on it and can result in spanning-tree loops.

Use the **spanning-tree portfast bpduguard default** global configuration command to globally enable BPDU guard on ports that are in a Port Fast-operational state. In a valid configuration, Port Fast-enabled ports do not receive BPDUs. Receiving a BPDU on a Port Fast-enabled port signals an invalid configuration, such as the connection of an unauthorized device, and the BPDU guard feature puts the port in the error-disabled state. The BPDU guard feature provides a secure response to invalid configurations because you must manually put the port back in service. Use the BPDU guard feature in a service-provider network to prevent an access port from participating in the spanning tree.

You can override the **spanning-tree portfast bpduguard default** global configuration command by using the **spanning-tree bpduguard** interface configuration command.

Use the **spanning-tree portfast default** global configuration command to globally enable the Port Fast feature on all nontrunking ports. Configure Port Fast only on ports that connect to end stations; otherwise, an accidental topology loop could cause a data packet loop and disrupt switch and network operation. A Port Fast-enabled port moves directly to the spanning-tree forwarding state when linkup occurs without waiting for the standard forward-delay time.

You can override the **spanning-tree portfast default** global configuration command by using the **spanning-tree portfast** interface configuration command. You can use the **no spanning-tree portfast default** global configuration command to disable Port Fast on all ports unless they are individually configured with the **spanning-tree portfast** interface configuration command.

Examples

This example shows how to globally enable the BPDU filtering feature:

```
Switch(config)# spanning-tree portfast bpdudfilter default
```

This example shows how to globally enable the BPDU guard feature:

```
Switch(config)# spanning-tree portfast bpduguard default
```

This example shows how to globally enable the Port Fast feature on all nontrunking ports:

```
Switch(config)# spanning-tree portfast default
```

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

Related Commands

Command	Description
show running-config	Displays the current operating configuration. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 > Cisco IOS File Management Commands > Configuration File Commands .
spanning-tree bpdudfilter	Prevents a port from sending or receiving BPDUs.
spanning-tree bpduguard	Puts a port in the error-disabled state when it receives a BPDU.
spanning-tree portfast (interface configuration)	Enables the Port Fast feature on an interface in all its associated VLANs.

spanning-tree portfast (interface configuration)

Use the **spanning-tree portfast** interface configuration command to enable the Port Fast feature on an interface in all its associated VLANs. When the Port Fast feature is enabled, the interface changes directly from a blocking state to a forwarding state without making the intermediate spanning-tree state changes. Use the **no** form of this command to return to the default setting.

spanning-tree portfast [**disable** | **trunk**]

no spanning-tree portfast

Syntax Description	disable	(Optional) Disable the Port Fast feature on the specified interface.
	trunk	(Optional) Enable the Port Fast feature on a trunking interface.

Defaults The Port Fast feature is disabled on all interfaces; however, it is automatically enabled on dynamic-access ports.

Command Modes Interface configuration

Command History	Release	Modification
	12.0(5.2)WC(1)	This command was first introduced.
	12.1(9)EA1	The disable and trunk keywords were added.

Usage Guidelines Use this feature only on interfaces that connect to end stations; otherwise, an accidental topology loop could cause a data packet loop and disrupt switch and network operation.

You can enable this feature when the switch is operating in the per-VLAN spanning-tree plus (PVST+), rapid-PVST+, or the multiple spanning-tree (MST) mode.

This feature affects all VLANs on the interface.

A port with the Port Fast feature enabled is moved directly to the spanning-tree forwarding state without waiting the standard forward-time delay.

You can use the **spanning-tree portfast default** global configuration command to globally enable the Port Fast feature on all nontrunking interfaces. However, the **spanning-tree portfast** interface configuration command can override the global setting.

If you configure the **spanning-tree portfast default** global configuration command, you can disable Port Fast on a port that is not a trunk port by using the **no spanning-tree portfast** interface configuration command.

The **no spanning-tree portfast** interface configuration command is the same as the **spanning-tree portfast disable** interface configuration command.

Examples

This example shows how to enable the Port Fast feature on an interface:

```
Switch(config)# interface fastethernet0/2
Switch(config-if)# spanning-tree portfast
```

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

Related Commands

Command	Description
show running-config	Displays the current operating configuration. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 > Cisco IOS File Management Commands > Configuration File Commands .
spanning-tree bpdufilter	Prevents a port from sending or receiving bridge protocol data units (BPDUs).
spanning-tree bpduguard	Puts a port in the error-disabled state when it receives a BPDU.
spanning-tree portfast (global configuration)	Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled ports or enables the Port Fast feature on all nontrunking ports.

spanning-tree stack-port

Use the **spanning-tree stack-port** interface configuration command to enable cross-stack UplinkFast (CSUF) on an interface and to accelerate the choice of a new root port when a link or switch fails or when spanning tree reconfigures itself. Use the **no** form of this command to return to the default setting.

spanning-tree stack-port

no spanning-tree stack-port

Syntax Description

This command has no arguments or keywords.

Defaults

CSUF is disabled on all interfaces.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

This command is effective only if you enable the UplinkFast feature by using the **spanning-tree uplinkfast** global configuration command.

Use this command only on access switches.

The CSUF feature is supported only when the switch is running per-VLAN spanning-tree plus (PVST+). It is not supported when the switch is running rapid PVST+ or multiple spanning-tree (MST).

You can enable CSUF only on one stack-port Gigabit Interface Converter (GBIC) interface. The stack port connects to the GigaStack GBIC multidrop backbone. If you try to enable CSUF on a Fast Ethernet or a copper-based Gigabit Ethernet port, you receive an error message.

If CSUF is already enabled on an interface and you try to enable it on another interface, you receive an error message. You must disable CSUF on the first interface before enabling it on a new interface.

Examples

This example shows how to enable CSUF on the GBIC interface:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# spanning-tree stack-port
```

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

Related Commands	Command	Description
	show running-config	Displays the current operating configuration. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 > Cisco IOS File Management Commands > Configuration File Commands .
	spanning-tree uplinkfast	Accelerates the choice of a new root port when a link or switch fails or when spanning tree reconfigures itself.

spanning-tree uplinkfast

Use the **spanning-tree uplinkfast** global configuration command to accelerate the choice of a new root port when a link or switch fails or when the spanning tree reconfigures itself. Use the **no** form of this command to return to the default setting.

spanning-tree uplinkfast [**max-update-rate** *pkts-per-second*]

no spanning-tree uplinkfast [**max-update-rate**]

Syntax Description

max-update-rate *pkts-per-second* (Optional) The number of packets per second at which update packets are sent. The range is 0 to 32000.

Defaults

UplinkFast is disabled.
The update rate is 150 packets per second.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5.2)WC(1)	This command was first introduced.
12.1(6)EA2	The <i>pkts-per-second</i> range was changed to 0 to 65535.
12.1(13)EA1	The range for the <i>pkts-per-second</i> was changed from 0 to 65535 to 0 to 32000.

Usage Guidelines

Use this command only on access switches.

The UplinkFast feature is supported only when the switch is running per-VLAN spanning-tree plus (PVST+). It is not supported when the switch is running rapid PVST+ or multiple spanning-tree (MST).

When you enable UplinkFast, it is enabled for the entire switch and cannot be enabled for individual VLANs.

When UplinkFast is enabled, the switch priority of all VLANs is set to 49152. If you change the path cost to a value less than 3000 and you enable UplinkFast or UplinkFast is already enabled, the path cost of all interfaces and VLAN trunks is increased by 3000 (if you change the path cost to 3000 or above, the path cost is not altered). The changes to the switch priority and the path cost reduces the chance that the switch will become the root switch.

When UplinkFast is disabled, the switch priorities of all VLANs and path costs of all interfaces are set to default values if you did not modify them from their defaults.

When spanning tree detects that the root port has failed, UplinkFast immediately switches over to an alternate root port, changing the new root port directly to FORWARDING state. During this time, a topology change notification is sent.

Do not enable the root guard on interfaces that will be used by the UplinkFast feature. With UplinkFast, the backup interfaces (in the blocked state) replace the root port in the case of a failure. However, if root guard is also enabled, all the backup interfaces used by the UplinkFast feature are placed in the root-inconsistent state (blocked) and prevented from reaching the forwarding state.

If you set the max-update-rate to 0, station-learning frames are not generated, so the spanning-tree topology converges more slowly after a loss of connectivity.

Examples

This example shows how to enable UplinkFast:

```
Switch(config)# spanning-tree uplinkfast
```

You can verify your setting by entering the **show spanning-tree summary** privileged EXEC command.

Related Commands

Command	Description
show spanning-tree summary	Displays a summary of the spanning-tree port states.
spanning-tree stack-port	Enables cross-stack UplinkFast (CSUF) on an interface and accelerates the choice of a new root port when a link or switch fails or when spanning tree reconfigures itself.
spanning-tree vlan root primary	Forces this switch to be the root switch.

spanning-tree vlan

Use the **spanning-tree vlan** global configuration command to configure spanning tree on a per-VLAN basis. Use the **no** form of this command to return to the default setting.

```
spanning-tree vlan vlan-id {forward-time seconds | hello-time seconds | max-age seconds |
priority priority | {root {primary | secondary} [diameter net-diameter
[hello-time seconds]]}}
```

```
no spanning-tree vlan vlan-id [forward-time | hello-time | max-age | priority | root]
```

Syntax Description

<i>vlan-id</i>	VLAN range associated with a spanning-tree instance. You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1005 when the standard software image (SI) is installed.
forward-time <i>seconds</i>	Set the forward-delay time for the specified spanning-tree instance. The forwarding time determines how long each of the listening and learning states last before the interface begins forwarding. The range is 4 to 30 seconds.
hello-time <i>seconds</i>	Set the interval between hello bridge protocol data units (BPDUs) sent by the root switch configuration messages. The range is 1 to 10 seconds.
max-age <i>seconds</i>	Set the interval between messages the spanning tree receives from the root switch. If a switch does not receive a BPDU message from the root switch within this interval, it recomputes the spanning-tree topology. The range is 6 to 40 seconds.
priority <i>priority</i>	Set the switch priority for the specified spanning-tree instance. This setting affects the likelihood that the switch is selected as the root switch. A lower value increases the probability that the switch is selected as the root switch. The range is 0 to 61440 in increments of 4096. Valid priority values are 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected.
root primary	Force this switch to be the root switch.
root secondary	Set this switch to be the root switch should the primary root switch fail.
diameter <i>net-diameter</i>	Set the maximum number of switches between any two end stations. The range is 2 to 7.

Defaults

Spanning tree is enabled on all VLANs.

The forward-delay time is 15 seconds.

The hello time is 2 seconds.

The max-age is 20 seconds.

The primary root switch priority is 24576.

The secondary root switch priority is 28672.

Command Modes Global configuration

Command History	Release	Modification
	12.0(5.2)WC(1)	This command was first introduced.
	12.1(9)EA1	The priority <i>priority</i> range changed from 1 to 65535 to 1 to 61440 (in increments of 4096).
	12.1(13)EA1	The value for the <i>vlan-id</i> variable was changed.

Usage Guidelines

Disabling the STP causes the VLAN to stop participating in the spanning-tree topology. Interfaces that are administratively down remain down. Received BPDUs are forwarded like other multicast frames. The switch does not detect and prevent loops in a VLAN if STP is disabled for that VLAN.

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

When disabling or re-enabling the STP, you can specify a range of VLANs that you want to disable or enable.

When the STP is disabled and then enabled, all assigned VLANs continue to be its members. However, all spanning-tree bridge parameters are returned to their previous settings (the last setting before the VLAN was disabled).

You can enable spanning-tree options on a VLAN that has no interfaces assigned to it. The setting takes effect when you assign interfaces to it.

When setting the **max-age** *seconds*, if a switch does not receive BPDUs from the root switch within the specified interval, it recomputes the spanning-tree topology. The **max-age** setting must be greater than the **hello-time** setting.

The **spanning-tree vlan *vlan-id* root** command should be used only on backbone switches.

When you enter the **spanning-tree vlan *vlan-id* root** command, the software checks the switch priority of the current root switch for each VLAN. Because of the extended system ID support, the switch sets the switch priority for the specified VLAN to 24576 if this value will cause this switch to become the root for the specified VLAN. If any root switch for the specified VLAN has a switch priority lower than 24576, the switch sets its own priority for the specified VLAN to 4096 less than the lowest switch priority. (4096 is the value of the least-significant bit of a 4-bit switch priority value.)

When you enter the **spanning-tree vlan *vlan-id* root primary** command, the switch recalculates the **forward-time**, **hello-time**, **max-age**, and **priority** settings. If you previously configured these parameters, the switch overrides and recalculates them.

When you enter the **spanning-tree vlan *vlan-id* root secondary** command, because of support for the extended system ID, the software changes the switch priority from the default value (32768) to 28672. If the root switch should fail, this switch becomes the next root switch (if the other switches in the network use the default switch priority of 32768, and therefore, are unlikely to become the root switch).

Examples

This example shows how to disable the STP on VLAN 5:

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

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

This example shows how to set the spanning-tree forwarding time to 18 seconds for VLANs 20 and 25:

```
Switch(config)# spanning-tree vlan 20,25 forward-time 18
```

This example shows how to set the spanning-tree hello-delay time to 3 seconds for VLANs 20 to 24:

```
Switch(config)# spanning-tree vlan 20-24 hello-time 3
```

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

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

This example shows how to reset the **max-age** parameter to the default value for spanning-tree instances 100 and 105 to 108 :

```
Switch(config)# no spanning-tree vlan 100,105-108 max-age
```

This example shows how to set the spanning-tree priority to 8192 for VLAN 20:

```
Switch(config)# spanning-tree vlan 20 priority 8192
```

This example shows how to configure the switch as the root switch for VLAN 10 with a network diameter of 4:

```
Switch(config)# spanning-tree vlan 10 root primary diameter 4
```

This example shows how to configure the switch as the secondary root switch for VLAN 10 with a network diameter of 4:

```
Switch(config)# spanning-tree vlan 10 root secondary diameter 4
```

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

Related Commands

Command	Description
show spanning-tree vlan	Displays spanning-tree information.
spanning-tree cost	Sets the path cost for spanning-tree calculations.
spanning-tree guard	Enables the root guard or the loop guard feature for all the VLANs associated with the selected interface.
spanning-tree port-priority	Sets an interface priority.
spanning-tree portfast (global configuration)	Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled ports or enables the Port Fast feature on all nontrunking ports.
spanning-tree portfast (interface configuration)	Enables the Port Fast feature on an interface in all its associated VLANs.
spanning-tree uplinkfast	Enables the UplinkFast feature, which accelerates the choice of a new root port.

speed

Use the **speed** interface configuration command to specify the speed of a port. Use the **no** form of this command to return the port to its default value.

speed { **10** | **100** | **1000** | **auto** | **nonegotiate** }

no speed



Note

You cannot configure speed or duplex mode on Gigabit Interface Converter (GBIC) ports, but for certain types of GBICs, you can configure speed to not negotiate (**nonegotiate**) if they are connected to a device that does not support autonegotiation.

Syntax Description

10	Port runs at 10 Mbps.
100	Port runs at 100 Mbps.
1000	Port runs at 1000 Mbps (only valid for Gigabit Ethernet ports).
auto	Port automatically detects whether it should run at 10 or 100 Mbps on Fast Ethernet ports or at 10, 100, or 1000 Mbps on 10/100/1000 and SFP-module ports.
nonegotiate	Autonegotiation is disabled and the port runs at 1000 Mbps. This option is valid and visible only on 1000BASE-X, -LX, and -ZX GBIC ports. Gigastack GBICs and 1000BASE-T GBICs do not support disabling of autonegotiation.

Defaults

For Fast Ethernet and 10/100/1000 ports, the default is **auto**.

For 100BASE-FX ports, the default is 100 Mbps.

For GBIC-module ports, the default is 1000 Mbps.

For small form-factor pluggable (SFP)-module ports, the default is **auto**.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5.2)WC(1)	This command was first introduced.
12.1(11)EA1	The nonegotiate keyword was added.

Usage Guidelines

The applicability of this command depends on the switch on which you enter this command.

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

On non-Long-Reach Ethernet (LRE) switches, Fast Ethernet ports, except for 100BASE-FX ports, can be configured at 10 or 100 Mbps. The 10/100/1000 Ethernet interfaces on the Catalyst 2950T-24, Catalyst 2950T-48-SI, and Catalyst 2955T-24 switches operate at 10 or 100 Mbps in either half- or full-duplex mode or at 1000 Mbps only in full-duplex mode.

You cannot configure the speed on GBIC interfaces, but you can configure the speed to not negotiate (**nonegotiate**) for the 1000BASE-SX, -LX, or -ZX GBICs, if they are connected to devices that do not support autonegotiation. GBIC-module ports support only 1000 Mbps. The speed values of 10 Mbps and 100 Mbps are not supported.

**Note**

The 100BASE-FX ports on Catalyst 2950C-24 switches do not support the **speed** command. These ports operate only in 100-Mbps and full-duplex mode.

On LRE switches, LRE Gigabit Ethernet ports are set to **auto** by default. A copper connection (10/100/1000) autonegotiates with the device at the other end of the link for the speed setting and then forces the speed setting to the negotiated value. A fiber SFP connection also autonegotiates with the device at the other end of the link but only accepts a connection at 1000 Mbps.

You can use the command line interface (CLI) to configure or force SFP-module ports to values other than 1000 Mbps, but the port still continues to run at 1000 Mbps. You can configure a copper connection to 10, 100, or 1000 Mbps.

On LRE switches, the speed setting for a Gigabit Ethernet port has a close relationship to the setting for duplex mode. Fiber SFP-module ports are always forced to 1000 Mbps and to full-duplex mode. Copper ports can run in either full- or half-duplex mode at 10 or 100 Mbps but is forced to run in full-duplex mode at 1000Mbps. When you configure the speed and duplex settings, autonegotiation is disabled, and speed and duplex settings can cause a mismatch.

The **speed** command is not supported on LRE interfaces. Use the **cpe speed** interface configuration command to set the speed of individual customer premises equipment (CPE) ports.

**Note**

For guidelines on setting the switch speed and duplex parameters, refer to the “Configuring the Switch Interfaces” and the “Configuring LRE” chapters in the switch software configuration guide for this release.

Examples

This example shows how to set Fast Ethernet port 1 to 100 Mbps:

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# speed 100
```

This example shows how to set port 1 to **auto** on an LRE switch:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# speed auto
```

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

Related Commands	Command	Description
	cpe speed	Sets the speed of a CPE port.
	duplex	Specifies the duplex mode of operation for switch ports.
	show controllers lre status	Display the status for rate selection. Use the sequence keyword to display the status of a sequence for an LRE interface.
	show interfaces	Displays the administrative and operational status of all interfaces or a specified interface.
	show running-config	Displays the current operating configuration. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 > Cisco IOS File Management Commands > Configuration File Commands .

storm-control

Use the **storm-control** interface configuration command to enable broadcast, multicast, or unicast storm control on a port and to specify the action taken when a storm occurs on a port. Use the **no** form of this command to disable storm control for broadcast, multicast, or unicast traffic and disable the specified storm-control action.

```
storm-control {{{broadcast | multicast | unicast} level {level [level-low] | pps pps pps-low}} |
action {shutdown | trap}}
```

```
no storm-control {{{broadcast | multicast | unicast} level} | action}
```

Syntax Description	{broadcast multicast unicast} Determines the type of packet-storm suppression. <ul style="list-style-type: none"> • broadcast—Enable broadcast storm control on the port. • multicast—Enable multicast storm control on the port. • unicast—Enable unicast storm control on the port.
level	Configures the rising and falling suppression levels as a percentage of total bandwidth or in packets per second.
<i>level [level-low]</i>	Defines the rising and falling suppression levels as a percentage of total bandwidth, up to two decimal places. <ul style="list-style-type: none"> • <i>level</i>—Rising suppression level; valid values are from 0 to 100 percent. Block the flooding of storm packets when the value specified for <i>level</i> is reached. • <i>level-low</i>—(Optional) Falling suppression level; valid values are from 0 to 100. This value must be less than the rising suppression value.
<i>pps pps pps-low</i>	Defines the rising and falling suppression levels in packets per second. This option is supported only on non-Long-Reach Ethernet (LRE) Catalyst 2950 switches. <ul style="list-style-type: none"> • <i>pps</i>—Rising suppression level; valid values are from 0 to 4294967295. Block the flooding of storm packets when the value specified for <i>pps</i> is reached. • <i>pps-low</i>—Falling suppression level; valid values are from 0 to 4294967295. This value must be equal to or less than the rising suppression value.
action	Action taken when a storm occurs on a port. The default action is to filter traffic and not send an Simple Network Management Protocol (SNMP) trap.
shutdown	Disables the port during a storm.
trap	Sends an SNMP trap when a storm occurs.

Defaults

Broadcast, multicast, and unicast storm control are disabled.

The default action is to filter traffic and to not send an SNMP trap.

Command Modes Interface configuration

Command History

Release	Modification
12.1(6)EA2	This command was first introduced. It replaced port storm-control command.
12.1(14)EA1	The pps pps pps-low option was added.

Usage Guidelines

Use the **storm-control** command to enable or disable broadcast, multicast, or unicast storm control on a port. After a port is disabled during a storm, use the **no shutdown** interface configuration command to enable the port.

The suppression levels can be entered as a percentage of total bandwidth. A suppression value of 100 percent means that no limit is placed on the specified traffic type. This feature is enabled only when the rising suppression level is less than 100 percent. If no other storm-control configuration is specified, the default action is to filter the traffic causing the storm and to send no SNMP trap.

If your switch is a non-LRE Catalyst 2950 switch, the suppression levels can also be entered as the rate at which traffic is received in packets per second. A suppression value of 4294967295 packets per second means that no limit is placed on the specified traffic type. This feature is enabled only when the rising suppression level is less than 4294967295 packets per second. If no other storm-control configuration is specified, the default action is to filter the traffic causing the storm and to send no SNMP trap.

When a storm occurs and the action is to filter traffic, if the falling suppression level is not specified, the switch blocks all traffic until the traffic rate drops below the rising suppression level. If the falling suppression level is specified, the switch blocks traffic until the traffic rate drops below this level.

When a multicast or unicast storm occurs and the action is to filter traffic, the switch blocks all traffic (broadcast, multicast, and unicast traffic) and sends only Spanning Tree Protocol (STP) packets.

When a broadcast storm occurs and the action is to filter traffic, the switch blocks only broadcast traffic. The **trap** and **shutdown** options are independent of each other.

Examples

This example shows how to enable broadcast storm control on a port with a 75.67 percent rising suppression level:

```
Switch(config-if)# storm-control broadcast level 75.67
```

This example shows how to enable multicast storm control on a port with a 87 percent rising suppression level and a 65 percent falling suppression level:

```
Switch(config-if)# storm-control multicast level 87 65
```

This example shows how to enable multicast storm control on a port with a 2000-packets-per-second rising suppression level and a 1000-packets-per-second falling suppression level on a non-LRE Catalyst 2950 switch:

```
Switch(config-if)# storm-control multicast level pps 2000 1000
```

This example shows how to enable the **shutdown** action on a port:

```
Switch(config-if)# storm-control action shutdown
```

This example shows how to enable the **trap** action on a port:

```
Switch(config-if)# storm-control action trap
```

This example shows how to disable the **shutdown** action on a port:

```
Switch(config-if)# no storm-control action shutdown
```

You can verify your settings by entering the **show storm-control** privileged EXEC command.

Related Commands

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

switchport access

Use the **switchport access** interface configuration command to configure a port as a static-access or dynamic-access port. If the mode is set to access, the port operates as a member of the configured VLAN. If set to dynamic, the port starts discovery of its VLAN assignment based on the incoming packets it receives. Use the **no** form of this command to reset the access mode to the default VLAN for the switch.

```
switchport access vlan {vlan-id | dynamic}
```

```
no switchport access
```

Syntax Description

access vlan <i>vlan-id</i>	Configure the interface as a static-access port; valid values are from 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1005 when the standard software image (SI) is installed.
access vlan dynamic	Specify that the access mode VLAN is dependent on the VLAN Membership Policy Server (VMPS) protocol. The port is assigned to a VLAN based on the source MAC address of a host (or hosts) connected to the port. The switch sends every new MAC address received to the VMPS server to obtain the VLAN name to which the dynamic-access port should be assigned. If the port already has a VLAN assigned and the source has already been approved by the VMPS, the switch forwards the packet to the VLAN.

Defaults

All ports are in static-access mode in VLAN 1 if the port is not connected to a device running Dynamic Trunking Protocol (DTP). The default access VLAN for an access port is VLAN 1.

All ports are dynamic trunk ports.

A dynamic-access port is initially a member of no VLAN and receives its assignment based on the packet it receives.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5.2)WC(1)	This command was first introduced.
12.1(6)EA2	The dynamic keyword was added.

Usage Guidelines

The **no switchport access** command resets the access mode VLAN to the appropriate default VLAN for the device.

The port must be in access mode before the **switchport access vlan** command can take effect. For more information, see the **switchport mode** command.

An access port can be assigned to only one VLAN.

The VMPS server (such as a Catalyst 6000 series switch) must be configured before a port is configured as dynamic.

These restrictions apply to dynamic-access ports:

- The software implements the VLAN Query Protocol (VQP) client, which can query a VMPS such as a Catalyst 6000 series switch. The Catalyst 3550 switches are not VMPS servers. The VMPS server must be configured before a port is configured as dynamic.
- Use dynamic-access ports only to connect end stations. Connecting them to switches or routers that use bridging protocols can cause a loss of connectivity.
- Configure the network so that Spanning Tree Protocol (STP) does not put the dynamic-access port in an STP blocking state. The Port Fast feature is automatically enabled on dynamic-access ports.
- Dynamic-access ports can only be in one VLAN and do not use VLAN tagging.
- Dynamic-access ports cannot be configured as:
 - Members of an EtherChannel port group (dynamic-access ports cannot be grouped with any other port, including other dynamic ports).
 - Source or destination ports in a static address entry.
 - Monitor ports.

Examples

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

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

You can verify your settings by entering the **show interfaces *interface-id* switchport** privileged EXEC command and examining information in the Administrative Mode and Operational Mode rows.

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.
switchport mode	Configures the VLAN membership mode of a port.

switchport block

Use the **switchport block** interface configuration command to prevent forwarding of unknown multicast or unicast packets. Use the **no** form of this command to allow forwarding of unknown multicast or unicast packets.

switchport block { multicast | unicast }

no switchport block { multicast | unicast }

This command is available only on these switches:

- Catalyst 2950 Long-Reach Ethernet (LRE) switches running Cisco IOS Release 12.1(14)EA1 or later
- Catalyst 2950G-12-EI, 2950G-24-EI, 2950G-24-EI-DC, 2950G-48-EI, and 2955 switches running Cisco IOS Release 12.1(19)EA1 or later

Syntax Description	multicast	unicast
	Specify that unknown multicast traffic should be blocked.	Specify that unknown unicast traffic should be blocked.

Defaults Unknown multicast and unicast traffic are not blocked.

Command Modes Interface configuration

Command History	Release	Modification
	12.1(14)EA1	This command was first introduced.

Usage Guidelines By default, all traffic with unknown MAC addresses is sent to all ports. You can block unknown multicast or unicast traffic on protected or non-protected ports. If unknown multicast or unicast traffic is not blocked on a protected port, there could be security issues.

Blocking unknown multicast or unicast traffic is not automatically enabled on protected ports; you must explicitly configure it.



Note

For more information about blocking packets, refer to the software configuration guide for this release.

Examples This example shows how to block unknown multicast traffic on an interface:

```
Switch(config-if)# switchport block multicast
```

You can verify your setting by entering the **show interfaces interface-id switchport** privileged EXEC command.

Related Commands	Command	Description
	<code>show interfaces switchport</code>	Displays the administrative and operational status of a switching port, including port blocking and port protection settings.

switchport mode

Use the **switchport mode** interface configuration command to configure the VLAN membership mode of a port. Use the **no** form of this command to reset the mode to the appropriate default for the device.

switchport mode { **access** | **dynamic** { **auto** | **desirable** } | **trunk** }

no switchport mode

Syntax Description

access	Set the port to access mode (either static-access or dynamic-access depending on the setting of the switchport access vlan interface configuration command). The port is set to access unconditionally and operates as a nontrunking, single VLAN interface that transmits and receives nonencapsulated (non-tagged) frames. An access port can be assigned to only one VLAN.
dynamic auto	Set the interface trunking mode dynamic parameter to auto to specify that the interface convert the link to a trunk link.
dynamic desirable	Set the interface trunking mode dynamic parameter to desirable to specify that the interface actively attempt to convert the link to a trunk link.
trunk	Set the port to trunk unconditionally. The port is a trunking VLAN Layer 2 interface. The port transmits and receives encapsulated (tagged) frames that identify the VLAN of origination. A trunk is a point-to-point link between two switches or between a switch and a router.

Defaults

The default mode is **dynamic desirable**.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5.2)WC(1)	This command was first introduced.
12.1(6)EA2	The dynamic auto and dynamic desirable keywords were added.

Usage Guidelines

Configuration by using the **access** or **trunk** keywords takes affect only when you configure the port in the appropriate mode by using the **switchport mode** command. The static-access and trunk configurations are saved, but only one configuration is active at a time.

If you enter **access** mode, the interface changes into permanent nontrunking mode and negotiates to convert the link into a nontrunk link even if the neighboring interface does not agree to the change.

If you enter **dynamic auto** mode, the interface converts the link to a trunk link if the neighboring interface is set to **trunk** or **desirable** mode.

If you enter **dynamic desirable** mode, the interface becomes a trunk interface if the neighboring interface is set to **trunk**, **desirable**, or **auto** mode.

If you enter **trunk** mode, the interface changes into permanent trunking mode and negotiates to convert the link into a trunk link even if the interface connecting to it does not agree to the change.

The **no switchport mode** form resets the mode to **dynamic desirable**.

Trunk ports cannot coexist on the same switch.

To autonegotiate trunking, the interfaces must be in the same VTP domain. Trunk negotiation is managed by the Dynamic Trunking Protocol (DTP), which is a point-to-point protocol. However, some internetworking devices might forward DTP frames improperly, which could cause misconfigurations. To avoid this, you should configure interfaces connected to devices that do not support DTP to not forward DTP frames, which turns off DTP.

- If you do not intend to trunk across those links, use the **switchport mode access** interface configuration command to disable trunking.
- To enable trunking to a device that does not support DTP, use the **switchport mode trunk** and **switchport nonegotiate** interface configuration commands to cause the interface to become a trunk but to not generate DTP frames.

Examples

This example shows how to configure a port for access mode:

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

This example shows how set the interface to dynamic desirable mode:

```
Switch(config-if)# switchport mode dynamic desirable
```

This example shows how to configure a port for trunk mode:

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

You can verify your settings by entering the **show interfaces *interface-id* switchport** privileged EXEC command and examining information in the Administrative Mode and Operational Mode rows.

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.
switchport access	Configures a port as a static-access port.
switchport trunk	Configures the trunk characteristics when an interface is in trunking mode.

switchport nonegotiate

Use the **switchport nonegotiate** interface configuration command to specify that Dynamic Trunking Protocol (DTP) negotiation packets are not sent on the Layer 2 interface. The switch does not engage in DTP negotiation on this interface. Use the **no** form of this command to return to the default setting.

switchport nonegotiate

no switchport nonegotiate

Syntax Description This command has no arguments or keywords.

Defaults The default is to use DTP negotiation to determine trunking status.

Command Modes Interface configuration

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

Usage Guidelines The **no** form of the **switchport nonegotiate** command removes **nonegotiate** status.

This command is valid only when the interface switchport mode is access or trunk (configured by using the **switchport mode access** or the **switchport mode trunk** interface configuration command). This command returns an error if you attempt to execute it in **dynamic (auto or desirable)** mode.

Internetworking devices that do not support DTP might forward DTP frames improperly and cause misconfigurations. To avoid this, you should turn off DTP by using the **switchport no negotiate** command to configure the interfaces connected to devices that do not support DTP to not forward DTP frames.

When you enter the **switchport nonegotiate** command, DTP negotiation packets are not sent on the interface. The device does or does not trunk according to the **mode** parameter given: **access** or **trunk**.

- If you do not intend to trunk across those links, use the **switchport mode access** interface configuration command to disable trunking.
- To enable trunking on a device that does not support DTP, use the **switchport mode trunk** and **switchport nonegotiate** interface configuration commands to cause the interface to become a trunk but to not generate DTP frames.



Note

On GigaStack GBICs, dynamic trunking is supported only when one port of a GigaStack GBIC is being used. If trunking is required on a GigaStack GBIC where both ports are in use, use the **switchport mode trunk** and **switchport nonegotiate** interface configuration commands on both GBIC interfaces to cause the interfaces to become trunks.

Examples

This example shows how to cause an interface to refrain from negotiating trunking mode and to act as a trunk or access port (depending on the **mode** set):

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

You can verify your setting by entering the **show interfaces *interface-id* switchport** privileged EXEC command.

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.
switchport mode	Configures the VLAN membership mode of a port.

switchport port-security

Use the **switchport port-security** interface configuration command without keywords to enable port security on an interface. Use the keywords to configure secure MAC addresses, a maximum number of secure MAC addresses, or the violation mode. Use the **no** form of this command to disable port security or to set the parameters to their default states.

```
switchport port-security [mac-address mac-address] | [mac-address sticky [mac-address]] |
  [maximum value] | [violation {protect | restrict | shutdown}]
```

```
no switchport port-security [mac-address mac-address] | [mac-address sticky [mac-address]] |
  [maximum value] | [violation {protect | restrict | shutdown}]
```

Syntax Description	
mac-address <i>mac-address</i>	(Optional) Specify a secure MAC address for the port by entering a 48-bit MAC address. You can add additional secure MAC addresses up to the maximum value configured.
mac-address sticky <i>[mac-address]</i>	<p>(Optional) Enable the interface for <i>sticky learning</i> by entering only the mac-address sticky keywords. When sticky learning is enabled, the interface adds all secure MAC addresses that are dynamically learned to the running configuration and converts these addresses to sticky secure MAC addresses.</p> <p>Specify a sticky secure MAC address by entering the mac-address sticky <i>mac-address</i> keywords.</p> <p>Note Although you can specify a sticky secure MAC address by entering the mac-address sticky <i>mac-address</i> keywords, we recommend using the mac-address <i>mac-address</i> interface configuration command to enter static secure MAC addresses.</p>
maximum <i>value</i>	(Optional) Set the maximum number of secure MAC addresses for the interface. The range is from 1 to 132. The default is 1.
violation	(Optional) Set the security violation mode or the action to be taken if port security is violated. The default is shutdown .
protect	(Optional) Set the security violation protect mode. When the number of secure MAC addresses reaches the limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses or increase the number of maximum allowable addresses. You are not notified that a security violation has occurred.

restrict	(Optional) Set the security violation restrict mode. When the number of secure MAC addresses reaches the limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses or increase the number of maximum allowable addresses. In this mode, you are notified that a security violation has occurred. Specifically, an SNMP trap is sent, a syslog message is logged, and the violation counter increments.
shutdown	(Optional) Set the security violation shutdown mode. In this mode, a port security violation causes the interface to immediately become error-disabled and turns off the port LED. It also sends an SNMP trap, logs a syslog message, and increments the violation counter. When a secure port is in the error-disabled state, you can bring it out of this state by entering the errdisable recovery cause psecure-violation global configuration command, or you can manually re-enable it by entering the shutdown and no shut down interface configuration commands.

Defaults

Port security is disabled.

When port security is enabled, if no keywords are entered, the default maximum number of secure MAC addresses is 1.

Sticky learning is disabled.

The default violation mode is **shutdown**.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(6)EA2	This command was first introduced. It replaced the port security and mac-address-table secure commands.
12.1(11)EA1	The mac-address sticky [<i>mac-address</i>] option was added.

Usage Guidelines

A secure port can have from 1 to 132 associated secure addresses. The total number of available secure addresses on the switch is 1024.

After you have set the maximum number of secure MAC addresses allowed on a port, you can add secure addresses to the address table by manually configuring them, by allowing the port to dynamically configure them, or by configuring some MAC addresses and allowing the rest to be dynamically configured.

You can delete dynamic secure MAC addresses from the address table by entering the **clear port-security dynamic** privileged EXEC command.

You can enable sticky learning on an interface by using the **switchport port-security mac-address sticky** interface configuration command. When you enter this command, the interface converts all the dynamic secure MAC addresses, including those that were dynamically learned before sticky learning was enabled, to sticky secure MAC addresses. It adds all the sticky secure MAC addresses to the running configuration.

You can delete a sticky secure MAC addresses from the address table by using the **clear port-security sticky mac-addr** privileged EXEC command. To delete all the sticky addresses on an interface, use the **clear port-security sticky interface-id** privileged EXEC command.

If you disable sticky learning, the sticky secure MAC addresses are converted to dynamic secure addresses and are removed from the running configuration.

If you save the sticky secure MAC addresses in the configuration file, when the switch restarts or the interface shuts down, the interface does not need to relearn these addresses. If you do not save the configuration, they are lost.

If you specify **restrict** or **shutdown**, use the **snmp-server host** global configuration command to configure the Simple Network Management Protocol (SNMP) trap host to receive traps.

It is a security violation when one of these situations occurs:

- The maximum number of secure MAC addresses have been added to the address table, and a station whose MAC address is not in the address table attempts to access the interface.
- An address learned or configured on one secure interface is seen on another secure interface in the same VLAN.

When a secure port is in the error-disabled state, you can bring it out of this state by entering the **errdisable recovery cause psecure-violation** global configuration command, or you can manually re-enable it by entering the **shutdown** and **no shut down** interface configuration commands.

A secure port has these limitations:

- Port security can only be configured on static access ports.
- A secure port cannot be a dynamic port, a dynamic access port or a trunk port.
- A secure port cannot be a destination port for Switched Port Analyzer (SPAN).
- A secure port cannot belong to a Fast EtherChannel or Gigabit EtherChannel port group.
- You cannot configure static secure or sticky secure MAC addresses on a voice VLAN.
- When you enable port security on an interface that is also configured with a voice VLAN, you must set the maximum allowed secure addresses on the port to at least two. If any type of port security is enabled on the access VLAN, dynamic port security is automatically enabled on the voice VLAN. You cannot configure port security on a per-VLAN basis.
- When a voice VLAN is configured on a secure port that is also configured as a sticky secure port, all addresses detected on the voice VLAN are learned as dynamic secure addresses while all addresses detected on the access VLAN (to which the port belongs) are learned as sticky secure addresses.
- To enable port security on an 802.1X port, you must first enable the 802.1X multiple-hosts mode on the port (for switches running the EI software).
- The switch does not support port security aging of sticky secure MAC addresses.

Examples

This example shows how to enable port security:

```
Switch(config-if)# switchport port-security
```

This example shows how to set the action that the port takes when an address violation occurs:

```
Switch(config-if)# switchport port-security violation shutdown
```

This example shows how to set the maximum number of addresses that a port can learn to 20.

```
Switch(config-if)# switchport port-security maximum 20
```

This example shows how to enable sticky learning and to enter two sticky secure MAC addresses:

```
Switch(config-if) # switchport port-security mac-address sticky
Switch(config-if) # switchport port-security mac-address sticky 0000.0000.4141
Switch(config-if) # switchport port-security mac-address sticky 0000.0000.000f
```

You can verify your settings by entering the **show port-security** privileged EXEC command.

Related Commands	Command	Description
	clear port-security	Deletes from the MAC address table a specific dynamic secure address or all the dynamic secure addresses on an interface.
	clear port-security sticky	Deletes from the MAC address table a specific sticky secure address, all the sticky secure addresses on an interface, or all the sticky secure addresses on a switch.
	show port-security	Displays the port security settings defined for the port.

switchport port-security aging

Use the **switchport port-security aging** interface configuration command to set the aging time and type for secure address entries or to change the aging behavior for statically configured secure addresses on a particular port. Use the **no** form of this command to disable port security aging or to set the parameters to their default states.

```
switchport port-security aging {static | time time | type {absolute | inactivity}}
```

```
no switchport port-security aging {static | time | type}
```

Syntax Description		
static		Enable aging for statically configured secure addresses on this port.
time <i>time</i>		Specify the aging time for this port. The valid range is from 0 to 1440 minutes. If the time is 0, aging is disabled for this port.
type absolute		Set the aging type as absolute aging. All the secure addresses on this port age out after the time (minutes) specified and are removed from the secure address list.
type inactivity		Set the aging type as inactivity aging. The secure addresses on this port age out only if there is no data traffic from the secure source address for the specified time period.

Defaults

The port security aging feature is disabled. The default time is 0 minutes.

The default aging type is absolute.

The default static aging behavior is disabled.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

To enable secure address aging for a particular port, set the port aging time to a value other than 0.

To allow limited-time access to specific secure MAC addresses, set the aging type as **absolute**. When the device sends traffic again, the deleted secure addresses are relearned.



Note

The absolute aging time could vary by 1 minute, depending on the sequence of the system timer.

To allow continuous access to a limited number of secure addresses, set the aging type as **inactivity**. This removes the secure address when it becomes inactive, and other addresses can become secure.

To allow unlimited access to a secure address, configure it as a secure address, and disable aging for the statically configured secure address by using the **no switchport port-security aging static** interface configuration command.

Examples

This example sets the aging time as 2 hours for absolute aging for all the secure addresses on Fast Ethernet interface 0/1.

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport port-security aging time 120
```

This example sets the aging time as 2 minutes for inactivity aging type for configured secure addresses on Fast Ethernet interface 0/2.

```
Switch(config)# interface fastethernet0/2
Switch(config-if)# switchport port-security aging time 2
Switch(config-if)# switchport port-security aging type inactivity
Switch(config-if)# switchport port-security aging static
```

This example shows how to disable aging for configured secure addresses.

```
Switch(config-if)# no switchport port-security aging static
```

Related Commands

Command	Description
show port-security	Displays the port security settings defined for the port.
switchport port-security	Enables port security on a port, restricts the use of the port to a user-defined group of stations, and configures secure MAC addresses.

switchport priority extend

Use the **switchport priority extend** interface configuration command to set a port priority for the incoming untagged frames or the priority of frames received by the IP phone connected to the specified port. Use the **no** form of this command to return to the default setting.

switchport priority extend { *cos value* | **trust** }

no switchport priority extend

Syntax Description

cos value	Set the IP phone port to override the priority received from PC or the attached device. The class of service (CoS) value is a number from 0 to 7. Seven is the highest priority. The default is 0.
trust	Set the IP phone port to trust the priority received from PC or the attached device.

Defaults

The port priority is not set, and the default value for untagged frames received on the port is 0.

The IP phone connected to the port is set to not trust the priority of incoming traffic and overrides the priority with the CoS value of 0.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(9)EA1	This command was first introduced.
12.1(13)EA1	The none keyword was removed and replaced by the trust keyword.

Usage Guidelines

In Cisco IOS Release 12.1(13)EA1 or later, the **trust** keyword replaces the **none** keyword. To instruct the IP Phone to not trust the priority, you can use the **no switchport priority extend** or the **switchport priority extend cos 0** interface configuration command. In software releases earlier than Cisco IOS Release 12.1(13)EA1, use the **switchport priority extend none** interface configuration command.

Examples

This example shows how to configure the IP phone connected to the specified port to trust the received 802.1P priority:

```
Switch(config-if)# switchport priority extend trust
```

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

Related Commands	Command	Description
	show interfaces	Displays the administrative and operational status of a switching (nonrouting) port.
	switchport voice vlan	Configures the voice VLAN on the port.

switchport protected

Use the **switchport protected** interface configuration command to isolate unicast, multicast, and broadcast traffic at Layer 2 from other protected ports on the same switch. Use the **no** form of this command to return to the default setting.

switchport protected

no switchport protected

Syntax Description This command has no keywords or arguments.

Defaults No protected port is defined. All ports are nonprotected.

Command Modes Interface configuration

Command History	Release	Modification
	12.1(6)EA2	This command was first introduced. It replaced the port protected command.

Usage Guidelines The switchport protection feature is local to the switch; communication between protected ports on the same switch is possible only through a Layer 3 device. To prevent communication between protected ports on different switches, you must configure the protected ports for unique VLANs on each switch and configure a trunk link between the switches. A protected port is different from a secure port.

A protected port does not forward any unicast, multicast, or broadcast traffic to any other protected port. A protected port continues to forward unicast, multicast, and broadcast traffic to unprotected ports and vice versa.

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

Protected ports are supported on 802.1Q trunks.

Examples This example shows how to enable a protected port on Fast Ethernet interface 0/3:

```
Switch(config)# interface fastethernet0/3
Switch(config-if)# switchport protected
```

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

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

switchport trunk

Use the **switchport trunk** interface configuration command to set the trunk characteristics when the interface is in trunking mode. Use the **no** form of this command to reset all of the trunking characteristics to the defaults. Use the **no** form with keywords to reset those characteristics to the defaults.

```
switchport trunk {{allowed vlan vlan-list} | {native vlan vlan-id} | {pruning vlan vlan-list}}
```

```
no switchport trunk {{allowed vlan vlan-list} | {native vlan vlan-id} | {pruning vlan vlan-list}}
```

Syntax Description

allowed vlan <i>vlan-list</i>	Set the list of allowed VLANs that can receive and send traffic on this interface in tagged format when in trunking mode. See the following <i>vlan-list</i> format. The none keyword is not valid. The default is all .
native vlan <i>vlan-id</i>	Set the native VLAN for sending and receiving untagged traffic when the interface is in 802.1Q trunking mode. Valid IDs are from 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1001 when the standard software image (SI) is installed.
pruning vlan <i>vlan-list</i>	Set the list of VLANs that are enabled for VTP pruning when in trunking mode. The all keyword is not valid.

The *vlan-list* format is **all** | **none** | [**add** | **remove** | **except**] *vlan-atom* where:

- **all** specifies all VLANs from 1 to 4094 when the EI is installed and 1 to 1005 when the SI is installed. This keyword is not allowed on commands that do not permit all VLANs in the list to be set at the same time.
- **none** means an empty list. This keyword is not allowed on commands that require certain VLANs to be set or at least one VLAN to be set.
- **add** adds the defined list of VLANs to those currently set instead of replacing the list. Valid IDs are from 1 to 1005; extended-range VLAN IDs are valid in some cases.



Note You can add extended-range VLANs to the allowed VLAN list, but not to the pruning-eligible VLAN list.

Separate nonconsecutive VLAN IDs with a comma; do not enter a space after the comma. Use a hyphen to designate a range of IDs; do not enter a space before or after the hyphen.

- **remove** removes the defined list of VLANs from those currently set instead of replacing the list. Valid IDs are from 1 to 1005; extended-range VLAN IDs are valid in some cases.



Note You can remove extended-range VLANs (VLAN IDs greater than 1005) from the allowed VLAN list, but you cannot remove them from the pruning-eligible list.

Separate nonconsecutive VLAN IDs with a comma; do not enter a space after the comma. Use a hyphen to designate a range of IDs; do not enter a space before or after the hyphen.

- **except** lists the VLANs that should be calculated by inverting the defined list of VLANs. (VLANs are added except the ones specified.) Valid IDs are from 1 to 1005. Separate nonconsecutive VLAN IDs with a comma; do not enter a space after the comma. Use a hyphen to designate a range of IDs; do not enter a space before or after the hyphen.

- *vlan-atom* is either a single VLAN number from 1 to 4094 when the EI is installed and 1 to 1005 when the SI is installed, a list of nonconsecutive VLANs, or a continuous range of VLANs described by two VLAN numbers, the lower one first, separated by a hyphen.

For a list of nonconsecutive VLAN IDs, separate the VLAN IDs with a comma. Do not enter a space after the comma.

For a continuous range of VLAN IDs, use a hyphen to designate the range. Do not enter a space before or after the hyphen.

These are examples showing how to specify one or more VLANs:

- Single VLAN—101
- List of nonconsecutive VLANs—10,12,14,16,18
- Continuous range of VLANs—10-15
- List of VLAN continuous ranges—10-15,20-24
- List of nonconsecutive VLANs and VLAN continuous ranges—8,11,20-24,44

Defaults

VLAN 1 is the default native VLAN ID on the port.

The default for all VLAN lists is to include all VLANs.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(6)EA2	This command was first introduced.
12.1(14)EA1	The allowed vlan <i>vlan list</i> add , remove , and except keywords were modified to accept the VLAN 1 and VLANs 1002 to 1005 values.

Usage Guidelines

A trunk port cannot be a secure port or a monitor port. However, a static-access port can monitor a VLAN on a trunk port. The VLAN monitored is the one associated with the static-access port.

Allowed VLAN:

- To reduce the risk of spanning-tree loops or storms, you can disable VLAN 1 on any individual VLAN trunk port by removing VLAN 1 from the allowed list. This is known as VLAN 1 minimization. VLAN 1 minimization disables VLAN 1 (the default VLAN on all Cisco switch trunk ports), on an individual VLAN trunk link. As a result no user traffic, including spanning-tree advertisements, are sent or received on VLAN 1.

When you remove VLAN 1 from a trunk port, the interface continues to send and receive management traffic, for example, Cisco Discovery Protocol (CDP), Port Aggregation Protocol (PAgP), Link Aggregation Control Protocol (LACP), Dynamic Trunking Protocol (DTP), and VLAN Trunking Protocol (VTP) in VLAN 1.

- The **no** form of the **allowed vlan** command resets the list to the default list, which allows all VLANs.

Native VLANs:

- All untagged traffic received on an 802.1Q trunk port is forwarded with the native VLAN configured for the port.
- If a packet has a VLAN ID that is the same as the sending port native VLAN ID, the packet is sent without a tag; otherwise, the switch sends the packet with a tag.
- The **no** form of the **native vlan** command resets the native mode VLAN to the appropriate default VLAN for the device.

Trunk Pruning:

- The pruning-eligible list applies only to trunk ports.
- Each trunk port has its own eligibility list.
- If you do not want a VLAN to be pruned, remove it from the pruning-eligible list. VLANs that are pruning-ineligible receive flooded traffic.
- VLAN 1, VLANs 1002 to 1005, and extended-range VLANs (VLANs 1006 to 4094) cannot be pruned.

**Note**

The switch does not support Inter-Switch Link (ISL) trunking.

Examples

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

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

This example shows how to add VLANs 1, 2, 5, and 6 to the allowed list:

```
Switch(config-if)# switchport trunk allowed vlan add 1,2,5,6
```

This example shows how to remove VLANs 3 and 10 to 15 from the pruning-eligible list:

```
Switch(config-if)# switchport trunk pruning vlan remove 3,10-15
```

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

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.
switchport mode	Configures the VLAN membership mode of a port.

switchport voice vlan

Use the **switchport voice vlan** interface configuration command to configure voice VLAN on the port. Use the **no** form of this command to return to the default setting.

```
switchport voice vlan {vlan-id | dot1p | none | untagged}
```

```
no switchport voice vlan
```

Syntax Description		
	<i>vlan-id</i>	VLAN used for voice traffic. Valid IDs are from 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1001 when the standard software image (SI) is installed.
	dot1p	The telephone uses priority tagging and uses VLAN 0 (the native VLAN). By default, the Cisco IP phone forwards the voice traffic with an 802.1P priority of 5.
	none	The telephone is not instructed through the CLI about the voice VLAN. The telephone uses the configuration from the telephone key pad.
	untagged	The telephone does not tag frames and uses VLAN 4095. The default for the telephone is untagged.

Defaults

The switch default is not to automatically configure the telephone (**none**).

The telephone default is not to tag frames.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

You should configure voice VLAN on access ports.

When you enable port security on an interface that is also configured with a voice VLAN, you must set the maximum allowed secure addresses on the port to at least two.

If any type of port security is enabled on the access VLAN, dynamic port security is automatically enabled on the voice VLAN.

You cannot configure static secure MAC addresses on the voice VLAN.

The Port Fast feature is automatically enabled when voice VLAN is configured. When you disable voice VLAN, the Port Fast feature is not automatically disabled.

Examples

This example shows how to configure VLAN 2 as the voice VLAN:

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

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

Related Commands

Command	Description
show interfaces <i>interface-id</i> switchport	Displays the administrative and operational status of a switching (nonrouting) port.
switchport priority extend	Determines how the device connected to the specified port handles priority traffic received on its incoming port.

system mtu

Use the **system mtu** global configuration command to set the maximum packet size or maximum transmission unit (MTU) size for the switch. Use the **no** form of this command to restore the global MTU value to its original default value.

system mtu *bytes*

no system mtu

Syntax Description	<i>bytes</i>	Packet size in bytes. For valid values, see the “Usage Guidelines” section.
---------------------------	--------------	---

Defaults	The default MTU size is 1500 bytes.
-----------------	-------------------------------------

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

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

Usage Guidelines This table lists the valid system MTU values for the switches:

Switch	MTU size
Catalyst 2950G-12-EI	1500 to 1530 bytes
Catalyst 2950G-24-EI	
Catalyst 2950G-24-EI-DC	
Catalyst 2950G-48-EI	
Catalyst 2950 Long-Reach Ethernet (LRE) switches	
Catalyst 2955 switches	
Other non-LRE Catalyst 2950 switches	1500 bytes

The size of frames that can be received by the switch CPU is limited to 1500 bytes, no matter what value was entered with the **system mtu** command. Although frames that are forwarded or routed typically are not received by the CPU, in some cases packets are sent to the CPU, such as traffic sent to control traffic, Simple Network Management Protocol (SNMP), Telnet, or routing protocols.

If you enter a value that is outside of the range for the switch, the value is not accepted.



Note You cannot set the MTU on a per-interface basis.

Examples

This example shows how to set the maximum packet size to 1528 bytes:

```
Switch(config)# system mtu 1528
Switch(config)# exit
```

This example shows the response when you try to set a switch to an out-of-range number:

```
Switch(config)# system mtu 2000
                                     ^
% Invalid input detected at '^' marker.
```

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

Related Commands

Command	Description
show system mtu	Displays the maximum packet size set for the switch.
